

WinpowerG2 Manual

Table of Contents

1	Software Introduce.....	6
1.1	Main Functions	6
1.2	Software Structure	6
1.3	Basic Requirements	7
1.4	Application Scenarios	8
1.5	Shutdown Scenarios	9
2	Contextual help of the web interface	11
2.1	Log in.....	11
2.1.1	Retrieve password via email	13
2.1.2	Retrieve password via SMS	15
2.2	Overview.....	17
2.2.1	All sites.....	19
2.2.2	Favorite sites	21
2.2.3	IT architecture.....	22
2.3	Asset	23
2.3.1	UPS list.....	23
2.3.1.1	UPS details.....	29
2.3.2	Server	31
2.3.2.1	SPS list	33
2.3.2.2	IPMI list	35
2.3.2.3	VMware Center list	37
2.3.2.4	VMware ESXi list	39
2.3.2.5	SSH list.....	42
2.3.2.6	NetApp Cluster list	43
2.3.3	PDU list.....	45
2.3.3.1	PDU details	46
2.3.4	Redundant UPS.....	47

2.4	Shutdown Protection.....	48
2.4.1	Shutdown protection setting	48
2.4.1.1	Local shutdown	52
2.4.1.2	SPS shutdown	54
2.4.1.3	IPMI shutdown.....	55
2.4.1.4	SSH shutdown	56
2.4.1.5	VMware ESXi Standalone shutdown.....	57
2.4.1.6	VMware ESXi of vCenter shutdown	59
2.4.1.7	VMware Cluster shutdown.....	62
2.4.1.8	NetApp shutdown.....	65
2.4.1.9	Redundant shutdown	66
2.4.2	On/Off schedule	68
2.4.3	Battery test schedule	70
2.5	Events/Logs.....	72
2.5.1	Event log	72
2.5.2	Data log	74
2.5.3	Shutdown log.....	74
2.5.4	User log	76
2.5.5	Notification log	77
2.5.6	WOL log.....	77
2.6	System settings.....	78
2.6.1	System preferences	78
2.6.1.1	Alarm setting	79
2.6.1.2	Data format settings	79
2.6.1.3	Maintenance period setting	80
2.6.1.4	Log setting	80
2.6.2	Device data collection setting	80
2.6.2.1	Polling Settings.....	80
2.6.2.2	Log setting	81

2.6.3	User management	81
2.6.3.1	Account	82
2.6.3.2	User group	89
2.6.4	Site management	92
2.6.5	Serial port management	95
2.6.6	Signal threshold setting	96
2.6.7	Event subscription setting	97
2.6.8	Notification service setting	98
2.6.8.1	Email setting	98
2.6.8.2	SMS setting.....	100
2.6.9	Credential.....	101
2.6.10	Custom reminder.....	103
2.6.11	WOL Setting	104
2.6.12	LDAP login	106
2.6.13	HTTPS setting.....	107
2.6.14	License management.....	108
2.7	Other setting	110
2.7.1	Personal profile	110
2.7.2	Guide	110
2.7.3	Check version	111
3	How To	113
3.1	How to send Email/SMS.....	113
3.2	How to use beeps alarm	114
3.3	How to reset password for "admin"	116
3.4	How to apply for email app password	116
3.5	How to add UPS via USB/RS232 for Virtual Machine	117
3.6	How to set auto stop/start on VMware ESXi.....	120
4	Troubleshooting	121
4.1	Troubleshooting the Cause of WOL Failure.....	121

4.2	Resolve ports conflict	123
4.3	Reasons for failure to add devices and suggestions	124
4.4	Troubleshooting causes of NMC G2 card communication interruption.....	126
4.5	Search cards failed via Winpower on MacOSX	127
4.6	Communication Failure between Winpower and SPS.....	127

1 Software Introduce

Software supports the following operating systems:

- Windows and Windows server
- Linux system: RedHat, Ubuntu, Cent OS, Open SUSE, Fedora and so on
- Mac OSX
- VMware vSphere Virtualization system
- NetApp file system

1.1 Main Functions

- Winpower G2 is an upgraded version of WinpowerG1, which supports both local UPS USB/RS232 communication and remote network card communication protocols such as MQTT, SNMP, Modbus TCP
- Software supports PDU data collection and controls outlets on/off on the PDU
- Software supports Windows/Linux/Mac OSX and provides two installation methods: graphic mode and text mode. For Windows systems, it supports upgrade installation, and customer can choose whether to keep the old database and configuration files in installation process
- Software supports monitoring UPS real-time data and alarm events, recording UPS historical data and events, drawing data trend chart, supporting UPS parameter settings, supporting UPS battery self-test and output on/off, shutting down local and remote servers gracefully before UPS battery outage
- Software supports tray icon alarms, SMS or email notifications, etc. Protect key servers and prevent the equipment from being seriously damaged by sudden failures of the mains power supply
- Software supports monitoring and protecting remote servers such as VMware Vsphere, IPMI, SSH, SPS, NetApp
- Software supports multiply accounts and multiply sites management. The root site can be further divided into primary sites and secondary sites. It supports hierarchical permission management. The user in the different group can manage corresponding devices in the site

1.2 Software Structure

The software consists of three parts: **Service, Web interface, Tray icon**

Service

The core of the software runs in the background as a service. The service starts automatically when the system boot



On Mac OSX, the service will start automatically after logging in

Web interface

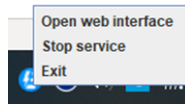
Customers can access to WinpowerG2 service through http/https using google, Edge, Firefox and other browsers. The credential for default account is "admin/admin". It is needed to change the password of admin for the first login after installation

Tray icon



- After logging in to the Windows/MacOSX system, the tray icon will appear in the bottom right corner of Windows taskbar or in the upper right corner of the MacOSX. Customers can open the web interface, start or exit the service through the tray icon. The UPS event alarms and shutdown countdown alarms will pop up to remind the customer



The language of tray icon and alarms pop-up box should be consistent with the language environment of the operating system



- The tray icon can show the status of the software service . There are two status icons:

	Blue color means the service is running
	Gray color means the service is stopped

1.3 Basic Requirements

Computer configuration

CPU Intel or AMD64

Processor 4 cores and above

4GB minimum memory, 8GB recommended

JDK/OS version

The software attached with OpenJDK21. For Windows systems, it is recommended to Windows 10 or above. For Linux, software only supports x86_x64. For Mac OSX, it is recommended to 11 or above.

Browser version

IE is not supported

Firefox Version 115.0 and later

Google Chrome, V114.0.5735.199 and later

Microsoft Edge, V114.0.1823.82 and later

Safari V16.4.1 (April 7, 2023) and later

Ports

Https/Http TCP port: 8081

SPS Communication UDP port: 6787, 6788, 6789

SNMP trap UDP port: 162

SNMP Communication UDP port: 161

IPMI TCP port: 623, 6000 (Once a new IPMI device is added, the port for IPMI device will automatically increase by 1 based on 6000)

MQTT TCP port: 8883

Display resolution

Maximum resolution: 1920*1080, Zoom 100%, layout 150%

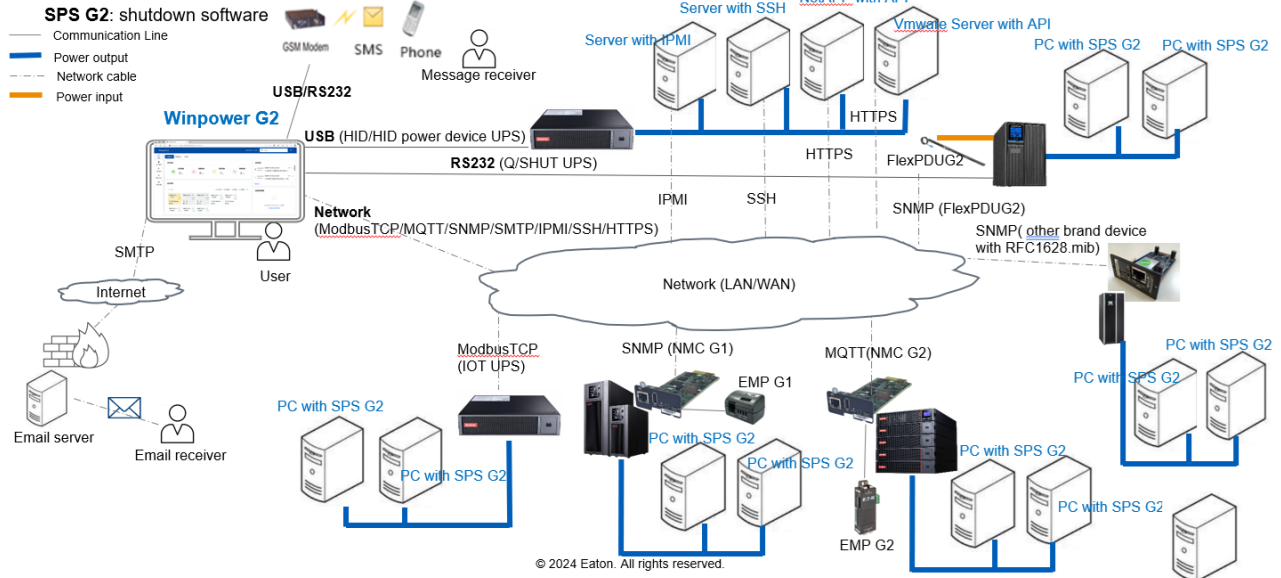
Minimum resolution: 1280*720, Zoom 100%, layout 150%

Other resolution: 1960*1200, Zoom 100%, layout 150%

To present a more suitable web interface, it is recommended to set the resolution to 1920 * 1080

1.4 Application Scenarios

Software support remote monitor for multiply network cards and servers. The free version software can monitor up to 100 power sources. If the number of devices exceeds 100, a license needs to be purchased

Winpower G2: monitoring & shutdown software

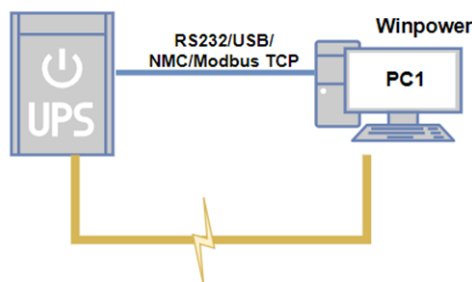
1.5 Shutdown Scenarios

Local shutdown protection

UPS supplies power to PC1. Winpower is installed on the host PC1 and communicates with UPS through RS232/USB/NMC/Modbus TCP. When the UPS mains power is abnormal, Winpower will shut down PC1 and turn off UPS gracefully

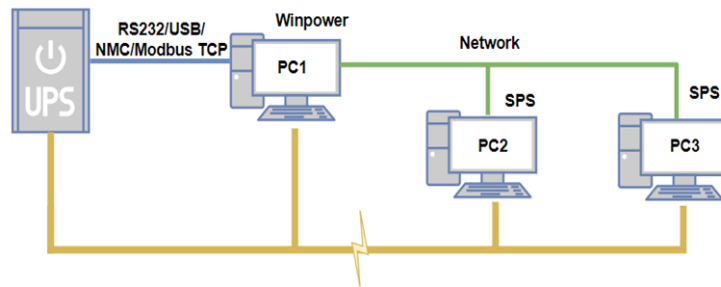


UPS shutdown is suitable for RS232/USB/Modbus TCP communication. If power source is NMC card, the UPS will be shut down by the card not by Winpower



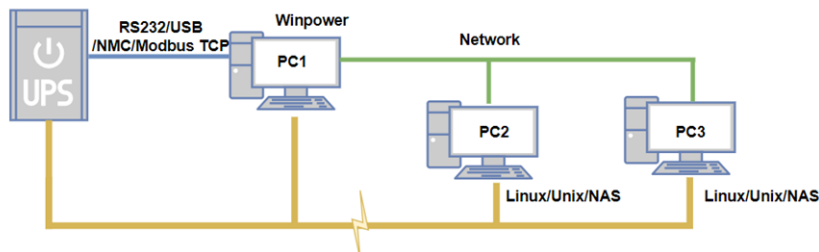
SPS shutdown protection

UPS supplies power to PC1, PC2 and PC3. Winpower is installed on the host PC1 and communicates with UPS via RS232/USB/NMC/Modbus TCP. SPS is installed on the slave PC2 and slave PC3 respectively. Set the shutdown conditions for Winpower and SPS. When the UPS mains power is abnormal, Winpower will notify SPS on PC2 and PC3 to perform the action to shut down PC2 and PC3 respectively. Winpower will shut down the host PC1 finally



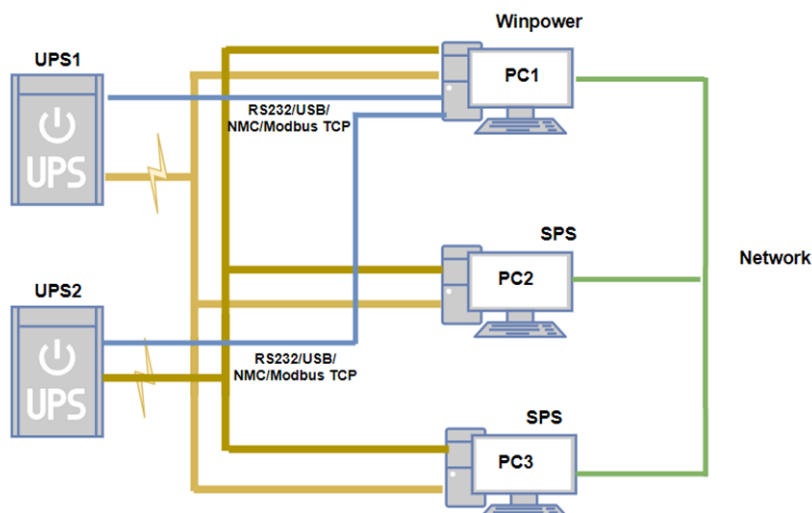
SSH shutdown protection

UPS supplies power to PC1, PC2 and PC3. Winpower is installed on the host PC1 and communicates with UPS via RS232/USB/NMC/Modbus TCP. PC2 and PC3 are Linux/Unix/NAS servers that SSH service is enabled. When UPS mains power is abnormal, Winpower will shut down PC2 and PC3 by calling SSH API firstly, then shut down the host finally



Redundant shutdown protection

UPS1 and UPS2 simultaneously supply power to PC1, PC2, and PC3. Winpower is installed on host PC1 and communicates with UPS1 and UPS2 through RS232/USB/NMC/Modbus TCP. UPS1 and UPS2 are move to one redundant group and set this group as power source. SPS is installed on slave PC2 and PC3 respectively. Winpower will combine all critical events of UPS and trigger the shutdown when all UPS can't support the load. When the shutdown conditions are met, Winpower will notify SPS to shut down PC2, PC3 firstly, then shut down the host PC1 finally



2 Contextual help of the web interface

2.1 Log in

1. Access to Winpower on local host through <https://localhost:8081>. Access to Winpower on remote host just replace "localhost" with the Winpower real IP address



The default password for the admin account is "admin". If the software host computer has multiple network cards, you can use any IP address to access.

2. Agree with the software's EULA for first login

Phone: _____
Email: _____
消费者服务联系信息。
电话: _____
电子邮件: _____

APPENDIX 1A
附录1A
Third Party Software
第三方软件

APPENDIX 1B
附录1B
Special Open Source Components
特殊开源组件

APPENDIX 2
附录2
Fees
费用
Free of charge
免费

Read completed and agree

3. Password is required to reset for first login. The password format must be between 8-20 characters and must contain at least three types of characters: lowercase letters, uppercase letters, digits, and special characters. You can move the mouse to "?" icon to view password restrictions



Special characters: ~!@#\$\$%^*

Change password

Password must be between 8 and 20 characters and contain at least three of following character types:
lowercase letters, uppercase letters,
digits, special characters

Old password:

* New password:

* Confirm password:

Confirm

4. View [System preferences](#) and get more login setting information
5. The login webpage language is consistent with the language used by the previous user

2.1.1 Retrieve password via email

1. Set the email SMTP firstly, check [Notification service setting](#)
2. On the login page, click "Forgot Password", click "Email", enter the account name (e.g. jones) then click "Get Verification Code"

Forgot password

×

Phone

Email

*

Account name :

Please enter account

*

New password ? :

Please enter password

*

Confirm password :

Please enter password

*

Verification code :

Please enter

Get verification code

Confirm


ⓘ


Sending verification codes requires configuring SMS and email services first.

[Help](#)

3. The email associated with account "jones" will receive an email containing a verification code

User password reset



To  Liu, Jones(刘琼)

Retention Policy

Inbox - Retain for 1 year (1 year)


Expires 2025/11/28


😊

↶

↷

➡





15:28

Dear user, hello!

Your account password is about to be reset, the verification code is: 394647.

Note: The verification code is valid for 1 hour. Please enter the verification code and reset your password within one hour.

4. Enter the "New password" and "Confirm password", as well as the verification code received in the email as above image, and click "Confirm" button to reset password

Forgot password

Phone

Email

*

Account name :

jones

*

New password ? :

.....

*

Confirm password :

.....

*

Verification code :

394647

Get verification code

Confirm

ⓘ

Sending verification codes requires configuring SMS and email services first.

[Help](#)



Retrieve password with a limit of sending verification code once per minute. Otherwise, software will pop up a message "The verification code has been sent, please try again later"

2.1.2 Retrieve password via SMS

1. Set the SMS firstly, Check [Notification service setting](#)

2. On the login page, click "Forgot Password", select "Phone", enter the account name (e.g. jones) then click "Get Verification Code"

Forgot password ×

☒ Phone ☐ Email

* Account name:


* New password ②:

* Confirm password:

* Verification code:

⚠ Sending verification codes requires configuring SMS and email services first.
[Help](#)





3. The phone number attached with account "jones" will receive a SMS message containing a verification code
4. Enter the "New password" and "Confirm password", as well as the verification code received via SMS, and click "Confirm" button to reset the password

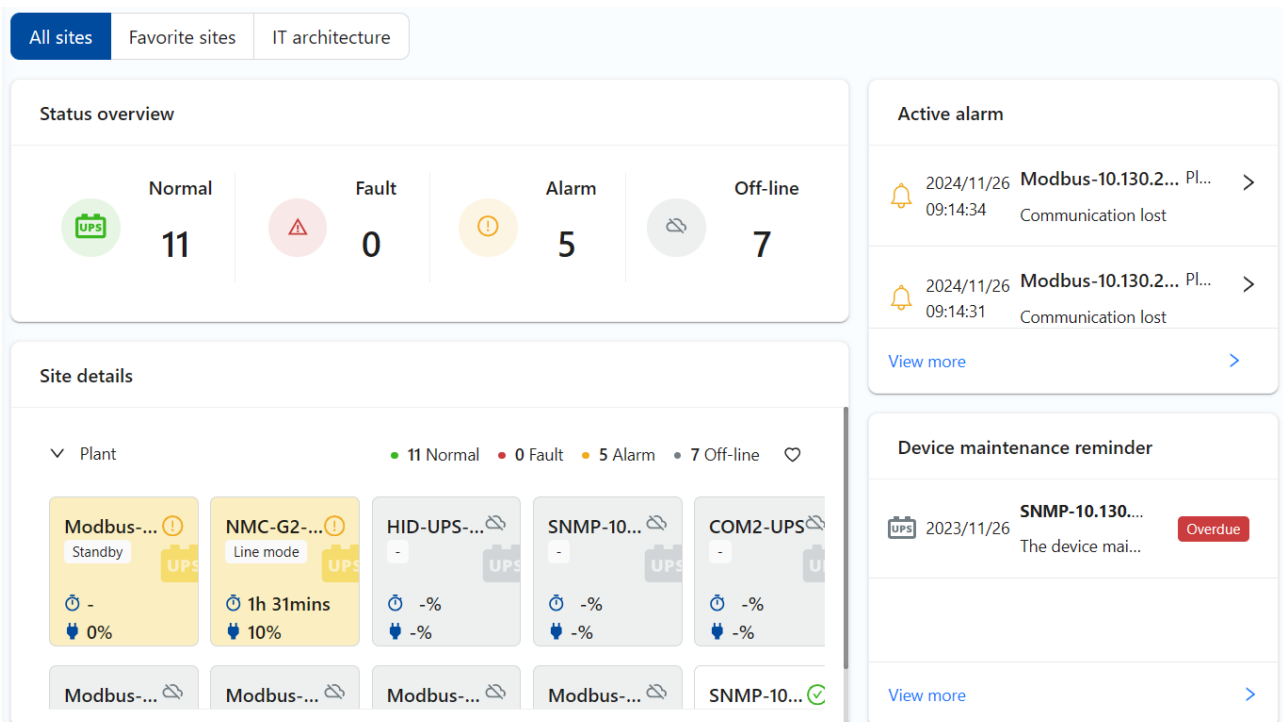
 Retrieve password with a limit of sending verification code once per minute. Otherwise, software will pop up a message "The verification code has been sent, please try again later"

2.2 Overview

Overview of all devices

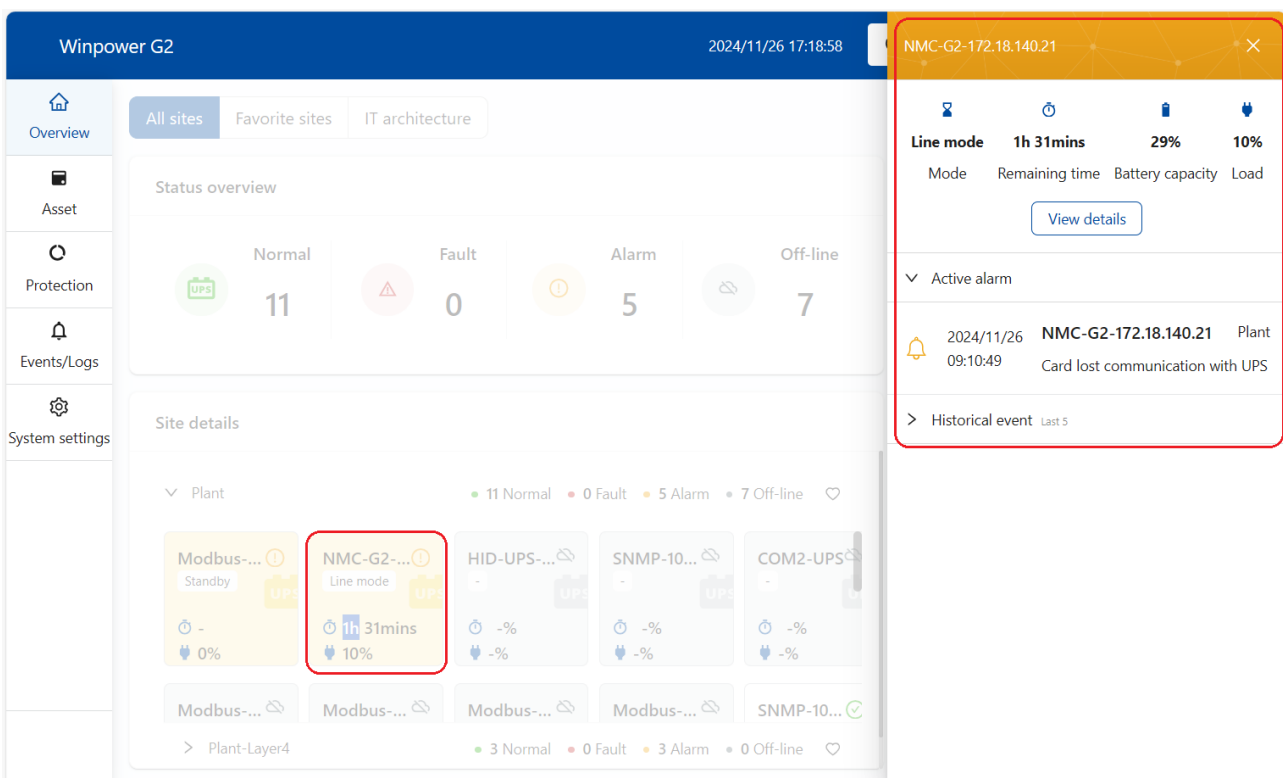
The overview page lists the status of all devices—for example, there are 11 devices in normal, 5 devices in alarm, 7 devices in off-line and 0 device in fault as below image. The overview page lists all sites and the devices in the site, lists the activated alarms at current, and lists all devices that have already or are about to expire and need to be maintained

Status	Definition	Icon
Fault	The device is experiencing serious fault	
Alarm	The device is experiencing general alarm	
Off-line	Communication is interrupted	
Normal	The device is working normally	



Overview of one device

Choose one of devices to display the parameters, active alarms, and historical events of current device



2.2.1 All sites

Root site overview

Log in as an administrator account and click on "Overview" to view all sub-sites and devices under the root site named "Plant". User can also select a sub-site from the drop-down list in the upper right corner to view the sub-site

The screenshot displays the Winpower G2 web interface. The top navigation bar shows the title 'Winpower G2', the date and time '2024/11/26 17:29:57', and a location dropdown menu currently set to 'Plant'. The left sidebar contains navigation links: Overview, Asset, Protection, Events/Logs, and System settings. The main content area is divided into several sections:

- Status overview:** A summary of system health with four categories:
 - Normal:** 11 (represented by a green circle with a checkmark)
 - Fault:** 0 (represented by a red circle with a triangle)
 - Alarm:** 5 (represented by a yellow circle with an exclamation mark)
 - Off-line:** 7 (represented by a grey circle with a cloud)
- Site details:** A section for the 'Plant' site, showing a summary of 11 Normal, 0 Fault, 5 Alarm, and 7 Off-line devices. Below this, there are five device cards:
 - Modbus-...:** Standby, 0% battery.
 - NMC-G2-...:** Line mode, 1h 31mins battery.
 - HID-UPS-...:** -%, -% battery.
 - SNMP-10-...:** -%, -% battery.
 - COM2-UPS-...:** -%, -% battery.
- Device maintenance reminder:** A reminder for 'SNMP-10.130...' dated 2023/11/26, marked as 'Overdue'.

A dropdown menu is open in the top right corner, showing a hierarchy: 'Plant' > 'Layer4' > 'RD-Lab' and 'PV-Lab'. The 'Plant' and 'Layer4' items are highlighted with a red border.

Primary site overview

Log in as "jones" account. "jones" belongs to the "Layer4" group which is reflected to primary site. "jones" can view all sub-sites ("RD Lab" and "PV Lab") under the "Layer4" site as well as all devices under each sub-site. User can also select a sub-site from the drop-down list in the upper right corner

Winpower G2 2024/11/27 09:42:45

Overview Asset Protection Events/Logs System settings

All sites Favorite sites IT architecture

Status overview

Normal 3 Fault 0 Alarm 3 Off-line 0

Site details

Layer4 3 Normal 0 Fault 3 Alarm 0 Off-line

PDU-10.1... 0.7A 70.8kWh PDU-10.1... 0A 22.3kWh

Layer4-RD-Lab 1 Normal 0 Fault 1 Alarm 0 Off-line

Layer4-PV-Lab 2 Normal 0 Fault 0 Alarm 0 Off-line

Device maintenance reminder

2023/11/26 SNMP-10.130... The device mai... Overdue

Secondary site overview

Log in with account "Sophie". "Sophie" belongs to "PVLab" group which is reflected to secondary site. "Sophie" can view "PV-Lab" site as well as all devices under this site.

Winpower G2 2024/11/27 09:51:40

Overview Asset Protection Events/Logs System settings

All sites Favorite sites IT architecture

Status overview

Normal 2 Fault 0 Alarm 0 Off-line 0

Site details

PV-Lab 2 Normal 0 Fault 0 Alarm 0 Off-line

SNMP-10... Buck mode 7h 46mins 0% NMC-G2... 5h 37mins 0%

Device maintenance reminder

Maintenance start time not set 2 To set

2.2.2 Favorite sites

Set favorite sites

Select the site then click on the heart-shaped symbol on the right, and the heart-shaped symbol will change to blue color that represent this site have been set to favorite site

Winpower G2 2024/11/27 10:50:04 Plant

Overview Asset Protection Events/Logs System settings

All sites Favorite sites IT architecture

Status overview

Normal	Fault	Alarm	Off-line
11	0	5	7

Site details

PDU-10.1... 0.6A 70.9kWh PDU-10.1... 0A 22.3kWh

> Plant-Layer4-RD-Lab 1 Normal 0 Fault 1 Alarm 0 Off-line

> Plant-Layer4-PV-Lab 2 Normal 0 Fault 0 Alarm 0 Off-line

Active alarm

2024/11/27 10:34:19 NMC-G2-172.18.1... Pl... Card lost communication...

2024/11/27 10:13:24 Modbus-10.130.2... Pl... Battery test failed

View more

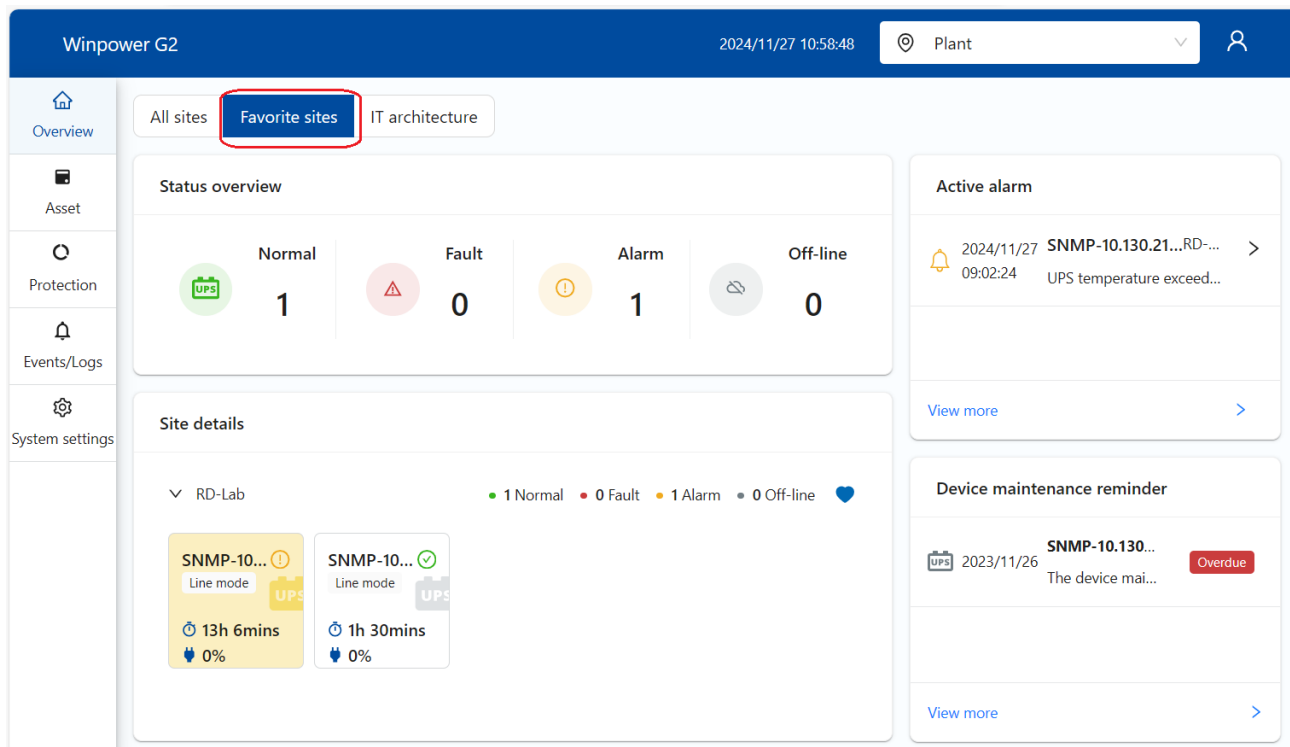
Device maintenance reminder

2023/11/26 SNMP-10.130... The device mai... Overdue

View more

Check favorite sites

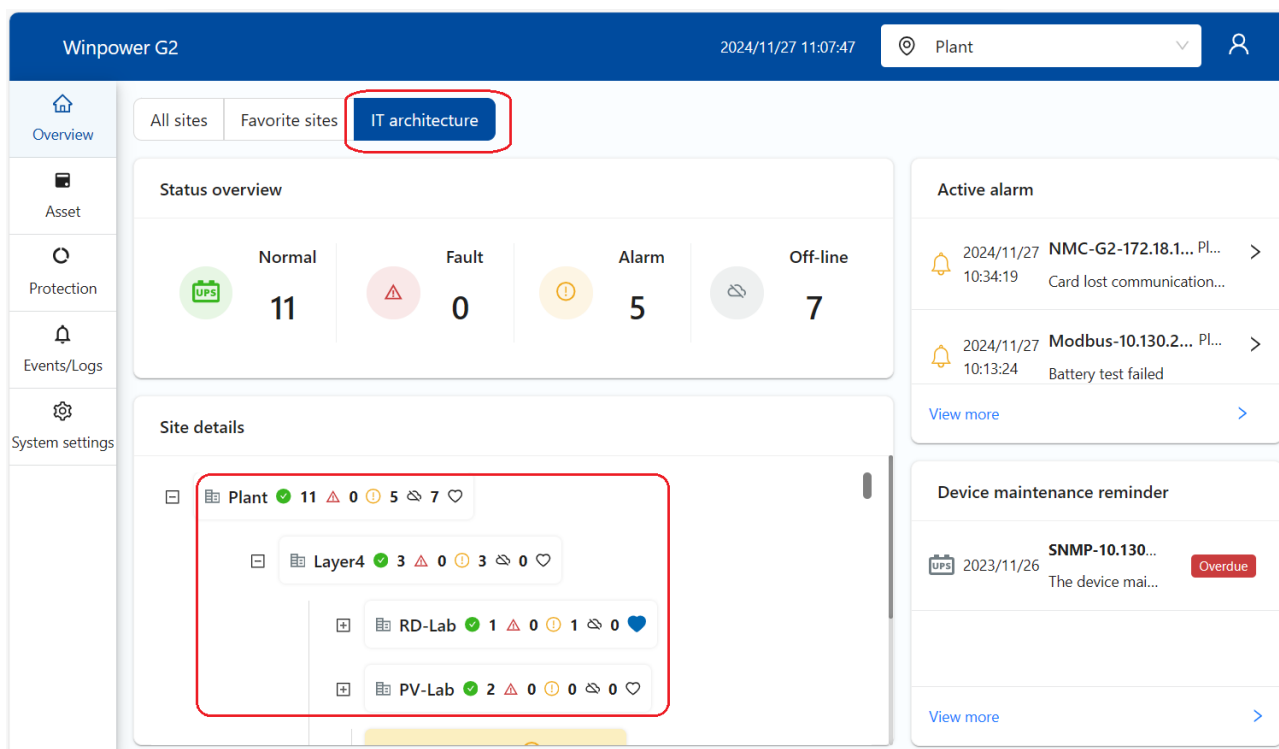
Click "Favorite sites", it will list all the favorite sites



2.2.3 IT architecture

The IT architecture is used to view the devices under the site hierarchically.

As shown in the figure below, the root site is "Plant", the primary site is "Layer4", and secondary site is "RD Lab" and "PV-Lab"



2.3 Asset

2.3.1 UPS list

This page displays the UPS list. You can add, edit, delete UPS devices and set parameters for the UPS.

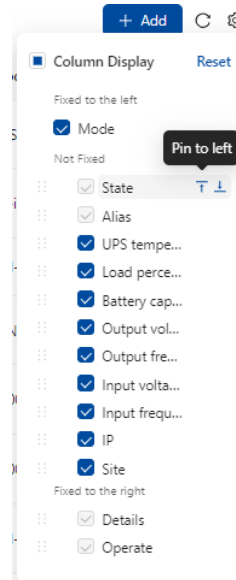
UPS																
<div> <div>State: Please select</div> <div>Alias: Please enter</div> <div>IP: Please enter</div> <div>Maintenance status: Please select</div> </div> <div> <div>Active: Please select</div> <div>Reset Query Collapse</div> </div> <div> <div>+ Add</div> <div></div> </div>																
State	Alias	Mode	UPS temperature	Load percentage	Battery capacity	Output voltage	Output frequency	Input voltage	Input frequency	IP	Site	Maintenance expiration date	Maintenance status	Active	Model	Details
<input type="checkbox"/>	SNMP-10.130.212.243	Buck mode	94.46°F	0%	100%	203.5V	50.0Hz	231.3V	-	10.130.212.243	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	UPS LINE-INT	Details
<input type="checkbox"/>	NMC-G2-10.130.212.244	Line mode	86.18°F	0%	100%	219.8V	50.0Hz	233.4V	50.0Hz	10.130.212.244	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	1K-i	Details
<input type="checkbox"/>	COMB-UPS	Bypass	87.8°F	0%	100%	232.6V	50.0Hz	232.6V	50.0Hz	-	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	ON-LINE	Details
<input type="checkbox"/>	NMC-G2-10.130.212.101	Line mode	85.64°F	0%	100%	229.7V	49.9Hz	234.3V	50.0Hz	10.130.212.101	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	INN211TKE	Details
<input type="checkbox"/>	NMC-G2-10.130.212.238	-	-	0%	100%	0.0V	0.0Hz	230.4V	50.0Hz	10.130.212.238	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	1000S	Details
<input type="checkbox"/>	NMC-G2-10.130.212.178	-	-	0%	100%	229.3V	50.0Hz	229.3V	50.0Hz	10.130.212.178	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	2200	Details
<input type="checkbox"/>	NMC-G2-10.130.212.181	Line mode	85.64°F	0%	100%	229.9V	50.0Hz	232.4V	50.0Hz	10.130.212.181	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	ON-LINE	Details
<input type="checkbox"/>	NMC-G2-10.130.212.109	Line mode	85.64°F	0%	100%	230.8V	50.0Hz	233.9V	50.0Hz	10.130.212.109	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	ON-LINE	Details
<input type="checkbox"/>	NMC-G2-10.130.212.171	Line mode	-	0%	100%	231.4V	50.0Hz	231.4V	50.0Hz	10.130.212.171	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	650	Details
<input type="checkbox"/>	SNMP-10.130.212.131	Line mode	88.34°F	0%	100%	230.2V	49.9Hz	229.1V	50.0Hz	10.130.212.131	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	ON-LINE	Details

1-10 of 19 items < 1 2 > 10 / page

View UPS

You can filter UPS by UPS status, maintenance status, activation status or entering alias and IP information. Clicking "Reset" button will clear all filtering conditions.

Click the settings icon in the upper right corner to pop up the column settings window. You can click the checkbox to select the column content to be displayed. You can drag up and down to change the position of the column, or click the pin icon to the right of the column name to pin it to left or right. Click the "Reset" button to restore the default display content and location.



This page is refreshed every 5 seconds. Click the refresh icon to refresh it immediately.

Click "Details" to jump to the device details page.

Add UPS

Click the "Add" button to search and add UPS devices.

Step 1 : Select the communication protocol according to the UPS connection type.

There are 4 communication protocols.

- Serial port/USB

Select the communication ports to be searched. For Linux and MacOSX systems, you can click the "Add" button to add a new serial port. For Windows systems, the serial ports are automatically detected. Please refer to [serial port management](#). For details on the USB/RS232 settings on the VMware ESXi server, see [How to add UPS via USB/RS232 for Virtual Machine](#).

- MQTT

The software monitors the UPS through the NMC G2 card. The NMC G2 card is a second-generation network management card. The software uses the MQTT protocol to communicate with it.

There are three IP options :

Local network - Search all IPs on the same network segment as the local system

Single IP - Enter single IP or multiple IPs separated by commas

IP segment - Enter the starting and ending addresses of the IPs you want to search for

Select credential:

Select an MQTT communication credential from the drop-down box or click "Create credential" button to create a new credential. The credentials are usually the login account and password of the card web page. The credential is only used to exchange certificates when searching. The credential will not be used in subsequent communications, subsequent communications will be verified through certificate encryption. If the card starts "Trust new client certificate for xx minutes" in "Settings → Certificate -> Pairing with Clients" web page, no credentials are required to search during this period (since it is a required option, just select any MQTT credential).

Search for adding devices

☒ 1 Select device type ☒ 2 Select communication proto ☐ 3 Search complete

Device type: ☒ UPS ☐ Server ☐ PDU

* Communication protocol:

* Search IP: ☐ Local network
☐ Single IP
☐ IP segment

* Select credential:

* Site:

- SNMP

Select the SNMP protocol when monitoring the UPS through the NMCG1 card or other SNMP network cards that support RFC1628 MIB. The IP configuration is the same as above. The credential needs to be consistent with the SNMP credential set by the card, and ensure that the card's SNMP is enabled.



The free version does not support RFC1628 MIB communication of third-party cards. If you need to monitor the UPS through the RFC1628 MIB of third-party cards, please purchase a [License management](#)

Search for adding devices

✓ Select device type — 2 Select communication proto 3 Search complete

Device type: ☒ UPS ☐ Server ☐ PDU

* Communication protocol:

* Search IP: ☐ Local network ☐ Single IP ☐ IP segment

* Port:

* Select certificate:

* Site:

- Modbus Tcp

UPS with IoT function needs to enable the Modbus TCP protocol from the LCD or IoT settings web before the software can communicate with it using the Modbus TCP protocol. IP configuration is the same as above.

Search for adding devices

✓ Select device type — 2 Select communication proto 3 Search complete

Device type: ☒ UPS ☐ Server ☐ PDU

* Communication protocol:

* Search IP: ☐ Local network ☐ Single IP ☐ IP segment

* Site:

Step 2 : Select the [site](#) where the device will be placed.

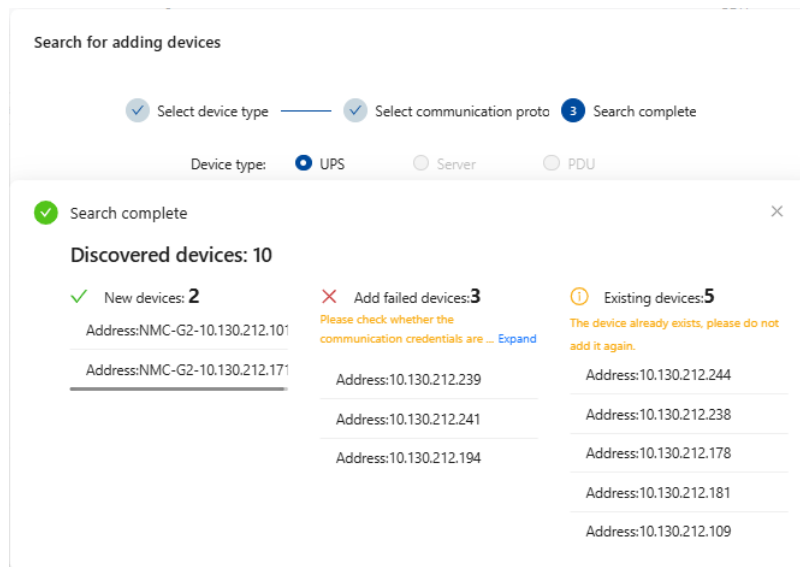
Step 3 : Click "Search" button to start searching for devices.

Step 4 : Wait for the search to complete and pop up the search results.

New devices: The new devices successfully searched and added. The aliases can be modified by device editing.

Add failed devices : The new device IPs were discovered but communication could not be established for various reasons. For details, see [reasons for failure to add devices and suggestions](#).

Existing devices: Device has been added. The IP is already used by an existing device and cannot be added again, even if protocols are different.



Batch operations

Select multiple UPSs and use the batch operation button in the upper right corner to set the maintenance start time, activate, disable and delete the devices in batches.

Selected 2 Item

Set maintenance start time

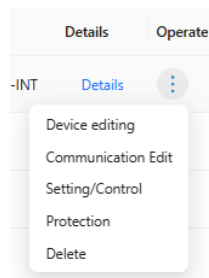
Volume activation of devices

Disable devices in batches

Delete devices in batches

<input checked="" type="checkbox"/>	State	Alias	Mode	UPS temperature	Load percentage	Battery capacity	Output voltage	Output frequency	Input voltage	Input frequency	IP	Site	Maintenance expiration date	Maintenance status	Active	Model	Details	Operate
<input checked="" type="checkbox"/>	🟢	SNMP-10.130.212.243	Buck mode	92.12°F	<div><div></div></div> 0%	<div><div></div></div> 100%	202.0V	49.9Hz	229.4V	-	10.130.212.243	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	UPS LINE-INT	Details	⋮
<input checked="" type="checkbox"/>	🟡	NMC-G2-10.130.212.244	Standby	86°F	<div><div></div></div> 90%	<div><div></div></div> 100%	0.0V	0.0Hz	228.3V	-	10.130.212.244	root	-	Maintenance time not set	<input checked="" type="checkbox"/>	LINE-INT	Details	⋮

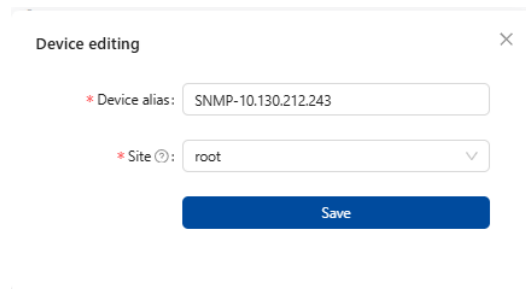
Single UPS operation



By clicking the 3 dots under the operation column, the operation menu will pop up, and you can perform the following operations on a single UPS:

- Device editing

You can modify the device's alias and site



Device editing

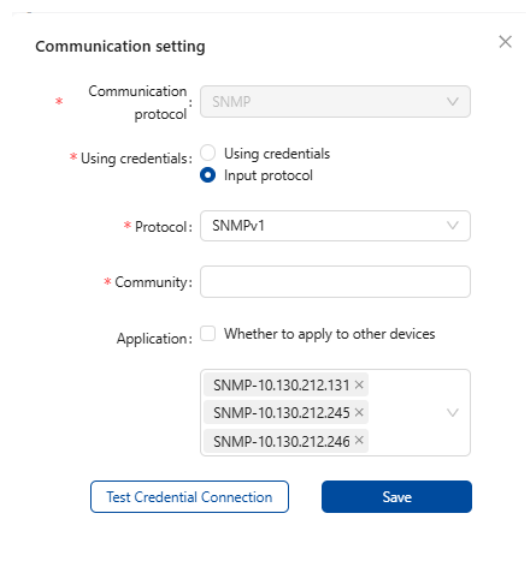
* Device alias: SNMP-10.130.212.243

* Site: root

Save

- Communication editing

Only devices communicate with SNMP protocol can edit communications. You can: modify the SNMP protocol credentials (select an existing credential or re-enter the credential parameters); test whether the credential connection is OK; apply current credential to other devices that selecting in the drop-down box.



Communication setting

* Communication protocol: SNMP

* Using credentials: ☐ Using credentials ☒ Input protocol

* Protocol: SNMPv1

* Community:

Application: ☐ Whether to apply to other devices

SNMP-10.130.212.131 ×
SNMP-10.130.212.245 ×
SNMP-10.130.212.246 ×

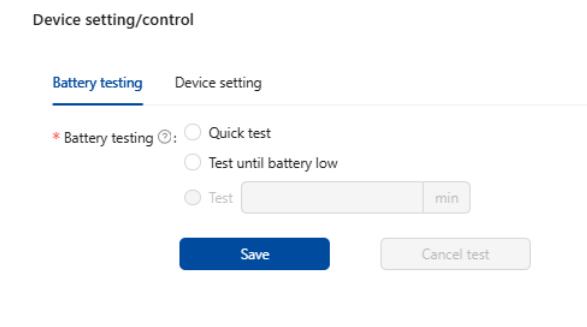
Test Credential Connection Save

- Setting/Control

Only serial port, USB and Modbus TCP UPS support setting and control.

You can perform UPS tests (unsupported test types are grayed out) or cancel ongoing tests. The "Cancel Test" button is enabled only when battery test is ongoing. Click the button to immediately send a test or cancel test command to the UPS. This is a control command and does not save the settings.

Battery testing of lithium battery UPS is not supported. The lithium battery UPS itself has a battery management system, and there is no need to perform battery self-test from the software.



Device setting/control

Battery testing Device setting

* Battery testing: ☐ Quick test ☐ Test until battery low ☐ Test

min

Save Cancel test

Device setting/control

Battery testing Device setting

* Battery testing ⓘ: ☐ Quick test
☐ Test until battery low
☐ Test min

Save Cancel test

Set UPS parameters (different UPS supports different parameters)

Device setting/control

Battery testing **Device setting**

Enable audible alarm ☐ Off

Enable auto restart ☒ On

Rated output voltage 220

Output group 1 automatic startup delay ⓘ 3 S

Converter mode ☐ Off

ECO mode ☐ Off

Rated output frequency 50

Output group 1 automatic shutdown delay ⓘ -1 S

Save

- Shutdown protection

Click this menu will go to the [shutdown protection settings](#) page

- Delete

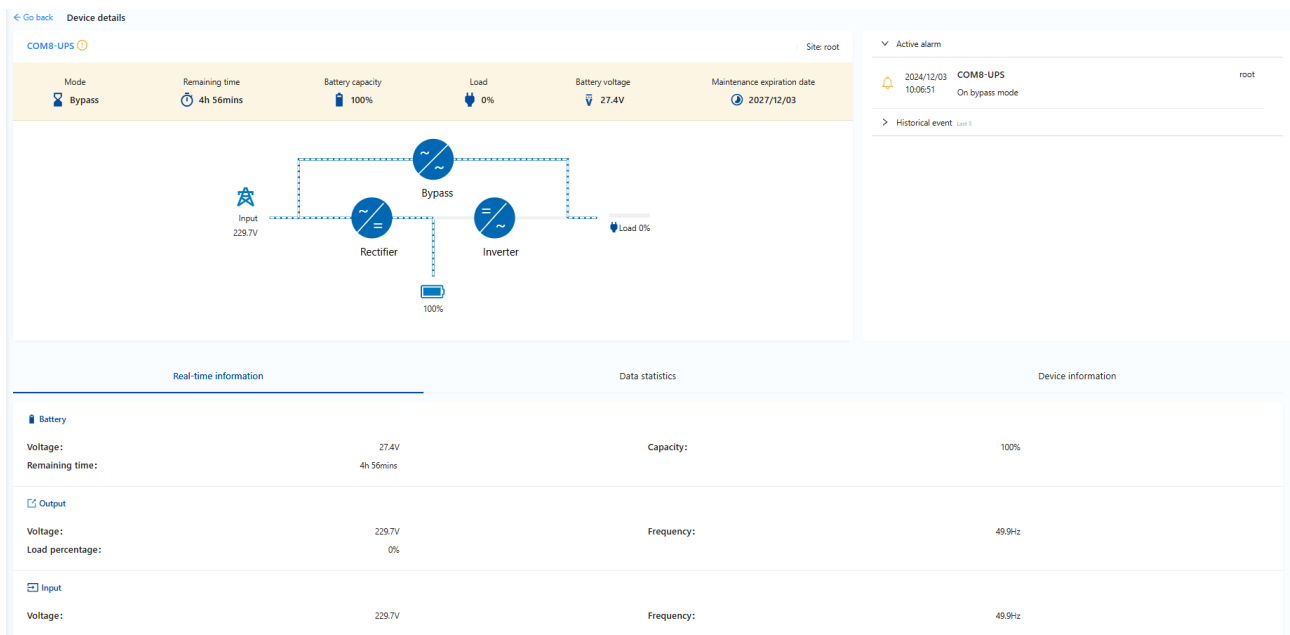
Click to delete device

- Activate/deactivate device

Drag and drop the activation button  to activate or deactivate a single device.

2.3.1.1 UPS details

This page displays the details of the UPS device.



Page layout

The left side of the upper part displays the device alias, status icon, site, key data and workflow diagram, and the right side displays currently active alarms and historical events.

There are 3 tabs in the lower part, which display the real-time information of the device, data statistics (discharge data and historical data) and device information respectively.

Real-time information

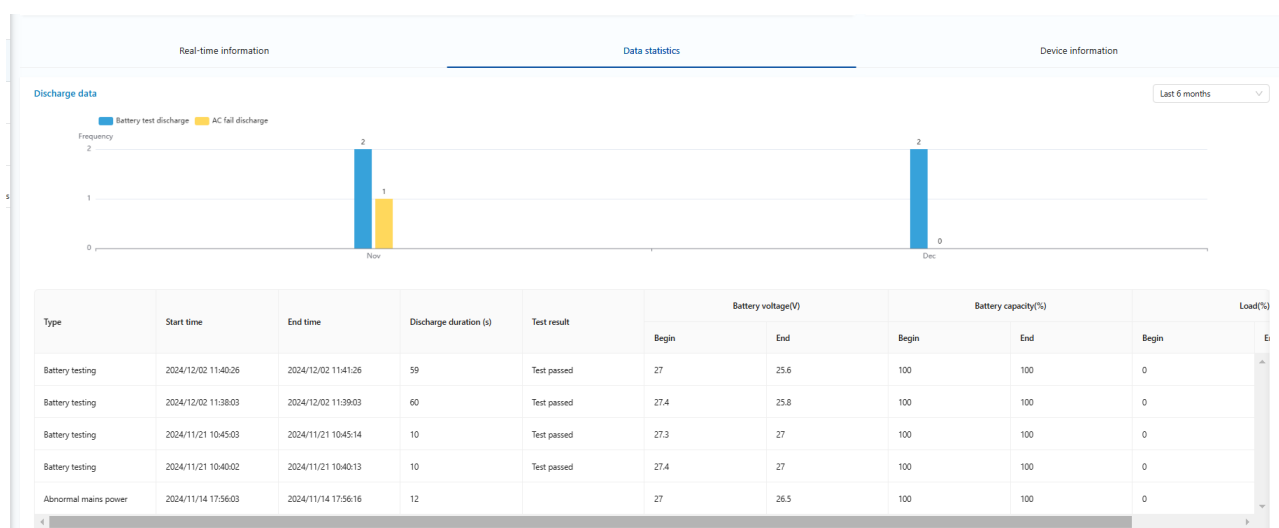
Displays real-time measured values of UPS battery, output, and input. The dual-input UPS will also display bypass data. If the card is connected to a sensor, the sensor data and status will also be displayed.

Data statistics

Data statistics include discharge data statistics and historical data trend charts.

- Discharge data

Discharge data can be viewed for the past six months or the past year. The bar graph shows the number of monthly battery tests and the number of abnormal mains discharges. The table displays detailed data for each discharge, including: discharge type, start time, end time, discharge duration, test results (only available for battery tests), battery voltage at the start, battery voltage at the end, battery capacity at the start, and end Battery capacity, load percentage at the start, load percentage at the end.



- Historical data trend chart

Trend charts of load percentage, battery voltage, input voltage, output voltage, and UPS temperature can be viewed by daily, monthly, and yearly.

The daily trend chart displays the historical data of that day.

Monthly and yearly trend charts display the average, maximum, and minimum values of data on a daily basis.

Device information

Display device-related information, of which "alias" and "site" can be modified in the [device editor of the UPS list](#).

"Contact name", "Contact email", and "Contact phone" are the administrator information entered when [creating the site](#). As shown in the figure below, the contact information of the "root" administrator of the site is shown.

"Maintenance expiration date" is calculated based on the [maintenance start time](#) and [maintenance period settings](#) of the device. Maintenance expiration date= maintenance start time + maintenance period.

Real-time information	Data statistics	Device information
Device information		
Serial number:		Maintenance expiration date: 2027/12/03
Alias: COM8-UPS		Communication parameters: COM8
Site: root		
Contact name: David		
Contact email: david@abc.com		
Contact phone: 13567876567		

2.3.2 Server

Add remote servers

Winpower supports various of protocols to add remote server or service, such as "SPS, IPMI, VMware Center, VMware ESXi, SSH, NetApp-Cluster"

Search for adding devices ✕

☒ Select device type ——— **2** Select communication proto **3** Search complete

Device type: ☐ UPS ☒ **Server** ☐ PDU

* Communication protocol: Please select ▼

SPS
 IPMI
 VMware Center
 VMware ESXi
 SSH
 NetAppCluster

Edit/Delete remote servers

- Edit: edit the site, user, and password
- Protection: jump to the “Shutdown Protection Settings” page
- Delete: delete the corresponding server or service

List search ▼
Please enter name
Q
+ Add

Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type	Source	Site	VM protection priority	Set protection priority	Operate
Unprotected	10.130.212.116	✔		10.130.212.116	SSH		Plant			⋮
– Unprotected	10.130.212.24	✔		10.130.212.24	vCenterServer		Plant			⋮
–	DPQRD	✔			Cluster		Plant			⋮
+	Esxi22.SSG5-Serial	✔	PoweredOn	10.130.212.22	Hypervisor		Plant			⋮
+	Esxi21.SSG5-Serial	✔	PoweredOn	10.130.212.21	Hypervisor		Plant			⋮
+	Esxi23.SSG5-Serial	✔	PoweredOn	10.130.212.23	Hypervisor		Plant			⋮
– Unprotected	FAS2720	✔	PoweredOn	10.130.212.13	NetAppCluster		Plant			⋮
	FAS2720-01	✔	PoweredOn		NetApp		Plant			⋮
	FAS2720-02	✔	PoweredOn		NetApp		Plant			⋮

Quickly search for servers

- Choose “List search”: Enter the remote server’s name, such as “Esxi”, it will remain only Esxi servers and other servers will be filtered out
- Choose “Tree search”: Enter the remote server’s name, such as “Esxi”, it will jump to the Esxi server, but other servers won’t be filtered out

UPS		Server			
List search		Esxi			
Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type
Unprotected	Esxi22.SSG5-Serial	✓	PoweredOn	10.130.212.22	Hypervisor
Unprotected	Esxi21.SSG5-Serial	✓	PoweredOn	10.130.212.21	Hypervisor
Unprotected	Esxi23.SSG5-Serial	✓	PoweredOn	10.130.212.23	Hypervisor

2.3.2.1 SPS list

Add SPS

Prerequisite: Install SPS software on the remote computer, port 8883 is opened

- Select "SPS" in "Communication protocol"
- Enter the start and end address of SPS IP, or enter a single IP address in the start IP address field of the "Custom IP"
- Enter the SPS username and password
- Set site for SPS host
- Set the power source for the SPS host. Before setting up the power source, please add the UPS firstly. Check [UPS list](#)

Search for adding devices

☒ Select device type ——— **2** ☒ Select communication proto **3** Search complete

Device type: ☐ UPS ☒ Server ☐ PDU

* Communication protocol:

* Custom IP [?]:

* SPS username:

* SPS password:


* Site:

* Power source: ☒ Single UPS ☐ Redundant UPS

Add

Search SPS

After the searching process is completed, the bottom right corner of the webpage will prompt the dialog that show the number of successfully added devices, the number of failed devices, and the reason for failure

 Failure Information Added successful devices:3 ✕

10.130.212.159 : Account or password is incorrect

10.130.212.186 : Account or password is incorrect

10.130.212.250 : Account or password is incorrect

SPS list

After successfully adding SPS, the SPS information will be displayed in the list as below image

Overview

Asset

Protection

Events/Logs

System settings

UPS

Server

PDU

Redundant UPS

List search

Please enter name

+

Add

Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type	Source	Operate
Protected	SPS-CNSHNWLABRDC50	✔	Running	10.130.212.43	SPS	HID-UPS-G699R0101!	⋮
Protected	SPS-dhcp-10-130-212-116	✔	Running	10.130.212.116	SPS	HID-UPS-G699R0101!	⋮

2.3.2.2 IPMI list

Add IPMI

Prerequisite: Server enabled IPMI service

- Select "IPMI" in "Communication protocol"
- Enter IPMI hostname/IP address, username and password
- Set site for IPMI host
- Set the power source for IPMI host. Before setting up the power source, it is necessary to add a UPS. Please check [UPS list](#)

Search for adding devices


1 Select device type — 2 Select communication proto 3 Search complete

Device type: ☐ UPS ☒ Server ☐ PDU

* Communication protocol: ▼

* Host name:

* User name:

* Password: 

* Site: ▼

Power source: ☒ Single UPS ☐ Redundant UPS

▼

IPMI list

After successfully adding the IPMI server, the IPMI host information will be displayed in the list as below image.

The column “Shutdown Configuration Status” show “Unprotected”, indicating that the power source for IPMI host haven’t been set and the shutdown protection haven’t been enabled

UPS

Server

PDU

Redundant UPS

List search

Please enter name

+ Add

Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type	Source	Site	Operate
Unprotected	10.130.212.40	✓	PoweredOn	10.130.212.40	IPMI	HID-UPS-G699R01019	roc	⋮
Unprotected	10.130.212.39	✓	PoweredOn	10.130.212.39	IPMI	HID-UPS-G699R01019	roc	⋮

2.3.2.3 VMware Center list

Add VMware Center

Prerequisite: Purchase copyright for VMware Center

- Choose "VMware Center" in the "Communication protocol"
- Enter vCenter hostname/IP, username, password
- Set the site for the vCenter server



vCenter is just a service, so there is no need to set power source for vCenter. Shutdown protection is for VMware ESXi host

Search for adding devices



☒ Select device type — ☒ Select communication proto **3** Search complete

Device type: ☐ UPS ☒ Server ☐ PDU

* Communication protocol: VMware Center ▼

* Host name:

* User name:

* Password: 👁

* Site: ▼

Add

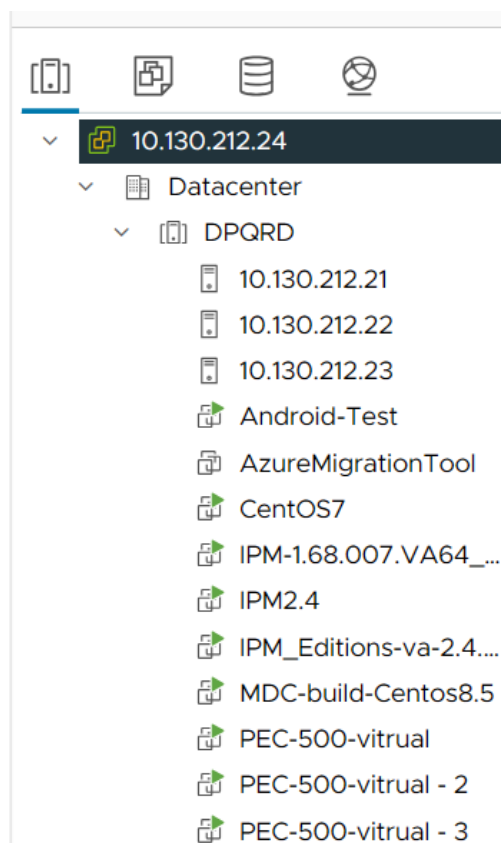
vCenter list

- After successfully adding the server, the vCenter topology architecture will be displayed as following:
vCenter Server-> Cluster->Hypervisor (ESXi host)-> Virtual Machine
- Virtual machine with installed vCenter or Winpower will be automatically set as critical virtual machine, while other virtual machines can be set to critical virtual machines manually

UPS		Server			PDU		Redundant UPS		
List search		Please enter name					+ Add		
Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type	Source	Site	Operate	
Unprotected	10.130.212.24	✓		10.130.212.24	vCenterServer		Plant	⋮	
	DPQRD	✓			Cluster		Plant	⋮	
	Esxi22.SSG5-Serial	✓	PoweredOn	10.130.212.22	Hypervisor		Plant	⋮	
	IPM-1.68.007.VA64_OVF10	✓	PoweredOn	10.130.212.207	Virtual Machine		Plant		
	SPS1	✓	PoweredOn		Virtual Machine		Plant		
	PEC-500-vitrual - 4	✓	PoweredOn		Virtual Machine		Plant		

Topology comparison

The topology of the Winpower side is consistent with the web of vCenter, check the image as below



2.3.2.4 VMware ESXi list

Add ESXi

Prerequisite: Purchase copyright for VMware ESXi



VMware ESXi is the standalone version of VMware, while VMware vCenter is the centralized monitoring version

- Choose "VMware ESXi" in the "Communication protocol"
- Enter ESXi hostname/IP, username, password
- Set the site for ESXi host
- Set the power source for ESXi host. Before setting up the power source, you need to add a UPS firstly. Please check [UPS list](#)

Search for adding devices

☒ Select device type **2** Select communication proto **3** Search complete

Device type: ☐ UPS ☒ Server ☐ PDU

* Communication protocol: VMware ESXi

* Host name:

* User name:

* Password:

* Site:

Power source: ☒ Single UPS ☐ Redundant UPS

Add

ESXi list

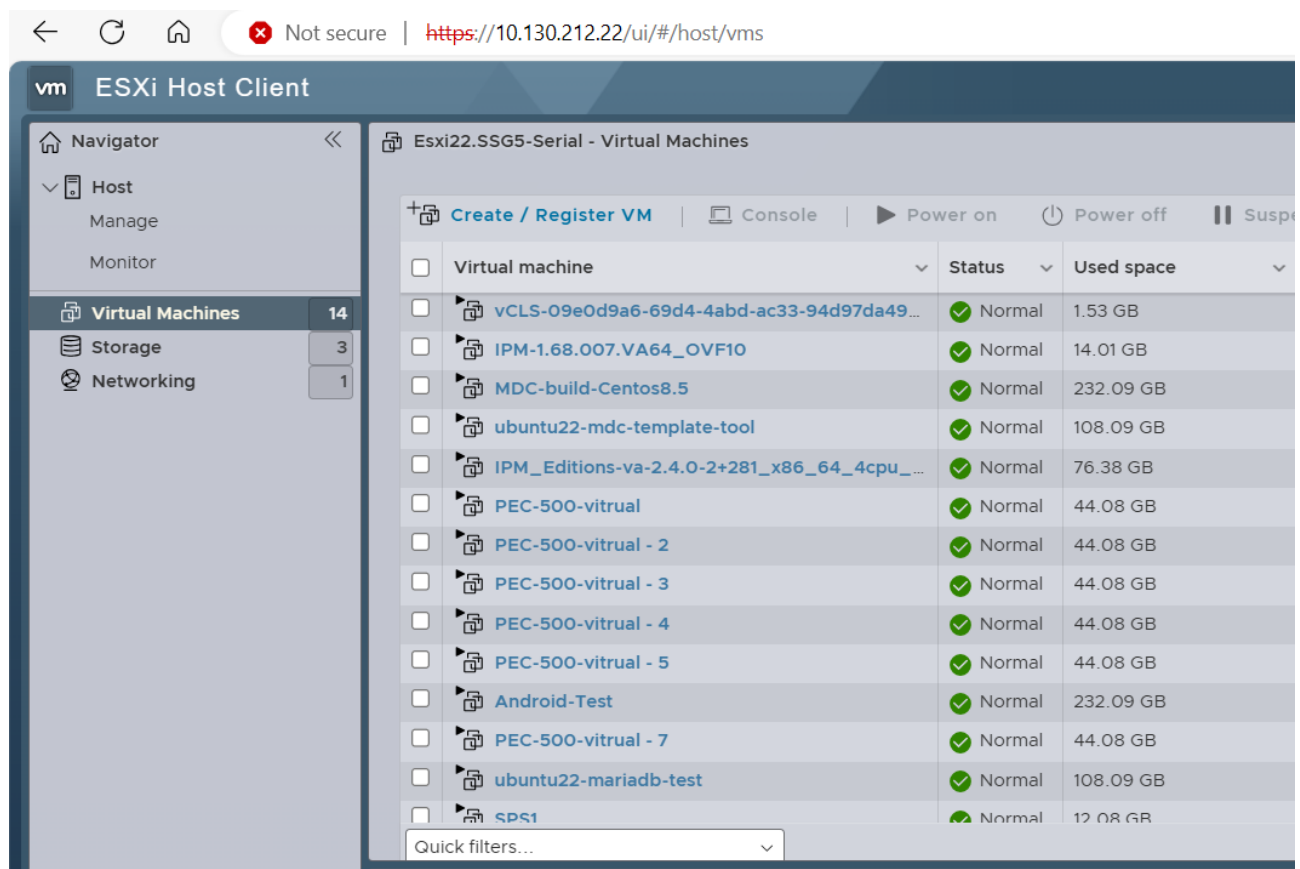
- After successfully adding the server, the ESXi topology architecture will be displayed as following:
ESXiServer (ESXi hosts) -> Virtual Machine

- Virtual machine with installed Winpower will be automatically set as critical virtual machine, and other virtual machines can't be set to critical virtual machines manually

Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type	Source	Site	Operate
Unprotected	Esxi22.SSG5-Serial	✓	PoweredOn	10.130.212.22	EsxiServer	NMC-G2-10.130.212.244	Plant	⋮
	SPS1	✓	PoweredOn		Virtual Machine		Plant	
	ubuntu22-mariadb-test	✓	PoweredOn		Virtual Machine		Plant	
	PEC-500-vitrua1 - 7	✓	PoweredOn		Virtual Machine		Plant	
	Android-Test	✓	PoweredOn		Virtual Machine		Plant	
	PEC-500-vitrua1 - 5	✓	PoweredOn		Virtual Machine		Plant	

Topology comparison

The topology of the Winpower side is consistent with the web of ESXi, check the image as below



2.3.2.5 SSH list

Add SSH

Prerequisite: Server enables SSH service, port 22 is opened

- Choose “SSH” in the “Communication protocol”
- Enter SSH hostname/IP, username and password
- Enter the SSH server port, the default port is 22
- Set the site for SSH host
- Set the power source for SSH host. Before setting up the power source, it is necessary to add a UPS. Please check [UPS list](#)

Search for adding devices



1 Select device type — 2 Select communication protocol 3 Search complete

Device type: ☐ UPS ☒ Server ☐ PDU

* Type: SSH

* Host name: 10.130.212.159

* Port: 22

* User name: root

* Password:

* Site: root

Power source: ☒ Single UPS ☐ Redundant UPS

NMC-G2-10.130.212.204 / output

Add

SSH list

After successfully adding the SSH, the SSH host information displayed in the list as below image.

“Communication status” represent the IPMI communication status. If the image color is green, it means the status is OK. If the image color is grey, it means the status is lost.

The column “Shutdown Configuration Status” show “Unprotected”, indicating that the power source for SSH host haven’t been set and the shutdown protection haven’t been enabled.

Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type
Unprotected	10.130.212.159	✓		10.130.212.159	SSH
Unprotected	10.130.212.250	✓		10.130.212.250	SSH

2.3.2.6 NetApp Cluster list

Add NetApp Cluster

- Choose “NetApp Cluster” in the “Communication protocol”
- Enter NetApp Cluster hostname/IP, username, password
- Set site for NetApp storage nodes



NetApp cluster is just a service, so there is no need to set the power source for it. Shutdown protection is only for NetApp storage nodes

Search for adding devices

☒ Select device type — ☒ Select communication proto **3** Search complete

Device type: ☐ UPS ☒ Server ☐ PDU

* Communication protocol:

* Host name:

* User name:

* Password:

* Site:

Add

NetApp list

- The column "NetAppCluster" lists all the NetApp storage nodes, there are two NetApp storage nodes as shown in the following image

Shutdown Configuration Status	Name	Communication status	Operate status	IP	Type	Source
Unprotected	FAS2720	✓	PoweredOn	10.130.212.13	NetAppCluster	
	FAS2720-01	✓	PoweredOn		NetApp	
	FAS2720-02	✓	PoweredOn		NetApp	

- The NetApp topology at Winpower side is consistent with the web of NetApp cluster, check below image.

ONTAP System Manager (Return to classic version)

Cluster Overview

NAME	FAS2720	DNS DOMAINS	netapp.com
VERSION	NetApp Release 9.6P3: Sun Sep 22 08:26:36 UTC 2019	NAME SERVERS	8.8.8.8
LOCATION	shenzhen	MANAGEMENT INTERFACES	10.130.212.13

Nodes

	FAS2720-02	FAS2720-01
UPTIME	24 day(s), 2:31:33	53 day(s), 7:29:30
MODEL	FAS2720	FAS2720
SERIAL NUMBER		
VERSION	NetApp Release 9.6P3: Sun Sep 22 08:26:36 UTC 2019	NetApp Release 9.6P3: Sun Sep 22 08:26:36 UTC 2019
MANAGEMENT	10.130.212.12	10.130.212.11

2.3.3 PDU list

This page allows you to view the PDU devices, add, edit, delete devices, and set parameters for the PDU.

UPS														Server					PDU					Redundant UPS				
Please enter name																												
<input type="checkbox"/>	Name	State	Input voltage	Input frequency	Input current	Apparent power	Active power	Energy	Factor	Rated Power	Remaining power	IP	Site	Maintenance expiration date	Maintenance status	Active	Details	Operate										
<input type="checkbox"/>	PDU-10.130.212.61		230V	50.0Hz	0.6A	129VA	43.0W	78.6kWh	0.33	3520W	3477W	10.130.212.61	childsite1	-	Maintenance time not set		Details											
<input type="checkbox"/>	PDU-10.130.212.62		231V	50.0Hz	0.0A	0VA	0.0W	24.8kWh	0.0	3520W	3520W	10.130.212.62	childsite1	-	Maintenance time not set		Details											
<input type="checkbox"/>	PDU-10.130.212.251		232V / 232V / 232V	50.0Hz	0.0A / 0.0A / 0.0A	0VA / 0VA / 0VA	0.0W / 0.0W / 0.0W	5.6kWh	0.0 / 0.0 / 0.0	3520W / 3520W / 3520W	3520W / 3520W / 3520W	10.130.212.251	childsite1	-	Maintenance time not set		Details											
<input type="checkbox"/>	PDU-10.235.226.6		230V	50.0Hz	0.6A	107VA	64.0W	67.2kWh	0.59	3520W	3456W	10.235.226.6	childsite1	-	Maintenance time not set		Details											

Click "Details" to jump to the [PDU details](#) page.

Add PDU

The software monitors PDU through the SNMP protocol. To control and set the PDU, you need to use communication credential with write permission. The parameters are as same as [SNMP protocol settings in UPS](#).

Batch operations

Select multiple devices and use the batch operation button in the upper left corner to perform batch operations on PDUs such as setting the maintenance start time, activating, disabling and deleting devices.

UPS

Server

PDU

Redundant UPS

Please enter name

Q

+ Add

Set maintenance start time

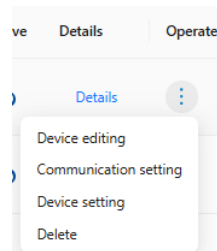
Volume activation of devices

Disable devices in batches

Delete devices in batches

<input checked="" type="checkbox"/>	Name	State	Input voltage	Input frequency	Input current	Apparent power	Active power	Energy	Factor	Rated Power	Remaining power	IP	Site	Maintenance expiration date	Maintenance status	Active	Details	Operate
<input checked="" type="checkbox"/>	PDU-10.130.212.61		230V	50.0Hz	0.6A	129VA	43.0W	78.7kWh	0.33	3520W	3477W	10.130.212.61	childsite1	-	Maintenance time not set		Details	
<input checked="" type="checkbox"/>	PDU-10.130.212.62		231V	50.0Hz	0.0A	0VA	0.0W	24.8kWh	0.0	3520W	3520W	10.130.212.62	childsite1	-	Maintenance time not set		Details	

Single device operation



By clicking the 3 dots under the operation bar, the operation menu pops up, and you can perform device editing (modify the device's alias and site), communication settings (modify communication credentials), and PDU parameter settings (system, outlet, sensor) and delete operations. **Communication credentials require write permission to perform PDU parameter settings.**

- Activate/deactivate device

Drag and drop the activation button to activate or deactivate a single device.

2.3.3.1 PDU details

This page displays the details of the PDU device, groups the outlets, and controls the on and off of the outlets.

Go back

Device details

PDU-10.130.212.251

IP: 10.130.212.251

Site: childsite1

Model: FLX75A318C3

5.6 kWh Energy

100000 W Rated Power

50.0 Hz Input frequency

Environment

23°C44%

Open

23°C39%

Open

Active alarm

2024/12/02 14:57:35

PDU-10.130.212.251 Door is opened

childsite1

2024/12/02 14:57:35

PDU-10.130.212.251 Door is opened

childsite1

2024/12/02 14:57:14

Automatically setting the local IP as the trap receiving address failed (the trap receiving list has been exhausted).

childsite1

Input

Voltage

232V

Current

0.0A

Factor

0.0

Active power

0.0W

Apparent power

0.0VA

Remaining Power

3520W

Outlet

Outlet Overview

Outlet opened

Outlet closed

ALL

Outlet.1

Outlet.2

Outlet.3

Outlet.4

Outlet.5

Outlet.6

Outlet.7

Outlet.8

Outlet.9

Page layout

The top displays system information, output and input real-time data.

The left side of the lower part displays the status and real-time values of the sensors (if any), as well as the current active alarms and historical events. The right side displays an overview of the outlet switch status and displays the switch status and real-time data of each outlet by group.

Control outlet on/off

Click the "All On" button in the outlet overview to turn on all outlets. Click the "All Off" button to turn off all outlets.


Click the "All On" button in the upper right corner of each group to turn on all outlets in the group. Click the "All Off" button to turn off all outlets in the group.

Drag the switch button of the outlet individually to control the on and off of a single outlet.



SNMP communication credentials are required to have write permissions on the device to set the PDU.

Group settings

Click the edit button  Group 2 to the left of the group name to pop up the group setting window. You can edit the group name, add or delete outlets in the group, then click the "Save" button to save the settings. A "Operation Successful" message will pop up if the save is successful.

X
Group Settings

Group name
Group 2

Outlet in group

Outlet_10 X

Outlet_11 X

Outlet_12 X

Outlet_13 X

Outlet_14 X

Outlet_15 X

Outlet_16 X

Outlet_17 X

Outlet_18 X

Outlet_19 X

Outlet_20 X

Outlet_21 X

Outlet_22 X

Outlet_23 X

Outlet_24 X

Addable sockets

Outlet_1 +

Outlet_2 +

Outlet_3 +

Outlet_4 +

Outlet_5 +

Outlet_6 +

Outlet_7 +

Outlet_8 +

Outlet_9 +

Save

2.3.4 Redundant UPS

Create redundant UPS group

Click "Asset"->"Redundant UPS"->"Add", Create a new redundant UPS group. Set the name for the group and choose the corresponding UPS as a group

* Name:

* Site:

* UPS:

- ☐ NMC-G2-10.130.212.101
- ☐ HID-UPS-X000-Y00000000000
- ☐ COM2-UPS
- ☐ Modbus-10.130.212.217
- ☐ NMC-G2-172.18.140.21
- ☐ SNMP-10.130.212.243
- ☐ SNMP-10.130.212.245
- ☒ HID-UPS-715318A00017
- ☒ HID-UPS-CP10M5178670001

[Save](#)

Check Redundant UPS

Click “View” button to see which UPS are included in the group

UPS

Server

PDU

Redundant UPS

Please enter name

Q

+ Add

Name	UPS	Site	Create time	Operate
PSGroup	<div>View</div>	Plant	2024/12/01 00:24:11	<div><div></div><div></div></div>

2.4 Shutdown Protection

2.4.1 Shutdown protection setting

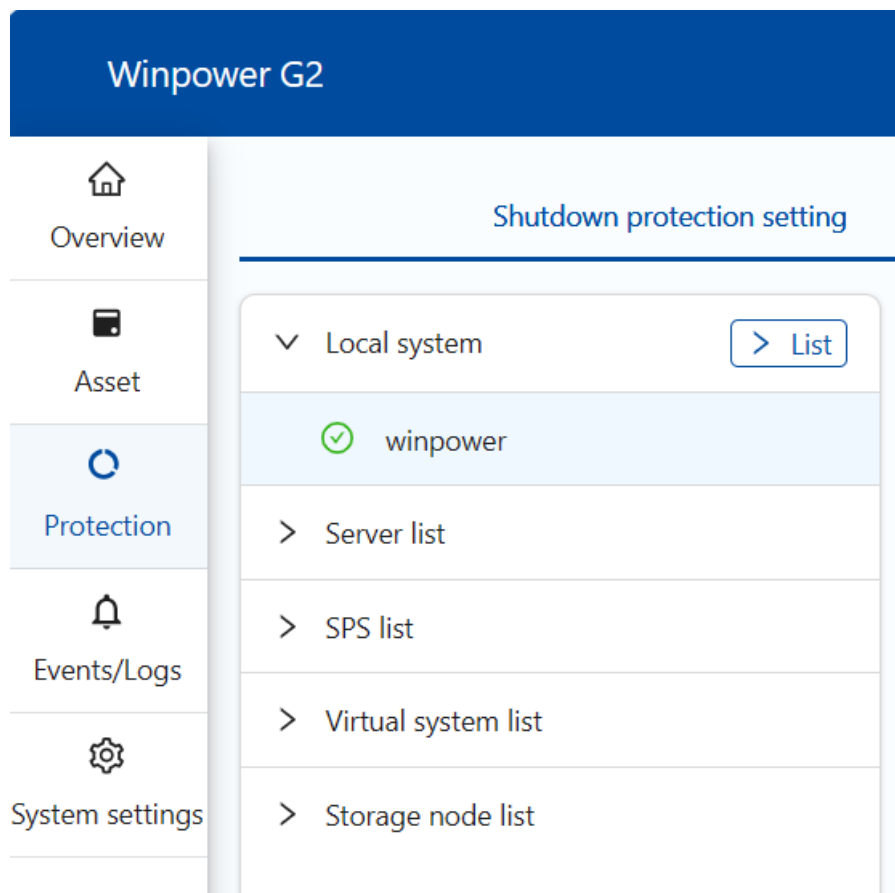
Shutdown list

- Local system: The host where Winpower is installed



If local host hasn't been set with power source and no shutdown action has been set, this node will display "Unprotected", indicating that the host has not yet been protected by the UPS

- Server list: SSH host, IPMI host, VMware ESXi host for vCenter
- SPS list: SPS host
- Virtual system list: VMware ESXi host for standalone, VMware Cluster
- Storage node list: NetApp cluster and NetApp storage nodes



Power source setting

- Method 1: Choose "Single UPS", the dropdown list will list all the power devices in the asset list, select the power source for the host. Before set the power source, it is necessary to add a UPS firstly, View [UPS list](#)

Shutdown protection setting

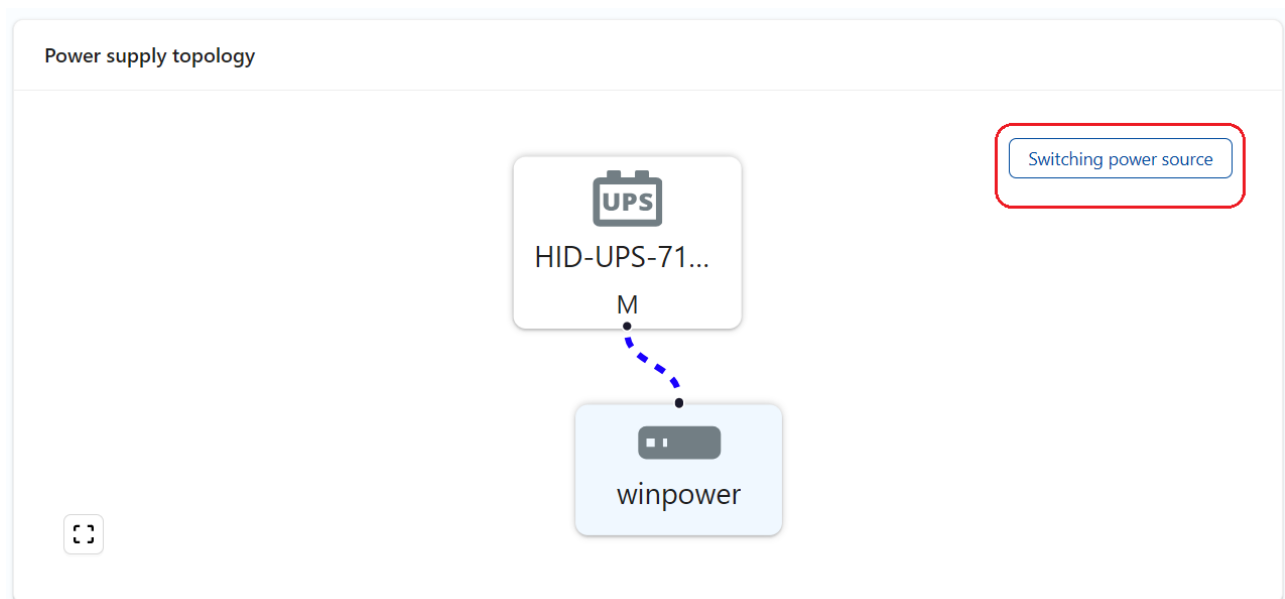
Save

Shutdown conditions
Shutdown action
Power source setting

Type: ☒ Single UPS ☐ Redundant UPS

* UPS:

- Method 2: Switch power source through the "Power supply topology"



Shutdown condition

- Shutdown when battery discharge for: When the discharge time of power source reaches the value, software will trigger the shutdown action
- Shutdown when battery low: When an alarm of low battery occurs for the power source, software will trigger the shutdown action
- Shutdown when the battery capacity is lower than: When the battery capacity of the power source is lower than the set value, software will trigger the shutdown action
- Shutdown when the battery remaining time is lower than: When the battery remaining time of the power source is lower than the set value, software will trigger the shutdown action
- UPS is going shut down: 1. If software communicates with the power source through USB/RS232/Modbus TCP, when the scheduled shutdown time is reached, the shutdown action will be triggered. 2. If software communicates with the power source through NMCG2 card, when the UPS enter to shutdown count down, the card will push shutdown notification to software, then software will trigger the shutdown action.
- If multiple conditions are selected, any one of them is met the shutdown action will be triggered



If the power source is NMCG1, the card won't push a shutdown notification to the software, so the shutdown conditions are based on shutdown condition in software side.
If the power source is NMCG2, the card will push a shutdown notification to the software. The shutdown condition depends on both software's shutdown condition and the card notification. Any condition is met, the shutdown action will be triggered



Some offline UPS haven't sent remaining battery time or battery capacity. In this case, even if the shutdown condition for the remaining battery time or battery capacity is set, the shutdown will not be triggered

Shutdown protection setting

[Save](#)

Shutdown conditions

Shutdown action

Power source setting



Shutdown when battery discharge for

s

Apply to other servers



Shutdown when battery low

Please select



Shutdown when the battery capacity is lower than

%



Shutdown when the battery remaining time is lower than

s



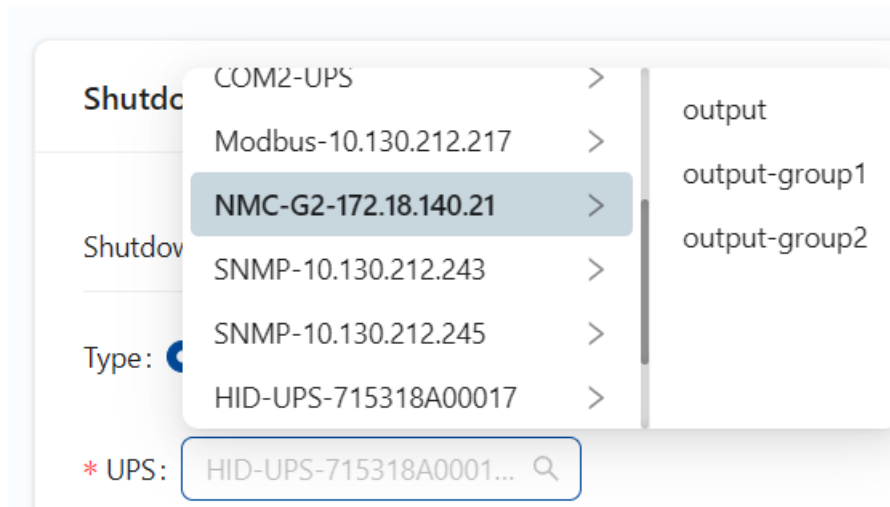
UPS is going shut down

Main output/LS output

- output: Power supply from main output, the shutdown condition is based on software side
- output-group1: Power supply from LS1 section, shutdown condition is based on both the "shutdown conditions" on software side and the automatic shutdown delay of LS1 which is calculated by UPS firmware. Whichever condition is met will trigger shutdown action
- output-group2: Power supply from LS2 section, shutdown condition is based on both the "shutdown conditions" on software side and the automatic shutdown delay of LS2 which is calculated by UPS firmware. Whichever condition is met will trigger shutdown action



Not all UPS have LS1 and LS2, some UPS don't have LS, some UPS only have LS1, and some UPS have both LS



2.4.1.1 Local shutdown

Prerequisite

Check [Shutdown protection setting](#) , Set power source and shutdown conditions

Shutdown script

- Shutdown script: Upload script and script will be saved to "script" subdirectory of software installation directory
- Script execution time: The maximum execution time of the script. If the script is successfully executed, the system will immediately shut down or hibernate. If the script execution fails, the system will shut down or hibernate till the "script execution time" reaches
- Script execution method: On Windows, there are two options: service or non-service. Service mode refers to execute scripts with "Network service" owner, while non-service mode refers to execute script with "login user" owner. For interaction script, the script must be executed in a non-service mode



No need to set "script execution method" on Linux and Mac OSX

- Test: Click the "Test" button to execute the script according to "Script execution method"
- View script execution log: View the result of executing the script

System shutdown

- Shutdown: OS will be shutdown
- Hibernate: OS will be hibernated
- Execution time: The time required for the OS to shut down or hibernate, it also means the delay time for UPS shutdown
- Test: Click the test button, OS will immediately shut down or hibernate

Shut down UPS

“Shut down UPS” means shut down UPS output. it is only applied to the power source that is communicated with software through USB/RS232/Modbus TCP. If “Shut down UPS” is enabled, once the shutdown condition is met and the script execution has been completed, software will send a shutdown command to UPS with the delay time of "Execution time"



If the power source is communicated with software through cards, UPS will be shut down by card not by software, so this item will turn gray

Shutdown protection setting

[Save](#)

Shutdown conditions Shutdown action Power source setting

☐ Shutdown script

Script execution method ☒ Service ☐ Non service

☒ System shutdown ☒ Shutdown ☐ Hibernate

☒ Shut down UPS

Shutdown protection scenario



Please distinguish between “UPS is going shut down” in Shutdown condition and “Shut down UPS” in Shutdown action. The former is OS shutdown triggering condition, while the latter is UPS shutdown action

Scenario 1: Set the shutdown condition to “battery capacity is lower than 30%”, Set the shutdown action to “Shut down UPS is enabled” and “Shutdown script is enabled”

When the battery capacity is lower than 30% ->run the script ->OS shutdown ->After the "Execution time" (default 2 minutes) reaches, UPS shut down



If the script run successfully, OS shut down immediately. If script fails, wait for the "Script execution time"(default 60s, if less than 60s also counts as 60s)

Scenario 2: Set the shutdown condition to “battery capacity is lower than 30%”, Set the shutdown action to “Shut down UPS is disabled” and “Shutdown script is disabled”

When the battery capacity is lower than 30% ->OS shutdown->UPS discharge until the battery is depleted

Scenario 3: Set the shutdown condition to "UPS is going shut down", Set the shutdown action to "Shutdown script is disabled"

When the UPS scheduled shutdown time reaches ->OS shutdown ->After the "Execution time" (default 2 minutes) reaches, UPS shut down



If the UPS is not set as a power source, the UPS shutdown will be executed according to UPS on/off schedule. Once the UPS is set as a local system power source, the "Execution time" will be added to UPS shutdown delay time

2.4.1.2 SPS shutdown

Prerequisite

- Check [SPS list](#) , add SPS server
- Check [Shutdown protection setting](#) , Select SPS host in "Server list", set power source and shutdown conditions

Shutdown action

- shutdown: SPS host will be shut down
- Hibernation: SPS host will be hibernated
- No Action: If script is enabled, only the script will be executed, OS won't take any action
- Save and Test: Click the button, verify whether the SPS host can be shut down or hibernated manually
- Shutdown script: Click "Go to SPS for configuration", it will jump to SPS website. The customer can configure script via SPS website
- Shutdown delay time: After receiving the shutdown notification from Winpower, SPS will wait for the timer to reach then execute shutdown or hibernation
- Shutdown time: The time required for SPS shutdown or hibernation



The shutdown action also can be set on the SPS website, and the shutdown configuration in Winpower side will be synchronized with SPS side in real-time



The maximum execution time of the shutdown script is automatically determined to be 2/3 of the "Shutdown time", ensuring that 1/3 of the remaining time is reserved for shutting down or hibernating the system

Shutdown protection setting

Save

Shutdown conditions

Shutdown action

Power source setting

Shutdown action

☒ shutdown
☐ Hibernation
☐ No Action

Save and Test

Shutdown script

[Go to SPS for configuration](#)

Shutdown delay time

60

s

Shutdown time

60

s

Shutdown protection scenario

Scenario 1: Set the shutdown condition to "battery capacity is lower than 30%"

When the battery capacity of power source is less than 30%, software will send a shutdown notification to SPS ->SPS start shutdown countdown (default 60s) ->When countdown is ended, SPS will execute script. If the script is successfully executed, OS shut down immediately. If the script fails, it will wait for the maximum execution time of the script (about 40s, $60 \times 2/3 = 40$) ->SPS host shut down



If the power is restored within the SPS shutdown countdown, the shutdown will be canceled

Scenario 2: Set the shutdown condition to "UPS is going shut down"

10 minutes before UPS scheduled shutdown time reaches, Software will send an alarm notification to SPS every 1 minute ->When the UPS scheduled shutdown time reaches, SPS start shutdown countdown (default 60s) ->when countdown is ended, SPS will execute the script ->SPS host shut down ->When the "Shutdown time" (default 60s) reaches, UPS shut down



If the UPS is not set as a power source, the UPS shutdown will be executed according to UPS on/off schedule. Once the UPS is set as a power source for SPS, the "Shutdown delay time" plus "Shutdown time" will be added to UPS shutdown delay time

2.4.1.3 IPMI shutdown

Prerequisite

- Check [IPMI list](#) , add IPMI server
- Check [Shutdown protection setting](#) , Select IPMI host in "Server list", set power source and shutdown conditions

Shutdown Action

- Shutdown: When the shutdown condition is met, software will call the Java API to shut down the remote IPMI server
- Test: Click the test button to shut down the remote IPMI server immediately

Shutdown protection scenario

Scenario 1: Set the shutdown condition to "battery capacity is lower than 30%"

When the battery capacity of the power source is less than 30%, Software will shut down the IPMI server

Scenario 2: Set the shutdown condition to "UPS is going shut down"

When the UPS scheduled shutdown time reaches ->Software will shut down the IPMI server->After 2 minutes, UPS will shut down



If the UPS is not set as a power source, UPS shutdown will be executed according to UPS on/off schedule. Once the UPS is set as a power source for IPMI server, 2 minutes will be added to UPS shutdown delay time

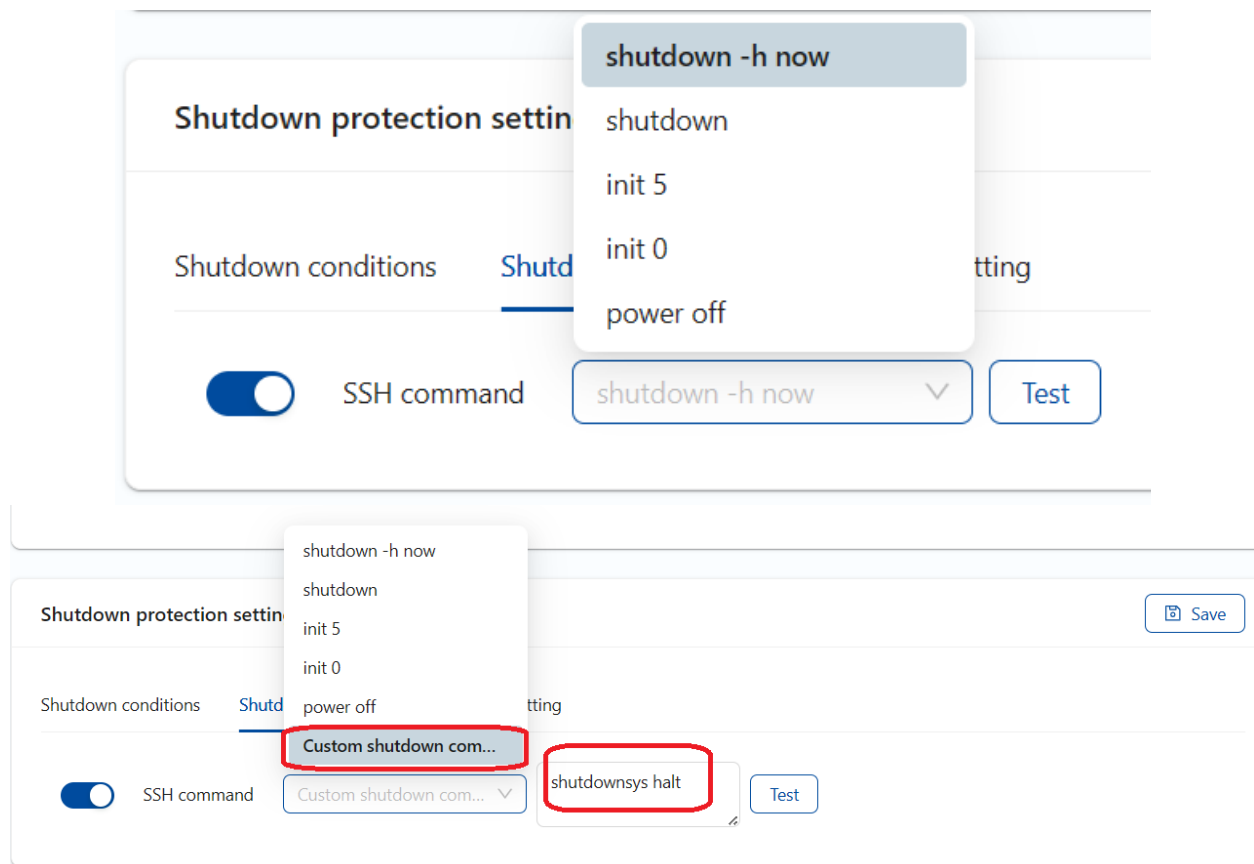
2.4.1.4 SSH shutdown

Prerequisite

- Check [SSH list](#) , add SSH server
- Check [Shutdown protection setting](#) , Select SSH server in "Server list", set power source and shutdown conditions

Shutdown Action

- SSH Command: Software logs in to SSH through Java API and sends a shutdown command to the remote SSH server
- Specified shutdown command: There are five kinds of specified shutdown commands are supported: "shutdown -h now", "shutdown", "init 5", "init 0", "power off"
- Custom shutdown command: Choose "Custom shutdown command", input any SSH shutdown command and save it
- Test: Click the test button, Software will send a shutdown command to the SSH server immediately



Shutdown protection scenario

Scenario 1: Set the shutdown condition to "battery capacity is lower than 30%"

When the battery capacity of the power source is less than 30%, Winpower will shut down the SSH server

Scenario 2: Set the shutdown condition to "UPS is going shut down"

When the UPS scheduled shutdown time reaches ->Winpower will shut down the SSH server->After 2 minutes, UPS will shut down



If the UPS is not set as a power source, the UPS shutdown will be executed according to UPS on/off schedule. Once the UPS is set as a power source for SSH server, 2 minutes will be added to UPS shutdown delay time

2.4.1.5 VMware ESXi Standalone shutdown

Prerequisite

- Check [VMware ESXi list](#) , add a standalone VMware ESXi host

- Check [Shutdown protection setting](#) , Choose the VMware ESXi host in “Virtual system list”, set power source and shutdown conditions
- knowledge [How to set auto stop/start on VMware ESXi](#)

Shutdown action

- Shutdown: Winpower will shut down the ESXi host through Java API



Virtual machine shutdown requires installing VMware tool, Winpower sends the shutdown command to the virtual machine firstly, once the virtual machine response that shutdown command is not supported, Winpower will change to send “power off” command

- Turn off all VMs before shutting down the host: If this function is selected, Winpower will shut down the virtual machines disorderly. If Winpower is installed on one of the virtual machines, it is automatically identified as the critical virtual machine, and the critical virtual machine will be shutdown at last



If the “auto start/stop” function is enabled on ESXi host, please unselect “Turn off all VMs before shutting down the host”. Because all virtual machines will automatically shut down before ESXi host shut down by itself.

- ESXi shutdown timeout: The maximum time value for waiting for all virtual machines to shut down (the status from on to off)



If the virtual machine has not been shut down when the “ESXi shutdown timeout” is met, software will send “power off” command to the virtual machine

- Test: Click “Test” button, ESXi host will shut down immediately

Shutdown protection setting

Save

Shutdown conditions

Shutdown action

Power source setting

Shutdown

☐ Turn off all VMS before shutting down the host

ESXi shutdown timeout

120

s

Test

Shutdown protection scenario

Scenario 1: Disable “auto start/stop” on ESXi, Set the shutdown condition to “battery capacity of less than 30%”, Shutdown action enable “Turn off all VMs before shutting down the host”

When the battery capacity of the power source is less than 30% -> Software will shut down the virtual machine firstly -> Wait for all virtual machines to be shut down -> host will shut down



if all the VMs have been shut down, host will shut down immediately, otherwise wait for the “ESXi shutdown timeout” reaches (default 120 seconds)

if Winpower is installed on one of the virtual machines, it is automatically identified as the critical virtual machine, and the critical virtual machine will be shutdown at last

Scenario 2: Enable “auto start/stop” on ESXi, Set the shutdown condition to “battery capacity of less than 30%”, Shutdown action disable “Turn off all VMs before shutting down the host”

When the battery capacity of the power source is less than 30% -> the host will immediately shut down, and the virtual machines will be shut down through “auto start/stop” function embedded on ESXi host

Scenario 3: Enable “auto start/stop” on ESXi, Set the shutdown condition to “UPS is going shut down”, Shutdown action disable “Turn off all VMs before shutting down the host”

When the UPS shutdown scheduled time is met -> host will immediately shut down, and the virtual machines will be shut down through “auto start/stop” function embedded on ESXi host -> The time for “ESXi shutdown timeout” (default 120s) has been reached, UPS shut down



If the UPS is set as power source for ESXi host, the UPS scheduled shutdown time will be added with “ESXi shutdown timeout” as the UPS shutdown delay time. If UPS is set as power source for multiply ESXi hosts, the shutdown delay time will be the maximum value of “ESXi shutdown timeout” in all hosts

2.4.1.6 VMware ESXi of vCenter shutdown

Prerequisite

- Check [VMware Center list](#), add VMware vCenter
- Check [Shutdown protection setting](#). Choose the VMware ESXi host in “Server list”, set power source and shutdown conditions
- Knowledge [How to set auto stop/start on VMware ESXi](#), knowledge DRS function

Shutdown Action - Set Shutdown Mode

- Shutdown Mode: ESXi host enter to shutdown mode, host will shut down
- Shutdown timeout: The maximum time value for waiting for all virtual machines to shut down (virtual machine status from on to off)

- **Shutdown all virtual machines:** If this function is selected, Software will shut down the virtual machines disorderly. The virtual machine installed with Winpower or vCenter will be identified as the critical VMs automatically, and the critical VMs will be shutdown at last



It is recommended to enable this function because virtual machines maybe migrate from one host to another, so “auto start/stop” is not very reliable on ESXi host with vCenter



Virtual machine shutdown requires VMware tool, Software will send shutdown command to virtual machine firstly, once the virtual machine response that shutdown command is not supported, software will change to send “power off” command

Test: Click “Test” button, ESXi host will shut down immediately

Shutdown Action - Set Maintenance Mode

- **Maintenance Mode:** When the ESXi host enters maintenance mode, virtual machines will automatically be migrated to other hosts depending on DRS function
- **Maintenance timeout:** The maximum time wait for the ESXi host to enter maintenance mode
- **Test:** Click “Test” button, ESXi host will enter to maintenance mode immediately



When software detects that the power source has been restored, it will send a command to exit maintenance mode

Shutdown Action - Set Shutdown Mode and Maintenance Mode simultaneously

The host enters maintenance mode firstly, all the virtual machines will be migrated to another host, and the host enters shutdown mode finally



If the host fails to enter maintenance mode, after waiting for “Maintenance timeout”, the software will forcibly shut down all VMs and host. The virtual machine with installed Winpower or vCenter will be automatically identified as critical VMs and will be shutdown at last, while other virtual machines will shut down disorderly

Shutdown protection scenario

Scenario 1: Set the shutdown condition to "battery capacity of less than 30%", Shutdown action enable "Shutdown Mode" and enable "Shutdown all virtual machines"

When the battery capacity of the power source is below 30% ->Software will shut down the virtual machines firstly->Wait for all virtual machines to be shut down->Host will shut down



if all the VMs have been shut down, host will shut down immediately, otherwise host will wait for the "Shutdown timeout" (default 120 seconds)

The virtual machine has been installed Winpower or vCenter will be automatically identified as critical VMs. Critical VMs will be shut down at last, while other virtual machines will shut down disorderly

Scenario 2: Set the shutdown condition to "battery capacity of less than 30%", Shutdown action enable "Maintenance Mode"

When the battery capacity of the power source is below 30% ->Host enter to maintenance mode, the virtual machines will be migrated to another host->Once mains power restores, the host will exit maintenance mode when Winpower service start



If entering maintenance mode fails, wait for the "Maintenance timeout" time (default 120 seconds) reaches, Software will forcibly shut down the virtual machines and host

Scenario 3: Set the shutdown condition to "battery capacity of less than 30%", Shutdown action enable "Maintenance Mode" and enable "Shutdown Mode"

When the battery capacity of the power source is below 30% ->Host enter to maintenance mode, the virtual machines will be migrated to another host->Host will shut down

Scenario 4: Set the shutdown condition to "UPS is going shut down", Shutdown action enable "Shutdown Mode" and enable "Shutdown all virtual machines"

When the UPS shutdown scheduled time is met->Software will shut down the virtual machines firstly->>Host will immediately shut down->The time for "Shutdown timeout" (default 120 seconds) has been reached, UPS shut down



If the UPS is set as power source for ESXi host and enable "Shutdown Mode", the UPS scheduled shutdown time will be added with "Shutdown timeout" as the UPS shutdown delay time

Scenario 5: Set the shutdown condition to "UPS is going shut down", Shutdown action enable "Shutdown Mode" and enable "Maintenance Mode"

When the UPS shutdown scheduled time is met->Host enter to maintenance mode, the virtual machines will be migrated to another host ->Host will shut down->When the "Shutdown timeout" (default 120s) plus "Maintenance timeout" (default 120s) has been reached, UPS shut down



If the UPS is set as power source for ESXi host and enable "Shutdown Mode" and "Maintenance Mode", the UPS scheduled shutdown time will be added with "Shutdown timeout" plus "Maintenance timeout" as the UPS shutdown delay time. If UPS is set as power source for multiply ESXi hosts, the shutdown delay time will be the maximum value of "Shutdown timeout" plus "Maintenance timeout" in all hosts

2.4.1.7 VMware Cluster shutdown

Prerequisite

- Check [VMware Center list](#) , add VMware vCenter
- Check [Shutdown protection setting](#) , Choose the VMware cluster in "Virtual system list", set power source and shutdown conditions
- All hosts in the same cluster are powered by the same power source
- Knowledge [How to set auto stop/start on VMware ESXi](#),knowledge DRS and HA function

Shutdown Action

- Shutdown cluster: All hosts and virtual machines in the same cluster are gracefully shut down in order to priority
- Virtual machine migration timeout: The maximum time value for waiting for all virtual machines to be migrated to another host
- Virtual machine shutdown timeout: The maximum time value for waiting for all virtual machines to be shut down



If the virtual machine migration or shutdown fails, the software will send the “power off” command

- View Settings: View and set the priority of virtual machines, you can set certain important virtual machines (such as domain name server) as the critical virtual machine manually



Virtual machines installed with Winpower or vCenter is automatically identified as the critical virtual machine



The host where the vCenter is located is automatically identified as a critical host, while other hosts are identified as non-critical hosts

- Automatically start non critical virtual machines: Enable this function, Winpower will set all virtual machines to the “auto start” list during shutdown process. When the host boots, all virtual machines will be turned on automatically

Shutdown protection setting

Save

Shutdown conditions

Shutdown action

Power source setting

Shutdown cluster

Virtual machine migration timeout 120 s

Virtual machine shutdown timeout 120 s

Automatically start non critical virtual machines

Test

View Settings

Screenshot (Ctrl-

Set critical VMs

- Virtual machines installed with Winpower or vCenter is automatically identified as the critical virtual machine, the priority of vCenter is “Infra (vCenter)”. Other virtual machines have two priority “Critical” or “Non-critical”
- Click “Set” button to set the virtual machine as critical manually. Click “Cancel” button to set the virtual machine as non-critical manually

Virtual machine importance level settings



Name	Communication status	Operate status	Host name	key	Protection priority	Operate
VMware vCenter Server8.0	connected	poweredOn	localhost	Virtual Machine	Infra(vCenter)	<button>Set</button>
ubuntu22-3	connected	poweredOn		Virtual Machine	Critical	<button>Cancel</button>
Ubuntu 22-1	connected	poweredOn	santak-ubuntu22	Virtual Machine	Critical	<button>Cancel</button>
win11	connected	poweredOn		Virtual Machine	Critical	<button>Cancel</button>
ubuntu22-sps-test	connected	poweredOn		Virtual Machine	Non-critical	<button>Set</button>
tina	connected	poweredOn	dhcp-10-130-212-228	Virtual Machine	Non-critical	<button>Set</button>
IPM2.4	connected	poweredOn	eaton-rc-000C29E0B92A	Virtual Machine	Non-critical	<button>Set</button>
win10	connected	poweredOn		Virtual Machine	Non-critical	<button>Set</button>
Win10-1	connected	poweredOn		Virtual Machine	Non-critical	<button>Set</button>
VCOM-6.9.0	connected	poweredOn	vcom.local	Virtual Machine	Non-critical	<button>Set</button>

< 1 2 3 4 >

Cancel

OK

Shutdown protection scenario

Scenario 1: Set the shutdown condition to "battery capacity of less than 30%", Shutdown action enable "Automatically start non critical virtual machines", HA is disabled

When the battery capacity of the power source is below 30% ->Set DRS to manual mode (if it is already in manual mode, there will be no action) ->Enable "auto start" for all non-critical hosts, and set all virtual machines to "auto start" list on every non-critical host->Migrate the critical virtual machines to critical host(host with vCenter installed is considered as the critical host) ->Shut down all non-critical virtual machines ->Shut down non-critical hosts ->Enable "auto start" for the critical host, and set all virtual machines to "auto start" list on critical host->shut down critical host ->Once mains power restore, all virtual machines will automatically turn on, and VMware's configuration will be restored as before shutdown

Scenario 2: Set the shutdown condition to battery capacity of less than 30%, Shutdown action disable "Automatically start non critical virtual machines", HA is disabled

When the battery capacity of the power source is below 30% ->Set DRS to manual mode (if it is already in manual mode, there will be no action) ->Migrate the critical virtual machines to critical host(host with vCenter installed is considered as the critical host)->Shut down all non-critical virtual machines->Shut down non-critical hosts ->Enable "auto start" for the critical host, and set all critical virtual machines to "auto start" list on critical host->shut down critical host ->Once mains power restore, only critical virtual machines will automatically turn on, and VMware's configuration will be restored as before shutdown

Scenario 3: Set the shutdown condition to battery capacity of less than 30%, Shutdown action disable "Automatically start non critical virtual machines", HA is enabled

When the battery capacity of the power source is below 30% ->Disable HA ->Set DRS to manual mode (if it is already in manual mode, there will be no action) ->Migrate the critical virtual machines to critical host(host

with vCenter installed is considered as the critical host)->Shut down all non-critical virtual machines->Shut down non-critical hosts ->Enable "auto start" for the critical host, and set all critical virtual machines to "auto start" list on critical host->shut down critical host ->Once mains power restore, only critical virtual machines will automatically turn on, and VMware's configuration will be restored as before shutdown

2.4.1.8 NetApp shutdown

Prerequisite

- Check [NetApp Cluster list](#) , add NetApp server
- Check [Shutdown protection setting](#) , Understand the shutdown conditions

Set power source

Set the power source through the Netapp Cluster node. One power source simultaneously supply power to all storage Netapp nodes

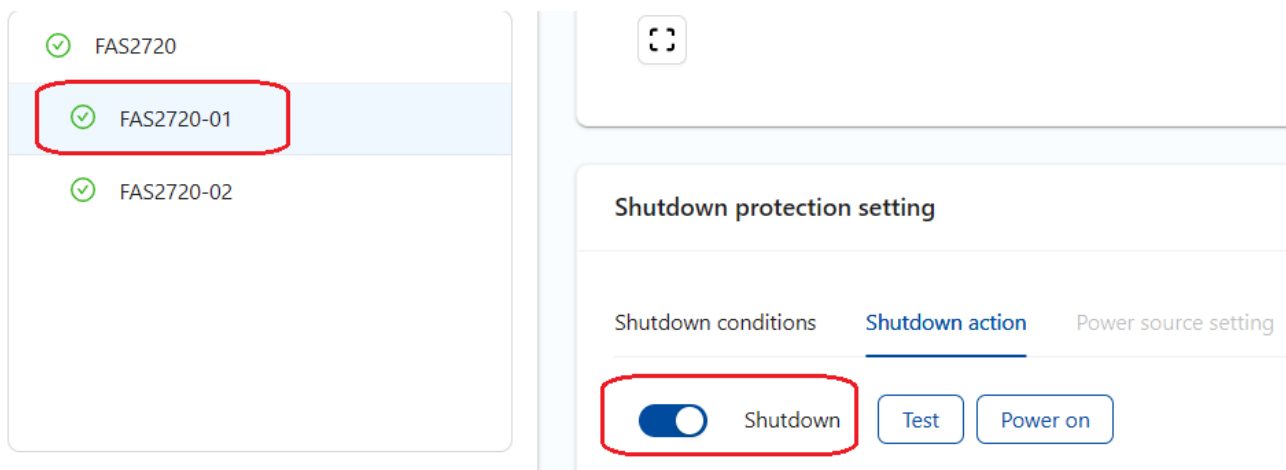
The screenshot displays the NetApp management interface. On the left, a sidebar shows a navigation menu with 'Storage node list' selected. Below it, a list of storage nodes is shown: 'FAS2720' (highlighted with a red box), 'FAS2720-01', and 'FAS2720-02'. All nodes are marked as 'Connected' and 'Unprotected'. On the right, a diagram shows a 'UPS' icon connected to a 'M' (Master) node, which is then connected to two storage nodes, 'FAS2720-02' and 'FAS2720-01'. Below the diagram, the 'Shutdown protection setting' section is visible, with tabs for 'Shutdown conditions', 'Shutdown action', and 'Power source setting'. The 'Power source setting' tab is active, showing 'Type: Single UPS' and 'UPS: SNMP-10.130.212.245 /...'. A red asterisk indicates a required field.

Shutdown Action

- Shutdown: When the shutdown condition is met, the storage node will be shutdown
- Power On: Power on selected storage node immediately
- Test: Shut down selected storage node immediately



Different storage nodes can be set different shutdown condition and action



Shutdown protection scenario

Scenario 1: Set the shutdown condition to “battery capacity is lower than 30%” for node1, Set the shutdown condition to “battery capacity is lower than 20%” for node2

When the battery capacity of the power source is less than 30%, node1 shut down, and the data on node1 is automatically migrated to node2. When the battery capacity of the power source is less than 20%, node2 shut down

Scenario 2: Set the shutdown condition to “battery capacity is lower than 30%” for node1, Disable shutdown function for node2

When the battery capacity of the power source is less than 30%, node1 shut down, and the data on node1 is automatically migrated to node2. node2 won't shut down-----This method is not recommended

Scenario 3: Set the shutdown condition to “UPS is going shutdown” for both node1 and node2

When the UPS scheduled shutdown time reaches ->Software will shut down both node1 and node2->After 2 minutes, UPS shut down



If the UPS is not set as a power source, the UPS shutdown will be executed according to UPS on/off schedule. Once the UPS is set as a power source for NetApp cluster, 2 minutes will be added to UPS shutdown delay time

2.4.1.9 Redundant shutdown

Set redundant group as power source

1. Create redundant group according to [Redundant UPS](#)
2. Select the redundant group from the drop-down list as the power source

Shutdown protection setting

Shutdown conditions

Shutdown action

Power source setting

Type: ☐ Single UPS ☒ Redundant UPS

* Redundant UPS:

PSGroup

Shutdown protection scenario

Scenario 1: Set the shutdown condition to "battery capacity is lower than 30%", Set power source to Redundant group that including UPS1 and UPS2, Mains power for both UPS1 and UPS2 cut off

When the battery capacity of both UPS1 and UPS2 are below 30%, local or remote shutdown action will be triggered

Scenario 2: Set the shutdown condition to "battery capacity is lower than 30%", Set power source to Redundant group that including UPS1 and LS for UPS2, Mains power for both UPS1 and UPS2 cut off

When the battery capacity of both UPS1 and UPS2 are below 30%, local or remote shutdown action will be triggered



Software will ignore the LS shutdown condition within the redundant group

Scenario 3: Set the shutdown condition to "battery capacity is lower than 30%", Set power source to Redundant group that including UPS1 and LS for UPS2, Mains power for UPS1 cut off, the main power for UPS2 is normal

As long as one UPS mains power is normal in the group, local or remote shutdown action won't be triggered

Scenario 4: Set the shutdown condition to "battery capacity is lower than 30%", Set power source to Redundant group that including UPS1 and UPS2, Mains power for UPS1 cut off and UPS2 output is off

When the battery capacity of UPS1 is below 30%, local or remote shutdown action will be triggered



If UPS output is off, or UPS is communication lost, or UPS is in bypass mode, the UPS will be excluded from redundant group

2.4.2 On/Off schedule

This page allows you to add, edit and delete UPS power on and off schedule tasks.



Only UPS with local communication (serial port/USB) and Modbus TCP communication support power-on/off schedule.

Shutdown protection setting

On/Off schedule

Battery test schedule

Please filter devices

+ Add

Period	Start time	Action	UPS	Execution logs	Operate
Every 3 months	1th 09:00:00	Test until battery low	Modbus-10.130.212.219	View	✎ ✖
Once	2024/11/21 10:47:00	Quick test	COM8-UPS	View	✎ ✖

<

1

>

The list displays all the power on and off scheduled tasks. If you select a device through the drop-down box in the upper left corner, the task list will only display the power on and off scheduled tasks of the selected device.

Click the edit icon in the "Operate" column to modify the scheduled task, and click the delete icon to delete the scheduled task.

Click the "Add" button in the upper right corner to add a on/off schedule task. Filter UPS devices by site, select the UPS that needs to be scheduled for power on and off, and then select the period (once, daily, weekly), shutdown time, and restart time. When the period is daily, you can choose to exclude weekends. After setting, click the "Add" button to save.

On/Off schedule

* Site: root

* UPS:
☐ COM8-UPS
☐ Modbus-10.130.212.221
☐ Modbus-10.130.212.217
☐ Modbus-10.130.212.219
☐ Modbus-10.130.212.230
☐ Modbus-10.130.212.218
☐ Modbus-10.130.212.220
☐ Modbus-10.130.212.247

* Period: Daily

☐ Exclude weekends

* Shutdown time: Select time

* Restart time: Select time

Add



The shutdown time in the settings refers to the time when the shutdown sequence starts, not the time when the UPS is shut down. There will be a delay in the actual UPS shutdown, and the delay time is the maximum value of the maximum time required to shut down the protected servers and the minimum shutdown delay time of the UPS (12s or 1min depends on UPS protocol).



Application scenario 1: The schedule is set to shut down at 19:00 on Friday afternoon and turn on at 8:00 on Monday morning. Automatically shut down unused servers and power supplies on weekends to save power. **Note: The shutdown condition of the server must choose UPS shutdown in order to shut down the server safely before the UPS shuts down.** After the UPS restarts, the server automatically starts by enabling the BIOS automatic restart function after power recovery.

Application scenario 2: The schedule setting period is daily, choose to exclude weekends, the shutdown time is 19:00 pm, and the startup time is 8:00 am. In this way, it can automatically shut down after get off work on weekdays, automatically turn on in the morning before going to work, shut down on Friday afternoon, and turn on on Monday morning.

Click the "View" link in the "Execution logs" column to view the on/off schedule task execution log.

Shutdown schedule execution logs				
	Result	Execution time		
—	Success	20/11/2024 17:56:00		
Result	Device alias	Type		
OK	COM8-UPS	Scheduled shutdown		
⊖	Fail	20/11/2024 17:37:00		
Result	Device alias	Type		
Device is abnormal, cannot carry out shutdown now	COM8-UPS	Scheduled shutdown		
			Cancel	OK

2.4.3 Battery test schedule

This page allows you to add, edit and delete UPS battery test schedule tasks.



Only UPS with local communication (serial port/USB) and Modbus TCP communication support battery test schedule.

The battery test schedule of lithium battery UPS is not supported. The lithium battery UPS itself has a battery management system, and there is no need to perform battery test from the software.

Shutdown protection setting		On/Off schedule		Battery test schedule		
Please filter devices ▾				+ Add		
Period	Start time	Action	UPS	Execution logs	Operate	
Every 3 months	1th 09:00:00	Test until battery low	Modbus-10.130.212.219	View	✎	🗑
Once	2024/11/21 10:47:00	Quick test	COM8-UPS	View	✎	🗑
						< 1 >

The list displays all the battery test scheduled tasks. If you select a device through the drop-down box in the upper left corner, the task list will only display the battery test scheduled tasks of the selected device.

Click the edit icon in the "Operate" column to modify the scheduled task, and click the delete icon to delete the scheduled task.

Click the "Add" button in the upper right corner to add a battery test schedule task. Filter UPS devices by site, select the UPS that needs to be scheduled for battery test, and then select the test type (some UPS does not

support testing at a specific time and testing to low battery level), period(once, monthly, every 3 months, every 6 months), and test start time. After setting, click the "Add" button to save.



The period selection of "Every 3 Months" will be executed in January, April, July and October, and the selection of "Every 6 Months" will be executed in January and July.

If "During the test cycle, if the UPS has discharged, skip the test" is selected, it means that if a battery discharge event has occurred due to abnormal mains power during this test cycle, this test schedule task will no longer be executed.

Click the "View" link in the "Execution logs" column to view the battery test schedule task execution log.



The results only indicate whether the test task was successfully sent to UPS. The battery test results can be viewed from UPS details >>Data statistics

Battery test schedule execution logs

Cancel

OK



2.5 Events/Logs

2.5.1 Event log

This page displays the event logs of all devices, including: event status (active alarm, historical event), level (information, general alarm, critical alarm, fault), description, device name, start time, and end time. Events can be filtered by different combinations of conditions.

Overview	Event	Time: Start date → End date	Event status: Active alarm	Device name: Please enter device name	More filters	Export to excel
Asset	Data log	Event level: Event level	Event description: Please enter event description			
Protection						
Events/Logs						
System settings						

Event status	Event level	Event description	Device name	Start time	End time
Active alarm	⚠	On bypass mode	COM8-UPS	2024/11/06 17:13:53	-
Active alarm	⚠	UPS temperature exceeds the set value of the card	SNMP-10.130.212.131	2024/11/06 17:12:57	-
Active alarm	⚠	Output off	SNMP-10.130.212.245	2024/11/06 17:12:55	-
Active alarm	ℹ	Automatically set local IP as Trap receiving address successfully.	PDU-10.130.212.61	2024/11/06 15:54:17	-
Active alarm	⚠	Input Voltage (A) exceeds limit(Value:227, lower limit:190, upper limit:220)	PDU-10.130.212.61	2024/11/06 15:54:17	-

Event Level	Icon
Fault	
Critical alarm	

Event Level	Icon
General alarm	
Information	

Click the export button to export event logs to an excel file as follows:

Device name	Description	Level	Status	Start time	End time
SNMP-10.235.226.102	Communication lost	General Alarm	Active	2024/11/07 13:51:23	
SNMP-10.130.212.101	Communication lost	General Alarm	Active	2024/11/07 13:51:08	
SNMP-10.130.212.245	Output off	General Alarm	Active	2024/11/07 13:48:45	
SNMP-10.130.212.131	UPS temperature exceeds the set value of the card	General Alarm	Active	2024/11/07 13:48:13	
PDU-10.130.212.61	Input Voltage (A) exceeds limit(Value:229, lower limit:190, upper limit:220)	General Alarm	Active	2024/11/07 13:48:07	
COM8-UPS	On bypass mode	General Alarm	Active	2024/11/07 13:47:57	
SNMP-10.130.212.245	Output off	General Alarm	Inactive	2024/11/06 18:00:09	
SNMP-10.130.212.131	UPS temperature exceeds the set value of the card	General Alarm	Inactive	2024/11/06 18:00:07	
PDU-10.130.212.61	Input Voltage (A) exceeds limit(Value:229, lower limit:190, upper limit:220)	General Alarm	Inactive	2024/11/06 17:59:51	
COM8-UPS	On bypass mode	General Alarm	Inactive	2024/11/06 17:59:50	
COM8-UPS	On bypass mode	General Alarm	Inactive	2024/11/06 17:13:53	
SNMP-10.130.212.131	UPS temperature exceeds the set value of the card	General Alarm	Inactive	2024/11/06 17:12:57	
SNMP-10.130.212.245	Output off	General Alarm	Inactive	2024/11/06 17:12:55	
SNMP-10.130.212.101	On battery mode	General Alarm	Released	2024/11/06 17:12:54	2024/11/06 17:13:02
SNMP-10.130.212.101	Bypass input abnormal	General Alarm	Released	2024/11/06 17:12:54	2024/11/06 17:13:02
SNMP-10.130.212.101	Main AC is not OK	General Alarm	Released	2024/11/06 17:12:54	2024/11/06 17:13:02
PDU-10.130.212.61	Automatically set local IP as Trap receiving address successfully.	Information	Inactive	2024/11/06 15:54:17	
PDU-10.130.212.61	Input Voltage (A) exceeds limit(Value:227, lower limit:190, upper limit:220)	General Alarm	Inactive	2024/11/06 15:54:17	

The corresponding relationship between the event status displayed on the web page and the status in the exported file is as follows:

Event status on web	Status on exported file	Description
Active alarm	Active	The event is in active
Historical event	Released	The event has been released and has an end time
	Inactive	<p>Events are usually set to inactive status in two situations:</p> <ul style="list-style-type: none"> When device communication is lost, all active events will be set to inactive, and the end time will be set to the time when the communication loss occurred. When the software terminates due to system shutdown, the currently active events are still active in the database. When the software is started next time, the status of these events will be set to inactive without an end time.

All device events and their levels can be viewed on the [event subscription setting](#) page.

The default keep time of event logs is 90 days. You can change the log settings on the [device data collection settings](#) page.

2.5.2 Data log

This page displays the historical data logs of all UPS devices, and the data can be filtered according to different combinations of conditions.

Collection time	Device name	Input voltage (V)	Input frequency(Hz)	Output voltage (V)	Output frequency (Hz)	Battery voltage(V)	Load percentage(%)	Mode
2024/11/13 16:00:00	SNMP-10.130.212.243	227.9	-	226.6	49.9	81.6	0	Line mode
2024/11/13 16:00:00	SNMP-10.235.226.93	230 229 228	50	220 220 220	50	-	4	Line mode
2024/11/13 16:00:00	SNMP-10.130.212.245	226	50	0	0	82.5	0	Standby
2024/11/13 16:00:00	NMC-62-10.130.212.244	230.2	50	219.8	50	41.3	0	Line mode
2024/11/13 16:00:00	SNMP-10.130.212.171	228	49.9	227	49.9	12.8	0	Line mode
2024/11/13 16:00:00	HID-UPS-715318400017	228	49.9	0	0	41	0	Standby
2024/11/13 16:00:00	SNMP-10.130.212.131	225.9	49.9	230	50	50.6	0	Line mode
2024/11/13 16:00:00	SNMP-10.130.212.246	228.7	-	0	0	41	0	Shutdown Mode
2024/11/13 15:00:00	SNMP-10.130.212.243	227.4	-	227	49.9	81.6	0	Line mode
2024/11/13 15:00:00	SNMP-10.235.226.93	230 230 228	50	220 220 220	50	-	4	Line mode

Click the settings icon in the upper right corner to pop up the column settings window. You can click the checkbox to select the column content to be displayed, and click the reset button to restore the default display content.

Export to excel

Column Display Reset

- ☒ Collection ...
- ☒ Device name
- ☒ Input volta...
- ☒ Input frequ...
- ☒ Output vol...
- ☒ Output fre...
- ☒ Battery vol...
- ☒ Load perce...
- ☐ State
- ☒ Mode
- ☐ Active pow...
- ☐ Apparent p...
- ☐ UPS tempe...
- ☐ Battery te...
- ☐ Battery cap...
- ☐ Battery run...

Click the export button to export data logs to an excel file.

The default data keep time is 90 days, and the default recording interval is 1 hour. The settings can be changed on the [device data collection setting](#) page.

2.5.3 Shutdown log

Prerequisite

"Shutdown log" doesn't been enabled as default, you need to choose "Shutdown log" checkbox in the [System preferences](#)

Log setting

Enable/disable logging

☒ Event logs
 ☒ Data log
 ☐ User log
 ☐ Notification log
 ☐ Shutdown log
 ☐ WOL log

[Save](#)

Shutdown log

The shutdown log records the shutdown tasks and results of local and remote servers, mainly including the following content:

- Device Type: Local, SPS, IPMI, Virtual Machine, VMware ESXi, Hypervisor, SSH, NetApp as so on
- Shutdown State: Shutdown, Power off, Hibernate, Migrate as so on
- Shutdown Type: 1. Event (Shutdown is caused by events) 2. Control (Shutdown is caused by UPS on/off schedule) 3. Test (Shutdown is caused by test)
- Result: Success or Failure
- Reason: Reasons for triggering shutdown, such as battery discharge time is met
- Remark: Reasons for task execution failure

Click “Export to excel” button and all shutdown logs will be exported and saved in Excel format

Winpower G2 2024/12/06 10:35:10 root

Overview

Asset management

Shutdown protection

Events/Logs

System settings

Event

Data log

Shutdown log

User log

Time: Start date → End date

Device type: Please select a device type

Device name: Please enter device name

IP: Please enter IP

[Export to excel](#) [Log setting](#)

Time	Device name	IP	Device type	Power source	Shutdown State	Shutdown Type	Reason	Result	Remark
2024/09/14 16:21:38	DPQRD		Cluster	SNMP-10.130.212.235	Recover vSphere DRS configuration	Event	AC restore	Success	
2024/09/14 15:57:52	Esxi23.SSG5-Serial	10.130.212.23	Hypervisor		Set vm auto start/stop	Event	UPS battery discharging time is greater than or equal to the set time	Success	Cluster shutdown:Set critical virtual n start/stop with the host
2024/09/14 15:57:47	Esxi21.SSG5-Serial	10.130.212.21	Hypervisor		Shutdown	Event	UPS battery discharging time is greater than or equal to the set time	Success	Cluster shutdown

Shutdown log filter

You can filter the shutdown logs via various filters. If you choose “Virtual Machine”, only shutdown logs of the virtual machines can be seen as shown in the figure below

Winpower G2 2024/12/06 10:48:36 root

Time: Start date → End date Device type: Virtual Machine Device name: Please enter device name IP: Please enter IP Export to excel Log setting

Time	Device name	IP	Device type	Power source	Shutdown State	Shutdown Type	Reason	Result	Remark
2024/09/14 13:15:59	vCLS-09e0d9a6-69d4-4abd-ac33-94d97da49dc2		Virtual Machine		Shutdown	Event	UPS battery discharging time is greater than or equal to the set time	Success	Cluster shutdown
2024/09/14 13:15:59	Win10-1	10.130.212.136	Virtual Machine		Shutdown	Event	UPS battery discharging time is greater than or equal to the set time	Success	Cluster shutdown

2.5.4 User log

Prerequisite

"User log" doesn't been enabled as default, and you need to choose "User log" checkbox in the [System preferences](#)

Log setting

Enable/disable logging

☒ Event logs ☒ Data log ☐ User log ☐ Notification log ☐ Shutdown log ☐ WOL log

Save

User log

User logs record the user actions including "Login", "Log out", "Edit user", "Change password" and "Reset password"

Winpower G2 2024/12/06 00:22:52 Plant

Time: Start ... → End d... Type: Type Account name: Please enter acc... IP address: Please enter IP Export to excel Log setting

Account	Operate results	Type	IP	Operate time	Remark
admin	success	Login	127.0.0.1	2024/12/06 00:22:28	Login success
admin	fail	Login	127.0.0.1	2024/12/06 00:22:25	User does not exist or password is wrong
jinhua	success	Log out	127.0.0.1	2024/12/06 00:22:17	Logout success
jinhua	success	Change password	127.0.0.1	2024/12/06 00:22:17	Change password success
admin	success	Login	127.0.0.1	2024/12/06 00:21:38	Login success

User log filter

You can filter the user log via various filters. If choose "Change password" in the Type list, only "Change password" logs can be seen as below image

The screenshot shows the Winpower G2 interface with the 'User log' selected in the left sidebar. The 'Type' filter is set to 'Change password'. The table below shows the resulting logs:

Account	Operate result	IP	Operate time	Remark
jinhua	success	127.0.0.1	2024/12/06 00:29:36	Change password success
admin	success	127.0.0.1	2024/12/06 00:25:47	Change password success
jinhua	success	127.0.0.1	2024/12/06 00:22:17	Change password success

2.5.5 Notification log

Prerequisite

"Notification log" doesn't been enabled as default, you need to choose "Notification log" checkbox in the [System preferences](#)

The 'Log setting' page shows the following configuration:

- Enable/disable logging:
 - ☒ Event logs
 - ☒ Data log
 - ☐ User log
 - ☐ Notification log
 - ☐ Shutdown log
 - ☐ WOL log

A 'Save' button is located at the bottom right.

Notification log

The Notification log record the emails or SMS. for example, the custom notification sent by emails or SMS, and events sent by emails or SMS

The screenshot shows the Winpower G2 interface with the 'Notification log' selected in the left sidebar. The table below displays the notification logs:

Receiver	Notification status	Notification type	Notification content	Remark	Time
[REDACTED]	Success	Email	Check battery status via battery self test		2024/12/06 00:50:03
[REDACTED]	Success	Email	Check battery status via battery self test		2024/12/06 00:40:04

2.5.6 WOL log

The wake-on-LAN log is not enabled by default. You can enable it in [System Preferences>>Log Setting](#).

The log record content is as follows:

Time: Wake-on-LAN occurrence time

MAC address: MAC address of the server being woken up

Description: The description information entered during setting, if it is a wake-up test, the description is "Test"

Result: Displays "Sent successfully" or "Sent failed". Successful sending does not mean successful wake-up. Please refer to [troubleshooting the cause of network wake-up failure](#).

Failure Information: If sending wake-up fails, record the specific failure information, otherwise it is empty.

Time:		Result:	MAC:	Description	
Start date	→ End date	Send results	Please enter MAC address	Please enter description	Export to excel Log setting
Wake up time	MAC address	Description	Result	Failure Information	
2024/11/15 11:41:51	40-1C-83-65-17-64	Test	Sent successfully		
2024/11/15 11:27:21	40-1C-83-65-17-64	Test	Sent successfully		
2024/11/15 09:38:46	40-1C-83-65-17-64	Server-19	Sent successfully		

Records can be filtered by different combinations of conditions. Click the export button to export the records as an excel document. Click the "Log setting" link in the upper right corner to enter [System Preferences >> Log Settings](#) to turn off LAN wake-up logging.

2.6 System settings

2.6.1 System preferences

Account settings

Number of simultaneous logins: The number of simultaneous logins supported by the same account. If it exceeds the number, the oldest connection token will automatically expire. The default number is 1.

Session timeout: The validity period of the user's login. After this period, the user will be logged out automatically. The default is 60 minutes and enabled, and can be disabled.

Password expiration time: The default is 365 days and enabled, can be disabled.

Lock account when failed logins exceed: If fail to log in using an incorrect password for more than this limit, the account will be locked for a period of time. Default is 5 times.

Lock time: The time the account is locked after consecutive failed logins. Default is 10 minutes.

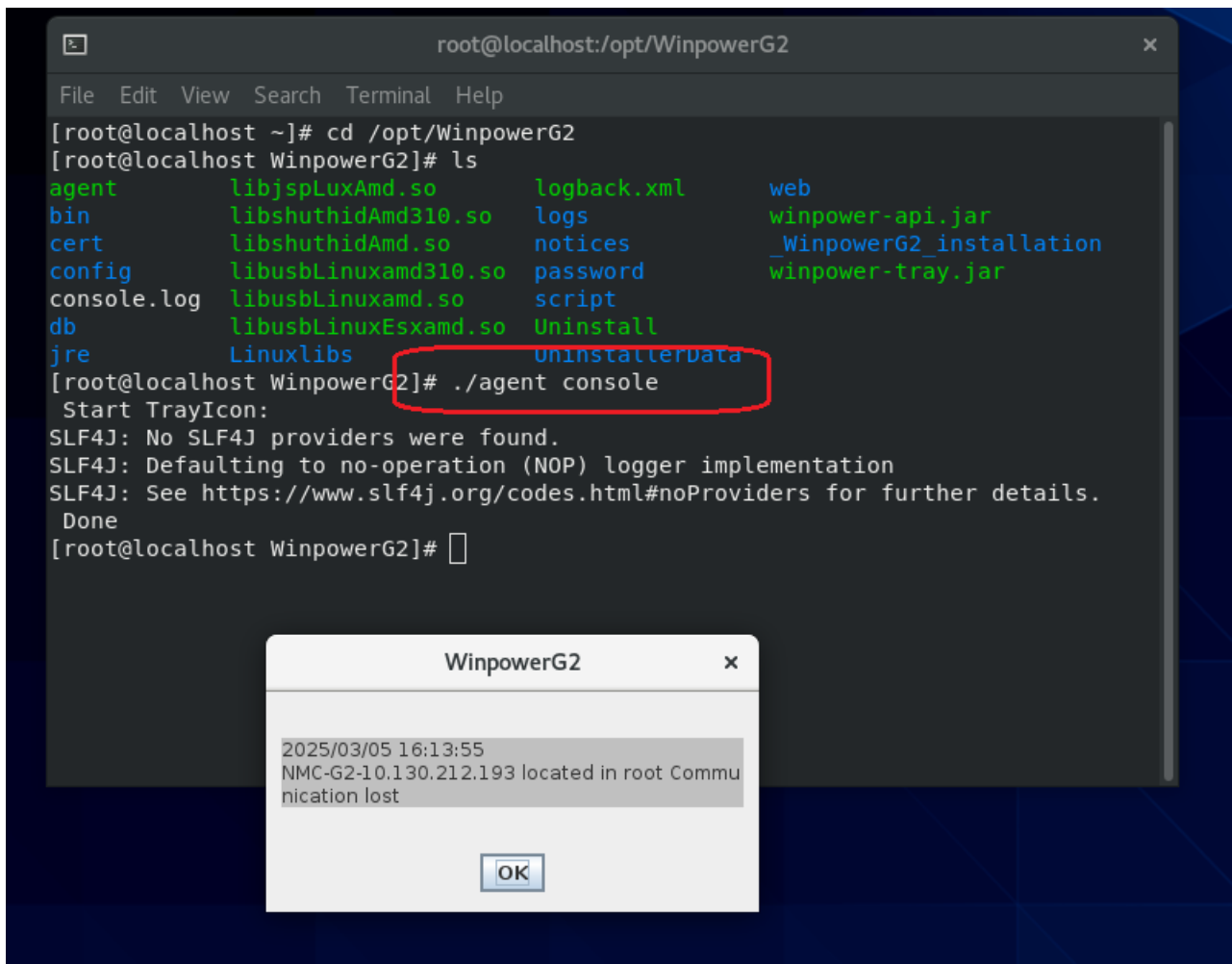
Account settings

* Number of simultaneous logins: 1	* Lock account when failed logins exceed: 5
* Session timeout: 60 mins Enable <input checked="" type="checkbox"/>	* Lock time: 10 mins
* Password expiration time: 365 days Enable <input checked="" type="checkbox"/>	

Save

2.6.1.1 Alarm setting

Whether to display alert pop-up box on tray icon: Enabled by default. If enabled this item, when an alarm occurs, it will pop up alarm dialog via software tray icon on Windows and Mac OSX. For the Linux system, enter command “./agent console” firstly to enable alarm pop-up dialog.



2.6.1.2 Data format settings

Date format: Select the date display format. There are 3 formats available: yyyy/mm/dd, dd/mm/yyyy and mm/dd/yyyy. Among them, yyyy is the year, mm is the month, and dd is the day.

Temperature unit: The UPS and its ambient temperature display units are optional in degrees Celsius or Fahrenheit. The sensor temperature unit of the PDU follows the setting on the PDU Web and will not be affected by this setting.

2.6.1.3 Maintenance period setting

Automatically set maintenance start time: Disabled by default. If it is enabled, when a new device is discovered, the current time will be automatically set to the maintenance start time.

Maintenance period: The default is 3 years, and the range can be set from 1 to 5 years.

Reminder start time: When the remaining maintenance time is less than this set value, a reminder that the device maintenance is about to expire will be displayed in the [Overview>>Device Maintenance Reminder](#) window. The default reminder start time is 30 days, and the range can be set from 7 to 90 days.



The maintenance start time of the device can be set by selecting the devices in [UPS list](#) or [PDU list](#), and then then clicking "Set Maintenance Start Time" button.

Maintenance period setting

* Maintenance period:

3

years

* Reminder start time ⓘ:

30

days

* Automatically set maintenance start time ⓘ:

☐

Save

2.6.1.4 Log setting

Set whether to record logs. Device events and data logs are recorded by default and cannot be canceled. User logs, notification logs, shutdown logs, and LAN wake-up logs are not recorded by default. You can turn on logging here.

Log setting

Enable/disable logging

☒ Event logs

☒ Data log

☐ User log

☐ Notification log

☐ Shutdown log

☐ WOL log

Save

2.6.2 Device data collection setting

2.6.2.1 Polling Settings

SNMP polling interval: The default is 15 seconds, and the range can be set from 3 to 3600 seconds.

SNMP trap port: SNMP trap receiving port, the default is 162. It needs to be consistent with the trap port setting on the SNMP device to receive trap information. If it is prompted that the port is occupied, refer to [how to resolve port conflicts](#).

Modbus polling interval: The default is 15 seconds, and the range can be set from 3 to 3600 seconds.

Polling Settings

* SNMP polling interval: s

* Modbus polling interval: s

* SNMP trap port:

[Save](#)

2.6.2.2 Log setting

Set the interval and duration for saving device data/event logs.

Data logging interval: The range can be set from 1 minute to 1 day, and the default is 1 hour. The unit can be selected through the unit drop-down box. There are 3 options: minutes/hours/days.

Data storage duration: The settable range is 7-365 days, and the default is 90 days.



When the data storage duration is met, software will delete “data log” that exceed the storage duration

Event storage duration: The range can be set from 7 days to 3 years, and the default is 90 days. The unit can be selected through the unit drop-down box. There are 2 options: days/years.



When the event storage duration is met, software will delete “event log”, “user log”, “notification log”, “shutdown log”, and “WOL log” that exceed the storage duration

Log setting

* Data logging interval: hours

* Data storage duration: days

* Event storage duration: days

[Save](#)

2.6.3 User management

Reflection of User, User group, Site, and Device

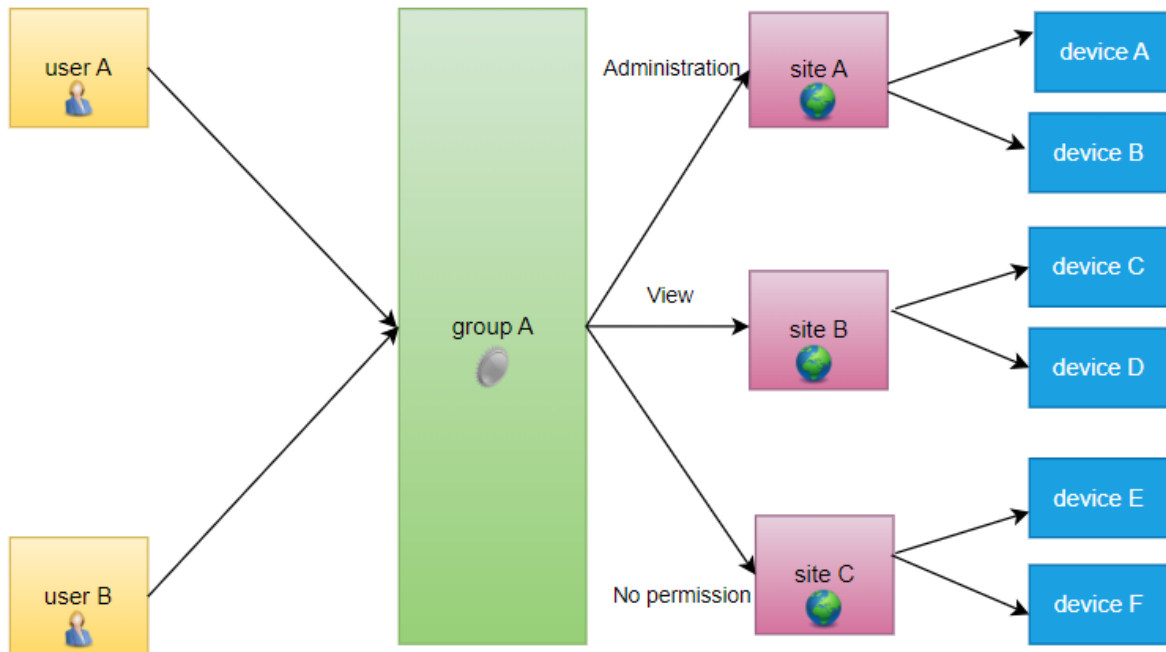
For example, user A and user B are in group A, and group A has management permission for site A and has view permission for site B, but no permission for site C



The device can be a UPS, PDU or remote server

- Administrator can manage all sites and devices

- Login with user A or user B, the user can view the parameters and alarms of devices A and B under site A, also can manage device A and device B—For example, setting UPS parameters, executing UPS on/off schedule, and battery self-test, such as on
- Login with user A or user B, the user can view the parameters and alarms of device C and device D under site B, but can't manage the device C and device D
- Login with user A or user B, user can't view device E and device F under site C



2.6.3.1 Account

Account name regular

Allow 4-128 bytes, allow alphanumeric, underscore, -, @, dot


Create administrator account

To create an administrator account, just move the account to the user group "System administrator group".



Administrators have the highest level of management privileges for all sites and devices


New users



* Account :

Nick name:

* Password : 

* User group: System administrator group 

Phone:

Email:

LDAP login: ☐ Enable

Create group account

Before creating an account for group, Please view [User group](#) and [Site management](#) to learn more information about group and site.

For example, create three accounts for three groups: "Layer4-group", "RDLab-group", "PVLab-group"



The new user login for the first time, software will reset a password compulsively. When creating account, try to fill in your email and phone number as much as possible. Email or phone number is needed for both event subscription and password retrieving

- Create "jones" user in "Layer4-group" group

Edit user

* Account ?

jones

Nick name:

1-128

Password ?

.....

* User group:

Layer4-group

Phone:

Email:

LDAP login:

☐ Enable

Save

- Create "jerry" account in "RDLab-group" group

Edit user



* Account ? :

Nick name :

Password ? :

* User group :

Phone :

Email :

LDAP login : ☐ Enable

Save

- Create "Sophie" account in "PVLab-group" group

Edit user



* Account ? :

Nick name:

Password ? :

* User group: PVLab-group

Phone:

Email:

LDAP login: ☐ Enable

Save

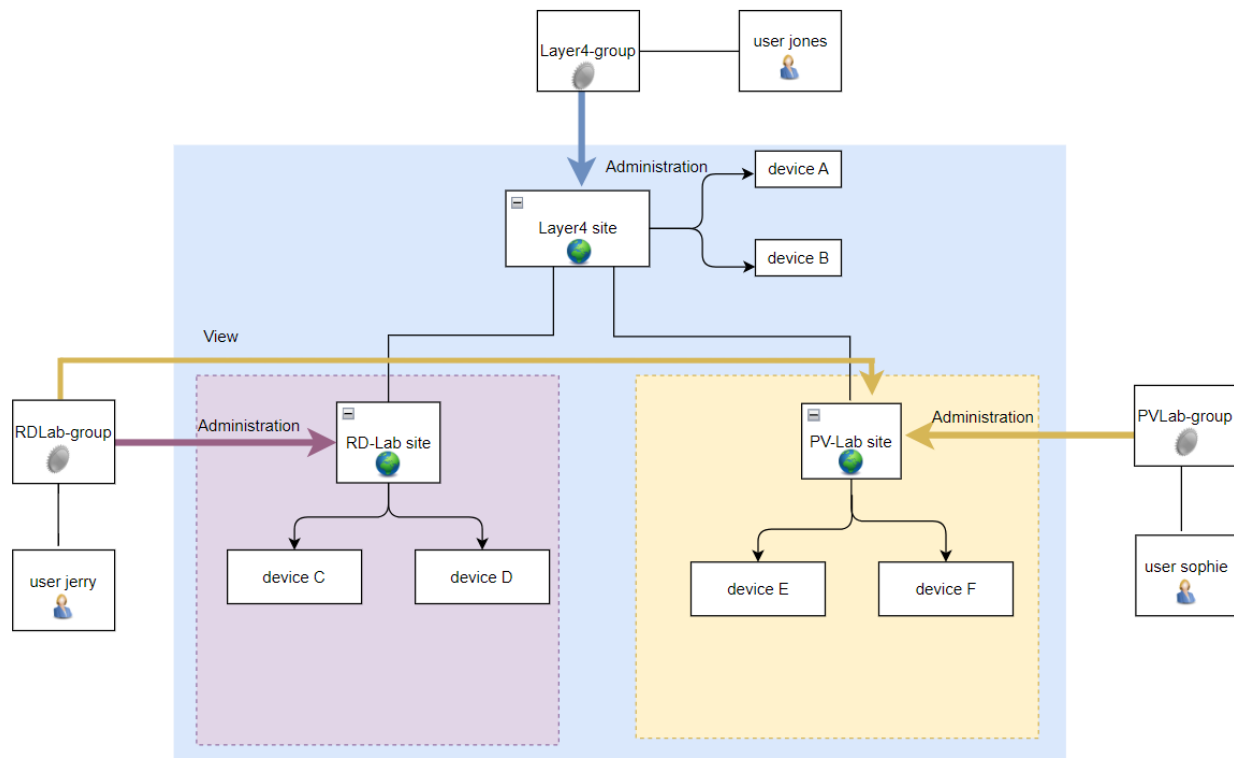
Account and User group relationship

After creating the accounts, you can see the relationship between account and user group as following

Account				
Account	Nick name	Phone	Email	User group
admin	SuperAdmin			System administrator group
jerry				RDLab-group
jones				Layer4-group
Sophie				PVLab-group

Permission topology

- Log in with "jones", this account can view and manage site "Layer4". "Layer4" is Primary site that permit to create sub-site under it. This account can view and manage the devices (device A, B, C, D, E, F) in "Layer4" site
- Log in with "jerry", this account can view and manage site "RD-Lab". "RD-Lab" is Secondary site that is unable to create a new sub-site under it. This account can view and manage the devices (device C and D) in "RD-Lab", and can view but can't manage the devices (device E and F) in "PV-Lab" site
- Log in with "Sophie", this account can view and manage site "PV-Lab". "PV-Lab" is Secondary site that is unable to create a new sub-site under it. This account can view and manage the devices (device E and F) in "PV-Lab" site



2.6.3.1.1 Reset password

If ordinary users forget password, please retrieve password with the help of the administrator.

1. Log in as administrator account. Click "User Management"->"Account", Select the account. For example, choose the account "Sophie", and click "Reset Password"

Account	Nick name	Phone	Email	User group	Language	LDAP login	Account status	Operate
admin	SuperAdmin			System administrator group	en	<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	Edit
jerry				RDLab-group	zh-CN	<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	Edit Reset password
jones				Layer4-group		<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	Edit Reset password
Sophie				PVLab-group		<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	Edit Reset password

Reset password

Are you sure to reset the user's password?

☐ Do you want to send the password through this account email

[Cancel](#) [OK](#)

2. It will pop up the new password as shown as below image, administrator send this new password to user "Sophie"

Account

User group

+ Add

Account	Nick name	Phone	Email	User group	Language	LDAP login	Account status	Operate
admin	SuperAdmin			System administrator group	en	<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	
jerry				RDLab-group	zh-CN	<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	Reset password
jones				Layer4-group	zh-CN	<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	Reset password
Sophie				PVLab-group	en	<input type="checkbox"/>	Enable <input checked="" type="checkbox"/>	Reset password

< 1 >

New password: 1HDF0_ami

×

3. Account "Sophie" can log in with the new password provided by the administrator. After logging in successfully, the software will forcibly reset the password



The password for one account can only be reset once per minute at most. Otherwise, Software will pop up "Too many requests"

2.6.3.2 User group

Concept of Group

User group can manage sites and devices under the site. Administrator can grant different user group with different permission. It is recommended to check [Site management](#) firstly

The software has added the administrator group named "System administration privileges" by default. All accounts in this group have administrator privileges

Create group

Log in with administrator, click "System setting" -> "User management" -> "User group" -> "add", create the group. for example, create three groups for three sites:

- Create group "Layer4-group" for "Layer4"
- Create group "RDLab-group" for "RD-Lab"
- Create group "PVLab-group" for "PV-Lab"

Account		User group		
		+ Add		
Name	Remark	User group members	Create time	Operate
System administrator group	System administration privileges	View	2024/11/11 13:44:13	Edit
Layer4-group		View	2024/11/26 11:14:37	Edit Delete Permissions
RDLab-group		View	2024/11/26 11:14:50	Edit Delete Permissions
PVLab-group		View	2024/11/26 11:15:04	Edit Delete Permissions
		< 1 >		

Group permission

The user group has three types of permissions for the site: Administration, view, and no permission.

- Administration has included the following permission:
 - Add/Delete/Edit site and sub-site
 - Add/Delete/Edit/Control devices in the site
 - Add/Delete/Edit "UPS on/off schedule" and "battery self-test schedule" in the site
 - Add/Delete/Edit redundant group in the site
 - Add/Delete/Edit remote servers in the site
 - Set the shutdown protection in the site
- View: The permission to view the site and devices in the site
- No permission: No permission to view the site or devices in the site

Grant permission to group

- Choose the group "Layer4-group", then click Permissions button. Grant Administration permission to Layer4 site

Permission management



User group list

- ☒ Layer4-group
☐ RDLab-group
☐ PVLab-group

Site list

Name	Permissions
Plant	<input type="radio"/> Administration <input type="radio"/> View <input checked="" type="radio"/> No permission
Layer4	<input checked="" type="radio"/> Administration <input type="radio"/> View <input type="radio"/> No permission
RD-Lab	<input checked="" type="radio"/> Administration <input type="radio"/> View <input type="radio"/> No permission
PV-Lab	<input checked="" type="radio"/> Administration <input type="radio"/> View <input type="radio"/> No permission

Cancel

OK



If the group have the administration permission for the parent site, it also has administration permission for all sub-sites by default. As shown in the above figure, Layer4-group also has administrator privileges for sub-sites RD-Lab and PV-Lab as default

- Choose the group “RDLab-group”, then click Permissions button. Grant Administration permission to RD-Lab site and grant View permission to PV-Lab

Permission management



User group list

- ☐ Layer4-group
☒ RDLab-group
☐ PVLab-group

Site list

Name	Permissions
Plant	<input type="radio"/> Administration <input type="radio"/> View <input checked="" type="radio"/> No permission
Layer4	<input type="radio"/> Administration <input type="radio"/> View <input checked="" type="radio"/> No permission
RD-Lab	<input checked="" type="radio"/> Administration <input type="radio"/> View <input type="radio"/> No permission
PV-Lab	<input type="radio"/> Administration <input checked="" type="radio"/> View <input type="radio"/> No permission

Cancel

OK

- Choose the group “PVLab-group”, then click Permissions button. Grant Administration permission to PV-Lab site

Permission management



User group list

- ☐ Layer4-group
☐ RDLab-group
☒ PVLab-group

Site list

Name		Permissions		
—	Plant	<input type="radio"/> Administration	<input type="radio"/> View	<input checked="" type="radio"/> No permission
—	Layer4	<input type="radio"/> Administration	<input type="radio"/> View	<input checked="" type="radio"/> No permission
	RD-Lab	<input type="radio"/> Administration	<input type="radio"/> View	<input checked="" type="radio"/> No permission
	PV-Lab	<input checked="" type="radio"/> Administration	<input type="radio"/> View	<input type="radio"/> No permission

Cancel

OK

2.6.4 Site management

Add site

Software supports 2 levels management for site, and default root site name “root” which is editable

1. Log in with administrator, click “System settings” -> “Site management” -> “Add”, add the new site





The contacted name, contacted phone, and contacted email are only used to remarked that admin can easily and quickly contact with site administrator. It is not related to “Event subscription”


2. Create primary site “Layer4” under the root site “Plant”

Add site



* Parent : Plant 

* Name: Layer4

Remark: 1-256 

Contact name: 1-128

Contact phone: Please enter

Contact email: Please enter

Save

3. Create secondary site "RD-Lab" and "PV-Lab" under the primary site "Layer4"

Add site



* Parent ?:

Layer4



* Name:

RD-Lab

Remark:

1-256



Contact name:

1-128

Contact phone:

Please enter


Contact email:

Please enter

View site

View the site via "List display" or "Tree display"

- Root site is "Plant"
- Primary site is "Layer4"
- Secondary sites are "RD-Lab" and "PV-Lab"

 List display

Name	Level	Remark	User group permissions	Create time
— Plant	Root site	top level area	View	2024/11/22 11:03:45
— Layer4	Primary site		View	2024/11/22 11:04:08
RD-Lab	Secondary site		View	2024/11/22 11:04:37
PV-Lab	Secondary site		View	2024/11/22 11:04:53

2.6.5 Serial port management

List all serial ports and their usage.

If it is a Windows system, the software automatically detects all serial ports in the system and does not support manual deletion and addition of serial ports.

If it is a Linux system, the software will list serial port devices such as /dev/ttyS0, /dev/ttyS1, /dev/ttyUSB0, /dev/ttyUSB1 by default, and supports manual addition or deletion of serial ports.



The default serial port name of the USB to serial port device in the Linux system is /dev/ttyUSB0 or /dev/ttyUSB1

If it is a MacOS system, the software does not add a default serial port. If a USB to serial port device is used, it needs to be added or deleted manually.

scroll

[+ Add](#)

Serial port name	In used	Operate
COM3	Used by SMS modem	
COM8	Used by device	

< 1 >

2.6.6 Signal threshold setting

This page can set the upper and lower alarm thresholds of the UPS signal. When the threshold is exceeded, an alarm will occur.

Signal name Input Voltage

Set threshold
 Input Voltage
 Load Percentage
 Battery Remaining Time
 Battery capacity
 The time of battery test ti...
 UPS Temperature
 Environment Temperature
 Environment Humidity

[Setting global thresholds](#)

	Signal name	Severely high	High	Severely low	Low	Unit
<input checked="" type="checkbox"/> Device	Input Voltage	1000	1000	0	0	V
<input checked="" type="checkbox"/> SNMP-10.130.212.131	Input Voltage	1000	1000	0	0	V
<input checked="" type="checkbox"/> SNMP-10.130.212.144	Input Voltage	1000	1000	0	0	V
<input checked="" type="checkbox"/> SNMP-10.130.212.171	Input Voltage	1000	1000	0	0	V
<input checked="" type="checkbox"/> SNMP-10.130.212.243	Input Voltage	1000	1000	0	0	V
<input checked="" type="checkbox"/> SNMP-10.130.212.245	Input Voltage	1000	1000	0	0	V
<input checked="" type="checkbox"/> SNMP-10.130.212.236	Input Voltage	1000	1000	0	0	V
<input checked="" type="checkbox"/> NMC-G2-10.130.212.244	Input Voltage	1000	1000	0	0	V

< 1 2 >

Signals that support threshold setting include: input voltage, load percentage, battery remaining time, battery capacity, time of battery test till low, UPS temperature, ambient temperature, and ambient humidity.



The threshold setting for the time of battery test till low is limited to serial port, USB and Modbus TCP UPS, and these UPS must be able to support testing to low voltage.

This setting is usually combined with battery testing to low schedule to assist in monitoring and judging the aging of the battery.

Detailed battery discharge data (voltage, capacity, load and discharge duration at the beginning and end) can be viewed on the [device details](#) page.

Global thresholds

Click "Setting global thresholds" to set the global threshold default value. When a new UPS device is added, the threshold value of the device will be set as the global default value. Modifying the global default value will not affect the threshold settings of existing devices.

Device threshold

Select the signal from the drop-down box, then select one or more devices, and click "Set Threshold" to modify the signal threshold of the selected devices.

2.6.7 Event subscription setting

Prerequisites

- SMTP mail server and personal receiving mailbox have been configured
- SMS Modem and personal mobile phone number have been configured



Configure the email server or SMS notification settings through [Notification service setting](#)

Subscribe to events

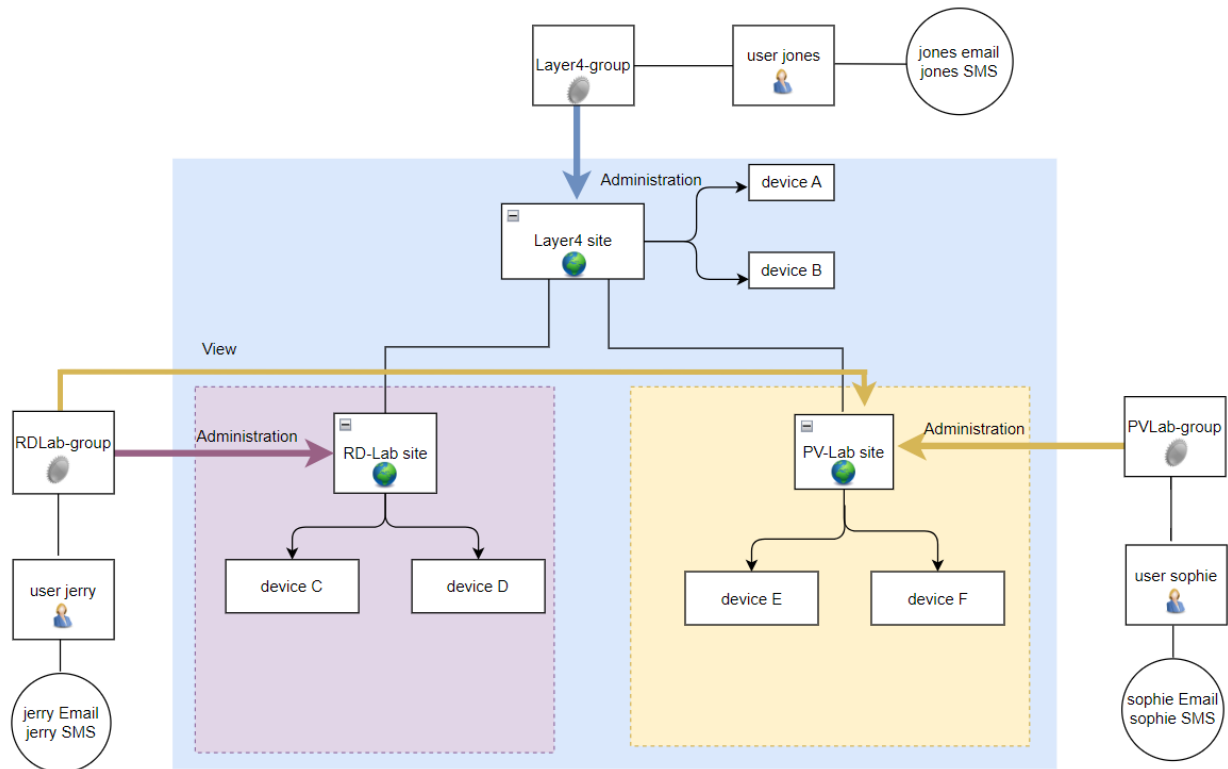
- This page lists all device event names, event levels, and whether SMS and emails need to be sent. Each account log in separately, and set on this page which event email and SMS notifications to receive. Enter the event name in the upper left corner and click the search button to filter the events. After selecting the events and notification methods to be subscribed, click the "Save" button to save it.

UPS device events and common events		PDU device events		
Please enter the event n...				
Event Name	Event level	Notification type		
		<input type="checkbox"/> All	<input type="checkbox"/> All	<input type="checkbox"/> All
UPS fault. Service required		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Module fault. Service required		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Communication lost		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Battery low		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Output overload		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Output short circuit		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Output off		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps

Event subscription topology diagram

- User jones, jerry, and Sophie all need to log in to the web respectively and set the events subscription

- User jones is in the Layer4 group and has administration permission for Layer4 site and its sub-sites. When the devices (device A, B, C, D, E, F) occur events, it will notify jones via jones' email and mobile phone
- User jerry is in the RDLab group and has administration for RD-Lab site and has view permission for PV-Lab site. Therefore, When the devices (device C, D, E, F) occur events, it will notify jerry via jerry's email and mobile phone
- User Sophie is in the PVLab group and has administration permission to the PVLab site. Therefore, When the devices (device E, F) occur events, it will notify Sophie via Sophie's email and mobile phone



Once the user group has view permission to the site and the user belongs to the group can receive notification from devices under the site

2.6.8 Notification service setting

2.6.8.1 Email setting


If you want to receive email notifications of events or receive verification codes via email to reset your password when you forget your password, you need to set up an SMTP server to send emails.

Email setting

* SMTP service:

* Sender:

* Sender alias:

Password: 

Test content:

* Port:

* Password verification: ☐

* Encryption type: ☐ No encryption ☐ TLS encryption ☐ SSL encryption

Test email:

SMTP service: SMTP server IP or domain name

Sender: Sender's email address

Sender alias: Sender name

Port: Port used by SMTP service

Password verification: Whether to enable password verification

Encryption type: Encryption method used by SMTP protocol

Password: Authorization code, it can also be called App password. Please check [How to apply for email app password](#)

Several common email SMTP server configuration references

Mail	SMTP server	Encryption type	Port
gmail	smtp.gmail.com	TLS	587
		SSL	465
outlook	smtp-mail.outlook.com	TLS	587
163	smtp.163.com	No encryption	25
		SSL	465 or 994
sina	smtp.sina.com	No encryption	25
		SSL	465
		TLS	587
qq	smtp.qq.com	TLS	587

Mail	SMTP server	Encryption type	Port
		SSL	465

After the SMTP server is set up and saved, it is recommended to enter the test receiving email and test content, and click the "Test" button to check whether the test email can be received to confirm that the SMTP server setting is correct. Email testing is limited to send once per minute.



The test mailbox is not the mailbox for receiving alarm notifications. Event alarm notifications will be sent to the mailbox set in the [personal profile](#) according to the individual's [event subscription settings](#).



When using an email server outside the company to send emails, the host where the software is installed must be directly connected to the Internet. If you are connecting to the Internet through a proxy, it is recommended to contact the IT department and use the company's internal email server to send emails.

2.6.8.2 SMS setting

If you want to receive SMS notifications of events or receive verification codes on your mobile phone to reset your password when you forget your password, you need to use a GSM SMS Modem that supports AT commands, connect to the SMS Modem through the serial port, and set the parameters of the SMS Modem correctly.

SMS setting

* Serial port:	COM3	* Baud rate:	9600
* Country code:	Add country code		
PIN:	<input type="checkbox"/>	PIN code:	4-8
Test content:	Please enter		
	Phone:	Please enter	<input type="button" value="Test"/>
	<input type="button" value="Save"/>		

Serial port: The serial port connected to the SMS Modem

Baud rate: The baud rate for SMS Modem operation is usually: 9600, 19200, 115200

Country code: The format of the phone number can be without the country code or with the country code. The phone number formatted with the country code looks like 8613723456789 (where the country code is 86). Without the country code, the same phone number would look like 13723456789. If you do not need to send international text messages, choose the format without country code.

PIN : PIN code refers to the SIM card personal identification password, 4-8 digits. When the PIN code is invalid for more than 3 times, the card will be automatically locked for protection. To unlock, you need to use

the PUK code to call the operator's customer hotline. (Different operators have different SIM card PIN code protection mechanisms. Some cannot be unlocked and can only be replaced with a new card). If the SIM card does not have a PIN code set, this setting is not required.

After setting and saving, it is recommended to enter the test content and mobile phone number, click the "Test" button, and check whether the mobile phone can receive the test message to confirm that the SMS Modem setting is correct. SMS testing is limited to send once per minute.



The mobile phone number here is only for receiving test messages, not for receiving alarm notifications. Event alarm notifications will be sent to the mobile phone number set in the [personal profile](#) according to the individual's [event subscription settings](#).

2.6.9 Credential

Each user can add, edit and delete communication credentials on this page. Its purpose is to reuse the saved communication credentials without repeatedly entering them when searching SNMP and MQTT devices.



Users only have permissions for credentials created by themselves and cannot view, edit, or delete credentials created by other users.

When adding a device, the selected credential information will be copied to the device credential information, and then the two will not be associated, that is, changes to the saved credentials will not affect the device credentials.

+ Add

Name	Protocol type	Operate
NMCG2card-Lab	MQTT	
pdu	SNMP-> SNMPv1	
snmpV3cards	SNMP-> SNMPv3	
snmpV1private	SNMP-> SNMPv1	
NMCG2card-office	MQTT	

Click the edit icon in the action column to modify the credential. Click the delete icon to delete the credential. Click the "Add" button in the upper right corner to add credentials.

The screenshot shows a 'Credential' form with the following fields and values:

- Name:** 1-128
- Protocol type:** SNMP
- Protocol:** SNMPv3
- Security level:** Please select
- User name:** 1-128
- Authentication:** Please select
- Authentication password:** 1-32

A blue 'Save' button is located at the bottom of the form.

Name: The name of the credential

Protocol type: Optional SNMP and MQTT. Different credential settings are displayed depending on the protocol selected. For example:

SNMPv3 credentials are set as follows

This screenshot shows the 'Credential' form with 'SNMPv3' selected in the 'Protocol' dropdown. The fields and their values are:

- Name:** 1-128
- Protocol:** SNMPv3
- Security level:** Please select
- User name:** 1-128
- Authentication:** Please select
- Authentication password:** 1-32

A blue 'Save' button is at the bottom.

MQTT credentials are set as follows

This screenshot shows the 'Credential' form with fields for MQTT credentials. The fields and their values are:

- Name:** 1-128
- User name:** Please enter
- Password:** Please enter

A blue 'Save' button is at the bottom.

After setting, click the "Save" button to save the credential.

2.6.10 Custom reminder

- title: Title of reminder email
- Reminder content: Detailed description for reminder content
- Period: Once, Monthly, Every 3 months



"Once" means only executing reminder for one time. "Monthly" means executing reminder for every month. "Every 3 months" means executing reminder in January, April, July, and October

- Reminder time: execute reminder in specific date and time
- Remind type: SMS and Mail



The prerequisite is that the email SMTP and SMS have been set, Please check [Notification service setting](#)

- Phones: The recipient's phone number of SMS, multiple recipients can be separated by ","
- Emails: The recipient's email address, multiple recipients can be separated by ","
- Start/End execution time: Execute reminder within the specified time if it is set. If not, no any time limit



Account who creating reminder can see the scheduled reminder, while other account can't see it

Set custom notifications



title: Check UPS Battery

* Reminder content: Check UPS battery status via battery self test

46 / 128

* Period: Every 3 months

* Reminder time: 2th 09:00:00

* Reminder type: ☒ SMS ☒ Mail

Phones: 137, 135

Emails: jonesliu@, tinaliu@

Start execution time: 2024-12-01

End execution time (?): 2025-12-01

Save

2.6.11 WOL Setting

The purpose of this function is to wake up remote computers whose BIOS does not support "automatic boot after AC recovery" through the monitoring software installed on the host that supports "automatic power on after AC recovery".

Prerequisites:

- The local host where the monitoring software is installed and the remote host to be waked up are located in the same network segment.

- The remote host BIOS supports and enables the wake-on-LAN function.
- The local system is protected by the monitoring software and shuts down. When restarting, it will wake up remote hosts according to the settings. **The shutdown action of the local system needs to be set to shutdown instead of hibernation.** Hibernation will not perform network wake-up. Refer to [Shutdown Protection Settings>>Local System](#).

Wake-up trigger conditions:

After the local system is shut down and protected by the monitoring software, when the system is restarted, the monitoring software will send wake-up magic packets to the set MAC address according to the timing set by WOL to wake up other hosts in the same network segment.

Wake on LAN settings

Click the “Add” button to add hosts that need to be woken from LAN. Fill in the following fields:

Server: MAC address of the host, required



MAC addresses are often labeled "Physical Address" or "Ethernet Physical Address"

The commands to check the MAC address on different systems are as follows:

Windows : ipconfig /all

Linux和macOS: ifconfig -a

Description: Optional

Wake up delay: Through this setting, multiple hosts can be started in sequence. Range from 0 to 3000 seconds, required.

Enable or not: Set whether to allow waking up of this server.

Clicking the "Test" button will immediately send a wake-up packet to the server to test whether the server can be successfully woken up.

Click the "Save" button to save the settings.

Wake-on-LAN logging is not enabled by default. If logging is required, it can be enabled in [System Preferences>>Log Settings](#).

After the log is turned on, you can view the LAN wake-up log records in [Events/Log>>Wake-on-LAN Log](#).

2.6.12 LDAP login

LDAP login setting

Enter LDAP setting parameters and enable LDAP. Please consult the local IT department for specific LDAP settings information

LDAP login setting


* Host name ?:	<input type="text" value=""/>	* Port:	<input type="text" value="3268"/>	<input type="checkbox"/> useSSL
* User name ?:	<input type="text" value="CN=,R,OU=Admin,DC=,DC=ac"/>	* Password ?:	<input type="password" value=""/>	
* BaseDn ?:	<input type="text" value="DC=ad,DC=,DC=com"/>	* Enable or not:	<input checked="" type="checkbox"/>	
* User name attribute:	<input type="text" value="userPrincipa"/>			

Create LDAP account



1. Click "System settings" -> "User management" -> "Add", create a Winpower account that has included in LDAP account
2. Choose LDAP checkbox. Once enable LDAP login, the password field will turn gray and can't be set. The new account can log in with the corresponding LDAP password


New users



* Account :

Nick name:

Password : 

* User group: 

Phone:

Email:

LDAP login: ☒ Enable



The password of LDAP account will never expire, also password reset is not supported

2.6.13 HTTPS setting

Enable https: Enable this function means you should access software through https. Disable this function means you should access software through http.

Port: The default https or http port is 8081 which can be modified. The port number is stored in the “\config\webconfig.yml” of software installation path. Once the port is modified, please restart software and then access using new port number.

Https certificate and Certificate password:

When software is released, it will also create a self-signed certificate that will never expire. The certificate is located in “\cert\server.jks” of software installation path. If the user intends to use own certificate, please

upload the certificate and password. Software only supports certificates in JKS (suffix jks) and PKCS12 (suffix pfx) formats.

Certificate generation methods:

- Cloud service providers such as Tencent Cloud and Alibaba Cloud will provide jks certificate, which can be directly applied for download. Please remember the password when applying
- Generate self-signed certificate using the built-in tools of JDK
- Generate server and client self-signed certificates using OpenSSL
- [FreeSSL.cn](https://www.freessl.cn/) is a website that provides free HTTPS certificate applications



Restart software service to take effect

HTTPS setting

* Enable https: ☒

Https credential: [Upload https crede...](#)

* Port:

Credential password:

Save

After changing the configuration,
you need to restart the service

2.6.14 License management

The free version of the software can monitor up to 100 devices and cannot connect to third-party SNMP 1628MIB UPS. If the number of devices exceeds 100 or you need to connect to a third-party SNMP 1628MIB UPS, please purchase a License.

The steps for license application and import are as follows:

- Click the download button to download the License Key file
- Please contact the supplier or service personnel for purchase details and provide the downloaded License Key file
- After receiving the .key license file provided by the supplier, upload it through the upload button to complete the License import. The license management page will display the maximum number of devices you can monitor and the license validity period.

If the license has a validity period, please renew it in time. After the license expires, the free version permissions will be restored. Third-party SNMP 1628MIB UPS and devices that exceed the quota (sorted by device creation time, and those added later will be set to inactive first) will be set to inactive status. The device will not be automatically activated after renewal, and inactive devices need to be activated manually.

- The software will automatically create a user reminder and send an email or SMS message to remind customers 90 days in advance before the expiration date of the license



The administrator account needs to set email or phone number in advance, otherwise it will prompt an expiration reminder has been failed to create, but it won't affect the use of the license

License information

Version: 0.0.0.0

License type: **VIP**


License validity period: 2025/01/22 — 2026/01/22

Apply for License: [Download](#)

Max number of access devices: 202

Import License: [⬆ Upload](#)

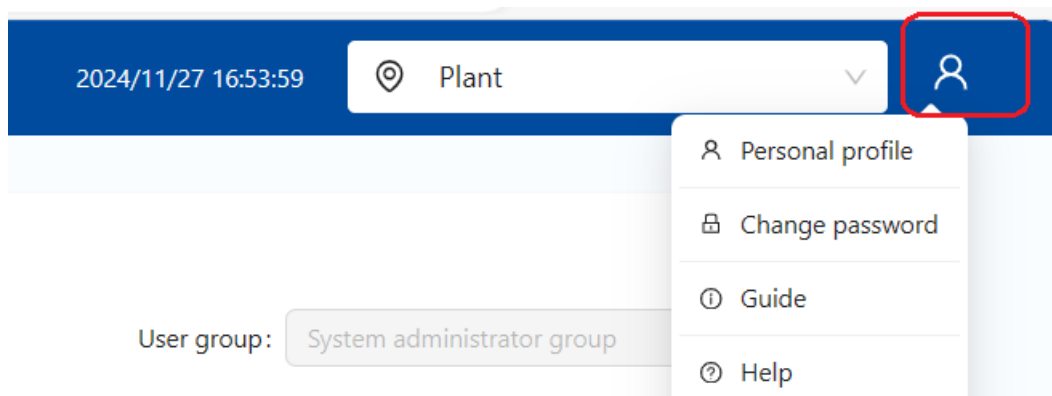
The expiration reminder has been successfully created as a custom reminder. If you need to modify it, please go to the scheduled reminder setting page to modify the reminder.

Identifier: 

2.7 Other setting

2.7.1 Personal profile

1. After logging in, click on the user profile image ->"Personal profile"



2. You can edit the Email, Phone and Language as so on



Event subscription and password retrieval both rely on the email or phone number. It is recommended to enter valid email address and phone number

Account information

User name: admin

User group: System administrator group

Nick name: SuperAdmin

Password expiration: 2025-11-21

Email: Please enter

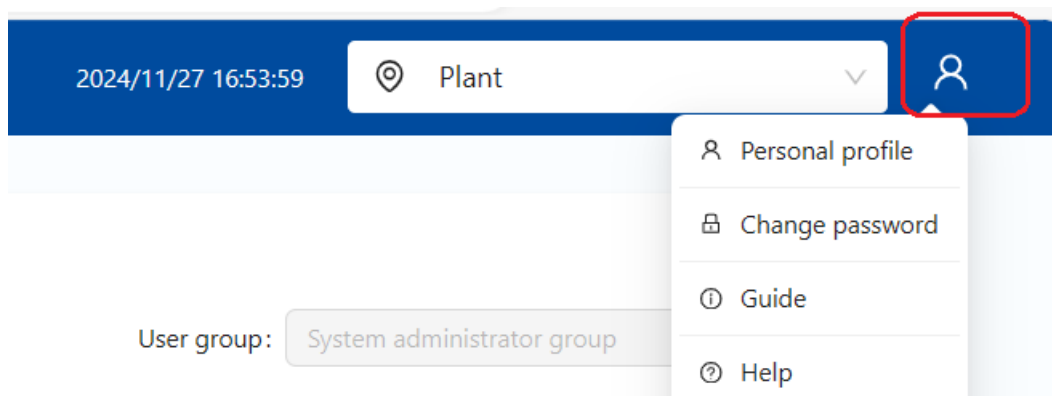
Language: English

Phone: Please enter

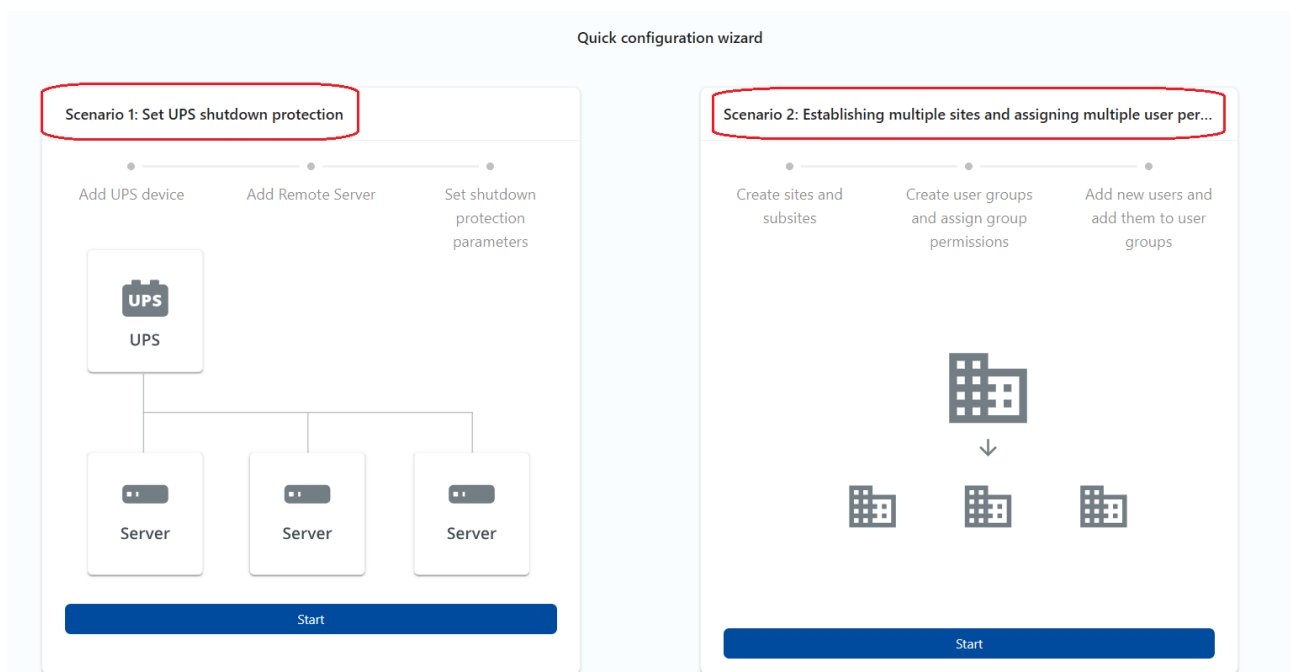
Save

2.7.2 Guide

1. After logging in, click on the user profile image ->"Guide"

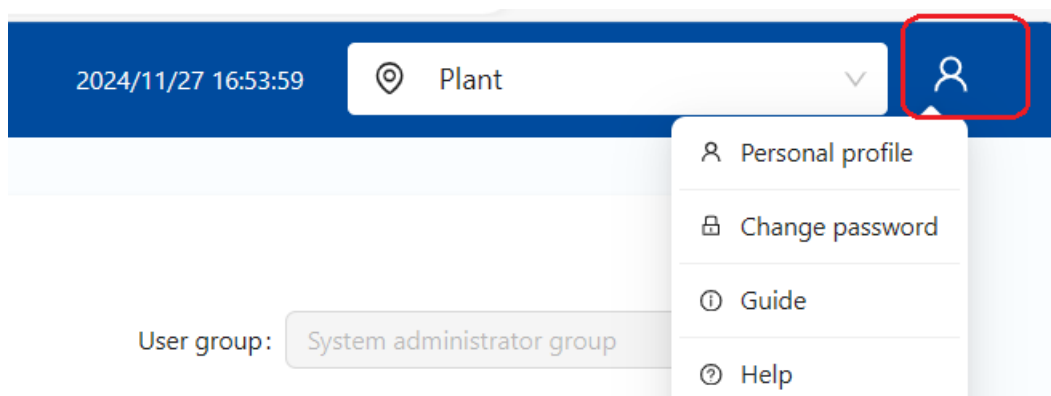


2. The software provides two application scenarios wizard: "Set up UPS shutdown protection" and "Establish multiple sites and assign multiple user permissions". Click the "Start" button to complete the configuration according to wizard

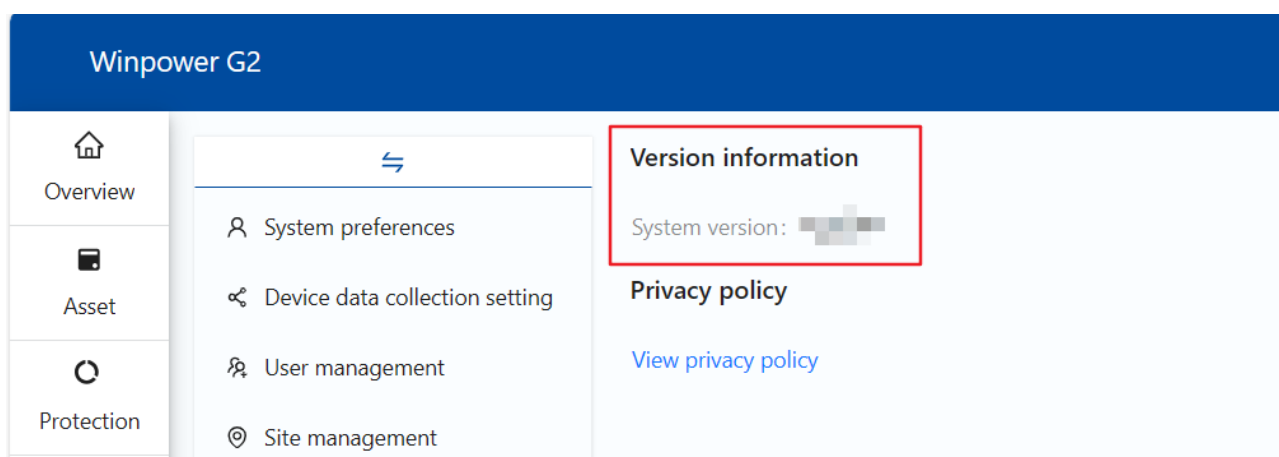


2.7.3 Check version

1. After logging in, click on the user profile image ->"About"



2. Check the version in "Version information" filed



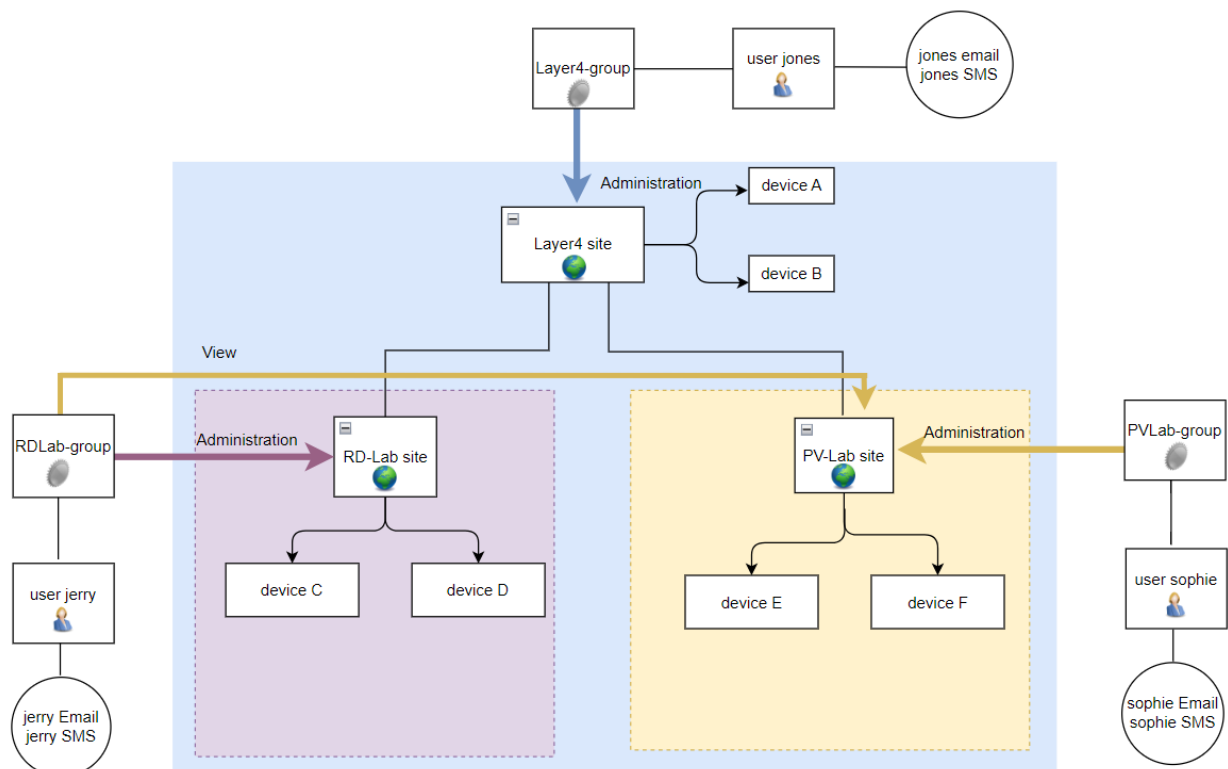
3 How To

3.1 How to send Email/SMS

1. Email and SMS notifications are associated with user, while users are associated with user group, user groups are associated with site, and sites are associated with devices. Different user manage different devices, so each user needs to set up recipient for emails and SMS and subscribe events separately.



The administrator account can manage all devices and receive alarm notifications from all devices

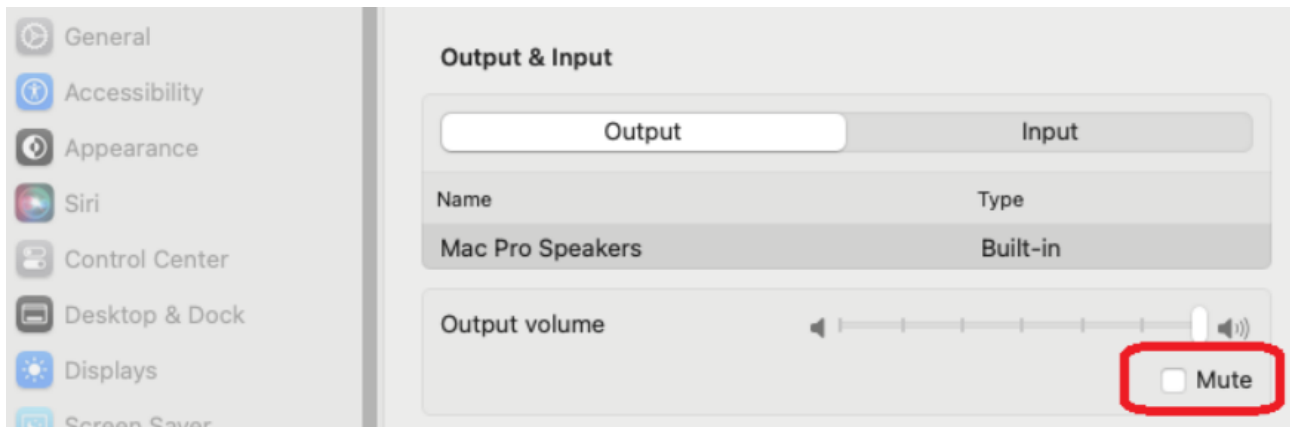


2. The administrator account should set up email service and SMS service firstly. Please refer to the details: [Notification service setting](#)
3. Personal account login, set the recipient for emails and phone number for SMS. Please refer to the details: [Personal profile](#)

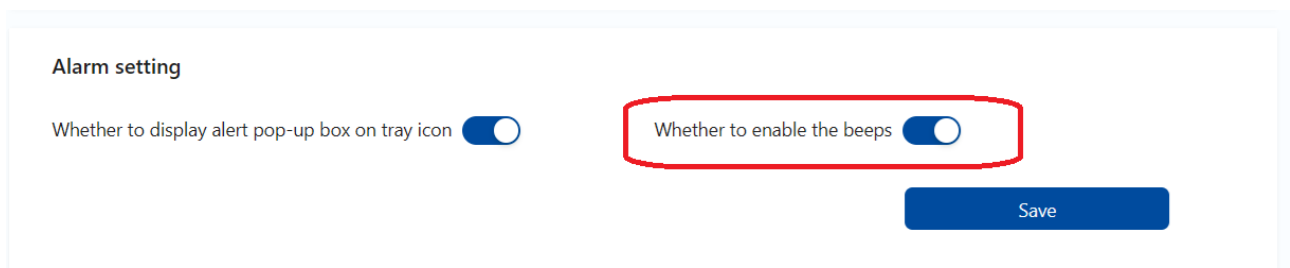
4. Personal account login, subscribe to Events -- Select the events you want to receive. Please refer to the details: [Event subscription setting](#)

3.2 How to use beeps alarm

1. The beeps alarm can only be set by the admin account, and other users don't have permission to set. Once the selected event is triggered, the host where the software is located will emit a beep alarm sound. Each event triggers a beep alarm once. The beep audio file is placed in the installation directory "\config\sound\alarm-bep.wav". Software allows users to replace the audio file with the same video name.
2. Audio play function should be enabled on the OS for Beeps alarm. For example, the following image is a screenshot of Mac OSX---The "mute" function must be disabled firstly.




3. Open the software web, click "System settings" -> "System preferences", enable the beeps function ---- by default, this function is not enabled











4. Click "System settings" -> "Event subscription setting", and select the events that require beeps alerts. You can also select the events you need to subscribe to through the "Event level" classification

UPS device events and common events

PDU device events

Please enter the event n... 

Save

Event Name	Event level 	Notification type		
		<input type="checkbox"/> All	<input type="checkbox"/> All	<input type="checkbox"/> All ⓘ
UPS fault. Service required		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Module fault. Service required		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Communication lost		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Battery low		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Output overload		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Output short circuit		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps
Output off		<input type="checkbox"/> SMS	<input type="checkbox"/> Email	<input type="checkbox"/> Beeps

5. If the event that triggers the beeps is already known, you can select "Turn off the current beeps" on the "Event" page.



Performing this action only turns off the current beeps. Once a new event occurs, the beeps alarm will sound again

Event

Data log

Shutdown log

Time: Start da... → End date

Event status: Active alarm

Device name: Please enter device ...

More filters

Event level: Event level

Event description: Please enter event d...

Turn off the current beeps

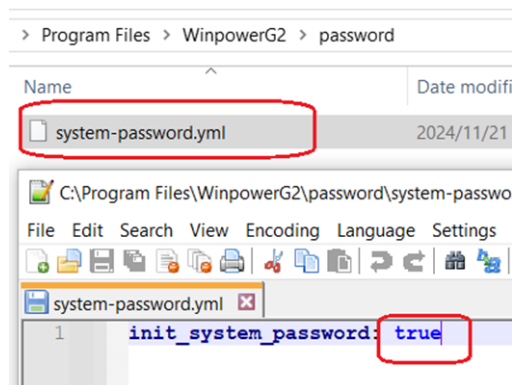
Export to excel

Event status	Event level	Event description	Device name	Start time
Active alarm		On battery mode	COM6-UPS	2025/08/05 17:15:11
Active alarm		Main AC is not OK	COM6-UPS	2025/08/05 17:15:10

3.3 How to reset password for "admin"

If the password for "admin" is forgotten without setting email SMTP or SMS, it can be retrieved through the configuration

1. Go to software installation path and modify the "system-password.yml" document under "password" folder. Set the value of "init_system_password" to "true"



2. Restart software service, the admin password will be set to "admin". the value of "init_system_password" will be changed to "false" automatically

3.4 How to apply for email app password

The method to obtain authorization codes or App password for email SMTP is different. Please consult to the related email service supplier for details.

For example, check how to get the app password for Gmail as below image

Solution

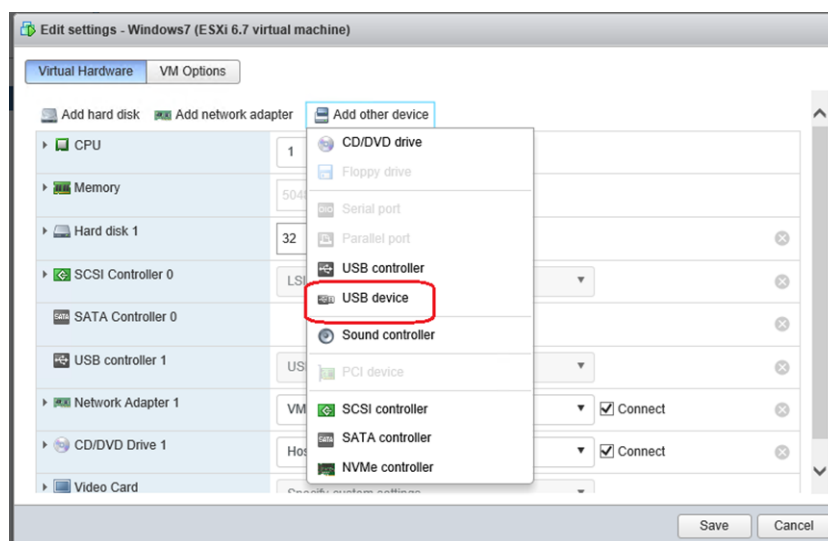
1. Sign in to your [Google Account](#).
2. Click **Security**.
3. Under **Signing in to Google**, click **App Passwords**. You may need to sign in. If you don't have this option, it might be because:
 - 2-Step Verification is not set up for your account.
 - 2-Step Verification is only set up for security keys.
 - Your account is through work, school, or other organization.
 - You turned on Advanced Protection.
4. Click **Select app** and choose the app.
5. Click **Select device** and pick the device you're using.
6. Click **Generate**.
7. Follow the instructions to enter the app password. The app password is the 16-character code in the yellow bar on your device.
8. Tap **Done**.

Tip: Most of the time, you'll only have to enter an app password once per app or device, so don't worry about memorizing it.

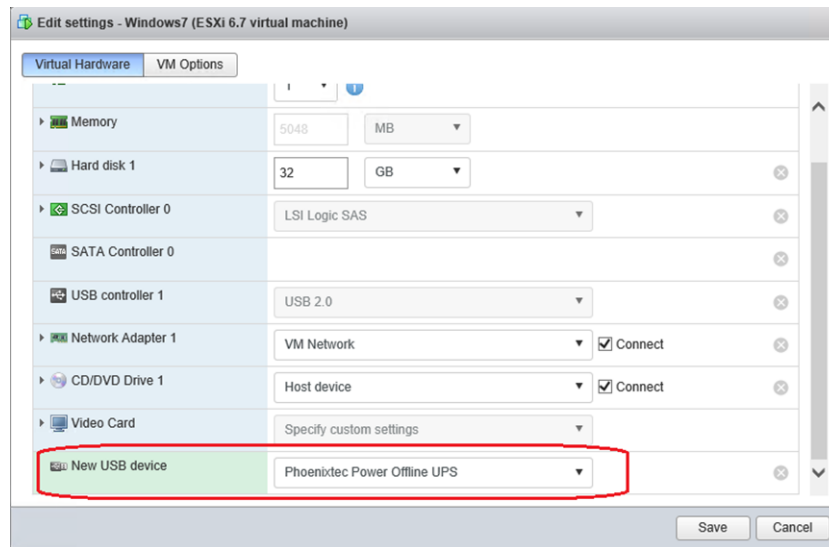
3.5 How to add UPS via USB/RS232 for Virtual Machine

USB Communication

1. Choose the virtual machine that has installed Winpower. Click "Edit settings"->"add other device"->"USB device", add the USB device

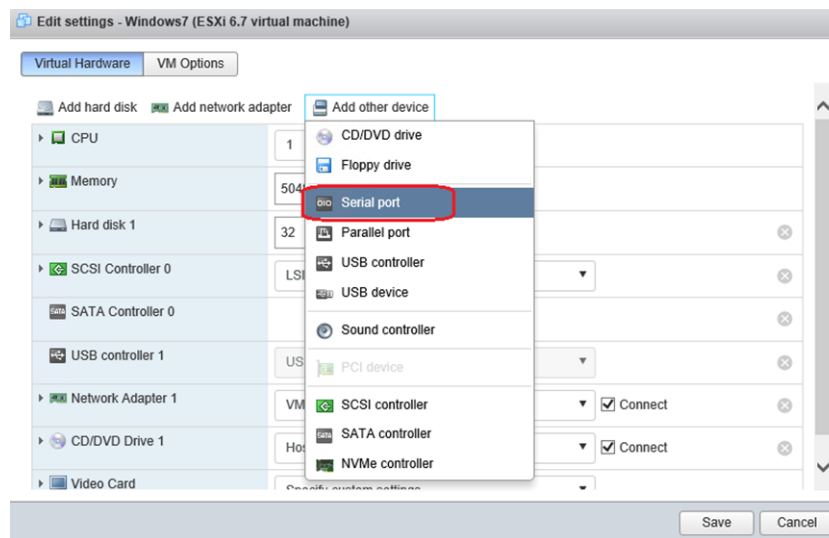


2. UPS USB is added successfully as below image

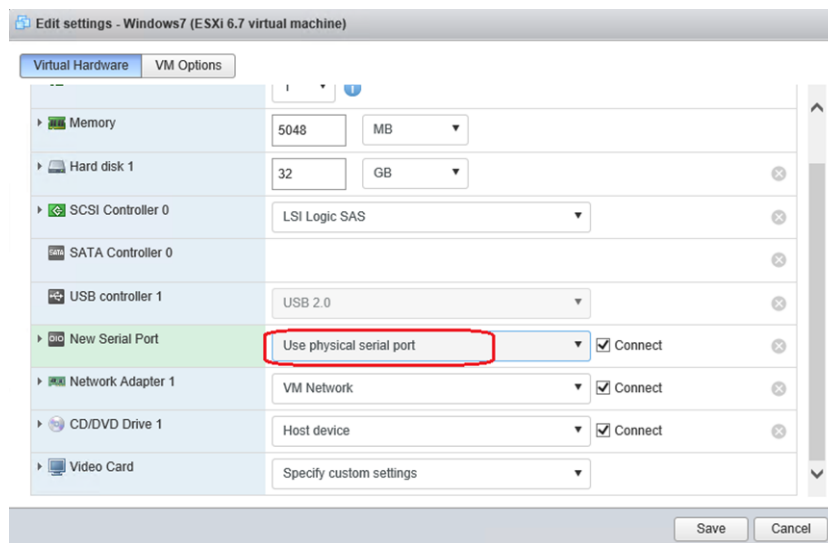


RS232 Communication

1. Shut down the virtual machine that has installed Winpower. Click "Summary"->"Edit setting"->"add"->"Serial Port"->"Use physical serial port", add Serial port. The default serial port name is "/dev/char/serial/uart0"

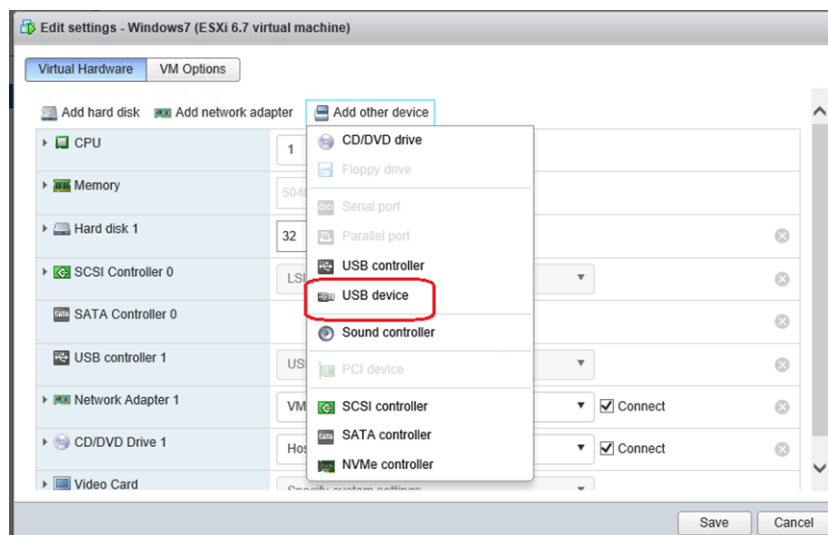


2. Choose "Use physical serial port ", add serial port device, restart the virtual machine

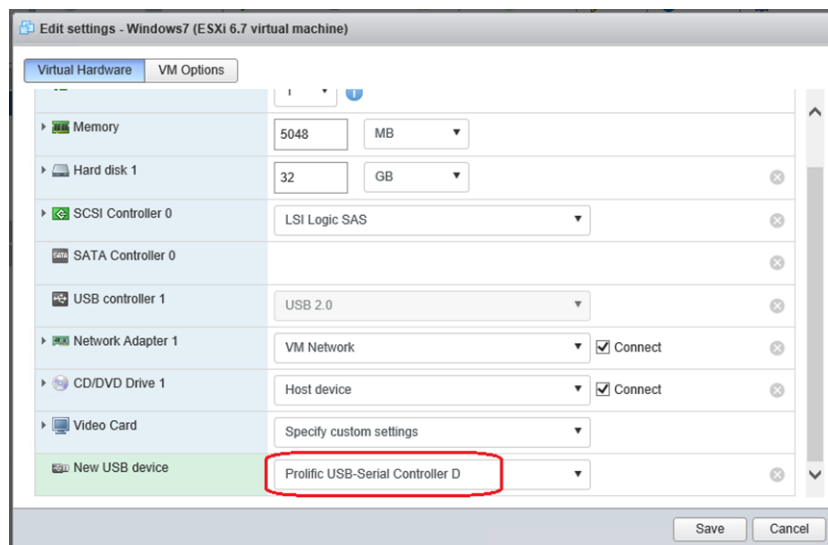


USB To RS232 Communication

1. Choose the virtual machine that has installed Winpower. Click "Edit settings"-> "add other device"->"USB device", add the USB device

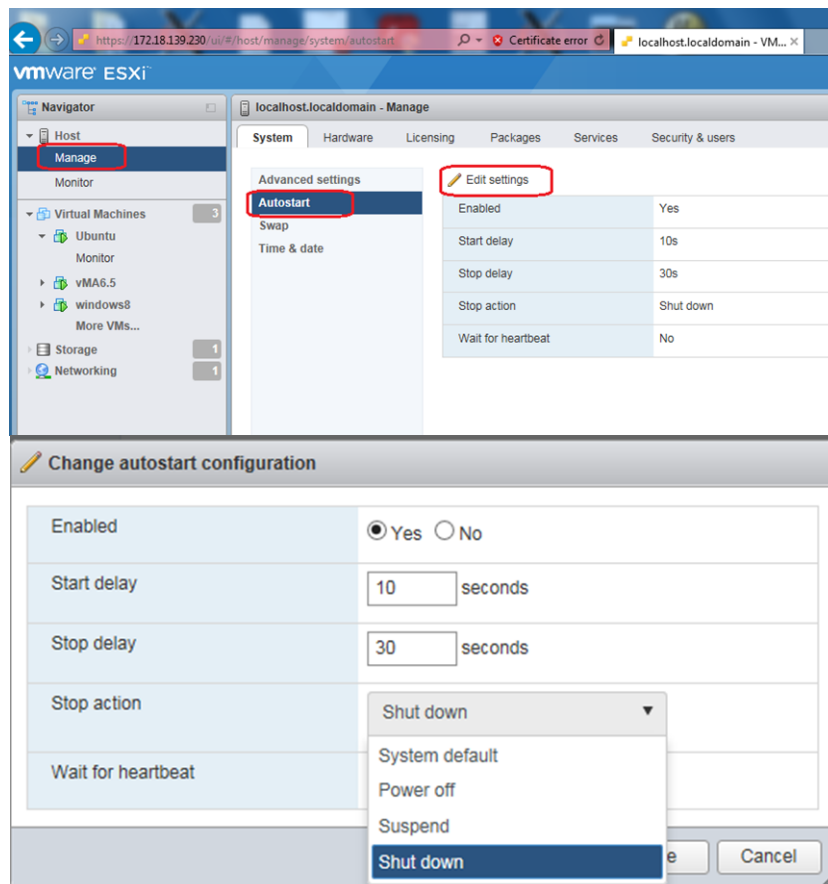


2. UPS USB-RS232 is added successfully as below



3.6 How to set auto stop/start on VMware ESXi

This is a built-in feature of VMware ESXi host. If enabled this feature, all virtual machines on the host will be automatically shut down before host shutting down, and all virtual machines on the host will be automatically started after host booting.



4 Troubleshooting

4.1 Troubleshooting the Cause of WOL Failure

If the remote host does not wake up as expected after the local system restarts, please [enable the network wake-up log](#) and check whether there is a wake-up record in the [wake-up log](#). If there is no record, it means that it has not been executed. Please check:

1. The shutdown protection action of the local system selects shutdown instead of hibernation. After selecting hibernation and restarting, network wake-up will not be performed!
2. Wake-on-LAN will only be executed when the local system is shut down and then restarted due to a power outage or shutdown schedule.

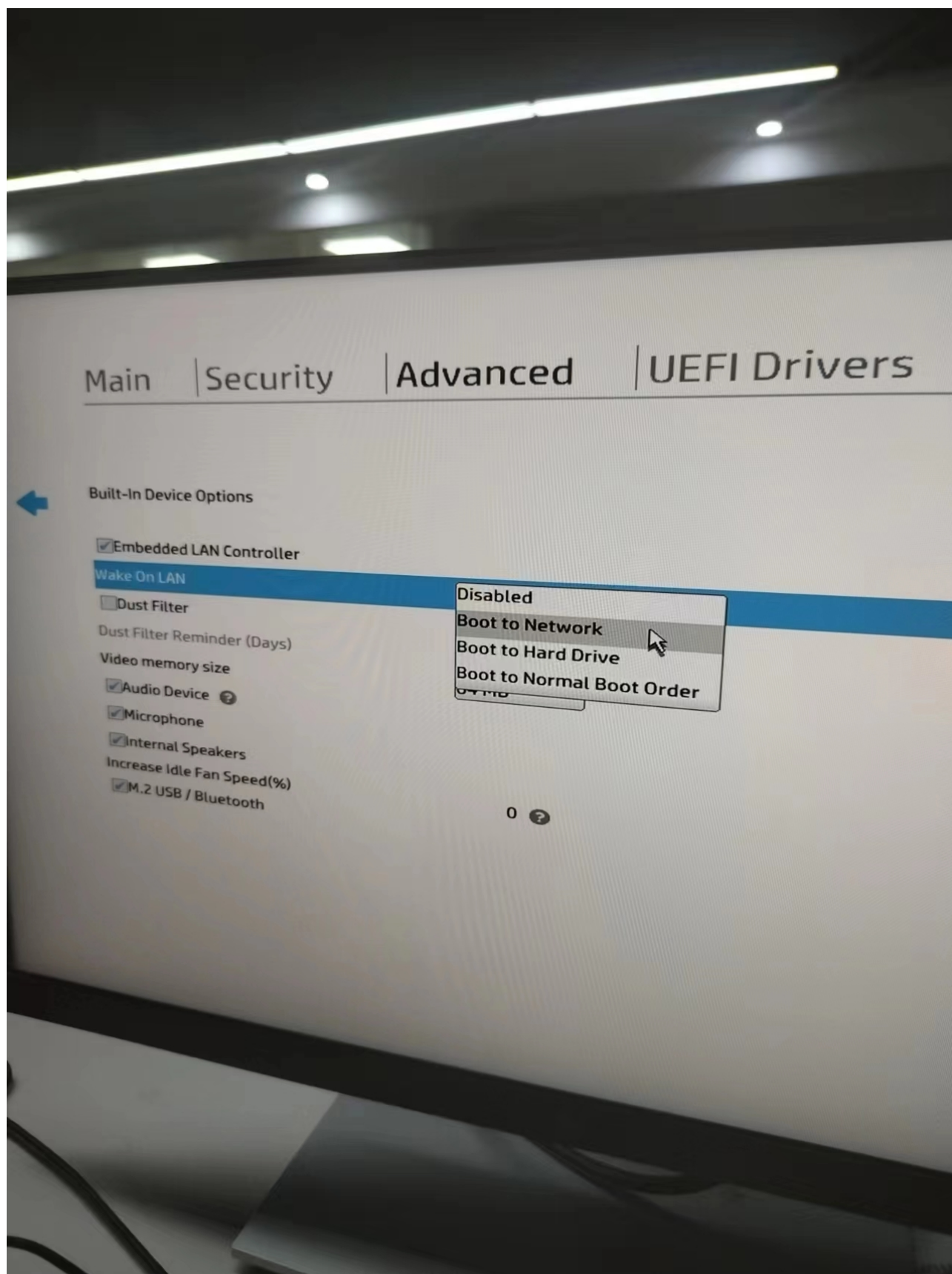
If there is a record and the result is that the transmission was successful, but the remote host has not been awakened, please confirm:

1. The remote host motherboard BIOS supports and enables the wake-on-LAN function

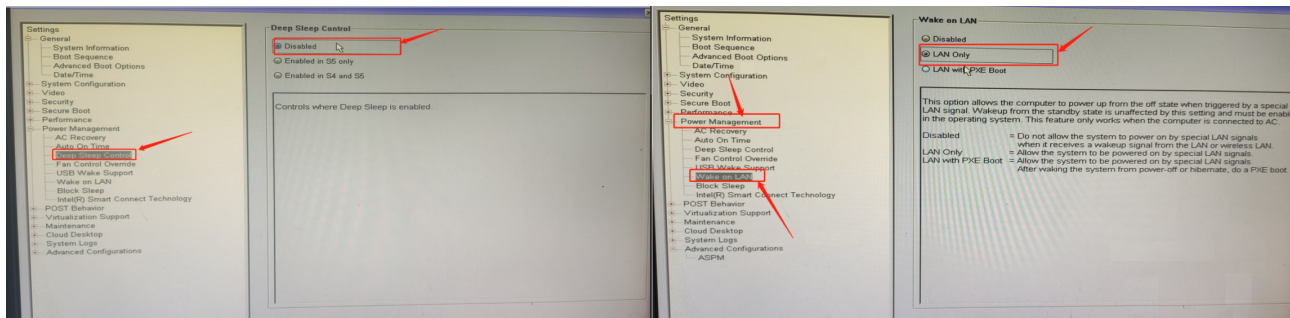
Enter the BIOS: If it is a DELL motherboard, keep pressing F12 when booting. For HP motherboards, press F10 to enter the BIOS.

Enable Wake On Lan in the BIOS settings. The location of the Wake On Lan setting varies on different motherboards. The following examples are for reference.

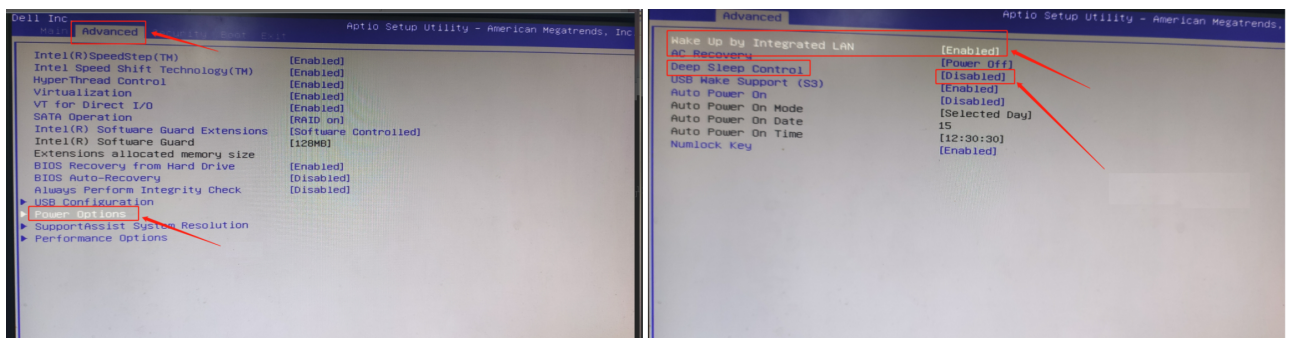
HP BIOS settings



Dell BIOS settings



Another Dell BIOS setup interface



2. The remote host and the host where the monitoring software is located are on the same network segment
3. MAC address is correct

If there is a record but the result is a failure to send, please check the system network.

4.2 Resolve ports conflict

If the network port to be used by the software is already occupied by another application, first check which application is occupying the port.

In Linux/macOSX systems, you can use **"lsof -i:port"** to check the specific port is occupied by which process. Then view the details of a specific process through **"ps -p PID -o comm,user,group,pid,ppid,cputime,mem,pcpu,command"**. where PID is the process ID of the process. This command will display the name of the process (comm), owner (user), group (group), process ID (pid), parent process ID (ppid), CPU time (cputime), memory usage (mem), and CPU usage. (pcpu) and startup command (command).

In Windows systems, enter **"netstat -ano | findstr port"** in the command prompt to see which process is occupying a specific port. You can then view the details of the process through Task Manager or **tasklist /fi "PID eq process-number"**.

Solution:

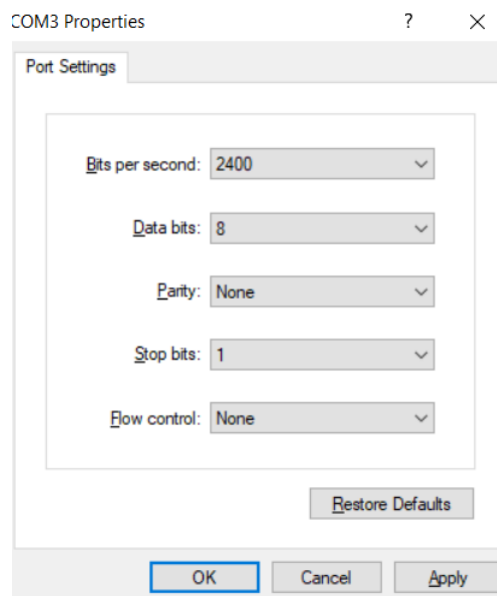
1. Free up the port by deactivating or uninstalling the app that's using it.

2. The software uses other free ports. For example, the https port used by the software can be modified in the [HTTPS settings](#). Enter the **netstat -an** command, which will list all currently used ports.

4.3 Reasons for failure to add devices and suggestions

Devices communicating through the serial port cannot be discovered

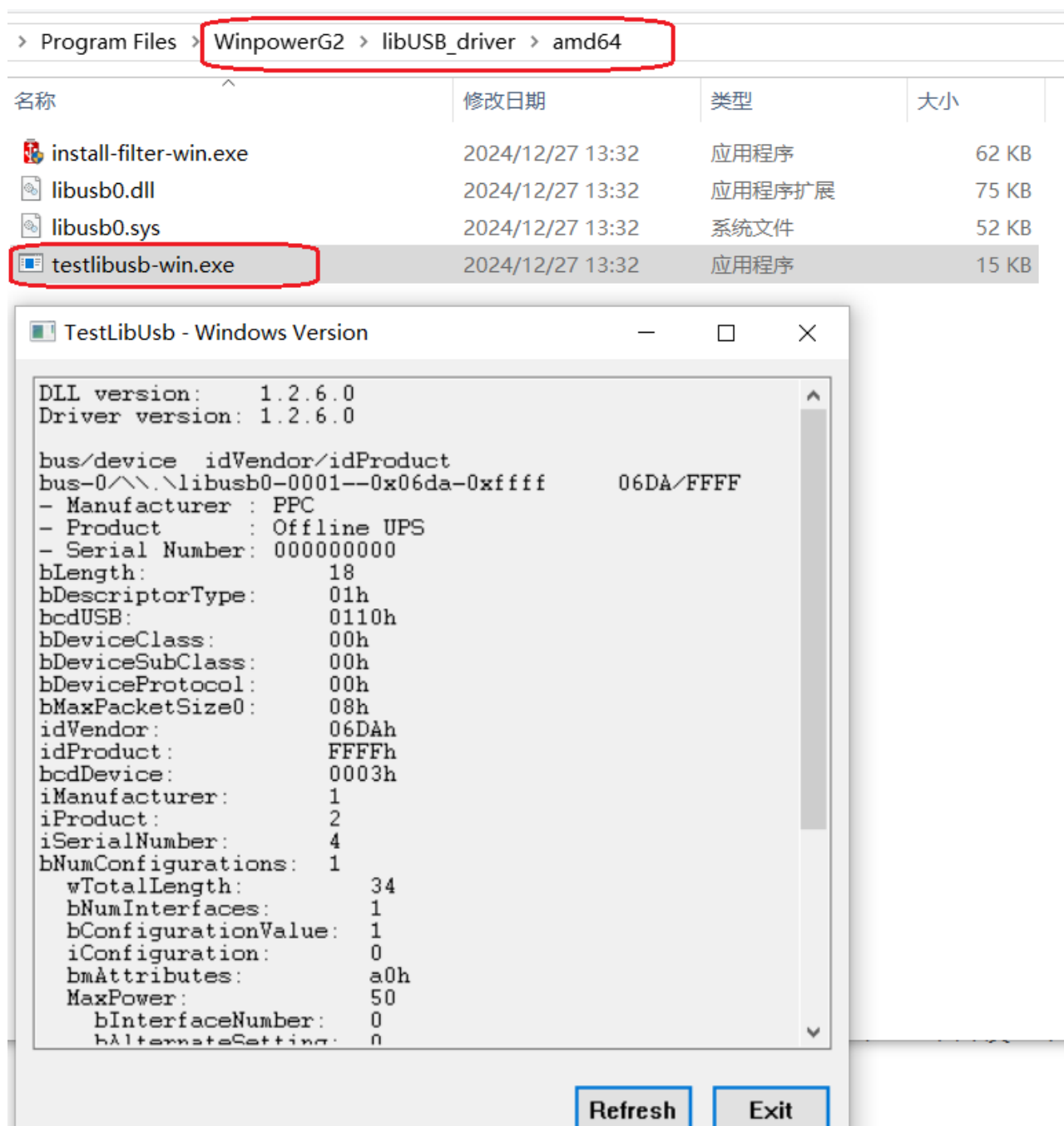
1. Confirm whether the serial port is occupied by other applications and the serial port and serial port cable are working properly. You can use the following configuration of the serial port tool (such as hypertrm.exe) to open the serial port : 2400 baud rate, 8 data bits, no parity, stop bit 1, no flow control.



2. Enter the "PI" or "Q1" command and press Enter to see if there is a reply from the UPS. If the serial port cannot be opened and shows that it is occupied, you need to close the software occupying the serial port or use another serial port. If the UPS does not reply, you need to check whether the serial port cable is loose or whether the UPS/computer serial port is normal.

Devices communicating through the USB cannot be discovered

1. Go to software installation path, go to the sub directory "\libUSB_driver\amd64", double click "testlibusb-win.exe". If displaying UPS information as the following image that indicate the USB driver has been installed normally
2. If the above steps still do not work, execute script "\libUSB_driver\InstallDriver.bat" in the installation directory with administrator privileges, and then execute "testlibusb-win.exe" to check if the USB device driver is loaded correctly



Possible reasons for failure to add NMC G2 card

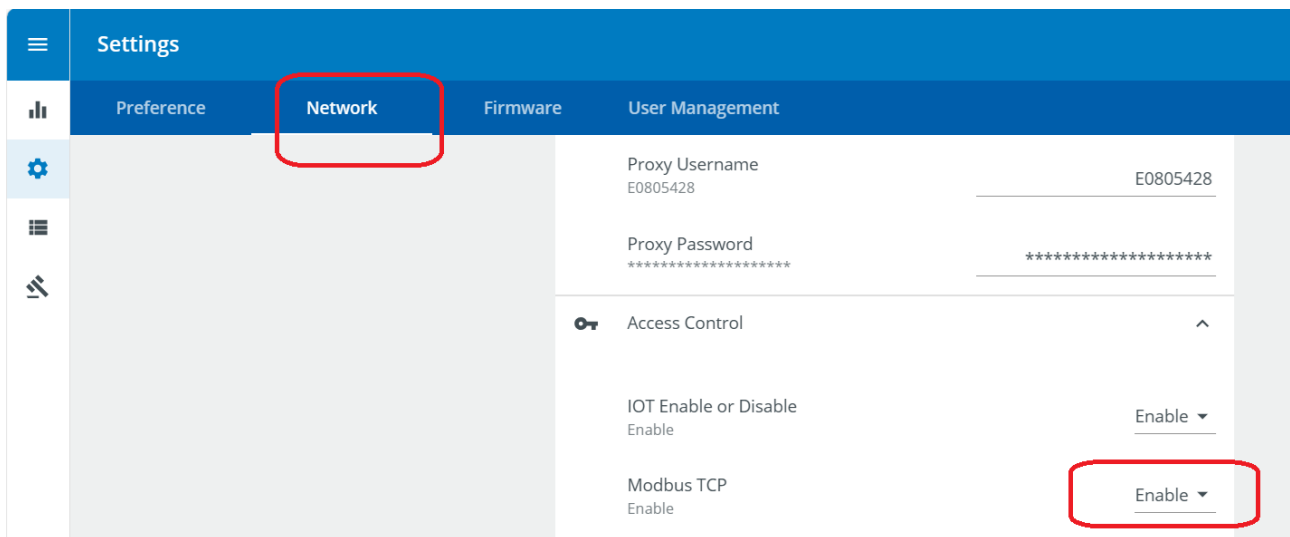
1. The MQTT account name and password are incorrect
2. The time setting of the NMC G2 card or the computer system time setting is incorrect. The time inconsistency causes the certificate verification to fail

Possible reasons for failure to add SNMP device

1. The SNMP protocol is not enabled on the card. You need to enable the SNMP protocol on the card's web page.
2. The version of the SNMP protocol and the certificate account and password are inconsistent with the card settings. Please make sure they are consistent.

Possible reasons for failure to add Modbus TCP device

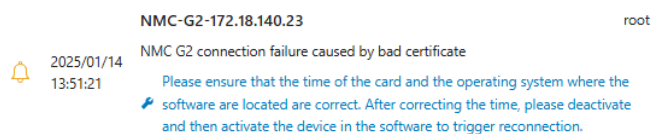
1. The Modbus TCP protocol is not enabled on the device. Please enable Modbus TCP from the LCD or web



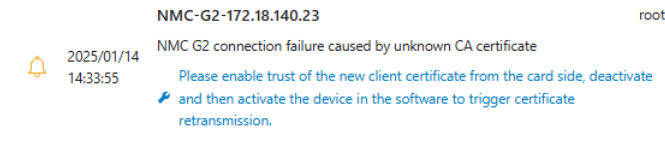
4.4 Troubleshooting causes of NMC G2 card communication interruption

When the software monitors the NMC G2 card and the communication is interrupted, the cause can be investigated from the following aspects:

1. Check whether the card is online, log in to the card web page through the card IP, and confirm that the card is running normally.
2. Confirm that the time setting of the card and the time setting of the computer system where the software is located are correct and the two times are consistent. Please check the device details page to see if there is an active alarm "NMC G2 connection failure caused by bad certificate". If this alarm occurs, you need to correct the time and then deactivate and activate the device in the software to trigger reconnection. If communication still cannot be restored, please try restarting the card and software.



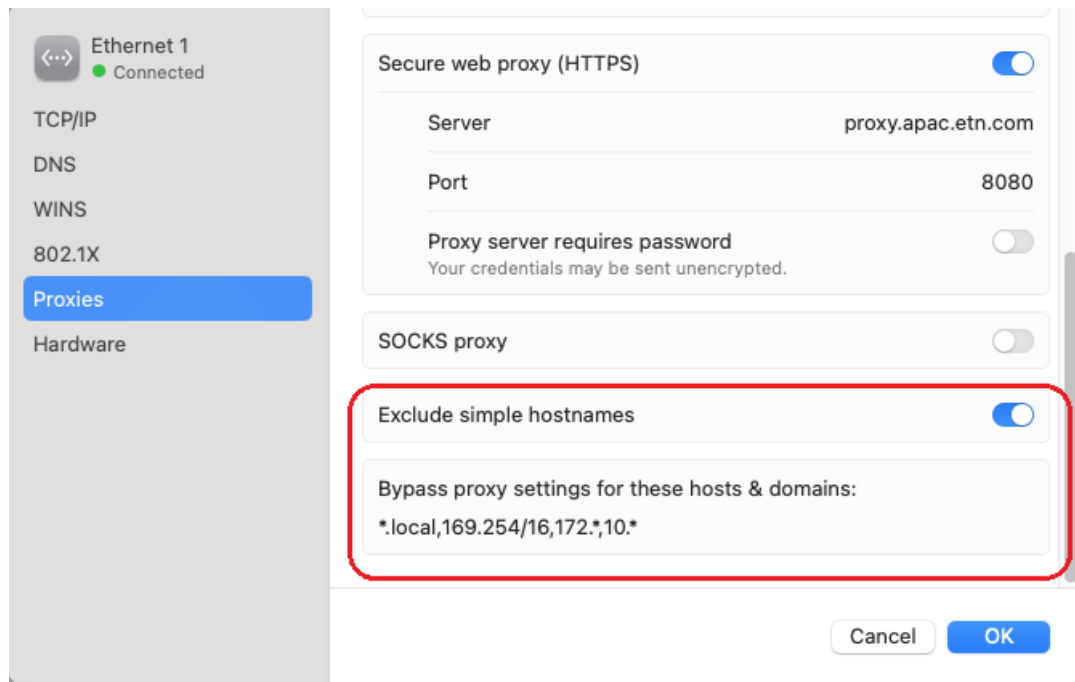
- Communication interruptions can also occur if the software agent is removed from the card's agent list or the software certificate is removed from the "Trusted Remote Certificates" from the card. If it is interrupted for this reason, an active alarm "NMC G2 connection failure caused by unknown CA certificate" appears on the device details page. If this warning occurs, please enable trusting the new client certificate on the card side for a period of time, deactivate and then activate the device in the software to trigger certificate retransmission. If normal communication still cannot be restored, please try restarting the card and software.



4.5 Search cards failed via Winpower on MacOSX

On Mac OSX, Winpower may encounter an issue that the cards such as Modbus TCP and NMCG2 can't be searched due to proxy settings.

Open Proxies, enable "Exclude simple hostnames", and permit HTTPS requests from the local machine to bypass the proxy



4.6 Communication Failure between Winpower and SPS

- Ensure that the network between Winpower and SPS can ping through each other

- i** If SPS is installed on Mac OS X, please search for SPS directly from the Winpower side instead of searching for Winpower from the SPS side

2. Open UDP port 6787 6788 6789 and TCP port 8081 8883 9443 for Winpower host and SPS host. Both “Inbound” and “Outbound” should be opened for the ports. Taking Windows as an example, the port settings are as follows

FileActionViewHelp

Windows Defender Firewall with Internet Access

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
UPSSoftware		All	Yes	Allow	No	Any	Any	Any	TCP	8081, 8883, 9443	Any
UPSSoftware		All	Yes	Allow	No	Any	Any	Any	UDP	6787-6789	Any
Virtual Machine Man...		All	Yes	Allow	No	System	Any	Any	TCP	5986	Any
Virtual Machine Man...		All	Yes	Allow	No	System	Any	Any	TCP	5985	Any

Windows Defender Firewall with Internet Access

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
UPSSoftware		All	Yes	Allow	No	Any	Any	Any	UDP	Any	6787-6789
UPSSoftware		All	Yes	Allow	No	Any	Any	Any	TCP	Any	8081, 8883, 9443
Desktop		All	Yes	Allow	No	Any	Any	Any	TCP	3389	Any
Active Directory Do...	Active ...	All	Yes	Allow	No	System	Any	Any	ICMPv4	Any	Any

3. If Winpower can't scan SPS and the web page prompts that the founded SPS device is 0, it should be caused by UDP port 6787 6788 6789 not being opened. Due to the stateless nature of the UDP port, it can't be confirmed whether it has been successfully opened or not.
4. If Winpower can scan for SPS and successfully add it, but the communication status shows “unknown” and can't get any data from SPS, it is due to the TCP port 8883 of MQTT not being opened. Since the TCP port is stateful, you can check whether the 8883 port of Winpower's remote host has been successfully opened by using “telnet” or “nc” command on the SPS host.

- i** “Telnet” is installed by default on Windows systems, while “nc” is installed by default on Linux and MacOSX,

- i** Please enter the command on the SPS host just like this:

```
telnet Winpower_IP 8883
```

```
nc Winpower_IP 8883
```