Power Master plus

User's Manual

Management

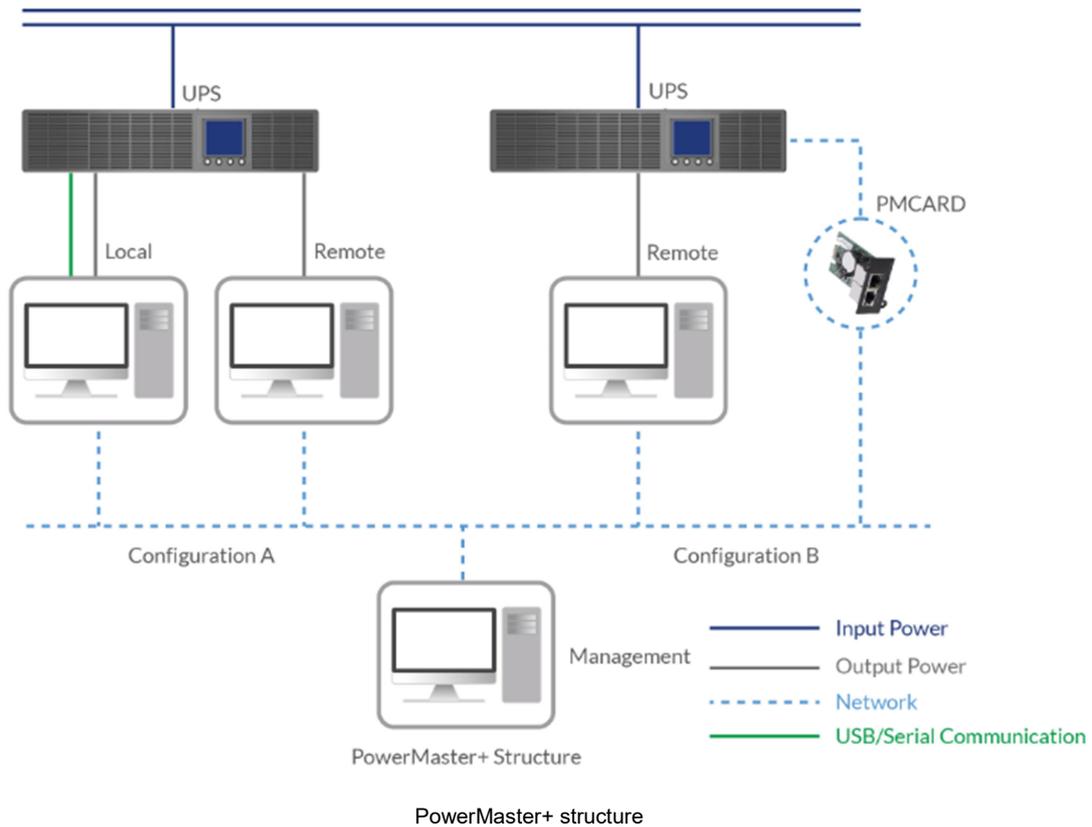**Rev. 1.0.2**

Table of Contents

1   Introduction

Power Master+ Management software simultaneously monitors and controls multiple UPS/PDU/ATS units and computers which have Local or Remote (modules from Power Master+) installed via the local network. It also logs events and results about commands for power management.

PowerMaster+ structure

Power Master+ Management provides users the following functions:

- Simultaneous monitoring of multiple UPS/PDU/ATS units, equipment and computers which have Local or Remote installed.
- Control access to all monitored UPS, PDU, computers and equipment.
- Detailed load management between UPS/PDU/ATS and all powered computers/equipment.
- Equipment groups for easy monitoring or individual access.
- Viewing additional information and status of monitored UPS, PDU, computers and equipment.
- Historical logs for events and results about demands to power management.

2 Getting Started

2.1 Prerequisites

2.1.1 Hardware Limitation

- Minimum Core 2 – Compatible CPU.
- 1 gigabytes (GB) of RAM recommended minimum; more memory generally improves responsiveness.
- Minimum of 1 GB of free space of hard disk.
- Serial port or USB port. (Required by the Local)
- Network interface.

2.1.2 Operating System

Power Master+ software can be installed and is supported on the following operating systems:

- 32-Bit Versions:
    - Windows 10
    - Windows 8
    - Windows 7
    - Centos 7+
    - Debian 10.1
    - Ubuntu 18.04 LTS
    - Citrix XenServer 7.2
    - Citrix Hypervisor 8.0 Express Edition (formerly XenServer)
    - VMware ESXi6.0+ (ESXi Free Edition is not supported)

- 64-Bit Versions:
    - Windows Server 2019
    - Windows Server 2012
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Hyper-V Server 2012
    - Windows Hyper-V Server 2012 R2
    - Windows 10
    - Windows 8
    - Windows 7
    - macOS 10.14
    - macOS 10.15
    - Centos 7+
    - Debian 10.1
    - Debian9

- ■ Ubuntu 18.04 LTS
- ■ Red Hat Enterprise 8
- ■ Red Hat Enterprise 7
- ■ Citrix XenServer 7.2
- ■ Citrix Hypervisor 8.0 Express Edition (formerly XenServer)
- ■ VMware ESXi6+ (ESXi Free Edition is not supported)

Note: Because of the abundance of different Linux builds, not all builds are tested with Power Master+ but most builds will be able to run the program.

2.1.3 Web Browser

Power Master+ softwareis accessed using a web browser and is compatible with the following browsers:
- ● Microsoft Edge
- ● Firefox
- ● Google Chrome
- ● Safari

2.2   Installation

2.2.1 Installation on Windows

After you have downloaded Power Master+ from Company Systems' website follow the setup installation wizard as described below.

● Click the Next button to start an installation.

Setup - PowerMaster Plus 1.0.1

Welcome to the PowerMaster Plus Setup Wizard

This will install PowerMaster Plus on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

[Next >] [Cancel]

● Select the destination directory.

Setup - PowerMaster Plus 1.0.1

Select Destination Directory

Where should PowerMaster Plus be installed?

Select the folder where you would like PowerMaster Plus to be installed, then click Next.

C:\Program Files (x86)\PowerMaster Plus   [Browse ...]

Required disk space: 225 MB
Free disk space: 62 GB

[< Back] [Next >] [Cancel]
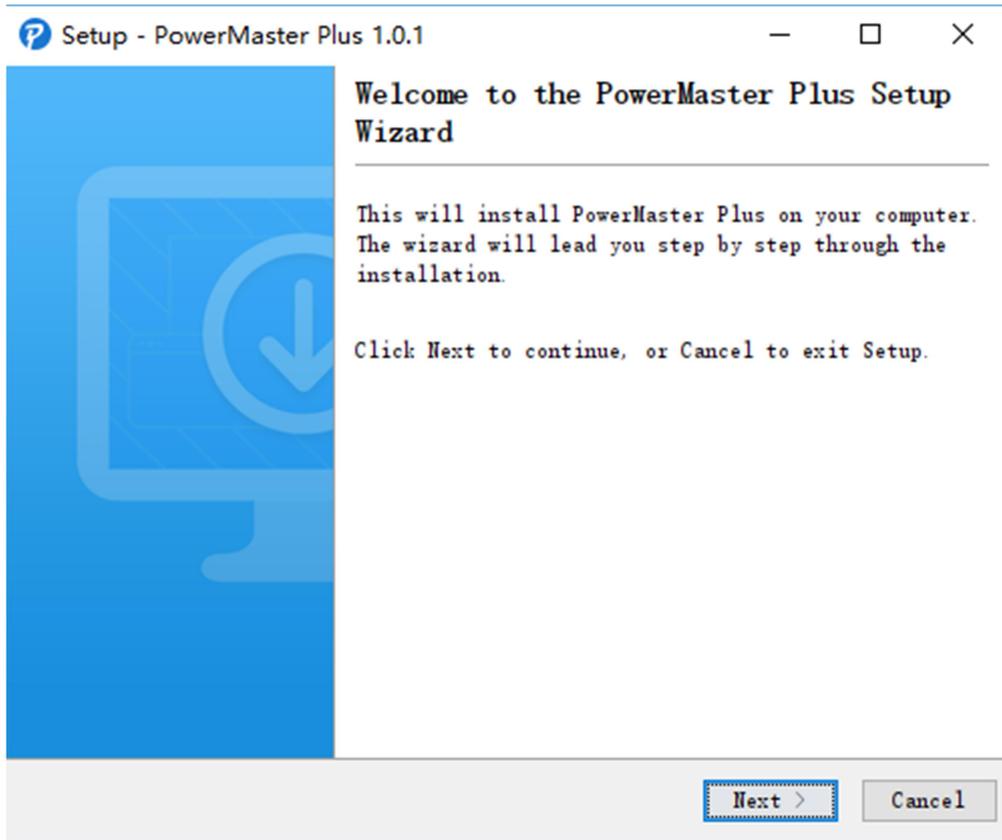
- Choose the component. Power Master+ Management only contains one module. In this step, only Management can be selected.

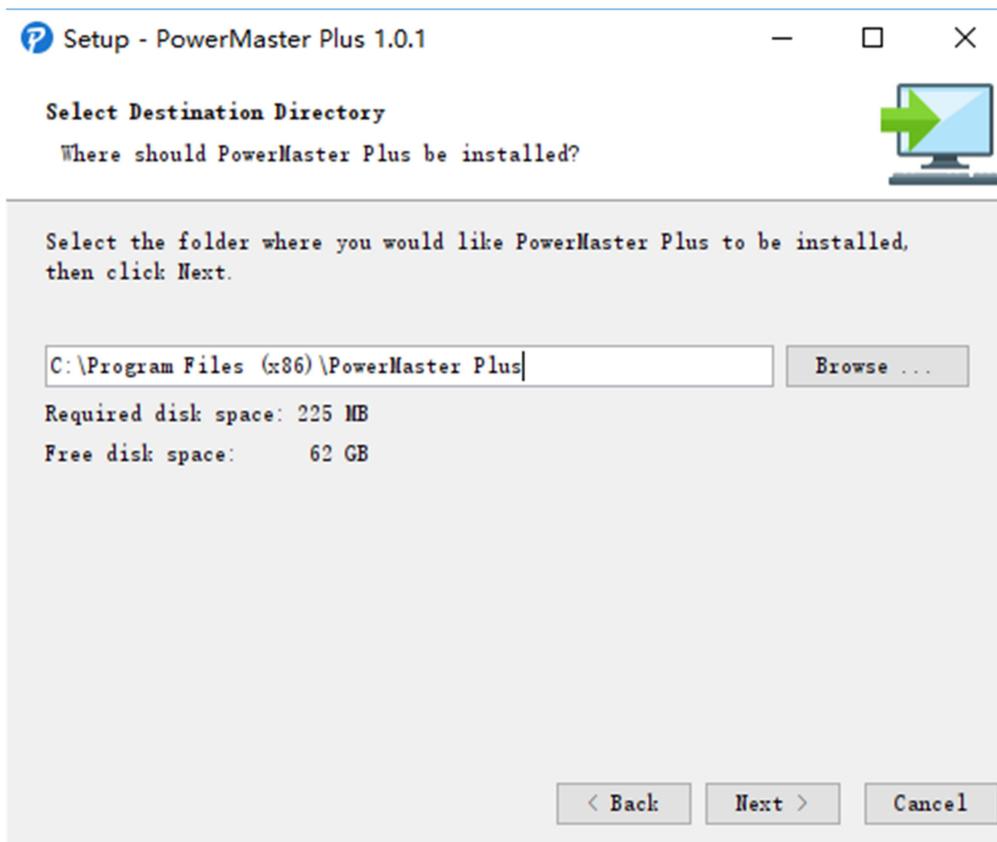- Click the Finish button to complete the installation.

2.2.2 Installation on macOS

After you have downloaded Power Master+ from Company Systems' website follow the setup installation wizard as described below.
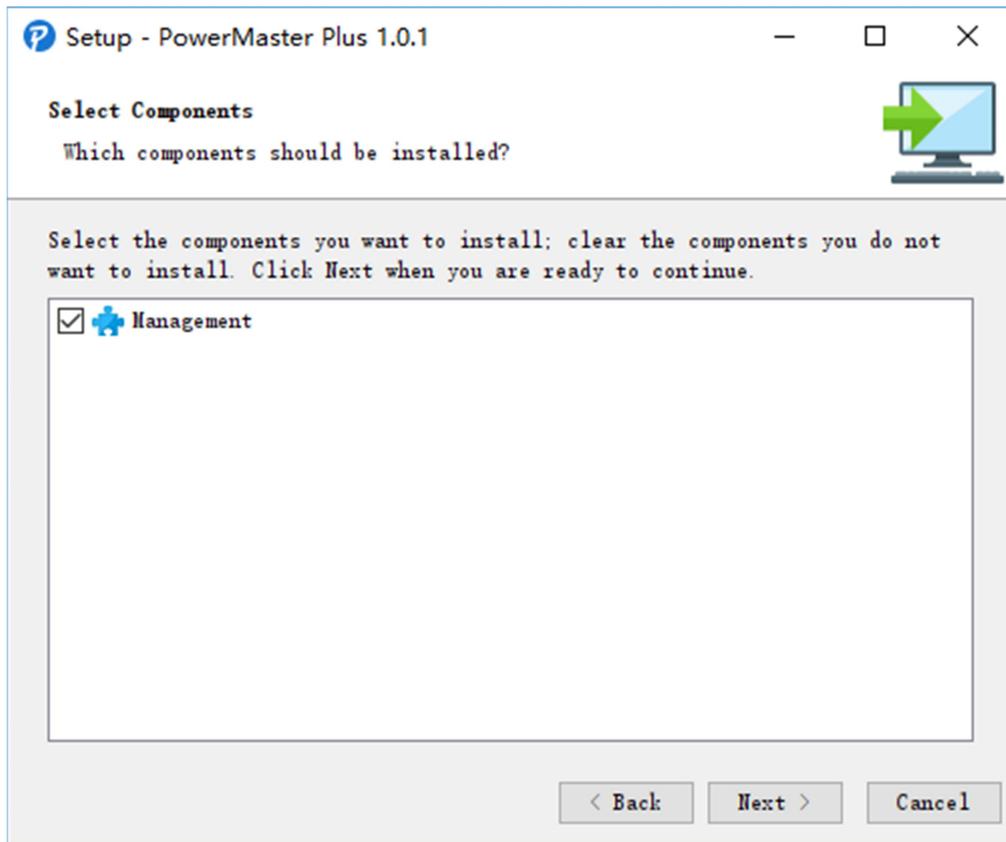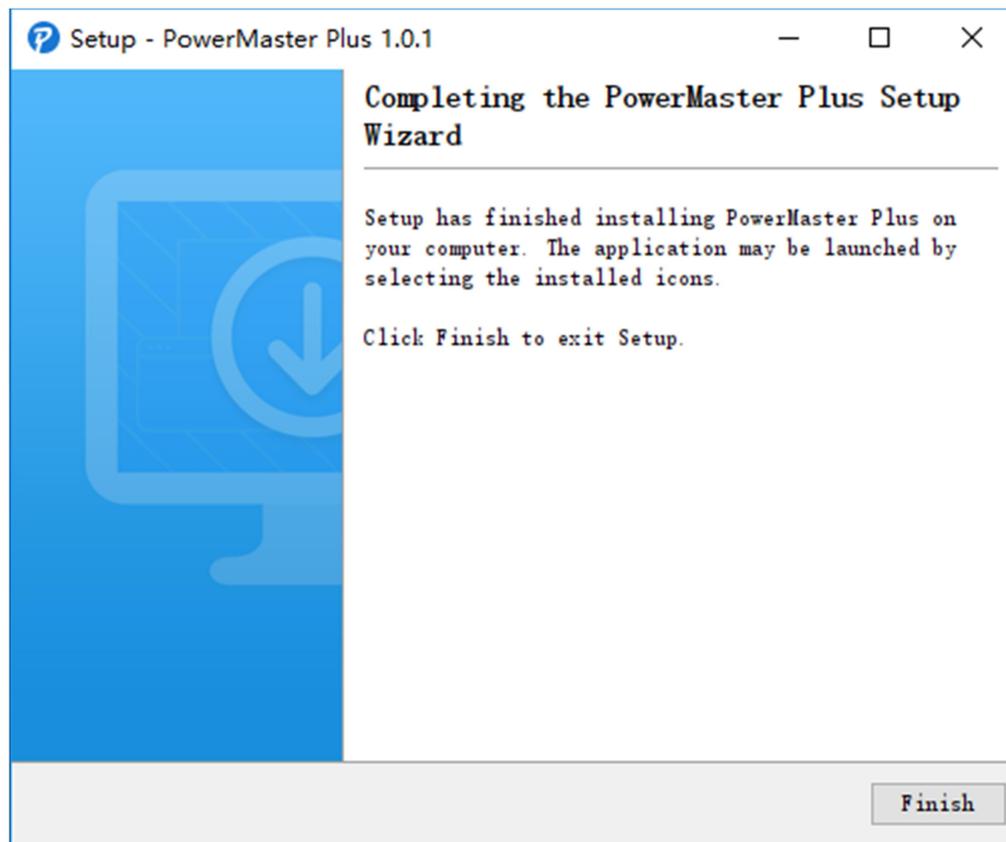
Click the Next button to start an installation.

● Select the destination directory.

● Choose the component. Power Master+ Management only contains one module. In this step, only Management can be selected.

- Click the Finish button to complete the installation.

2.2.3   Installation on Linux

After you have downloaded Power Master+ from Company Systems' website follow the setup installation wizard as described below. The installer is used to install the software and requires root permission. The installation wizard will guide users in completing the installation. Initiate the wizard by running the ./ppb-linux-

x86.sh command or double clicking ppb-linux-x86.sh on 32-bit systems or by running the ./ppb-linux-x86_64.sh command or double clickingppb-linux-x86_64.sh on 64-bit systems.

To install, follow below steps:

● Click the Next button to start an installation.

● Choose the destination directory.
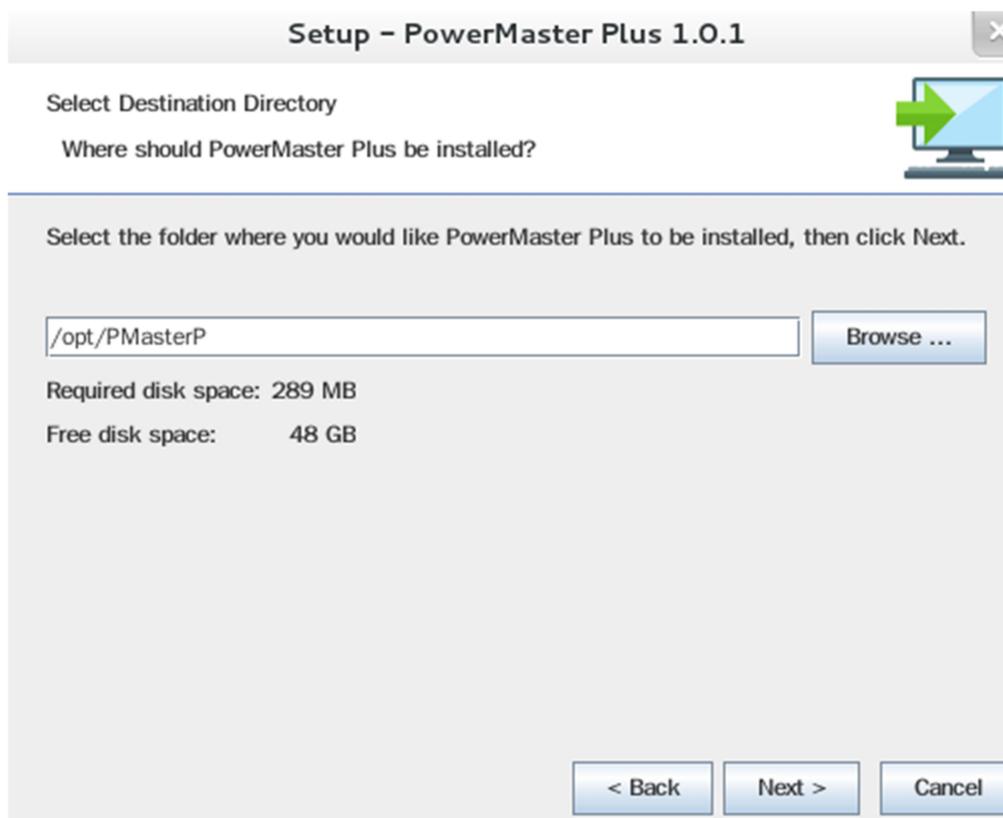
- Choose the component. Power Master+ Management only contains one module. In this step, only Management can be selected.
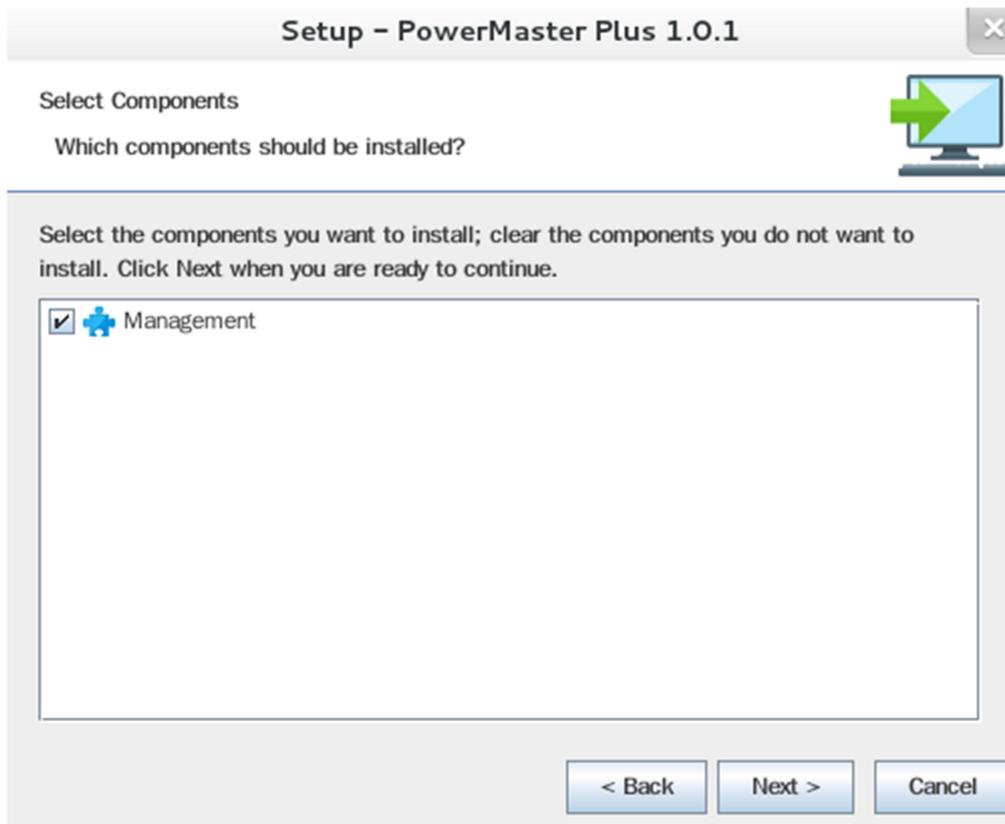
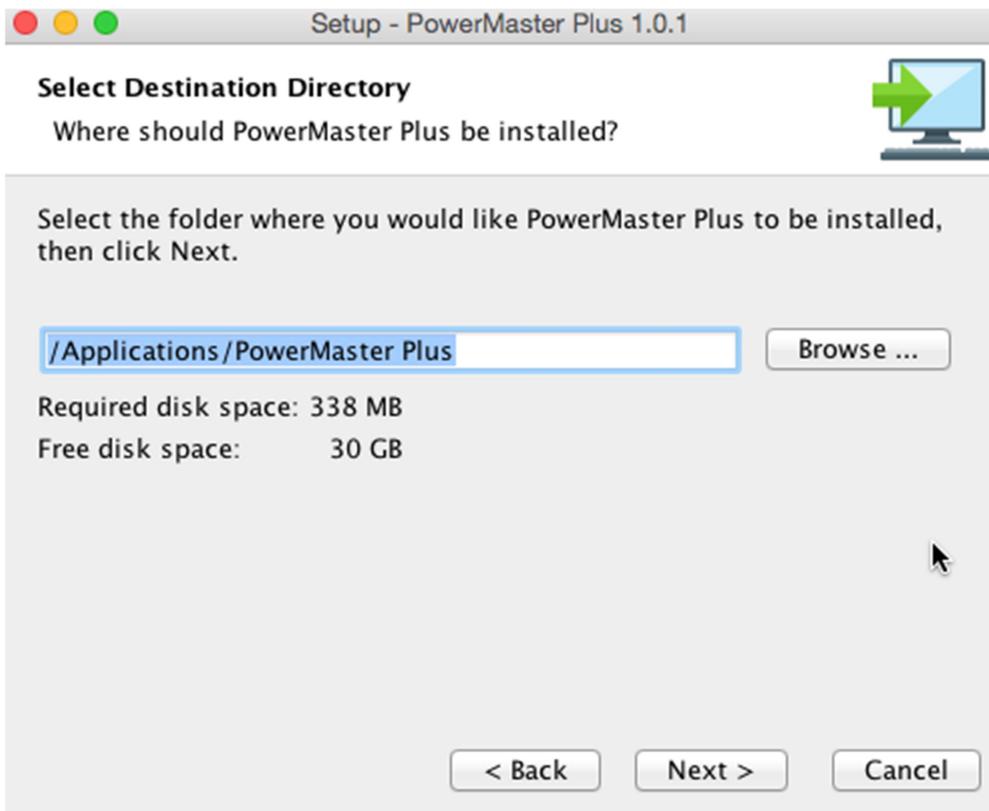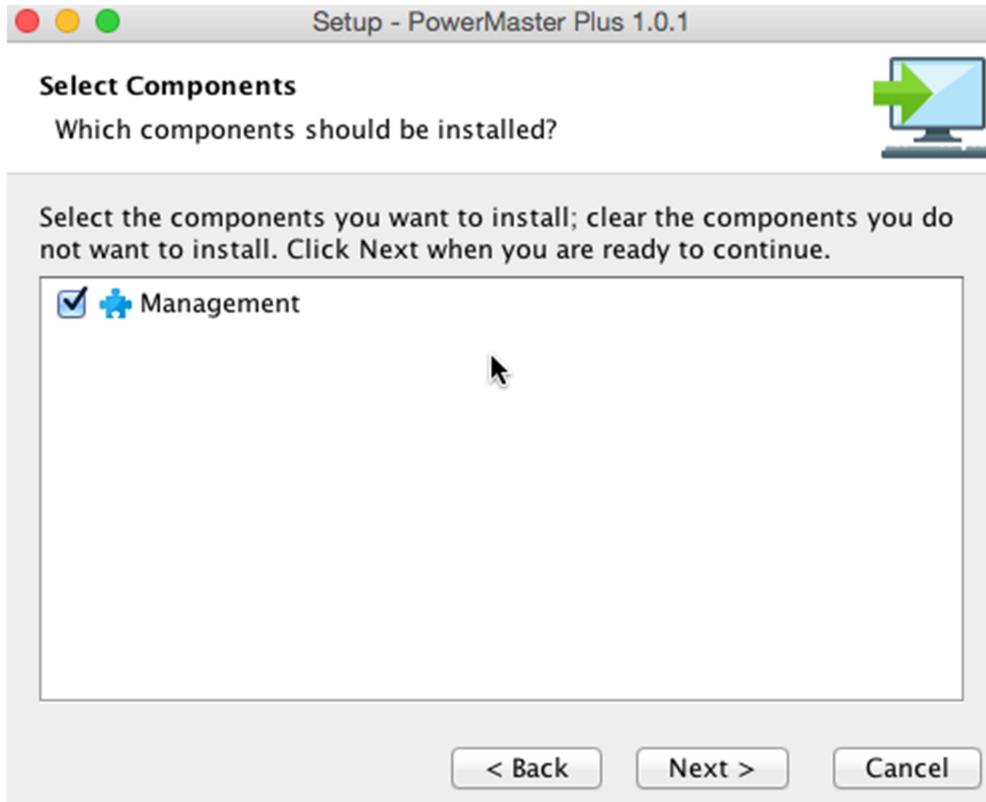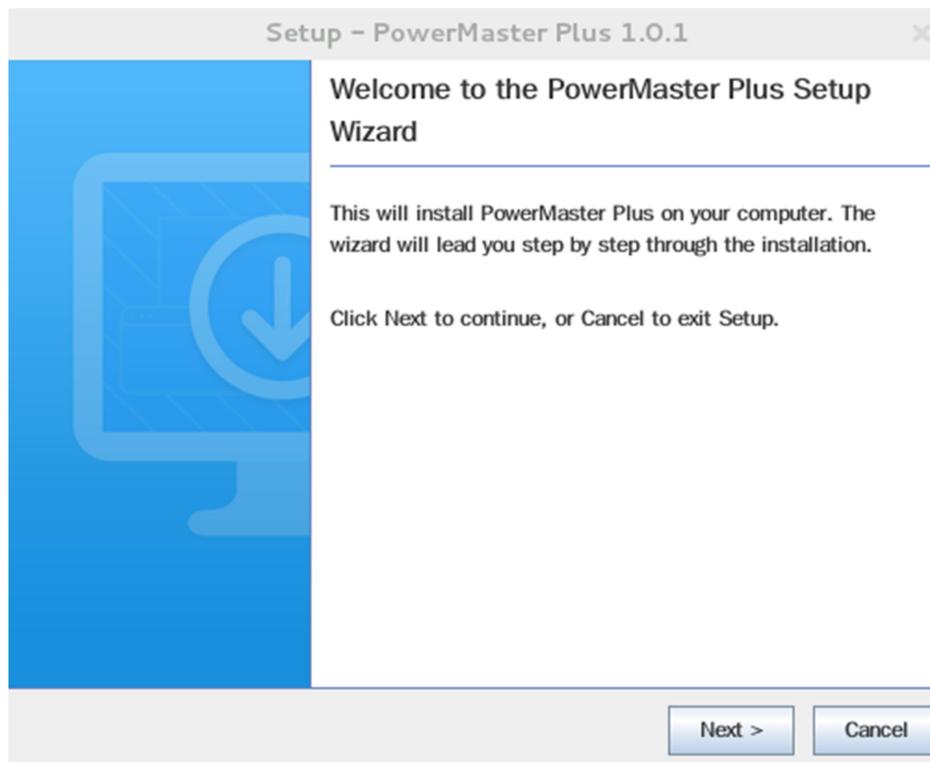- Click the Finish button to complete the installation.
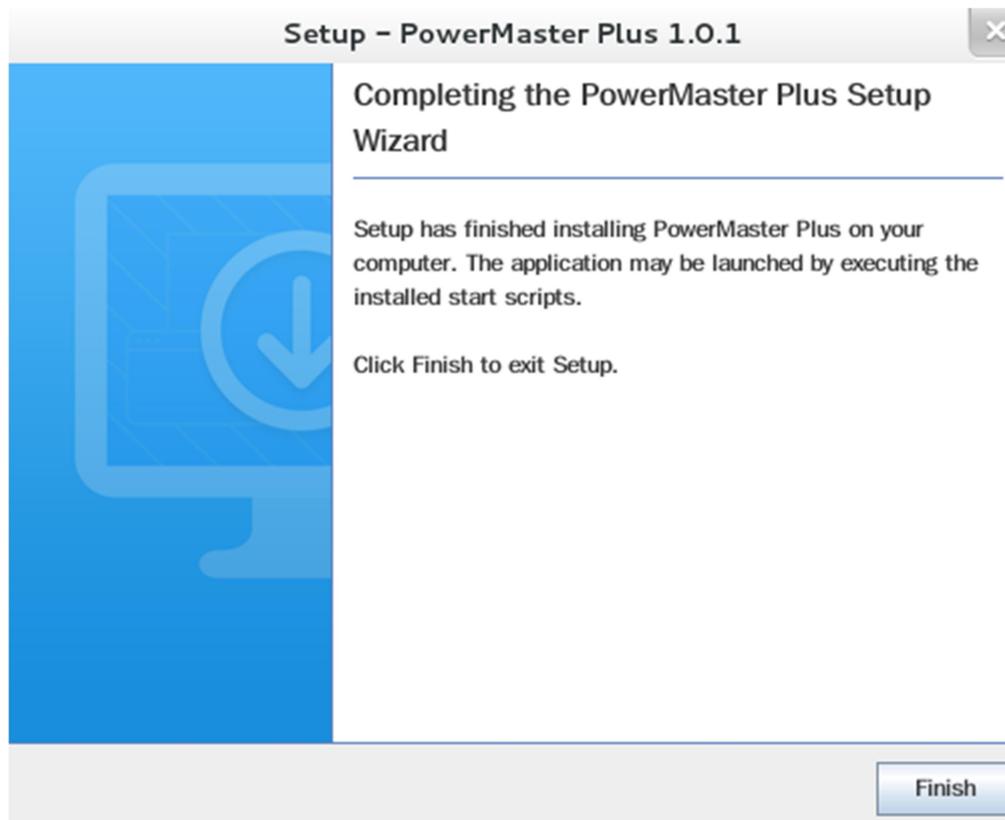
2.2.3.1　Installation in Text Mode

When the system does not support graphic mode, the Linux installation needs to be initiated in the terminal by using the ./ppb-linux-x86.sh-ccommand on 32-bit systems or use ./ppb-linux-x86_64.sh–ccommand on 64-bit systems.

The installation procedure will be initiated as following steps:

● Press Enter to start an installation.

```
Unpacking JRE ...
Starting Installer ...
This will install PowerMaster Plus on your computer.
OK [o, Enter], Cancel [c]
```

● Choose the destination location.

```
Select the folder where you would like PowerMaster Plus to be installed,
then click Next.
Where should PowerMaster Plus be installed?
[/opt/PMasterP]
```

● Choose the component. If one single computer is connected to the UPS directly via a USB or serial connection, Local should be installed. If the computer is powered by a UPS already connected to a Local, has a remote management card installed or is connected to a PDU, Remote should be installed.

Note: Local and Remote cannot be installed on the same computer.

```
Which components should be installed?
1: Management
Please enter a comma-separated list of the selected values or [Enter] for the de
fault selection:
[1]
```

● Installation procedure starts to process until the installation is complete.

```
Extracting files ...
                                                              Setup
 has finished installing PowerMaster Plus on your computer.

Finishing installation ...
```

2.3　Accessing Power Master+ Management

The Power Master+ Management web interface can be accessed following the directions below. To access the web interface on a local computer, select Start > All Programs >Power Master Plus>Power Master Plus Management in the Windows Desktop or enter the http://localhost:3052/management as the URL in the browser.

LaunchingPower Master+ software

On Linux, users can enter http://localhost:3052/managementin the address of the web browser to access the interface. Users can also enter the URL, http://localhost:3052/management in the local computer or http://hosted_computer_ip_address:3052/managementin the remote computer, to the address field of the web browser to access the Power Master+ software web interface. hosted_computer_ip_address is the IP address of the computer which has the Power Master+ software installed. For vMA on the ESX or ESXi, hosted_computer_ip_addressis the IP address of the vMA (Note:hosted_computer_ip_addressis the IP address of the host computer on ESX).

2.3.1 Login

The default username is admin and the password is admin. For security, it is recommended to change the username and password on the Web Browser Info /Account Information page after the initial login.
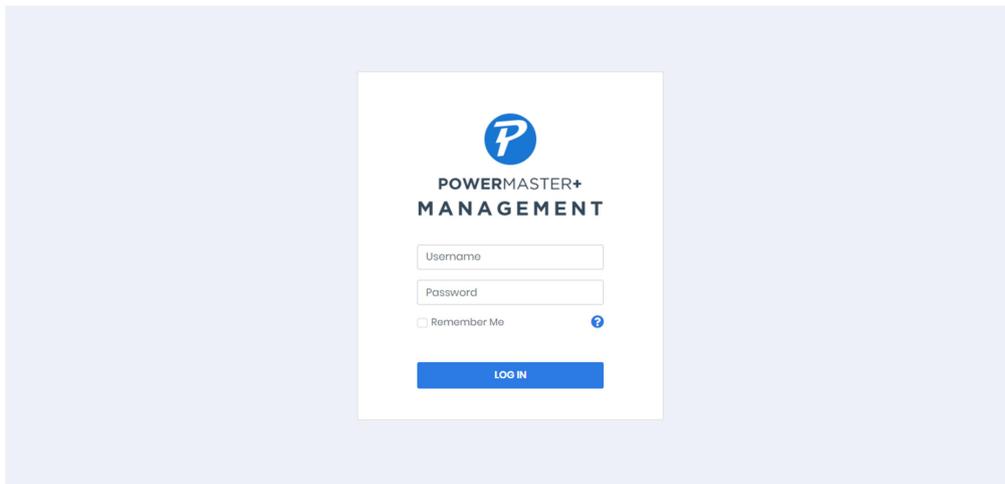
The login page

Selecting the Remember Me option on the login page allows the credentials to be remembered for automatic logon at the next session. To terminate the session, click the Logout button on the page. The session will timeout and you will be logged out if no activity takes place during the time of Session Timeout. The Session Timeout can be configured on the SETTING/Security/User page.

3 Using Power Master+ Management

3.1 DASHBOARD

DASHBOARD page provides the management of power equipment and infrastructures such as VMware virtualization. Below are the capabilities user can find in DASHBOARD page.

- Monitor status and events from a connected UPS/PDU/ATS.
- Issue commands to the UPS/PDU/ATSs such as a power off, power cycle or power restore.
- Request that the UPS perform a battery test, sound its alarm or mute the audible alarms.
- Manage equipment and computers which are powered by UPS units and PDUs, and order connected computers to shut down or a reboot.
- Manage grouped UPS/PDU/ATSs.
- Monitor the operating status from the infrastructures.
- Define detailed action setting for each event of the infrastructure's power source.
- Manage the service infrastructures.
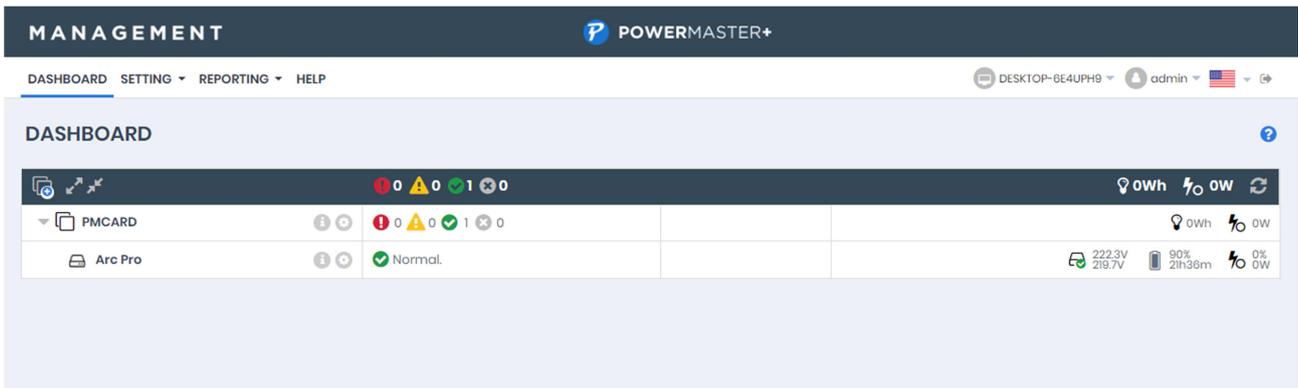
DASHBOARD page

3.1.1 Toolbar

The Toolbar provides information about the status of monitored devices and options to expand, add group or device.

Toolbar of DASHBOARD

These three buttons will allow users to add devices, expand or collapse all groups and device outlets.

	Add Device. Click this button then the *Add Device* dialogue box will appear. (The function is only applicable to the administrator and super administrator.)
	Expand All. This button will expand all groups and device outlets.
	Collapse All. This button will collapse all groups and device outlets.

The refresh button on the right side of the tool bar allows user to refresh DASHBOARD page.

⟳	Refresh. Click this button to refresh DASHBOARD page.

The other four icons indicate the amount of monitored devices that have had severe-level or warning-level events occur, the numbers of devices that have lost communication with Management and the number of devices that are normal.

⊘	Indicates severe-level power events such as *Runtime is insufficient.*
⚠	Indicates warning-level power events such as *Utility power failure.*
⊗	Indicates the devices which have lost communication with Management. Management cannot monitor or control computers and equipment when communication is lost.
✔	Indicates that there are no problems with these devices.

System will change the state according to the current power consumption of the entire system in past hour.

💡	Indicates the total power consumption of the entire system falls in a normal range.
💡↑	Indicates the total power consumption of the entire system exceeds the high threshold.
💡↓	Indicates the total power consumption of the entire system violates the low threshold.

System will change the state according to the current load of the entire system in past hour.

⚡○	Indicates the total load of the entire system is zero.
⚡◐	Indicates the total load of the entire system falls in a normal range.
⚡!	Indicates the total load of the entire system is overload.

3.1.2 Node Components

Each node has a name and an icon indicating what type it is. A UPS/PDU/ATS node provides detailed information about what power events have occurred and what the current status is.

The detail information for each node is available by clicking information icon ⓘ , and a context menu for each node is available by clicking setting icon ⚙ (The function is only applicable to the administrator and super administrator.). This allows users to view detailed information such as *Summary* or *Status,* or request operations such as *Shutdown* or *Restart.* A menu item becomes disabled when this operation is in progress or is not supported.
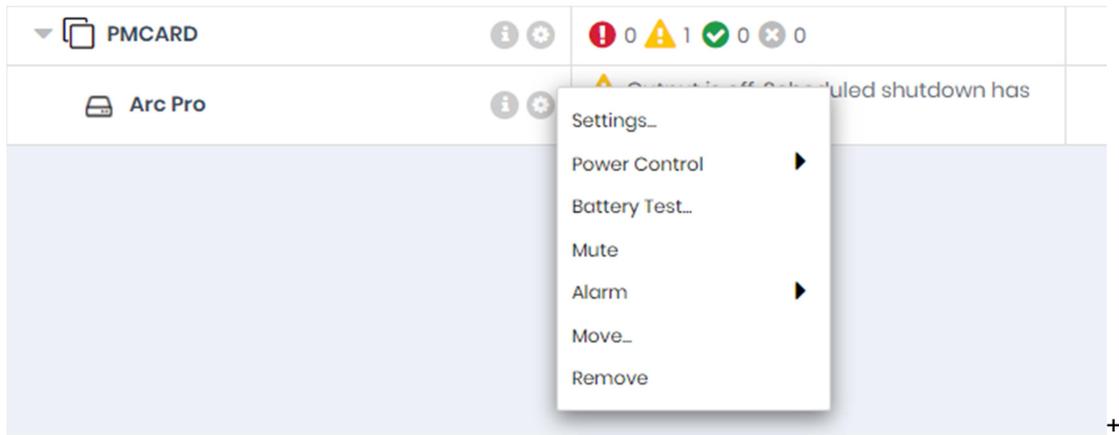
A context menu appears by accessing a device node.

Each node can be one of the following types:

	A Group.
	A UPS. This UPS may have an PMCARD or is connected to a computer which is controlled by Local.
	A UPS. A VMware vCenter server or VMware ESXi host is connected with this UPS.
	A PDU. This PDU may be set to connect to a monitored UPS.
	An ATS. This ATS may be set to connect with the UPS which could be monitored by Management.
	Indicates the computer connected with the UPS is a VMware ESXi host.
	Indicates that is a VMware vCenter server.
	Indicates that is a storage in a vCenter.
	Indicates that is a Cluster. The Cluster is included in a vCenter.
	Indicates that is a VMware ESXi host. The ESXi host may be included by a vCenter server.
	Indicates that is a vApp. A vApp is a group of virtual machines.
	Indicates that is a virtual machine running on the VMware ESXi server.

Each node also has a column that indicates what the current state is and what power events have occurred. The column in a UPS node displays power events such as *Utility power failure* or *Runtime is insufficient* event while the column in a PDU node displays power events such as *Input is low load* or *Input is overload.*

The UPS/PDU/ATS nodes display a brief operating status consisting of schedules, utility power, batteries, support load and outlets. The brief status column displays in gray when local or network communication has failed.

A UPS can have the following states:

🔋✓	Normal. The UPS is working normally.
🔋⚠	Power Failure. There is no utility power supplied to UPS.
	Bypass. The UPS has switched to bypass mode and is supplying direct utility power.
	Boost. The utility voltage is below the regular voltage and UPS is increasing the utility voltage.
	Buck. The utility voltage is beyond the regular voltage and UPS is decreasing the utility voltage.
	Test. A battery test is processing.

Batteries can have the following states when UPS is operating:

🔋✕	Not Present. Batteries are absent and there is no battery power.
🔋	Normal. Batteries are not being using.
	Charging. Batteries stops discharging due to a power event and are being charged.
	Discharging. The UPS is supplying battery power to its load.
	Fully Charged. Batteries are at 100% capacity.

UPS/PDU/ATSs have the following states according to their current load:

⚡○	No Load. There is no output load.
⚡◑	Low Load. The PDU is in a low load condition.
	Normal. The output power is normal.
	Near Overload. The PDU is near the overload condition.
⚡❗	Overload. Output consumption of equipment exceeds the rating load on UPS or the PDU is in an overload condition.

ATS have the following states on functioning:

🔌✓	ATS uses this input source as current source, and this source is normal.
🔌○	ATS uses this input source as redundant source, but this source is normal.
🔌❗	This power source of ATS is power failure.

The sensor on the UPS/PDU/ATS has the following states according to the environment temperature:

🌡	Normal. Indicates the temperature measured by the sensor is in a predefined normal range.
🌡↑	Overheated. Indicates the current temperature exceeds the high temperature threshold.
🌡↓	Undercooled. Indicates the current temperature violates the low temperature threshold.

The sensor on the UPS/PDU/ATS has the following states according to the relative humidity:

💧	Normal. Indicates the humidity as a percentage measured by the sensor is in a predefined normal range.

	Over wet. Indicates the current humidity exceeds the high humidity threshold.
	Dry. Indicates the current humidity violates the low humidity threshold.

A group has the following states according to the total power consumption:

	Indicates the total power consumption of the group falls in the normal range.
	Indicates the total power consumption of the group exceeds the high threshold.
	Indicates the total power consumption of the group violates the low threshold.

3.1.3 Power Device Management

(The contents in this section are only applicable to the administrator and super administrator.)

3.1.3.1 Add Device

In order to monitor and control power device UPS/PDU/ATS, these devices must be added to the Management by clicking Add Device button on the toolbar.

Add Device button on toolbar

The Add Device dialog will show up by clicking Add Device button.

Add Device dialog

All the devices already in Management will be shown on the list, choose the devices you want to add from the list then click SAVE button to complete. Click the refresh button to refresh the ⟳ device list. If the device you want to add is not on the list, go to page SETTING/Auto-Discover Range to edit the scan range. Please refer to SETTING/Auto-DiscoverRange for more details.

3.1.3.2　Move Device

Click the setting icon of the device you want to move and select Move in the context menu. A Move window will display and select the target group from the list. After selecting the target group, click SAVE to move the group.

3.1.3.3　Remove Device

Click the setting icon of the device you want to remove and click Remove in the context menu. Click SAVE to remove the device. When a device is removed, its powered computers and equipment will also be removed.

3.1.3.4　Change Settings

Click the setting icon of the device you want to change setting and click Settings in the context menu, a Setting window will appear. User can change the Name of this device or configure the proper thresholds to aware of violating consumption thresholds. Once the power consumption violates thresholds, Management will warn administrators of the violation. When the thresholds are set blank, Management will use the thresholds of the Default Energy in REPORTING/Energy Use/Settings page instead of the thresholds in Settings of each power device.

3.1.4　Power Device Details

UPS/PDU/ATS provides further information; this information will show up by clicking info icon of each device. This includes summary, status, information, UPS, and Energy.

Details of a UPS monitored by Local

3.1.4.1   Summary

The Summary tab provides an overview of the system information:

- Name: The name of the selected device.
- Status: Displays the present status of the selected UPS/PDU/ATS.
- Location: Where the UPS/PDU/ATS is located.
- Contact: Who to contact about the UPS/PDU/ATS.
- Address: The IP address of the UPS PMCARD, PDU or Local computer's network interface.
- PC and Equip.: The number of the powered computers and equipment.
- Outlets: The amount of outlets on the UPS/PDU/ATS.
- Outlet On: The outlets which are supplying power.
- Outlet Off: The outlets which are not supplying power.
- Power Source: The power source of the UPS, e.g. *Utility* or *Battery*.
- Remaining Runtime: The estimated amount of time remaining that the UPS can supply power, given its current load.
- Capacity: The capacity of the batteries expressed as a percentage of full charge.
- Statistics: Indicates the state of the device as *Normal*, *Severe*, *Warning* or *Lost*.
    - Severe: Devices with severe-level events such as *Overheat or Output is off*.
    - Warning: Devices with warning-level events such as *Utility power failure or Battery need replacement.*
    - Lost: Devices which have lost communication with Management.

- Type: The type of software the selected device is running, e.g. *Local*, *Remote* or *Equipment*.
- Current Source: Indicates which input source is being using and will be also annotated preferred or redundant source.
- Environment Sensor: Indicates whether the environment sensor has been installed on the UPS/PDU/ATS. Note: When the sensor cannot be detected anymore, it will be annotated *No Response.* Users can click the Uninstall to reflect it if it had been removed physically from the UPS/PDU/ATS.

3.1.4.2   Status

The Status tab displays details about the UPS/PDU/ATS.

- Current: The output current in Amps.
- Outlets: The status of each outlet on the UPS/PDU/ATS and the name of the connected computer or equipment.
- Input: Displays the status of the utility power supplied to the UPS.
- Voltage: The voltage of the utility power supplied to the UPS.
- Frequency: The frequency of the utility power supplied to the UPS in Hertz.
- Output: Displays the status of the output power that is being supplied to connected equipment.
- Load Consumption: The power draw of the connected equipment expressed as a percentage of the total load capacity. This displays as watts on some UPS models.
- Battery: Displays the status of the battery packs.
- Capacity: The capacity of the batteries, expressed as a percentage of full charge.
- Remaining Runtime: The estimated amount of time that the UPS can supply power to its load.
- System: Displays the operating status of the UPS.
- Envir. Temperature: Indicates the measured temperature from the environment sensor.
- Envir. Humidity: Indicates the measured humidity from the environment sensor.
- Contact: Indicates generic equipment connects to this sensor. Users can define the name and state in PMCARD web for each contact and monitor the state is normal.
- Source A Voltage: The voltage of the input power supplied to the source A of ATS.
- Source B Voltage: The voltage of the input power supplied to the source B of ATS.
- Load: The power draw of PDU/ATS supplying power to connected equipment.
- Bank # Load: The power of the PDU/ATS bank supplied power to the connected equipment.
- Bank # Current: The current of the PDU/ATS bank supplied power to the connected equipment.
- Phase: The phase information, including Name, Input Voltage and Current, of a 3-phase PDU.

3.1.4.3   Information

Information tab shows information about the UPS/PDU/ATS.

- Type: The type of the device, such as On-Line, Line Interactive or Sinewave Line Interactive for UPS; or Monitored or Switched for PDU/ATS.
- Model Name: The model name of the UPS/PDU/ATS.
- Firmware Version: The firmware version of the UPS/PDU/ATS**.**

- MAC address: The MAC address of the UPS PMCARD, PDU or Local computer's network interface.
- Serial Number: The serial number of the UPS.

  Note: This will give the internal serial number on some models.
- Power Rating: The Volt-Amp rating (VA) and power rating (Watts) of the UPS.
- Voltage Rating: The output voltage rating (Volts) of the UPS.
- Frequency Rating: The output frequency rating (Hz) of the UPS.
- Battery Replacement Date: The date that the batteries were last replaced. This should be set at the time of battery replacement. If this date has not been set, it is recommended that this date should be set immediately.
- External Battery Pack: The amount of external battery packs connected to the UPS.
- Outlets: The amount of outlets on the PDU/ATS.

3.1.4.4 UPS

The UPS tab shows the connected power sources of PDU/ATS, the IP address and Outlet of UPS.

3.1.4.5 Energy

The Energy tab shows the chart how to spend the energy in a specified period and also shows the energy statistics of the current target node and entire system.

Each UPS, PDU, ATS and outlet of Metered by Outlet PDU whose consumption will be logged per hour and each group which contains these UPS/PDU/ATS will work accumulating the consumption of data. These data which logged the consumption in the past can be gathered to render a chart in a past day, a past month, a past year and a past decade accordingly. Administrators will realize how much energy has been spent in a past period. Energy can be spent more efficiently and reduce the waste.

For PDU and outlets of Metered by Outlet PDU, the Peak Load value will also be recorded. Management will show the Peak Load value, the time when this value happens and the time when the Peak Value is reset.

3.1.5 Power Device Operations

(The contents in this section are only applicable to the administrator and super administrator.)

Management provides control functions for a UPS/PDU/ATS. Click the setting icon of each device or the outlet of this device, the context menu will show up.

3.1.5.1 Power Control

- Power Off: Click Power Off and a confirmation window will appear. Decide whether to perform an immediate or a sequenced power off then click OK to begin. When a UPS or a PDU initiates a sequenced power off, computers connected to the UPS/PDU/ATS that have Local or Remote installed

will initiate shutdown prior to the sequenced power off.

Note: A force power off will likely result in connected computers losing power.
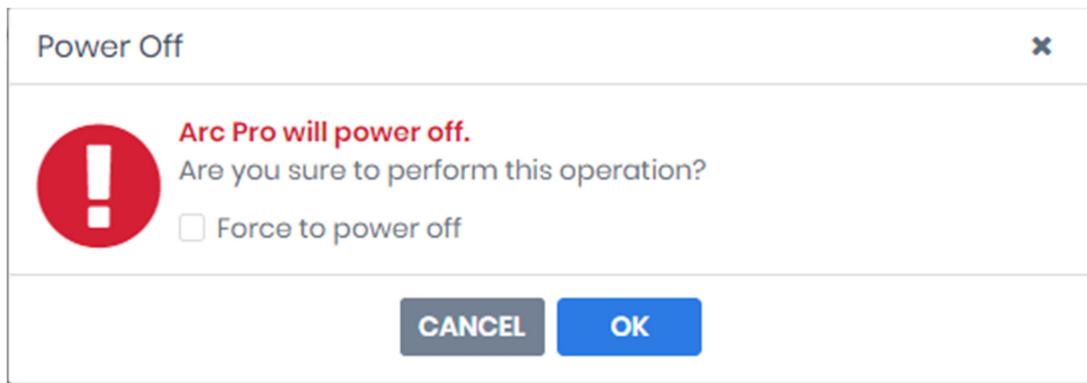
A confirmation window of a UPS power off operation

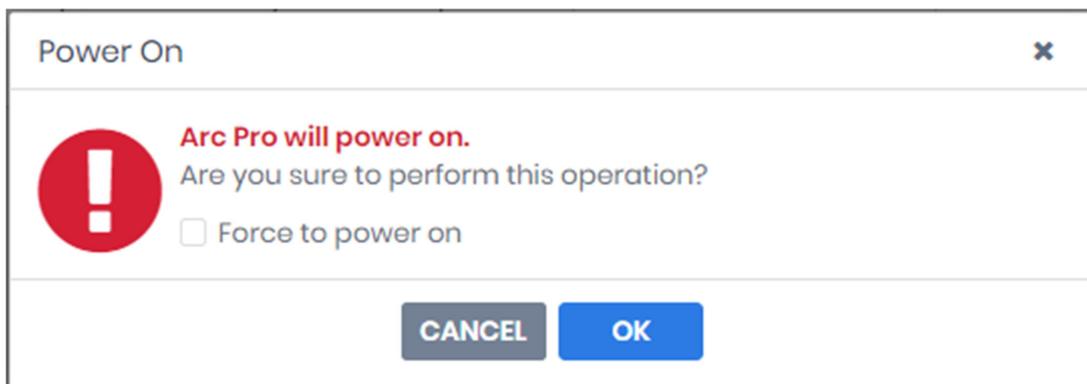- Power On: Click Power On to have the UPS/PDU/ATS turn on output power. Decide whether to turn on output power immediately or after a delay in the confirmation window. Click OK to begin.

  Note: Some computers require manual booting when a UPS or a PDU powers on. To change this, set the computers BIOS to boot when power is restored.

A confirmation window of a UPS power on operation

- Power Cycle: Initiates a Power Cycle on the UPS/PDU/ATS. This will turn the UPS/PDU/ATS off then back on or vice versa. Decide whether to initiate an immediate or a sequenced power cycle and click OK to begin. A sequenced power cycle will cause computers connected to the UPS/PDU/ATS that have Local or Remote installed to shut down prior to the power cycle.

  Note: A force power cycle off will likely result in connected computers losing power.
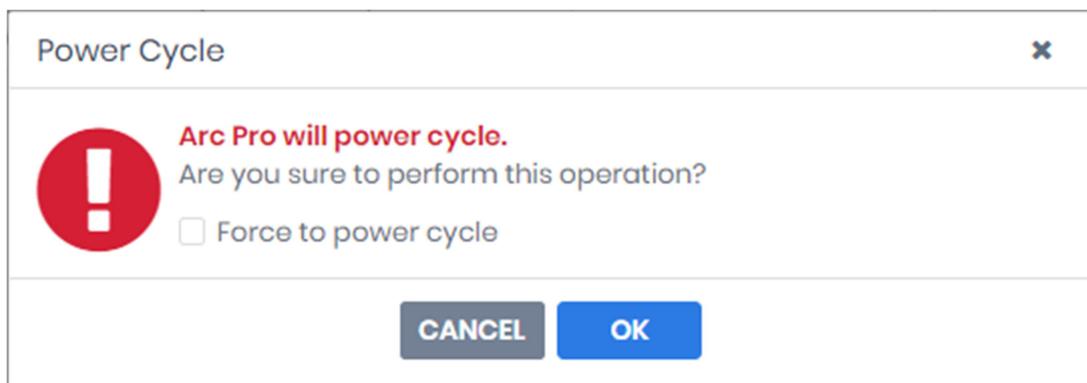
A confirmation window of a UPS power cycle operation

Note: If a PDU is connected to a UPS, a power off or a power cycle to the UPS may also cause all computers on this PDU to shutdown.

3.1.5.2   Battery Test

Click Battery Test from the context menu and the UPS will initiate a battery test.

3.1.5.3   Mute

Click Mute from the context menu to mute the alarm.

3.1.5.4   Alarm

Click Alarm from the context menu to enable or disable the UPS alarm.

3.1.5.5   Preferred Source

Click Preferred Source from the context menu to select which input source to be the primary one.

3.1.6   Infrastructure Management

(The contents in this section are only applicable to the administrator and super administrator.)

3.1.6.1   Add an Infrastructure

In order to monitor and control the VMware infrastructures, users can click the Add Devicebutton on the toolbar. An Add Device dialog will appear for users to add an infrastructure.

Add Device button on toolbar

The Add Device dialog will show up by clicking Add Device button. User can add VMware infrastructures in the section of Add Infrastructure. An "Add an Infrastructure" dialog will show up by clicking the Add button .Note: VMWare feature is not support ESXi free edition

Add Device dialog

Add an Infrastructure dialog

The detailed data is described below:

- Product: Specifies whether to add a vCenter server or an ESXi host.
- IP Address/Name: Configures the IP address or hostname for the vCenter server or the ESXi host.
- Port: Sets the port number for Management to access the vCenter host.
- Username: Sets the user name to access the vCenter server or ESXi host.
- Password: Sets the password for the username.
- Attach plugin to vCenter Server: Decides whether to attach a vCenter server plug-in. If this option is enabled, Management will install a plugin which expands the capability of vCenter server to present the Management web interface during establishing connection. After the plugin is installed, the vSphere Client interface will attach a new tab which displays Management web page.

Specify the product type and enter the necessary data. Press the SAVE button to add the infrastructure.

3.1.6.2　Update an Infrastructure

Click the setting icon of the vCenter server or ESXi host you wish to remove and select **Update** in the context menu, then the Update window will appear and allow you to configure the connection settings.

- Port: Sets the port number for Management to access the vCenter server.
- Username: Sets the user name to access the vCenter server or ESXi host.
- Password: Sets the password for the user name.
- Attach plugin to vCenter Server: Decides whether to attach a vCenter server plug-in.

Note: Changing the port, user name or password may cause communication loss with Management.

3.1.6.3　Remove an Infrastructure

Click the setting icon of the vCenter server or ESXi host you wish to remove and select **Remove** in the context menu. The Remove Infrastructure window will display. Click REMOVE to apply the removal.

If the plugin has been installed in vCenter server, the plugin will also be uninstalled during removal. If the infrastructure has been connected with the power device, the power source will also detach the infrastructure.

3.1.7　Infrastructure Details

The detail information of infrastructure will show up by clicking info icon of each node.

3.1.7.1　Summary

The Summary tab provides an overview of the infrastructure information:

- Virtual Machine: Indicates the selected infrastructure is virtual machines.

  - Name: The name of the selected virtual machine.
  - Status: Displays the present status of the selected virtual machine.
  - Address: The IP address of the virtual machine when the virtual machine is running.

- VMware vApp: Indicates the selected infrastructure is a VMware vApp.

  - Name: The name of the selected vApp.
  - Status: Displays the present status of the vApp.
  - VM Amount: The amount of virtual machines on the target vApp.

- VMware ESXi Host: Indicates the selected infrastructure is an ESXi host. It may be the ESXi host to which the selected virtual machine belongs.

  - Name: The name of the selected ESXi host.
  - Address: The IP address of the ESXi host.
  - Status: Displays the present status of the ESXi host.

- ■ Type: Specifies the node is ESX or ESXi host.
- ■ VM Amount: The amount of virtual machines on the target ESXi host.

- ● VMware Cluster: Indicates the selected infrastructure is a Cluster.

  - ■ Name: The name of the selected Cluster.
  - ■ Status: Displays the present status of the Cluster.
  - ■ DRS Status: Displays the present DRS (Distributed Resource Scheduler) status on the target Cluster.
  - ■ HA Status: Displays the present HA (High Availability) status on the target Cluster.
  - ■ ESXi Host Amount: The amount of ESXi hosts on the target Cluster.
  - ■ vApp Amount: The amount of vApps on the target Cluster.
  - ■ VM Amount: The amount of virtual machines on the target Cluster.

- ● VMware vCenter Server: Indicates the selected infrastructure is a vCenter server. It may be the vCenter server to which the selected ESXi host or selected virtual machine belongs.

  - ■ Name: The name of the selected vCenter server.
  - ■ Address: The IP address of the vCenter server.
  - ■ Status: Displays the present status of the vCenter server.
  - ■ ESXi Host Amount: The amount of the ESXi hosts of the target vCenter server.

- ● Storage: Indicates the selected infrastructure is a Storage.

  - ■ Name: The name of the selected Storage.
  - ■ Type: Specifies it is local or shared Storage.
  - ■ Status: Displays the present status of the Storage.

- ● UPS: Displays detailed information of the UPS which is supplying power to the selected infrastructure.

  - ■ Name: The name of the UPS.
  - ■ Address: The IP address of the UPS.
  - ■ Outlet: Indicates the outlet number and what the bank type of connected outlet.
  - ■ Status: Displays the present status of the UPS.

Note: Not each infrastructure provides the same information. The information will vary depending on infrastructure.
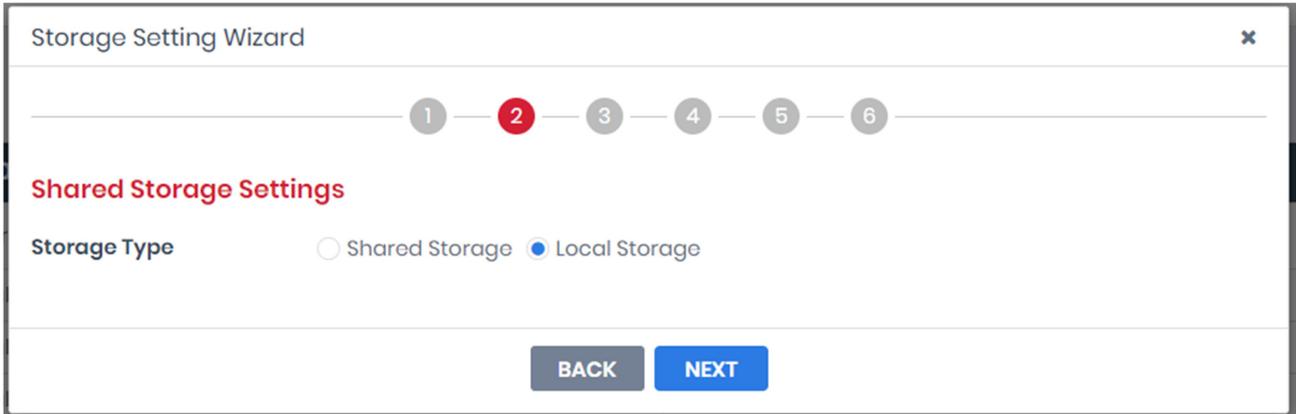
3.1.8 Infrastructure Setting Wizard

(The contents in this section are only applicable to the administrator and super administrator.)

Click Settings in context menu of root ESXi host (an ESXi host which is not under a vCenter server), Cluster, and Storage, a setting wizard will pop up. In the setting wizard, users can configure the Power Source, Shutdown Settings, and Event Action.

3.1.8.1   Shared Storage Setting

This step is only for Storages. Storages can be set as Local Storage or Shared Storage at this step, and only Shared Storage can be configured with power protection, shutdown settings and event action.

Shared Storage Settings Wizard page of Storage

3.1.8.2   Power Source Setting

The Power Source step in the setting wizard allows you to connect or disconnect the infrastructure with the target UPS. Users can choose each infrastructure from the Infrastructure column and set power source correctly respectively, only the infrastructure set with proper power source will be protected.

Only root ESXi hosts, Clusters and shared Storages can be set with power protection. In order to make sure that the infrastructure can be protected, you should connect the infrastructure to the target UPS by assigning the correct UPS.
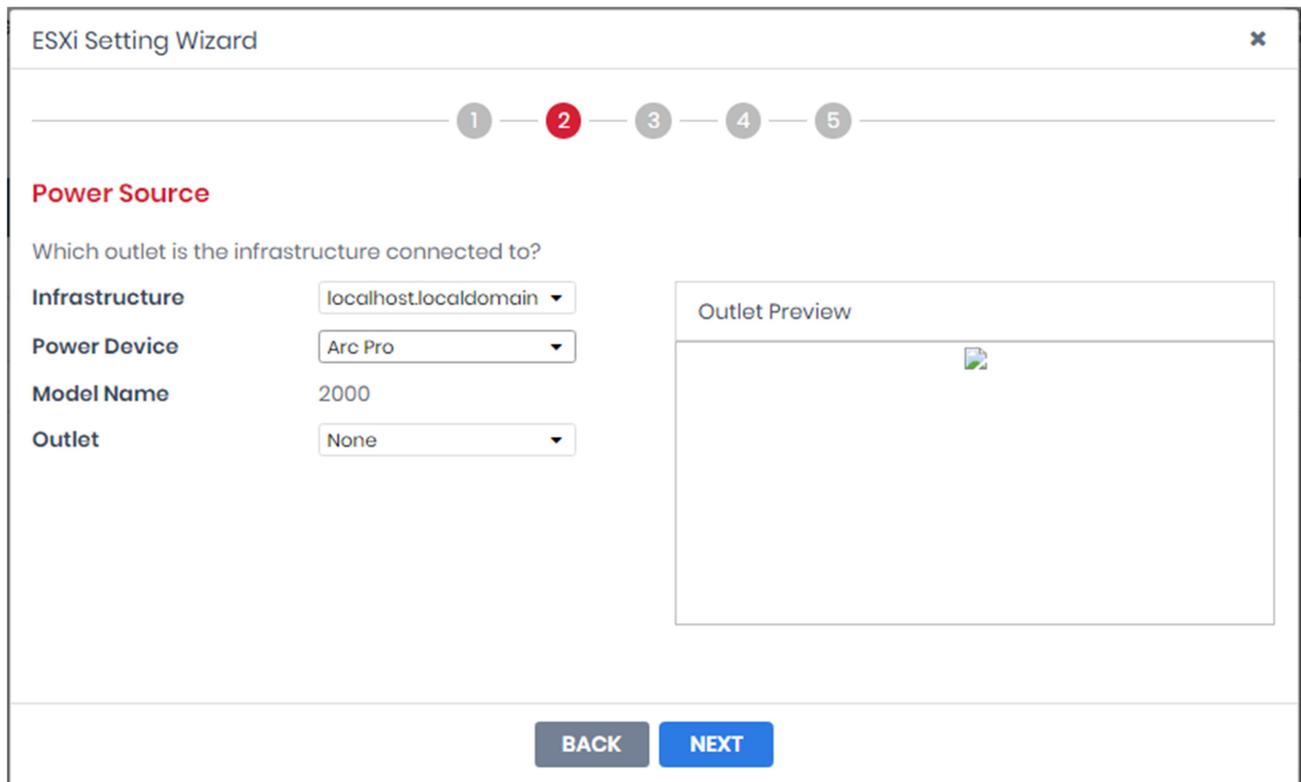
Power Source setting page of Cluster

In order to make sure that vCenter servers can be protected, you should complete the following steps according to your environment:

- If the vCenter server is a virtual appliance which has been deployed on the ESXi host, the ESXi host should also be added to the Service Infrastructure page. Connect the ESXi host with the UPS.
- If the vCenter server is running on a standalone Windows system, it is recommended to install Power Master+ Local or Remote to setup power protection.

Note:The only allowable power source for Service Infrastructure settings is a UPS system.

3.1.8.3 Shutdown Settings

The Shutdown Settings step configures the shutdown behavior and the necessary shutdown duration for vApp, virtual machine and ESXi host. Moreover, virtual machine migration can also be set in this step.

Shutdown Settings page of Cluster

- Virtual Machine Migrationisset if virtual machines migrate to other hosts when power events happen. The necessary migration duration for all virtual machines can also be set here. This option is available in theCluster Settings Wizard.
- vApp Shutdownconfigures the shutdown of vApp and also the necessary shutdown time for all vApps.
- Virtual Machine Shutdown configures the shutdown of a virtual machine and also the necessary shutdown time for all virtual machines.
- ESXi Shutdownconfigures the shutdown of an ESXi host and the necessary shutdown time for all ESXi hosts.

3.1.8.4   Event Action

When an ESXi host, Shared Storage or Cluster has the power source configured properly in the aforementioned section, Management can send the notification to the administrator and initiate a shutdown sequence if the event occurs.

Event Action setting page of Cluster

The Event Action step lists all events and allows users to configure the shutdown delay time for each event. Each event in the Event Action step will use the identical *Shutdown for Infrastructure* setting to the according event in the Event Action/Eventspage. When users change the shutdown delay time, the identical setting of the according event will be also changed.

After the *Custom* option is enabled, the selected event will be configurable. Users can change the shutdown delay time for each event and click NEXTto apply the setting. When the event occurs, Management will take the new shutdown delay time instead of the default one that can be configured in the Event Action/Eventspage.

3.1.8.5   Alarms for vCenter Server and ESXi Host

The vSphere includes the user-configurable events and alarms system. The alarm system logs the events happening throughout the vSphere and allows users to specify the conditions under which alarms are triggered. Alarms are notifications which are activated in response to events.

The Management will specify the alarm definitions for the vCenter servers and ESXi hosts selected in the inventory after the power source has been configured properly. When the power event occurs, the alarms will be issued from the Triggered Alarmsview under the Alarmtab.

The Management defines the below alarms and issues the alarm when its related events are triggered:

Alarm Definition	Description	Triggered Event	Trigger Level
PM UPS Communication Event	Alarm is triggered when Power Master+ lost communication with UPS.	Communication lost with UPS in battery mode.	Alert
		Communication lost with UPS.	Warning
		Communication established.	Normal
PM UPS Critical Event	Alarm is triggered when a critical UPS event occurs.	UPS Low battery.	Alert
		UPS Remaining runtime exhausted.	Alert
		UPS Utility power failure.	Warning
		UPS Power restored.	Normal

For example, when the utility power fails, a warning-level alarm whose name is PM UPS Critical Event will be issued in the Triggered Alarmsview under the Alarmtab. A related event will be logged in the Eventsview of the Tasks & Events tab.

Note: Triggered alarms are visible through the vSphere Client or vSphere Web Client connected to a vCenter server.

3.1.9   Group Management

(The contents in this section are only applicable to the administrator and super administrator.)

UPS/PDU/ATSs and infrastructure nodes can be grouped for easy management. Orders can then be issued to multiple devices in a group.

3.1.9.1   Add Group

Click Add Group button "+"on the Add Device dialog to create a new group after clicking Add Device button on the toolbar.

Add Group button on toolbar

You can also choose parents-group in the New Group dialog. Enter the new group name and choose the group under which the new group is, and then click SAVE button to add a new group.

New Group dialog

3.1.9.2 Edit Group

Select Edit from the context menu, an Edit Group window will appear. User can edit group name, edit devices and infrastructures nodes in the group, and set Energy Consumption Threshold of this group in the edit windows.

Edit Group dialog

3.1.9.3   Move Group

Click the Setting icon of the group you wish to move and select Move in the context menu. Select the target group from the list in the Group Move dialog. After selecting the target group, click SAVE to move the group.

3.1.9.4   Remove Group

Click the Setting icon of the group you wish to remove and select Remove from the context menu. The GROUP Remove window will open; click REMOVE to remove this group. Removing a group will not remove the sub-groups or the UPS/PDU/ATSs belonging to this group. These items will be moved to the main group.

3.1.10 Group Details

Click the information icon of the group, a detail windows will show up. User can find Summary and Energy details in that window.
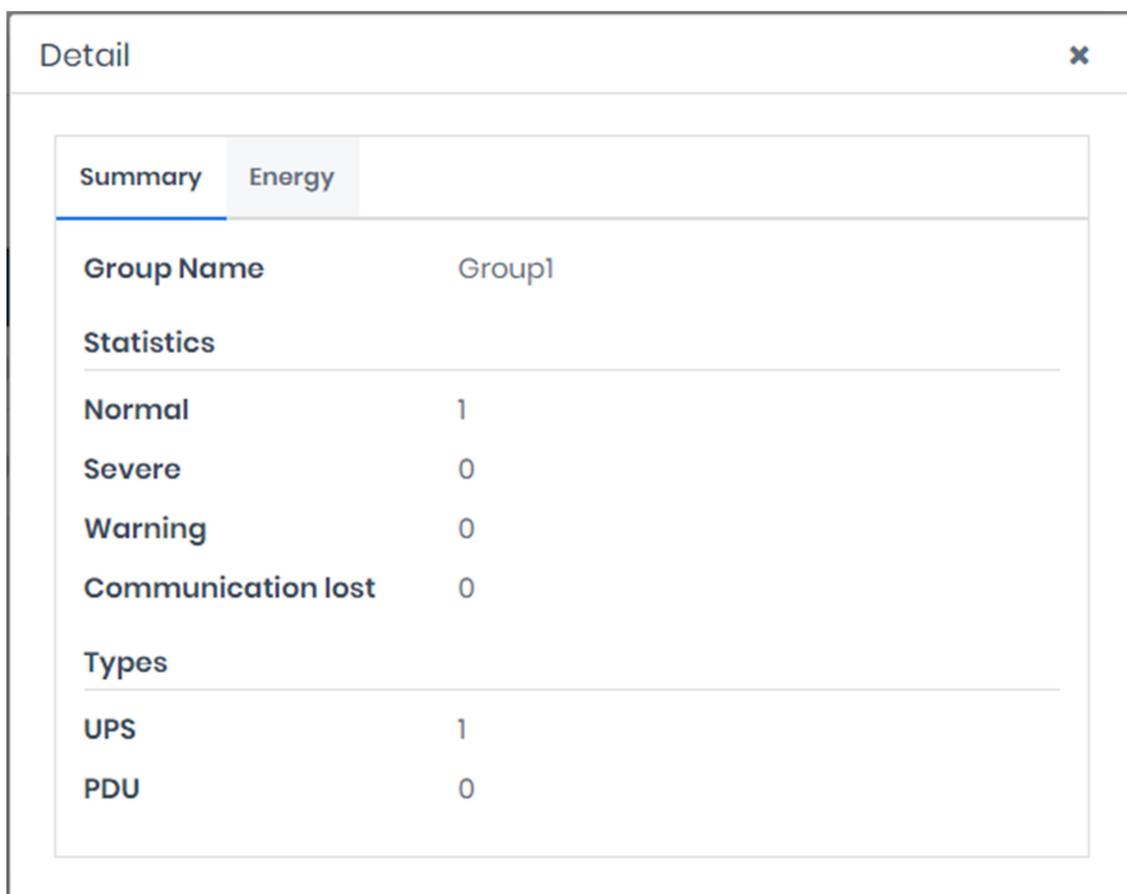
Summary tab of Details

3.1.10.1 Summary

Each group provides the statistics of all UPS/PDU/ATS from the Summary tab of Details and includes the following summary information:

● Group Name: A name of the selected group.
● Statistics: Indicates statistics about the operating conditions of the UPS/PDU/ATS:

- ■ Normal: Indicates a UPS/PDU/ATS which is normal.
- ■ Severe: Indicates a UPS/PDU/ATS with severe-level power events such as *Runtime is insufficient.*
- ■ Warning: Indicates a UPS/PDU/ATS with warning-level power events such as *Utility power failure.*
- ■ Communication Lost: Indicates a UPS/PDU/ATS which has lost communication with Management.
- Types: Indicates the statistics of UPS/PDU/ATS.

3.1.10.2 Energy

The Energy tab shows the chart how to spend the energy in a specified period and also shows the energy statistics of the current target group.

3.1.11 Group Operations

(The contents in this section are only applicable to the administrator and super administrator.)

Some or all devices in a group can have the following commands issued to them:

3.1.11.1 Computers on Outlets

- Shutdown/Restart: Select Shutdown or Restart from the context menu of the selected group and a pop-up window will appear. Pick the computers to shut down or restart from the list. Click OK to initiate the shutdown or restart.
  Note: If a group contains the UPS systems which have connected with PDU units, shutting down the selected group may cause the computers shutdown on these PDU units.

3.1.11.2 Power Control

- Power Off: Click Power Off and a confirmation window will appear. Pick the UPS/PDU/ATS from the list and decide whether to perform an immediate or a sequenced power off. Click OK to begin. When the UPS/PDU/ATS initiates a sequenced power off, computers with Local or Remote installed will initiate a shutdown prior to the sequenced power off. An immediate power off will likely cause those lose power.
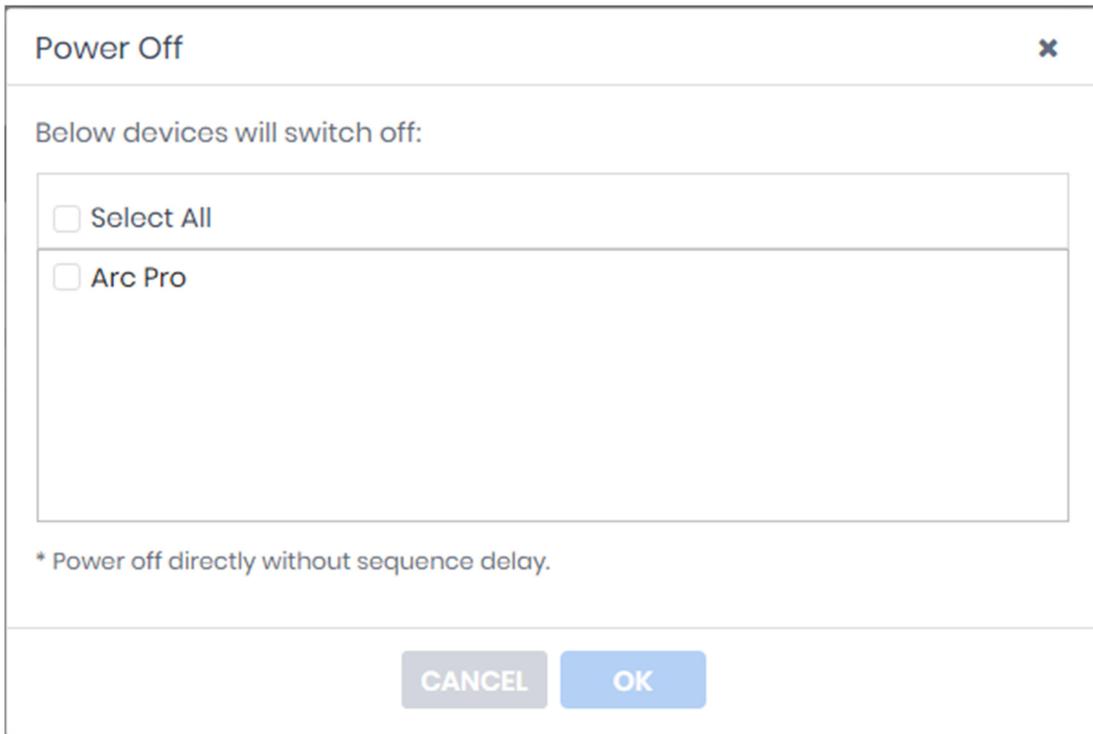
A confirmation window of a bulk power off operation

- Power On: Click Power On and a popup window appear. Pick the UPS/PDU/ATS from the list and determine whether to perform an immediate or a sequenced power on. Click OK to begin.

  Note: Some computers require manual booting when a UPS or a PDU powers on. To change this, set the computers BIOS to boot when power is restored.
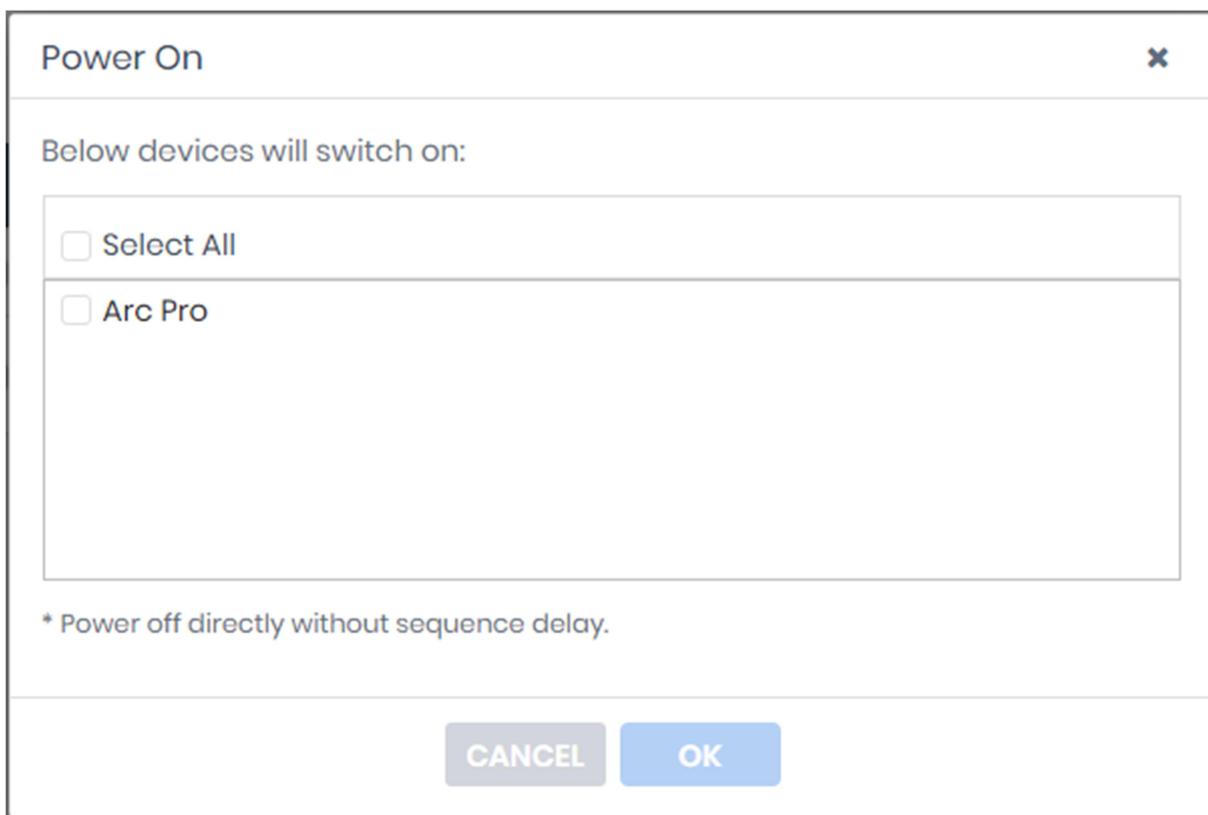
A confirmation window of a bulk power on operation

- Power Cycle: Click Power Cycle and a popup window appear. Pick the UPS/PDU/ATS from the list and determine whether to perform an immediate or a sequenced power cycle. Click OK to begin.
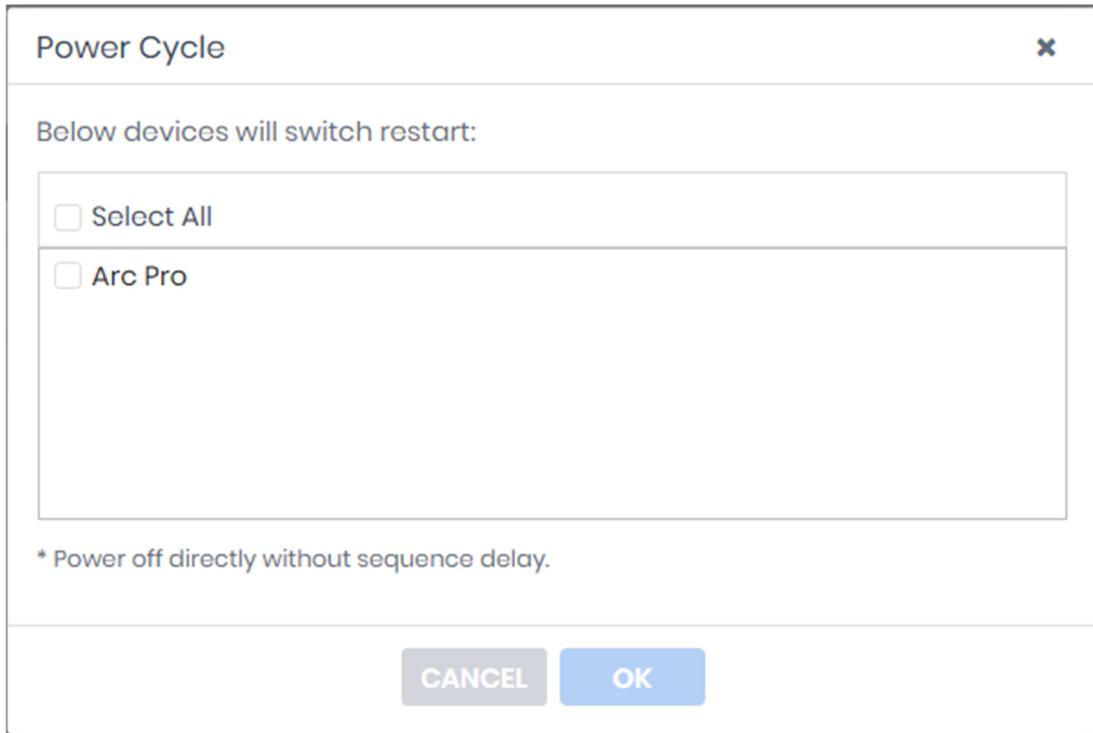
A confirmation window of a bulk power cycle operation

Note: If a group contains the UPS systems which has connected with PDU units, a power cycle or a power off to the selected group will result in computers shutdown on the PDU units.

3.1.11.3 Battery Test

Only UPS units can perform a battery test. Click Battery Test from the context menu of the selected group. All UPS units in that group will be listed in the confirmation window. Click OK to initiate the battery test on all selected UPS units.

3.1.11.4 Mute

Click Mute from the context menu to mute the alarm.

3.1.11.5 Alarm

Click Alarm from the context menu to enable or disable the UPS alarm.

3.2 SETTING

(The contents in this section are only applicable to the administrator and super administrator.)

3.2.1 Shutdown Events

An event is generated when the UPS/PDU/ATS encounters specific power conditions. The SETTING/ Shutdown Events page lists events that can be configured to shut down infrastructures. A shutdown sequence is only initiated by events specific for the target ESXi host.

● Shutdown: Determines whether to request the target ESXi host to be shut down and the delay before initiating the shutdown sequence. The shutdown will be canceled if the event is cleared during this delay time. The minimum delay time to initiate shut down is based on the time set for the execution of the notification to complete. This includes the notify delay time.

Note: The Management will use the Shutdown setting of each event here as the default shutdown delay time for each according event listed in the Event Action step of setting wizards of infrastructures. Refer to Event Actionsection for further details.

3.2.2 Notifications

An event is generated when the UPS/PDU/ATS encounters specific power conditions. The Management can monitor multiple power devices and computers and can be configured to notify users based on the event. The SETTING/Notifications page lists events and divides these events into several categories. Each event is allowed to configure the individual notification settings. The severity of each event is marked by a symbol.

The administrator can be notified when an event occurs. See SETTING/NotificationChannelspage for more details about the notification methods and recipient assignment. Use these parameters bellow to configure actions for individual events.

● Send: Determines whether to send a notification or not and sets the notification delay. If the event is cleared within the notification delay, the notification of the occurrence and the event cleared notification will not be sent.
● Repeat: Determines whether to send one additional notification after the initial notification. Only events which are of severe-level and warning-level type support a repeat notification.

3.2.3 Notification Channels

The administrator can be notified when an event occurs. In SETTING/NotificationChannelspage,users can configure several notification methods.

3.2.3.1 E-mail

● Service provider is *Gmail*:

Select the Gmail option at the *Provider* field. Click the CONNECT button to ask Google to authorize the Gmail account for an authorization to send an email notification. Fill the sender name and click Apply to save the settings.

Email service - Gmail

- Service provider is *Other*:

Select the Other option at the *Provider* field. Complete all details of E-mail account, and fields are explained below:

Email service

- Enabled: Specify whether the Local/Remote can use E-mail to send an email notification to recipients.
- Provider: Select the service provider of E-mail account.

- SMTP server address: Configure the SMTP server that will be used to send E-mail to a recipient's mailbox.

- Connection Security: Sets which secure connection for the SMTP service to send the E-mail.

- Service port: Sets the port number for the SMTP service to use.

- Sender name & Sender E-mail address: Configure the sender information for the E-mail.

- Authentication: Configure whether the SMTP server requires authentication or not. If authentication is required complete the necessary account and password field.

- Username: Sets the account to access the SMTP server.

- Password: Sets the password for the account.

3.2.3.2   Short Message Service (SMS)

Short Message Service (SMS) is a communication service used by mobile communication systems, using standardized communications protocols allowing the interchange of short text messages between mobile devices.

The Local/Remote sends mobile text messages to a receiver's mobile phone using an online SMS service. Users can choose Clickatell as a platform to send SMS or any SMS provider which sends a message via E-mail or HTTP. All account information and E-mail/HTTP specification must be acquired from the service provider before using SMS. The different SMS providers are described below:

- Provider is *Clickatell*:
  Select the Clickatell option at the *Service Provider* field. Complete all the account details from Clickatell with the *Username*, *Password* and *HTTP API ID* fields. The Verify function can be used once the *Activate>YES*option is checked and this option is selected and parameters are applied.

SMS(Short Message Service) service

- Provider accepts *HTTP POST* to send messages:

  This specification from an SMS provider is required before using the HTTP POST method to deliver messages to SMS providers. Select the Using HTTP POST option at the *Service Provider* field. Insert EVENT_ACTION_PHONE_NUMBER as recipient's mobile phone number and EVENT_ACTION_MESSAGE as the event message content described in the specification, and fill in the *URL* and *POST BODY* fields. The expressions will be replaced by the relevant content before the Local/Remote sends a notification to the SMS provider.

  e.g.

  > URL:*http://send-sms-company.com/sms*
  >
  > POST Body:*user=xxxxxx&password=xxxxxx&to*=EVENT_ACTION_PHONE_NUMBER
  >
  > *&text*=EVENT_ACTION_MESSAGE

- Provider accepts *HTTP GET* to sends messages:

  This specification from the SMS provider is required before using the HTTP GET method. Select the Using HTTP GET option at the Service Provider field. Insert the EVENT_ACTION_PHONE_NUMBERas recipient's mobile phone number and the EVENT_ACTION_MESSAGE as event message's content described in the specification, and fill in the *URL* field. The expressions will be replaced by relevant content before the Local/Remote sends a notification to SMS provider.

  e.g.

URL:*http://send-sms-company.com/sms?user=xxxxxx&password=xxxxxx&to*=EVENT_ACTION_PHONE_NUMBER*&text*=EVENT_ACTION_MESSAGE

- Provider accepts*E-mail* to send messages:

This specification from an SMS provider is required before using the E-mail to deliver the messages to SMS providers. Select the Using E-mail option at the *Service Provider* field. Insert EVENT_ACTION_PHONE_NUMBER as recipient's mobile phone number and the EVENT_ACTION_MESSAGE as event message content described in the specification. Fill in the *Address*, *Subject* and *Content* fields. The expressions will be replaced with relevant content before the Local/Remote sends a notification to the SMS provider.

e.g.

Address: *sms@send-sms-company.com*

Subject: *xxxxxx*

Content: *user:xxxxxx*

password:xxxxxx

*to:*EVENT_ACTION_PHONE_NUMBER

*text:*EVENT_ACTION_MESSAGE

Note: Each message sent by the SMS system through the SMS provider will be subject to the SMS provider fee.

3.2.3.3   XMPP Instant Massager

The XMPP (Extensible Messaging and Presence Protocol) is an open protocol for instant messaging. Users can setup the configuration to receive instant messages when an event has occurred. Users may contact a network administrator to verify if there is a XMPP Instant Messaging server in the network. If there is no XMPP Instant Messaging server, Google talk service can be used. Google Talk software can be downloaded and installed or Gmail can be used to receive event notifications via Google Talk. A local network XMPP Instant Messenger server can be setup by downloading open source XMPP Instant Messenger server software, such as Openfire. More server software information can be found on XMPP server software list.

XMPP Instant Messager service

To use XMPP Instant Messaging, users must provide a unique XMPP Instant Messaging Service account as a sender and assign different account as a receiver on Event Action/Notification Recipient page.

- Enabled: Specifies whether the Local/Remote XMPP Instant Messaging service to notification is active or inactive.
- Service address: Sets the XMPP server address according to your XMPP Server configuration. Select Google Talk to use predefined settings for Google Talk service.
- Service name: Sets the service name on an XMPP Instant Messaging server. This option is usually not required. Contact the systems administrator of the server for the service name if required.
- Service port: The port number which the XMPP Instant Messaging server will use.
- Username: Sets the account to access the XMPP Instant Messaging server.
- Password: Sets the password for the account.

Note: In order to make sure that the sender can send the XMPP notification to recipients, recipients should accept the invitation from sender.

3.2.3.4 Remote Desktop Services

Remote Desktop Services

Remote Desktop Service only works on Windows platforms. Options are explained below:

- Enabled: Specify whether to use this service to send a notification to recipients.

3.2.4 Recipients

Power Master+ Management can send notifications to multiple recipients in various ways, including Windows Alert Messages, Instant Messages and mobile phone text messages (SMS). The Notification Recipient page lists all recipients in the recipient list and displays all defined notifications and whether the notification is active.

Event Action/Recipient page

Recipients can be managed as follows:

- Add a new recipient: Click the ADD button to open the Add Receiver dialog. Enter all required data and click the SAVE button to add a new recipient to the list.
- Modify the recipient: Select the recipient you wish to modify and click EDIT button. After entering in the new data, click the SAVE button to complete.
- Remove the recipient: Select the recipient to remove from the recipient list, and then click DELETE buttonto complete the recipient deletion.

The recipient detail settings and descriptions are explained below:

- Active: States if the recipient is active.
- Language: The language to which the recipient prefers. The notification sent to this recipient uses this language to display content.
- Recipient Name: The name of the recipient. The recipient name must be unique.
- E-mail Address: The E-mail address of the recipient.
- XMPP Account: The XMPP Instant Messaging account of the recipient. See SETTING/Notification Channels for more details about XMPP.
- Computer Username: The computer user account name which is used to receive the windows alert messages. Due differences in the Messenger Service of different versions of Windows, please refer to the descriptions below:
    - If PowerMaster+ and the recipients are on Windows 7, Windows Server 2012or Windows 8, and then the alert messages will only be sent to a local user account on the computer running PowerMaster+.

Note: Computer Name filed and Alert column are only available on the Power Master+ which installed on Windows.

- Mobile Phone Number: The mobile number of the recipient to receive the mobile text message. It must contain the country code.
- Active Days: Configures the days on which recipients can receive the notification. Users can define the specific ways to notify the assigned administrators on different days.
- Active Time: Configures the time which recipients will receive the notification. Users can define the specific ways to notify the assigned administrators during different times.
- Enabled: Displays which notification(s) are active for the recipient.
- Test: Sends the notification in accordance with current settings in order to verify the function. The service can be tested only when the corresponding service on the Event Action/Settings page is configured as activated.

3.2.5 Auto-Discover Range

In order to search devices and computers in different segments or a specific range, users can set IP range on this page.

AUTO-DISCOVER RANGE		?
Auto-Discover Range		
IP Range ▲	Comment ⇕	
✔ 192.168.168.1 to 192.168.168.255	sz	

SETTING/Auto-Discover Range page

IP ranges can be managed as follows:

- Add a new IP range: Click the ADD button and an Add IP Range dialog will appear. Enter all required data and click the SAVE button to add a new IP range to the list.
- Modify the IP range: Select the IP range you wish to modify and click EDIT button. After entering in the new data, click the SAVE button to complete.
- Remove the IP range: Select the IP range to remove from the IP range list, and then click DELETE to complete the IP range deletion.

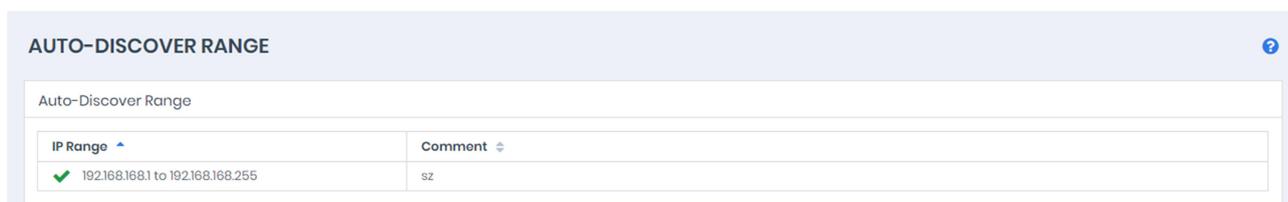The IP range detail settings and descriptions are explained below:

- Active: States if the IP range is active.
- IP Range: Set the range which used in devices and computers scanning.
- Comment: Sets the user-defined comments for this IP range.

3.2.6 Security

3.2.6.1 PowerMaster+ Secret Phrase

The Secret Phrase is used to create secure network communications between PowerMaster+ Applications such as Remote and Local, Remote and UPS PMCARD, or Remote and PDU. The default phrase is powermasteren.ecryption.key**.** The Secret Phrase can be configured on the SETTING/Security page in the Local and Remote, or on the System/Authentication page in the PDU and UPS PMCARD web interface. The Secret Phrase which is used in the Remote and devices must match.
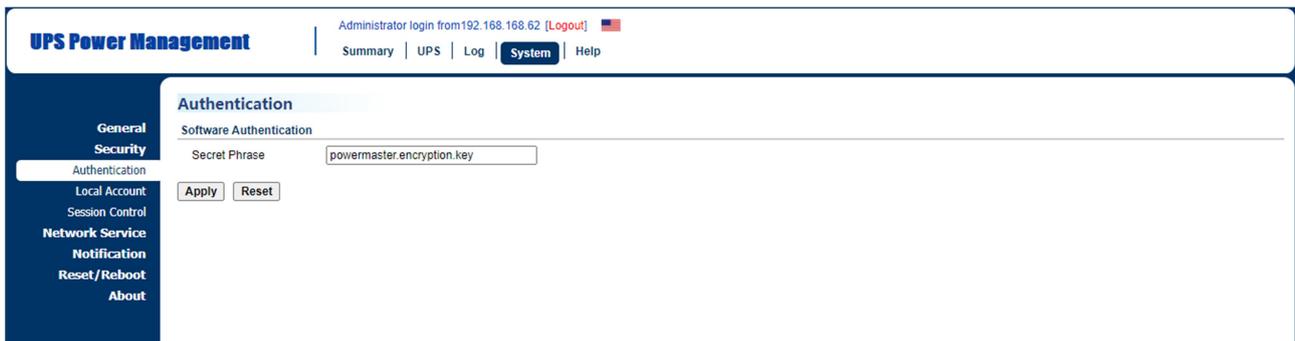
Secret Phrase on the System/Security page in the UPS PMCARD web

3.2.6.2 SSL Certificates

Import SSL Certificates

The user's browser that connects with the Power Master+ web interface will serve the SSL certificate. The certificate proves to the browser that the provider believes that it has issued a certificate to the owner of the Power Master+. The SSL Certificates section allows users to import your own SSL certificate and *SSL Certificate* displays the date and result for the last time to import SSL certificates. Users can import the certificates as following steps:

● Click the IMPORT button to start the *SSL Certificates Wizard*.
● Upload the SSL certificate file.
● Enter the *Key Passphrase* field and the *Key store Password* field. Click the IMPORT button to import the SSL certificates.

Note: Applying for a certificate from the commercial certificate provider will be subject to the provider fee.

Add SSL Certificate into Trust List

A certificate trust list is a pre-defined list of SSL certificates that have been signed by a trusted entity. A certificate trust list of Power Master+ is used to identify the certificate authority of another one with whom interacts. When importing a new SSL certificate, this will result in communication loss between the Local, Remote and Management.

As an example, when the Remote that has been connected with the Local imports a new SSL certificate, the Clint cannot interact with the Local. Users must to add the certificate of Remote into the trust list of the Local manually and thus the Local considers the Remote's SSL certificate valid.

Users can follow the steps to add the certificate into the trust list – Remote and Local, for example:

- Place the SSL certificate of the Remote as file extension of .crt in the
  <Local_installation_directory>/jre/lib/security.
- Switch to the *<Local_installation_directory>/jre/lib/security*directory in the command prompt.
  cd <Local_installation_directory>/jre/lib/security
- Run the below command to add the certificate to the trust list.
  <Local_installation_directory>/jre/bin/keytool.exe –import –trustcacerts –file <cert_name>.crt –alias<alias_name> – keystorecacerts.
- Enter "*changeit*" as the password for the certificate addition.
- Enter "y" to apply the certificate addition.
- Restart the Local service to reload the trust list and take effect. Refer to <u>How to restart PowerMaster+ service</u> of FAQ chapter for further details about how to restart Power Master+ service.

Note: Local_installation_diretory is the directory where the Power Master+ Local installation locates; cert_name is the filename of the certificate file and alias_name is the alias for the certificate available in the trust list.

Note: The aforementioned steps are applicable to the interactions between Power Master+ software.

Note: Due to security reasons, user may have to change the password to access the trust list. Refer to <u>How to change the password to access the trust list</u>.

3.2.6.3   SNMP

The Management can interact and access device information via SNMPv1 and SNMPv3.Fewer early UPS and PDU models which only accept SNMPv1 demands and newer models which support SNMPv3 can be controlled by Management.

Protocol Version: User can determine which SNMP protocol to use over the network communication between Management and devices. It is recommended to choose Both option because Remote attempts on the correct SNMP protocol for device to interact.

SNMPv1

SNMP Community. The Management uses this community to authenticate communication between the PDU and UPS in order to access their information. The default community is private. By default, the UPS/PDU/ATS uses private as the community with write permission, and public with read only permission. The community used by the Management to access the UPS/PDU/ATS must have write permission for an administrative power control.

SNMP Trap Community. The Management uses the community to authenticate the SNMP trap from the monitored PDU and UPS PMCARD. The community default is public. The IP address of the Management

computer must be added to the Trap Receiver list on the Network/Trap Notification page of the UPS PMCARD and the PDU to ensure that the community must match.

Note: The community can be configured on the Network/Access Control (or Network Service/SNMPv1 Service) page in the UPS remote management card (PMCARD) web or on the Network/SNMP Settings(or Network Service/SNMPv1 Service)page in the PDU web.

Note: The SNMP community is limited to 15 characters in the PDU and UPS PMCARD.

Note: If you have firewall software installed, configure the settings to allow access through port 3052 (UDP/TCP), port 53568 (TCP), port 162 (UDP) and port 53566(UDP). These ports must open because the Management uses them to establish the communication with PDU and UPS PMCARD.

SNMPv3

The Management will use the below SNMPv3 settings to interact with a secure device. These settings can be configured on the SETTING/Security page of Management and on the Network Service/SNMPv3 Service page of the UPS PMCARD/PDU/ATS web. These settings must be matched one.

- User Name: Specifies a username match for protocol.
- Authentication Protocol: Sets the protocol to be used for authenticating the network communication between the Remote and devices.
- Authentication Key: Sets the authentication key which is used for the aforementioned authentication protocol.
- Privacy Protocol: Sets the privacy protocol to be used for encrypting data during transmission between the Remote and devices.
- Privacy Key: Sets the privacy key to encrypt data for the aforementioned privacy protocol.

3.2.7 Advanced

3.2.7.1 Import and Export Profile Settings

Import and Export features allow users to back up profile of Power Master+ Management and quickly deploy Power Master+ Management to multiple PC/Servers. When Power Master+ Management has been setup completed, users can use Export feature to output the profile of Power Master+ Management. The next time, when a new PC/Server would be set up with Power Master+ Management, users can upload the profile with the Import feature to complete Power Master+ Management setting immediately.

Notice: The profile of Power Master+ Management only can be applied in Power Master+ Management.
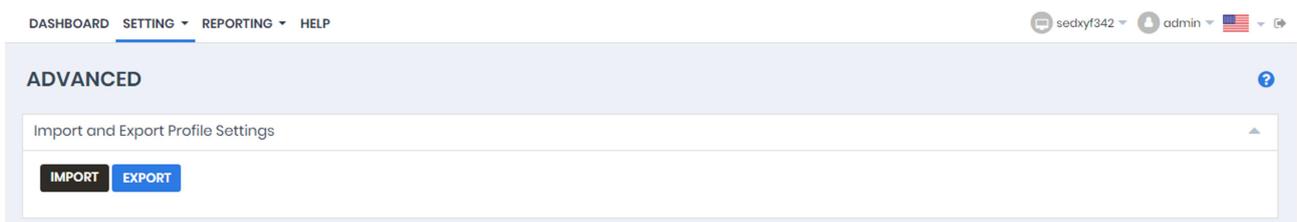
SETTING/Advanced page in the Management

3.2.7.2   Energy Event Command Scripts

The Power Master+ Management software can be configured to respond to specific events and perform command execution. The SETTING/Advanced page lists events that can be set to perform command execution. For details of each event, please refer to Event Details section.

System Command Scripts						
Active	Urgency	Event		Command	Duration	Delay
☐	⚠	Power consumption is too high		▾	<1 sec	Instan
☐	⚠	Power consumption is too low		▾	<1 sec	Instan

CANCEL   APPLY

Group Command Scripts						
Active	Urgency	Event		Command	Duration	Delay
☐	⚠	Power consumption is too high		▾	<1 sec	Instan
☐	⚠	Power consumption is too low		▾	<1 sec	Instan

CANCEL   APPLY

UPS Command Scripts						
Active	Urgency	Event		Command	Duration	Delay
☐	!	Battery capacity is critically low		▾	<1 sec	Instan
☐	!	Network communication lost with UPS in a power event		▾	<1 sec	Instan
☐	!	System is overheated		▾	<1 sec	Instan
☐	!	Network communication lost		▾	<1 sec	Instan
☐	⚠	UPS is faulty		▾	<1 sec	Instan
☐	⚠	Utility power failure		▾	<1 sec	Instan
☐	⚠	Batteries are not present		▾	<1 sec	Instan
☐	⚠	Output is off		▾	<1 sec	Instan
☐	⚠	UPS fatal internal abnormality		▾	<1 sec	Instan
☐	⚠	Power consumption is too high		▾	<1 sec	Instan

SETTING/Advanced page in the Management

The severity of each event is marked by a symbol. Severe level (!) indicates users must be alerted and the computer shut down to avoid an improper shutdown. Warning level (⚠) indicates a warning and users should be notified when it occurs. If a warning condition persists, a system shutdown may be imminent. Information level (ℹ)indicates the state of the UPS or that the utility power condition has changed.

A command will be executed when an event occurs.

● Active: Determines whether to execute a command. If the check box is unchekced, the command for this event and the corresponding event will not be executed.

● Command: Sets a command file to be executed when an event occurs. Shell scripts for the command file uses "cmd" as the filename extension. For more information about shell scripts read the detailed description in the "default.cmd" file in the "extcmd" folder in the Power Master+ installation directory. Customized shell scripts must be saved in the "extcmd" folder in the PowerMaster+ installation directory. The command file will be listed on the *Command/File* list and can be executed when the power event occurs.
Note: The command file name will be displayed in italics if the command file which had used cannot be found in the "extcmd" folder.

● Duration: Sets the estimated time for the command to complete. If the event requires the computer to shut down, this delay provides time for commands and scripted actions to complete before the shutdown is initiated.

● Delay: Determines whether to execute a command and sets the delay for the command execution. If the event is cleared within the command execution delay, the command for this event and the corresponding event will not be executed.

The following environment variables can be placed in external commands to identify which event and which stage to be executed.

- %EVENT_STAGE%: Indicates what stage of firing event to execute the commands. When an event first happens, it enters the OCCUR stage and the assigned commands will be executed. When an event is ended, the variable will be FINISH and the assigned commands will be executed.
- %EVENT%: Indicates which event is fired to execute the commands.
- %EVENT_CONDITION%: Indicates which the detailed event condition of a firing event.
- %MODULE_NO%: Indicates which UPS module on a firing event. This variable is used on Modular UPS models.

The following table lists all details of %EVENT% and %EVENT_CONDITION% variables.

%EVENT%	%EVENT_CONDITION%	Event Name
BATTERY_CRITICAL_LOW		Battery capacity is critically low.
ENTER_BYPASS		Enters bypass mode.
BATTERY_EXHAUSTED		Battery has been depleted.
EMERGENCY_OFF		EPO is active.
BATTERY_FULL		Battery is fully charged.
SHUTDOWN		Shutdown initiated.
BYPASS_FAILURE		Bypass power source has failed.
CAPACITY_INSUFFICIENT		Insufficient inverter capacity.
LOSS_REDUNDANT		Not enough power redundancy modules.
ABNORMAL		UPS input abnormality.
	NO_NEUTRAL	No neutral input.
	WIRING_FAULT	Site wiring fault.
FATAL_ABNORMAL[4]		UPS fatal internal abnormality.
	OUTPUT_OVERLOAD	Output is overloaded.
	BYPASS_OVERLOAD	Bypass is overloaded.
	MODULE_OVERLOAD	Module is overloaded.
	SHORT_CIRCUIT	Output circuit-short.
	MODULE_RECTIFIER_OVERHEAT[1]	Module rectifier is overheated.
	MODULE_INVERTER_OVERHEAT[1]	Module inverter is overheated.
	MODULE_INVERTER_PROTECTED[1]	Module inverter is protected.
	BATTERY_REVERSED	The polarity of battery is reversed.
	BYPASS_SEQUENCE_ERROR	The phase sequence of bypass is wrong.
COMMUNICATION_FAILURE[4]	LOST_IN_LOCAL	Local communication lost.

	LOST_IN_NETWORK[3]	Network communication lost.
FAULT[4]	GENERIC_FAULT	UPS is faulty.
	BYPASS_FAN_FAULT	Bypass fan is faulty.
	BYPASS_FAULT	Bypass is faulty.
	MODULE_RECTIFIER_FAULT[1]	Module rectifier is faulty.
	MODULE_INVERTER_FAULT[1]	Module inverter is faulty.
	MODULE_FAN_FAULT[1]	Module fan is faulty.
NO_BATTERY		Batteriesare not present.
RUNTIME_INSUFFICIENT		Available runtime is insufficient.
UTILITY_FAILURE		Utility power failure.
URGENT_COMMUNICATION_FAILURE[4]	LOST_IN_LOCAL	Local communication lost in a power event.
	LOST_IN_NETWORK	Network communication lost in a power event.
RUNTIME_WILL_EXHAUST		Remaining runtime will be exhausted.
OUTPUT_WILL_STOP		The output power is going to stop soon.
INPUT_NEAR_OVERLOAD[2]		Input is near overload.
INPUT_OVERLOAD[2]		Input is overloaded.
SHUTDOWN_TIME_INSUFFICIENT[2]		Shutdown time is in insufficient.
ATS FAULT[5]		ATS is faulty.
ALL_SOURCE_FAILURE[5]		Both input sources have power loss, ATS will not change input source
CURRENT_SOURCE_FAILURE[5]		ATS has automatically switched to redundant power source.
REDUNDANT_SOURCE_FAILURE[5]		ATS redundant power source has experienced a power failure.
ENV_SENSOR_LOST[6]		Environmental sensor is not responsive.
ENV_SENSOR_OVERHEAT[6]		Temperature is over the high threshold.
ENV_SENSOR_UNDERCOOL[6]		Temperature is under the low threshold.
ENV_SENSOR_OVERWET[6]		Humidity is over the high threshold.
ENV_SENSOR_OVERDRY[6]		Humidity is under the low threshold.
POWER_LOST		Power supply redundancy has been lost.
MBO_OUTLET_OVERLOAD[7]		A PDU outlet is overloaded.

MBO_OUTLET_NEAR_ OVERLOAD[7]	A PDU outlet is near overload.

[1]: *This event only occurs for the Modular UPS in Local.*

[2]: *This event only occurs for the PDU in Remote.*

[3]: *This event only occurs in Remote.*

[4]: *This %EVENT%variable must come with a %EVENT_CONDITION% variable.*

[5]: *This event only occurs for the ATS in Remote.*

[6]: *This event only occurs for the environmental sensor for UPS/PDU/ATS in Remote.*

[7]: *This event only occurs for the Metered by Outlet PDU in Remote.*

3.2.8   Network Configuration

3.2.8.1   Host IP Configuration

According to chapter 2.3, users can access Power Master+ Management through the default URL and can assign an IP to Power Master+ Management web browser in Host IP Configuration.

- Host IP: when the computer installed with Power Master+ Management has multiple IPs, users can choose one of the IPs for the web browser.

3.2.8.2   HTTPS

Power Master+ Management allows users to change the secure level and port explained below:

- HTPPS Secure: Enable this option for web access to be over the HTTPS connections.
- HTTPS Port: Determines which port to be used over the HTTPS connections. The default port is 53568.

Once the secure level is changed, the new secure level will be taken effect. All pages can't be displayed during the duration to restart server.

When HTTPS secure is enabled, the browser warning will be presented after the new level is taken effect. This indicates that the user's browser considers the connection is risky. Users can ignore the warning page and continue the web access, or provide a SSL certificate which is produced by the commercial certificate providers or any trusted certificate authority.

If the user has his own SSL certificate, refer toImport SSL Certificates section for further details how to import the new certificate.

3.2.9   Account Management

3.2.9.1   Session

The Session Timeout section is the option which determines the duration of the session after the login. If the page isn't accessed during this period and remains inactive, users will be logged out automatically. Users will need to login again.

3.2.9.2   Account List

- Account Name: Accounts of users in Power Master+ Management.
- Authority: The authority of this account. Power Master+ Management uses three levels of authority, including Super Administrator, Administrator, and User to perform management tasks. Each authority can access different system tasks. Three levels of authority are described in below table.

Menu	Page/Function	Authority		
		Super Administrator	**Administrator**	**User**
Dashboard	View	✓	✓	✓
Dashboard	Add & Control Device	✓	✓	
Setting	All pages	✓	✓	
Report	All pages	✓	✓	✓
Report	Setting & Delete	✓	✓	
Help	All pages	✓	✓	✓

Note: An authority can only add, modify authority level and delete an authority whose level is lower than itself.

- Update By: The account that built or edited this account.
- Update Time: The time this account was created or edited.

3.2.9.3   Filter

The Filter section allows filtering of the account action logs.

Filter pane on SETTING/Account Management page

- Dates: Select the Dates for the account action logs to be displayed.
- Times (Hours): Select the time range for the account action logs to be displayed.
- Records Per Page: Specify the number of records to show per page.

3.2.9.4   Account Action Logs

The Account Action Logs section records action logs of each account.

Account Action Logs					Page: ◁ 1 ▷ ⟳ 🖫 🗑
Date & Time ⇅	Account Name ⇅	Menu ⇅	Page ⇅	Action ⇅	Description ⇅
2020-06-18 01:24:15 PM	admin	Setting	Auto-Discover Range	ADD	Add auto-descover range
2020-06-18 01:11:16 PM	admin	Dashboard	Dashboard	Group Settings	Update device list of Group1
2020-06-18 01:11:16 PM	admin	Dashboard	Dashboard	Group Settings	Update settings of Group1
2020-06-18 01:10:40 PM	admin	Dashboard	Dashboard	Device Move	Move device Arc Pro to group Online1-3k
2020-06-18 01:10:10 PM	admin	Dashboard	Dashboard	Group Add	Add group Online1-3k
2020-06-18 11:37:56 AM	admin	Dashboard	Dashboard	Device Control	Power on Arc Pro
2020-06-18 11:37:08 AM	admin	Dashboard	Dashboard	Device Control	Power off Arc Pro
2020-06-18 10:32:18 AM	admin	Dashboard	Dashboard	Device Control	Power on Arc Pro
2020-06-18 10:30:42 AM	admin	Dashboard	Dashboard	SAVE	Update device list
2020-06-18 10:29:08 AM	admin	Dashboard	Dashboard	SAVE	Update device list
2020-06-18 10:28:58 AM	admin	Dashboard	Dashboard	Device Remove	Remove device Arc Pro
2020-06-18 10:28:48 AM	admin	Dashboard	Dashboard	SAVE	Update device list
2020-06-18 10:25:07 AM	admin	Dashboard	Dashboard	Device Control	Power on Arc Pro
2020-06-18 10:16:29 AM	admin	Setting	Network Configurations	APPLY	Update host IP settings
2020-06-18 10:16:18 AM	admin	Dashboard	Dashboard	Device Control	Power on Arc Pro

Account Action Logs page

Clicking the Previous and Next at the upper right corner of the account action log table allows users to view the other range of filtered log result backward or forward. Clicking Refresh⟳ will update the log result according to the current filter options and page settings.

Export

Click the Save🖫shortcut at the upper right corner of the account action log table and select CSV or PDF file as the export file format. The exported file will be saved in the default download directory of your web browser.

Clear All Logs

Click the Delete🗑shortcut at the upper right corner of the account action log table. A dialog box will show, saying all account action logs will be removed immediately after clicking DELETE. The log clearance is permanent and once applied the log files cannot be recovered.

3.2.10 Event Details

The section lists the power events of Power Master+ Management. The events are divided into below categories:

System

- Power consumption is too high. System power consumption has gone above the high threshold.
- Power consumption is too low. System power consumption has gone below the low threshold.

Group

- Power consumption is too high. Device group power consumption has gone above the high threshold.
- Power consumption is too low. Device group power consumption has gone below the low threshold.

UPS

- System is overheated. Internal UPS temperature is too high.
- Network communication lost. Management cannot establish communication with UPS on the network or established network communication has been interrupted.
- UPS is faulty. UPS has an internal malfunction. The UPS may not be operating properly and will not be able to affect a proper shutdown.
- Utility power failure. Utility power failure, battery power will be supplied.
- Battery is not present. Batteries are not present; the UPS cannot provide battery power in this condition.
- Available runtime is too low. There is not sufficient runtime for Power Master+ to perform a complete shutdown based on current configuration even if the battery is 100% charged.
  An excessive load or long shutdown time may cause this event. Reduce some UPS load or set a more accurate shutdown time to avoid this event.
- UPS fatal internal abnormality. The UPS is experiencing one or more of the following fatal abnormalities; UPS may shut down or stop output power unexpectedly.
- Power consumption is too high. UPS power consumption has gone above the high threshold.
- Power consumption is too low. UPS power consumption has gone below the low threshold.

- Shutdown initiated. A computer which connects with UPS initiated the shutdown process. The computer will shut down or enter hibernation.
- Battery has fully charged. Battery has fully charged. The capacity of battery is full.
- Battery capacity is critically low. Battery capacity is critically low; power could be lost immediately.
- An outlet on a UPS has turned on. A UPS outlet has been turned on. The outlet can afford the power to its connected equipment.

PDU

- Network communication lost. Management cannot establish communication with PDU on the network or established network communication has been interrupted.
- Input is near overload. A PDU is near an overload condition. The load level is near the safe load threshold for the PDU.
- Input is overloaded. A PDU is in an overload condition. The safe load threshold has been exceeded.
- Power consumption is too high. Power the specific PDU consumes has been exceeded the high threshold.
- Power consumption is too low. Power the specific PDU consumes has been violated the low threshold.
- Shutdown initiated. A computer connected to the UPS has initiated the shutdown process. The computer will shut down or enter hibernation soon.
- A PDU outlet is overloaded. An outlet of Metered by Outlet PDU is in an overload condition. The safe load threshold has been exceeded.
- A PDU outlet is near overload. An outlet of Metered by Outlet PDU is near an overload condition. The load level is near the safe load threshold for the outlet.

ATS

- Network communication lost. Management cannot establish communication with a ATS on the network or established network communication has been interrupted.
- ATS is faulty. ATS has an internal malfunction and may not operate properly.
- Both input sources have power loss, ATS will not change input source. ATS will not switch from one input source to another because both are experiencing power failures.
- Input is near overload. An ATS is near an overload condition. The load level is near the safe max load threshold for the ATS.
- Input is overloaded. An ATS is in an overload condition. The safe max load threshold for the ATS has been exceeded.
- Power consumption is too high. ATS power consumption has gone above the high threshold.
- Power consumption is too low. ATS power consumption has gone below the low threshold.
- Shutdown initiated. A computer connected to the ATS has initiated the shutdown process. The computer will shut down or enter hibernation soon.

3.3 REPORTING

3.3.1 System Logs

The System Logs page in Management provides users logs of recorded details from operations performed in Management. The logs can be used for analysis or to determine whether operations have been performed correctly.

Logs page

Each log has details which can be viewed by clicking the icon next the each log.Using the paging toolbar at the top of the log list allows users to view older logs by changing the page displayed; clicking the refresh icon updates the logs displayed in the list.

3.3.2 Event Logs

The Event Logs page records the event logs that can be analyzed whether the devices and the system are functioning well. Each log records what event occurred of the device.

Event Logs page

Using the Previous and Next at the upper right corner of the event log list helps users to view the other range of filtered log result backward or forward. Clicking Refresh ⟳ will update the log result to display in the list according to the current filter options and paging settings.

Export

Click the Save 💾 shortcut at the upper right corner of the event log table and select CSV or PDF file as the export file format. The exported file will be saved in the default download directory of your web browser.

Clear All Logs

(The function is only applicable to the administrator and super administrator.)

Click the Delete 🗑 shortcut at the upper right corner of the event log table, a confirm dialog will show up, all event logs will be removed immediately after clicking DELETE. The log clearing is permanent and once applied the log files cannot be recovered.

3.3.2.1 Settings

(The contents in this section are only applicable to the administrator and super administrator.)

● Entry Expiration: This option specifies how long the log files will be retained.
● Log to Windows Event Viewer: Determines to log events to Event Viewer additionally. Users can launch the Control Panel > Administration Tools > Event Viewer to review all events in the Application category of the Windows Logs directory.

    Note: Event Viewer is only function on the Windows platforms. If this option is not activated, you can activate this option by installing the PowerShell through Windows Update.

● Max Records: Indicates the maximum number of events that will be displayed.

3.3.2.2 Filter

After the configuration of the filter section is configured, click APPLY button to filter the logs.
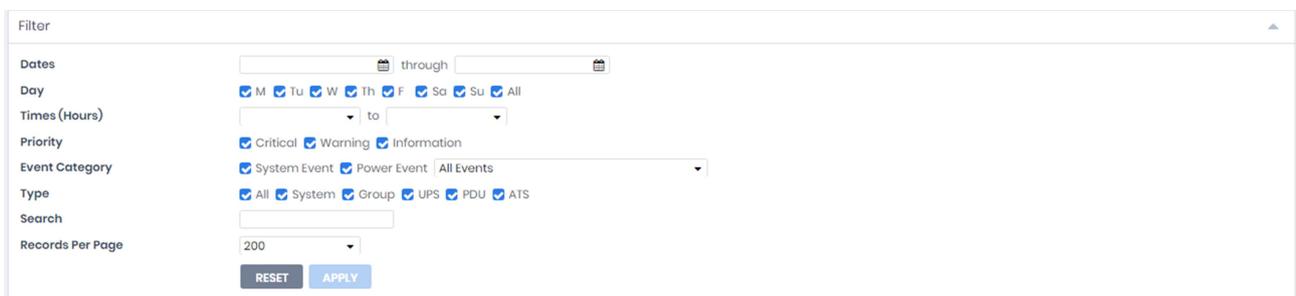
Filter pane on REPORTING/Event Logs page

● Dates: Selects the Date for the events to be displayed.
● Day: Selects the Day(s) for the events to be displayed.
● Times(Hours): Selects the time range for the events.

- Weekday: Choose the days of the event occurrence.
- Priority: The events can be filtered by Priority.
- Event Category: The events can be filtered by category. The events can be further divided by Power Event and System Event categories, and choosing the specific event.
- Records Per Page: Specify the number of records to show per page.

3.3.3 Energy Use

The Energy Use page shows a chart of how energy is spent in a specified period of time and also shows the energy statistics of the current target node and entire system.

3.3.3.1 Settings

(The contents in this section are only applicable to the administrator and super administrator.)

In this section, users can assign the rate of power consumption and carbon emission, and set energy use alerts. When the rates are updated, the information presented in the Statistics page will also be updated.

Energy Use/Settings

Management has the capability of reminding users of power consumption violations. The Setting page allows users to configure thresholds. When power consumption thresholds are violated, Management will notify the user.

- Cost Per kWh: Select the country the UPS is located in.
- CO_2 Emitted per kWh: The weight of equivalent emitted carbon when one kWh power is consumed and the unit of measurement.
- Energy Use Alerts

  Set the notifications thresholds for Power Master+ Management.

  - System Threshold. When the power consumption of the entire system exceeds the high threshold or violates the low threshold, the event "Power consumption is too high." or "Power consumption is too high." of system will occur, respectively.
  - Device & Groups Threshold. When the power consumption of the group or power equipment exceeds the high threshold or violates the low threshold, the event "Power consumption is too high." or "Power consumption is too high." of group or device will occur, respectively.

3.3.3.2 kWh Cost History

Because the rate of power consumption can vary over time, users can assign rates for different periods of time. Associated costs of historical periods will show in the table and user can edit or delete selected data. When rates are updated, the information displayed in the Metric section will also be updated.

Energy Use/kWh Cost History

3.3.3.3 Metrics

The Statistics page shows a chart of how energy is spent in a specified period of time and also shows the energy statistics of the current target node and entire system.
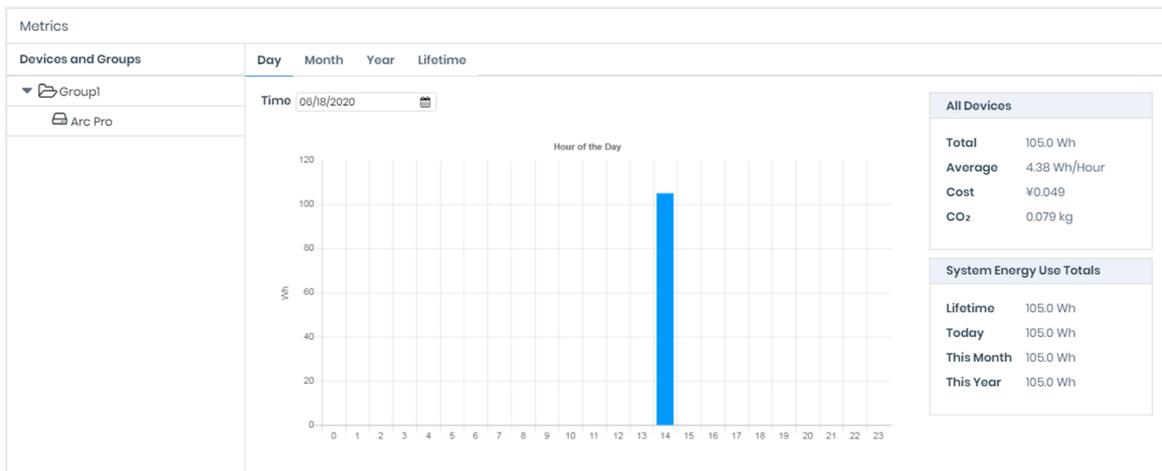
REPORTING/Energy Use page

The consumption of each UPS, PDU, ATS and outlet of Metered by Outlet PDU is logged on an hourly basis and each group that contains these UPS, PDU and ATS will accumulate the consumption data. Data logged can be used to render a chart over the past day, past month, past year and all past information accordingly. Users can see how much energy has been spent in a historical period of time.

The total and average power consumption of each selected group that contains UPS, PDU and ATS will be shown according to current chart. Management will also show the statistics on the total power consumption of today, this month, this year and entire system in the *System Energy* block.

3.4 Web Browser Info

The top-right corner of Power Master+ Management user interface shows the installation location, account information and provides language selection.
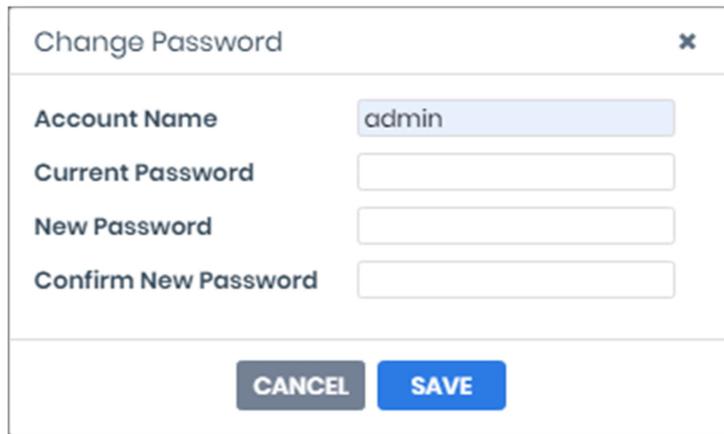

Web browser info

3.4.1 Power Master+ Management Installation Location

The name and IP of the computer that is installed with the Power Master+ Management is displayed.

3.4.2 Account Information

The Account Information section is used to change the Power Master+ Management login account information, including account name and password.

Account Information

Change Account Name or Password

- Enter the password in the Current Password field.
- Enter a new account name in the Account Name field if you want to change account name. Account name must be alpha numeric (0-9, A-Z and a-z).
- If you want to change password, enter a new password in the New Password field and enter the new password again in the Confirm Password field to confirm.
- Click SAVE to complete the change.

3.4.3 Language

Choose the language in which Power Master+ Management is displayed.

3.5 HELP

3.5.1 Power Master+

This section is an overview which includes the Power Master+ and host operating system. It also provides resources about contact website for assistances.

3.5.2 Content

The Content page provides an overview which introduces the brief functions of what Local, Remote or Management do and indicates how to get related online-help content for current function page. It indicates a button to access to online-help directly.

4 Technical Support

4.1 Troubleshooting

1. I cannot access the Power Master+ web interface after complete installation.

    Please follow the below steps resolve the problem:

    - Make sure that there is no other application utilizing port3052 (UDP/TCP) and port 53568 (TCP).Use a command prompt with the command "netstat -o" to obtain information about which ports are used by which programs.
    - Ensure the Power Master+ service is running on the hosted computer. If the service is stopped, restart the service and then try again in the same way.
    - Make sure the port3052 (UDP/TCP) and port 53568 (TCP) on the hosted computer are not blocked by a firewall.
    - Make sure the URL in the address filed of the browser for a remote computer is correct.

2. The Power Master+ installation failed.

    If the installation file is from Company web site, it may have downloaded incompletely or become corrupt. Download the installation file again.

3. I failed to extend the off-delay time of Necessary shutdown time option.

    - The communities on the SETTING/Security page in the Remote and on the Network/Access of Control page in the PDU may be not matched. Confirm that the communities with the write permission are matched.
    - The Remote may use the community without write permission to access the PDU. Please promote the permission of the community which is used by the Remote to access the PDU.

4. The shutdown occurs earlier than expected time.

    It may be caused by the following conditions:

    - When batteries have been used for a long time, they are unable to reach a full charge. Check to see if the output load is too high. A high load on the UPS will cause the batteries to discharge faster and the remaining runtime quickly decrease. Disconnect some load from the UPS to reduce the load in order to extend the runtime.
    - Verify that the batteries are fully-charged. If the capacity is too low, please charge the batteries to full capacity.

5. Pages cannot be displayed after I set up another port number in the Security/Network page.

    The port that was set up in the SETTING/Security page may be occupied by other applications or services. This indicates that the pages can't be accessed through the assigned port.

6. The host name and IP address at the Local's banner on the vMA of the VMware ESXi host displays Unknown.

    Follow below steps to correct this condition:

    ● Run the command *'sudo vi /etc/hosts'* with root permission.
    ● Add the below snippet with the IP address and hostname.
      192.168.1.1 hostname
      Note: IP address and host name can be inquired using the commands 'ifconfig' and 'hostname'.
    ● Restart the service using the commands '*sudo service pmasterpstop'* and '*sudopmasterpservice start'*
    ● Login the page again. The host name and IP address will be correct.

7. I have downloaded the Linux installer from the website. The installer cannot be launched.

    Before launching the Power Master+ installer, you must change its access permission on the installer. You must have executable permission on the PowerMaster+ installer; otherwise the message "Permission Denied" will be displayed.
    Run the below example command to change its permission of the 32-bit installer on 32-bit Linux platform. *sudochmodu+xpmasterp-XXX-linux-x86.sh*(XXX is the version number of Power Master+.)
    Run the below example command to change its permission of the 64-bit installer on 64-bit Linux platform. *sudochmodu+xpmasterp-XXX-linux-x86_64.sh*(XXX is the version number of Power Master+.)
    After the permission of the Power Master+ installer is changed, the installation procedure will be allowed to launch.

8. Inability to Shutdown NAS during Power Failure.

    When using sshpass tool cannot shut the NAS down during power failure, the version of the sshpass tool may be 1.04.
    The sshpass tool whose version is 1.04 will result in inabiltiy to shutdown NAS. You must check whether the version of the sshpass tool is 1.04. If the version is 1.04, you must change another version.

9. The Power Master+ installation file's digital signature is not valid.

It is caused because the operating system does not support the SHA-256 signature the installation file uses. Please follow the solutions below to resolve the problem for different versions of Windows:

● On Windows 8.1, Windows 8, Windows 7, Windows Server 2012 or Windows Server 2008 R2, please update the Windows via Windows Update to support SHA-256 signatures.
● On the version earlier than Windows 7 or Windows Server 2008 R2, please click Allow or Run when security warning dialog appeared after the installation file is opened.

4.2   FAQ

1. If multiple computers are connected to a single UPS, how do I determine which computer to install the Local or the Remote on to ensure each computer can be shut down gracefully in event of power outage?

   The computer that is connected to the UPS with a serial or USB cable should install the Local, and the remaining ones should install the Remote.

2. After the Power Master+ installation is complete, how do I access the web interface?

   On Windows, you can select the Start>All programs>PowerMaster+ Plus>PowerMaster+ Management(or PowerMaster+ Remote/ PowerMaster+ Local) for local use. You can also enter the URL, http://hosted_computer_IP_address:3052/management, in the address filed of the web browser from a remote computer.

   On Linux, you only enter the URL, http://localhost:3052/management, the address field of the web browser from a remote computer for a local access. You can also enter the URL, http://hosted_computer_IP_address:3052/management, in the address filed of the web browser from a remote computer.

3. Which operation systems are supported by Power Master+ software? And which browser supports them?

   Refer to the <u>Getting Started/Prerequisites</u> for more details.

4. **How can I make Power Master+ run a program when a particular event has occurred?**

   Create a .cmd file and save it into theextcmd folder of Power Master+ installation folder. Then write a command to run your own programs into this script file. Please refer to the default.cmd in the extcmd folder to write your own script.

5. I am not sure what the IP address of the UPS/PDU/ATS is. How can I obtain the correct IP address?

   Use the Power Device Network Utility tool to help you to find the correct IP address of UPS/PDU/ATS. This device list will list the all Company device's IP address on the local network.

6. How do I uninstall Power Master+?

   On Windows, go to Start>Control Panel>Add or RemovePrograms**.** Click the Change/Remove button of Power Master+ to uninstall the program.

   On Linux and VMware ESXi, only Power Master+ Remote can be installed. The default installation directory is /usr/local/PPB on the Linux platforms and/opt/PPB on VMware ESXi. Execute the uninstall.shcommand in the installation directory to uninstall the program.

7. How can I get a notice when a power condition has cleared?

   When a power condition is clear, it will broadcast a notification and also run the command file. A custom script can be created for events. The script can utilize the environment variable EVENT_STAGE to compare the key OCCUR to identify an event that has occurred or FINISH to identify an event that has cleared.

8. What network protocol is used in Power Master+?

   SNMP is used on communications between Remote, Management, PDU or UPS with remote management card. HTTP and HTTPS are used between the Local and the Remote.

9. What the network ports are used by Power Master+?

   Port 3052 (UDP/TCP), port 53568 (TCP),port 161(UDP), port 162 (UDP) and port 53566(UDP)

10. How do I ensure that the SNMP settings between the Remote and UPS/PDU/ATS are properly setup?

    To receive the trap notification from the UPS/PDU/ATS all the time, follow steps to verify the SNMP settings:

    ● Open the Network/Trap Notification page on the UPS/PDU/ATS web and the SETTING/Security page on the Remote.
    ● Confirm that the IP address of the Remote can be found on the Network/Trap Notification page of the UPS/PDU/ATS web. If the IP address can be searched, skip the step 3.
    ● If the IP address of the Remote could not be found, click the Trap Receiver shortcut of the Network/Trap Notification page to enter the Trap Configuration page. Enter the required data to add a new trap receiver.
    ● If the IP address of the Remote could be found, verify the SNMP settings are matched.

11. How do I determine that if my computer is using hibernation or not?

    If the operating system is Windows 7, Windows Server 2008,Windows 8, Windows 10, Windows Server 2012 or Windows Server 2016 please follow the below steps to enable the hibernation.
    ● Open the Command Prompt dialog box.
    ● Use the commandpowercfg.exe -hibernate onto enable the hibernation.

12. How do I upload the installer to vMA?

    ● Login the vSphere Client.
    ● Select the VMware host.
    ● Click Configuration.
    ● Select the target datastore from the right hand side.
    ● Right click the target datastore and click Browse Datastore.
    ● Click Upload button on the toolbar and select the file you want to upload.
    ● Click OK button to continue with the upload files into the target datastore.

13. How do I upgrade the virtual hardware version of vMA?

    For vMA running on ESXi 5.x, it is recommended to upgrade the virtual hardware to version 8. To upgrade the virtual hardware version of VMA as below steps:

    ● Start the vSphere Remote and power off the target vMA.

- Right-click the virtual machine and select the Upgrade Virtual Hardware menu option to upgrade virtual hardware.
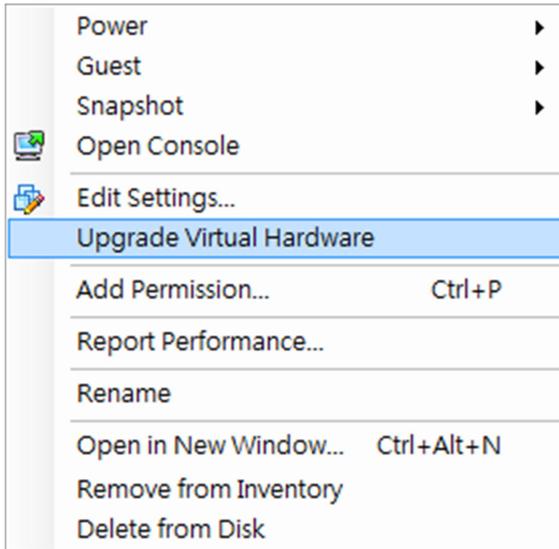
- Click Yes to continue with the vMA upgrade.

- Power on the vMA to make the changes take effect.

14. How do I restart the Power Master+ service?

   For windows, restart the service from the Power Master+ Service > Services > Administrative Tools > Control Panel.

   For Linux, run the commands in order to restart the service:*sudo service pmasterpdstop*and*sudo service pmasterpdstart*.

15. I cannot add the new SSL certificate into the trust list.

   Due the duplicate alias name is available in the trust list, the certificate cannot be added. In order to add the new certificate into the list, the certificate which has the duplicate alias name should be removed from the list. Follow the steps to remove the certificate:

- Switch to the *<Local_installation_directory>/jre/lib/security* directory in the command prompt.
   cd <Local_installation_directory>/jre/lib/security
- Run the below command to remove the certificate from the trust list.
   <Local_installation_directory>/jre/bin/keytool.exe –delete –alias <alias_name> -keystorecacerts
- Enter "*changeit*" as the password for the certificate removal.
- Enter "y" to apply the certificate removal.

- Restart the Local service to reload the trust list and take effect. Refer to <u>How to restart Power Master+ service</u> of FAQ chapter for more details.

16. I cannot successfully upload the profiles of Power Master+ Center to Power Master+ Management.

Please compress the etc and extcmd folders in the Power Master+ installation directory into a zip file as the file to be imported to the Power Master+ Management.
Power Master+ Center corresponds to Power Master+ Management.

5 Glossary

- Citrix XenServer: A virtual-machine monitor allows several guest operating systems to execute on the same computer hardware concurrently. XenServer is supported by Citrix systems, Inc.

- IP address: An IP address is a series of numbers that identifies a particular computer or NIC on a network. IP is an abbreviation for Internet Protocol.

- HTTPS:Abbreviation for HTTP Secure. It provides encryption and secure identification of servers by using HTTP with SSL/TLS protocol. HTTPS connection is usually used for the sensitive transaction.

- Power Device Network Utility: Is an easy to use tool to setup network configurations of the UPS PMCARD/PDU/ATS. This includes setting the IP address, subnet mask, or gateway of UPS PMCARD/PDU/ATS.

- PDU: A PDU is a device which provides power output controls for individual outlets and connected equipment. PDU is an abbreviation for Power Distribution Unit.

- SNMP: The simple network management protocol. It is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention.

- SSL: Abbreviation for Secure Sockets Layer. SSL is a transaction security standard that provides data encryption, server authentication, and message integrity.

- TCP/UDP: Family of protocols for the transport and network layers.

- TLS: Abbreviation for Transport Layer Security. TLS is a cryptographic protocol which provides communication security over the internet. TLS and SSL provide data encryption and server authentication for message reliability.

- vMA: Abbreviation for vSphere Management Assistant. A virtual machine that includes prepackaged software and supported by the VMware, Inc. allows administrators to run scripts and Locals to manage ESXi hosts.

- VMware ESXi: An enterprise-level computer virtualization product offered by VMware, Inc. It is a component of VMware's larger offering, VMware Infrastructure, and adds management and reliability services to the core server products.

- Virtual Appliance: A virtual machine image is designed to run on a virtualization platform developed by VMware, Inc. It is intended to eliminate the installation, configuration and maintenance costs associated with running complex stacks of software.

- VMware vCenter:A vSphere's centralized tool that allows for the management of multiple ESXi servers and virtual machines from different ESXi servers through a single console application.

- Microsoft Hyper-V Server: A native hypervisor-based server virtualization product being offered by Microsoft Corporation.

- ATS: ATS is an electrical switch that switches a load between two sources. It can switches power automatically to a generator or other standby power source after a power outage. ATS is an abbreviation for Automatic Transfer Switch.

- Environment Sensor: A sensor accessory that can be installed on UPS/PDU/ATS for monitoring environment condition and obtaining information about the temperature and humidity