PowerPanel® Business Edition
Installation Guide

For

Power Distribution Unit

Rev. 3

2011/03/03

Table of Contents

Introduction

The Power Distribution Unit (PDU) provides power output controls for individual outlets to your connected equipment. When the PDU turns off an outlet, any connected computers, running PowerPanel® Business Edition Client, are shut down in an orderly fashion, preventing data loss or a system crash due to an immediate power loss.

The Client establishes communication with the PDU via the network. When the PDU is preparing to turn off an outlet, which has a computer connected, the Client will be aware of this condition in advance and send a command to the computer to perform a graceful shutdown before the outlet is turned off. The Client must be installed on each computer requiring protection. Refer to the illustration below.
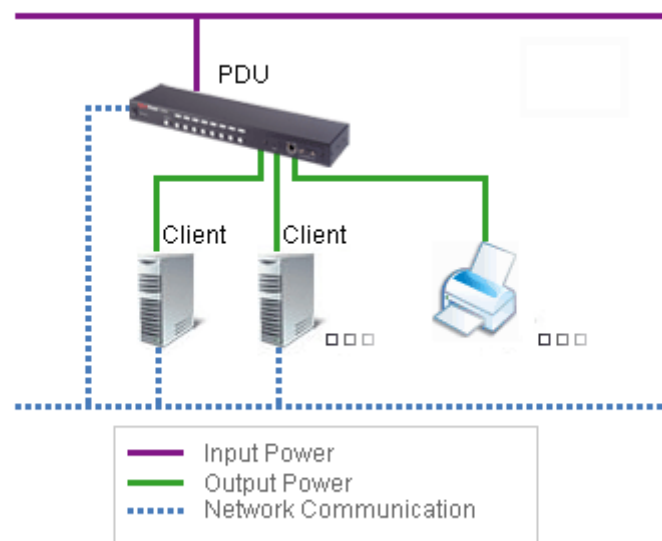
The PowerPanel® Business Edition Client can be installed on the various platforms to conform shutdown requirement including Windows, Linux, VMWare ESX/ESXi. Below sections describes special conditions to these platforms individually if necessary.

# Install PowerPanel® Business Edition Client

Installation on Windows

A popup page will be displayed automatically when inserting the PowerPanel® Business Edition installation CD. Users can click the **Install PowerPanel Business Edition** shortcut on the popup page to initiate the installation procedure. If the popup page is not displayed when inserting the CD, browse to the CD drive and open the folder named **software**, and then double click the file named **setup.exe** to start the installation procedure.
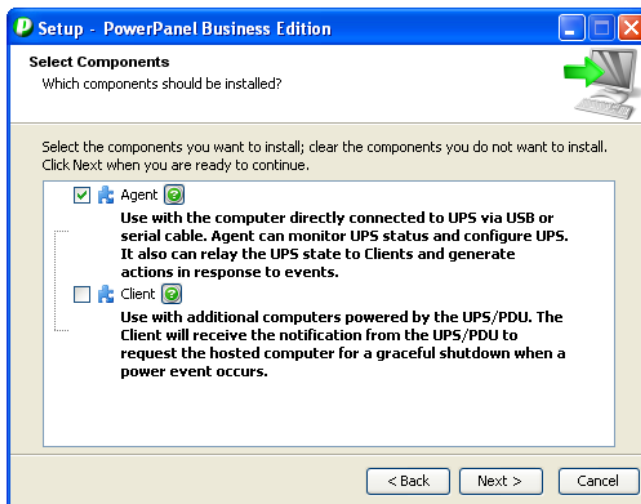
To install follow these steps:

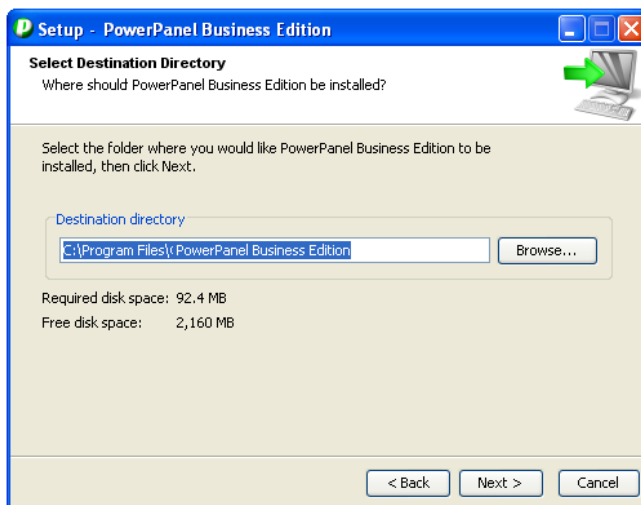- Click the **Next** button to start an installation.
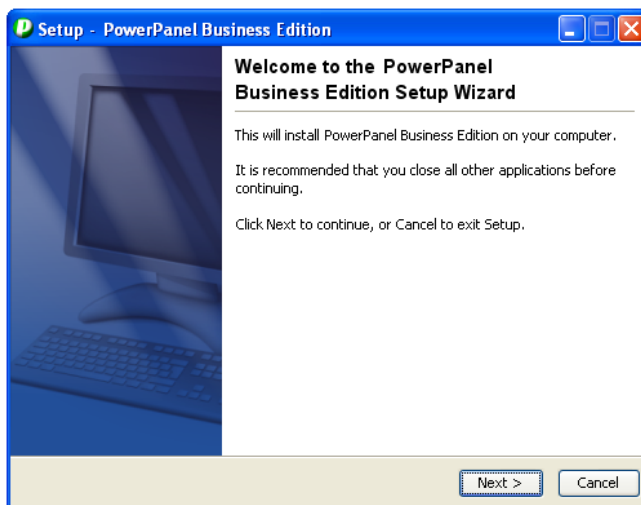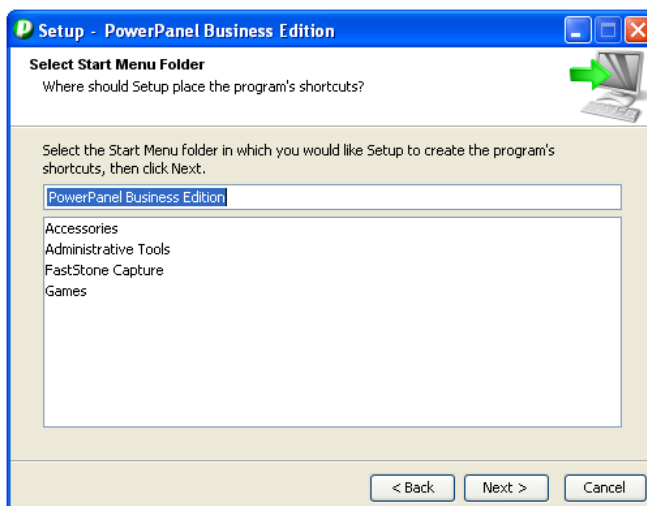

- Accept the license agreement.
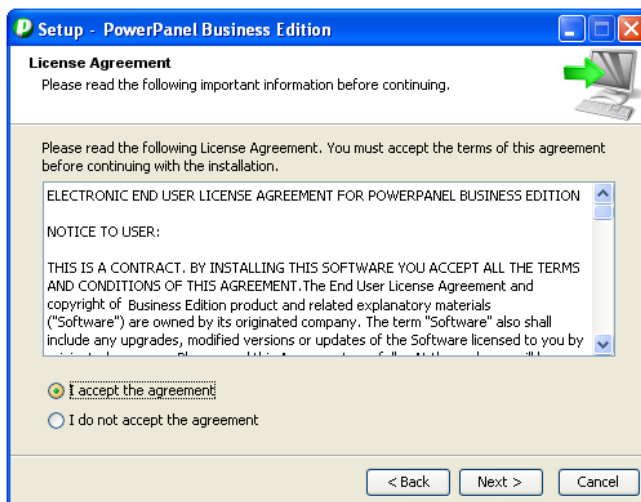
- **Choose the component.** In order to communicate with PDU, you have to select the Client instead of Agent to install.

- Choose the destination location.

- Choose the start menu folder.

- Click the **Finish** button to complete the installation.

Installation on Linux

On Linux, users may mount CD by using the mount command. Run **mount –t iso9660 /dev/scd0 /mnt/cdrom** as a root user. */dev/scd0* is the CD drive and */mnt/cdrom* will be the mount point.

Browse to the CD drive and find the installer named **setup.sh** in the **/software/linux** folder. The installer is used to install the Client and requires root permission. The installation wizard will guide users to complete the installation. Double click **setup.sh** or run the **./setup.sh** command to initiate an installation wizard on desktop.

To install follow these steps:

● Click the **Next** button to start an installation.

● Accept the license agreement.

- Click **Next** button to the next step. On Linux, only Client can be installed.

- Choose the destination location.

- The daemon **ppbed** will start during installation. Click **Next** button to continue.

- Click the **Finish** button to complete the installation.

*Note: The Linux installation will be also initiated by using the **./setup -c** command.in text mode. The detailed installation steps are described in **Installation on VMWare ESX/ESXi 4** section.*

Installation on VMWare ESX/ESXi 4

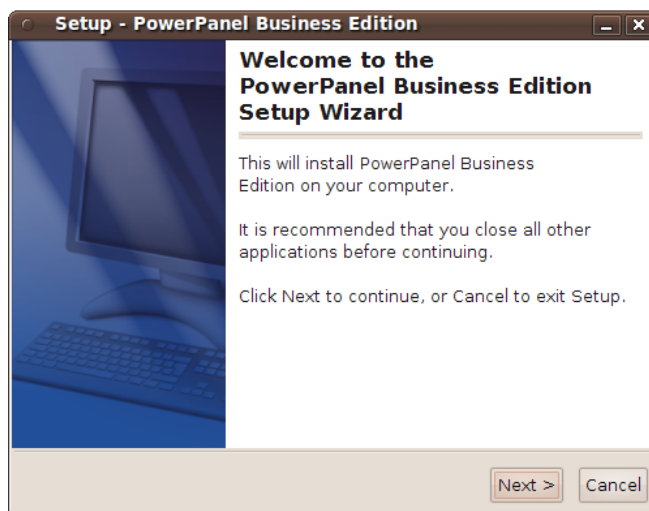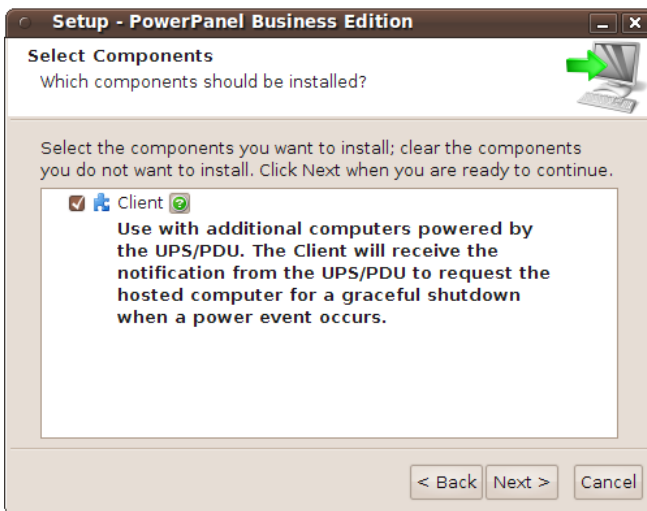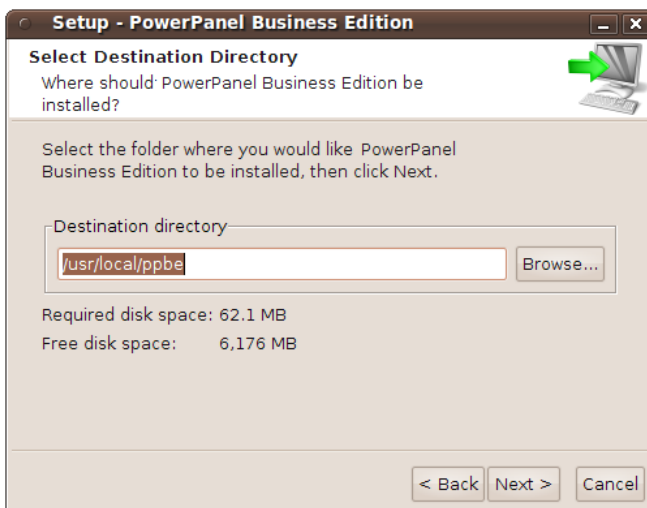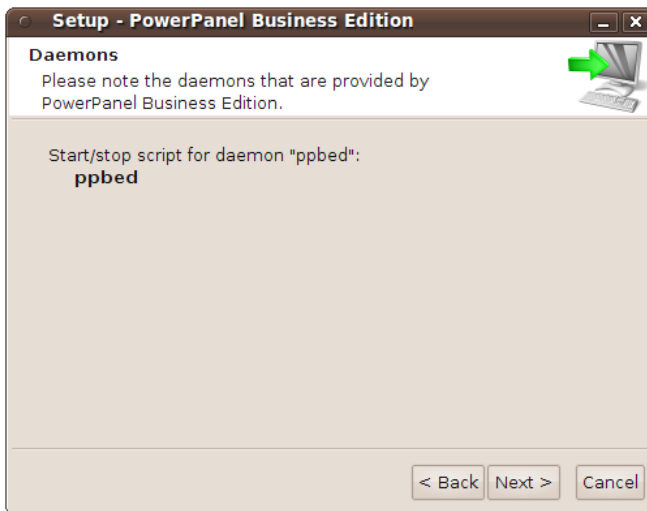On VMWare ESX/ESXi, users may mount CD by using the mount command. Run **mount /dev/scd0 /mnt/cdrom** as a root user. */dev/scd0* is the CD drive and */mnt/cdrom* will be the mount point.

Browse to the CD drive and find the installer named **setup.sh** in the /**software/linux** folder. The installer is used to install the Client and requires root permission. The installation wizard will guide users to complete the installation. Double click **setup.sh** or run the **./setup.sh** command to initiate an installation procedure.

*Note: Installation for **ESX** server must be launched on the **Service Console** (aka **Console Operation System**); installation for **ESXi** server must be launched on the **vMA** (**vSphere Management Assistant**) installed on the VMWare ESXi host computer.*

The installation procedure will be initiated as following steps:

- Press **Enter** to start an installation.

```
Starting Installer ...
This will install PowerPanel Business Edition on your computer.
OK [o, Enter], Cancel [c]
```

- **Accept the license agreement.**

```
YOUR ACCEPTANCE OF THE FOREGOING AGREEMENT WAS INDICATED DURING
INSTALLATION.

I accept the agreement
Yes [1], No [2]
```

- **Choose the component.** Click **Enter** for the default selection to install the Client.

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

- **Choose the destination location.**

```
Where should PowerPanel Business Edition be installed?
[/usr/local/ppbe]
```

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

```
Please wait for PowerPanel Business Edition configuring
Default username and password is "admin".
PowerPanel Business Edition may not do hibernation.
Finishing installation...
```

Note: In order to allow the interactions between physical and virtual machines, VMware tools have to be installed on each virtual machine. Refer to VMware ESX/ESXi Server documentation for further information about VMware Tools.

Verify Firewall Settings

The installer will automatically setup in order to ensure the PowerPanel Business Edition can pass through the firewall during installation. Users can verify the firewall settings or setup again according to following steps.

The firewall settings could be verified on Windows such as **Control Panel > System and Security > Windows Firewall > Allow programs to communicate through Windows Firewall** on Windows 7, **Control Panels > Security > Windows Firewall > All programs to communicate through Windows Firewall > Exceptions** tab on Windows Vista or **Control Panel > Network and Internet Connections > Windows Firewall > Exceptions** tab on Windows XP.

Most Linux distributions and VMWare ESX 4 have the firewall installed and startup. Once installation is complete, verify the below ports are open: UDP 161 (out), UDP 162 (in), TCP 3052 (in/out), UDP 3052 (in/out), TCP 8443 (in/out), UDP 53566 (in/out).

Use "*iptables"* command, which is supported by most Linux distributions, to list the open communication ports using in connection.

On Linux, use following command to open communication ports

```
iptables -I OUTPUT -p udp --dport 161 -j ACCEPT
iptables -I INPUT -p udp --dport 162 -j ACCEPT
iptables -I INPUT -p tcp --dport 3052 -j ACCEPT
iptables -I INPUT -p udp --dport 3052 -j ACCEPT
iptables -I OUTPUT -p tcp --dport 3052 -j ACCEPT
iptables -I OUTPUT -p udp --dport 3052 -j ACCEPT
iptables -I INPUT -p tcp --dport 8443 -j ACCEPT
iptables -I OUTPUT -p tcp --dport 8443 -j ACCEPT
iptables -I INPUT -p udp --dport 53566 -j ACCEPT
iptables -I OUTPUT -p udp --dport 53566 -j ACCEPT
service iptables save
```

On VMWare ESX 4 server, use following command to open communication ports:

```
esxcfg-firewall -o 161,udp,out,ppbed
esxcfg-firewall -o 162,udp,in,ppbed
esxcfg-firewall -o 3052,udp,out,ppbed
esxcfg-firewall -o 3052,udp,in,ppbed
esxcfg-firewall -o 3052,tcp,out,ppbed
esxcfg-firewall -o 3052,tcp,in,ppbed
esxcfg-firewall -o 53566,udp,out,ppbed
esxcfg-firewall -o 8443,tcp,out,ppbed
esxcfg-firewall -o 8443,tcp,in,ppbed
```

Access PowerPanel® Business Edition Client Interface

To access the Client interface in Windows, go to **Start > Programs > PowerPanel Business Edition > PowerPanel Business Edition Client** on Windows, which will take you to the login page. On Linux, user can also enter the URL as http://127.0.0.1:3052/client in the address of the web browser to access to the Client. The default username is **admin** and default password is **admin.**

Users can also enter the URL, **http://hosted_computer_ip_addres:3052/client**, in the address of the web browser to access the Client from a remote computer. **hosted_computer_ip_address** is the IP address of the computer which has the PowerPanel® Business Edition Client installed.

For security purposes, it is recommended you change the login username and password in the Client after login.

Establish Communication between Client and PDU

Setup SNMP Community between the Client and the PDU

The community is used for authentication processing on communication between the Client and the PDU. The

communities of the Client and the PDU must be matched. Users can setup the community on the *Community* field on **Network/SNMP Settings** page in the PDU and also can setup this community on *SNMP Community* field of the **Security/Authentication** page in the Client.

For security purposes, it is recommended to change the community in both sides. When the community in the PDU is changed, the community in the Client is also changed to match with the community in the PDU.

Refer to the **Security/Authentication** chapter on the user manual for more details about how to set up the matched communities.

*Note: The default community is **private** with read/write permission or **public** with read only permission in PDU.*

Assign a PDU IP Address in Client

Communication can be established through the network by assigning the Client an IP Address of the PDU. The IP address of the PDU can be assigned on the *Address* field of the *Device Network Address* block on the **Power Device/Communication** page in Client. To identify the IP address, users can pick an address from the device list which shows all devices on the local network. In order to ensure the PDU responds to the Client, the community configuration must be setup properly.

Assign Connected Outlet in Client

On the *Outlet* block of the **Power/Configuration** page, users can assign the PDU outlet which supplies power to the Client computer. The Client detects whether the off-delay time on the assigned outlet is sufficient for the hosted computer to shut down completely. If the configured time is insufficient, a message will display on the **System/Summary** page in the Client. Outlet assignment should match the outlet which is being used by the Client computer. In case the outlet assignment doesn't match with the actual connection, a different device on the assigned outlet would lose power and finally results in data loss or system crash because of no complete shutdown.

Setup Necessary Shutdown Time

Each computer running the Client requires the sufficient time to be shut down completely before the PDU turns off the connected outlet for any reason. Therefore users could set up this sufficient time at the *Necessary shutdown time* option on **Event Action/Action Settings** page in the Client.

When the PDU outlet connected to a computer running Client is to be turned off, the outlet should not be turned off by the PDU until the Client computer is shut down completely. Make sure that the *Off Delay Time* for the connected outlet is setup properly in the **Outlet/Configuration** page in the PDU.

The Client will detect whether the off-delay time is sufficient for the Client computer to shut down gracefully and give a warning to users that the computer running Client could be shut down improperly due to insufficient time. Click the **Setup** button in the warning block to set up a sufficient time for the *Delay Off Time* setting on the connected outlet of the PDU. Users can also set up the sufficient time on *Delay Off Time* manually in the

PDU web interface.

Configure Startup and Shutdown of Virtual Machines on VMWare ESX/ESXi 4

In order to assure that all virtual machines and VMware ESX/ESXi server host could be shut down gracefully, use **vSphere Client** to configure the automatic startup and shutdown for virtual machines on VMware ESX/ESXi server host. Following procedure will guide you to configure the automatic startup and shutdown properties of each virtual machine:

● Select topmost VMware ESX/ESXi server host from the tree hierarchy on the left side. Go to **Configuration** → **Virtual Machine Startup/Shutdown** menu → **Properties**.
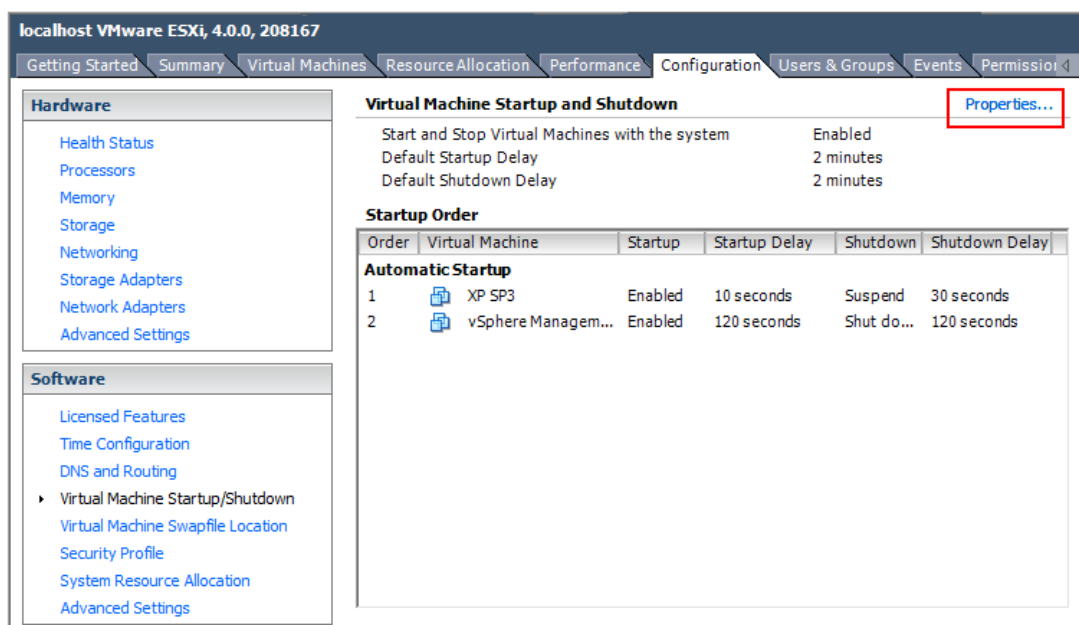
● Set **Allow virtual machines to start and stop automatically with the system** option enabled and move all virtual machines from **Any Order** to **Startup Order**. The **Shutdown Action** option of the **Default Shutdown Delay** block should be changed to **Suspend** to protect all virtual machines.
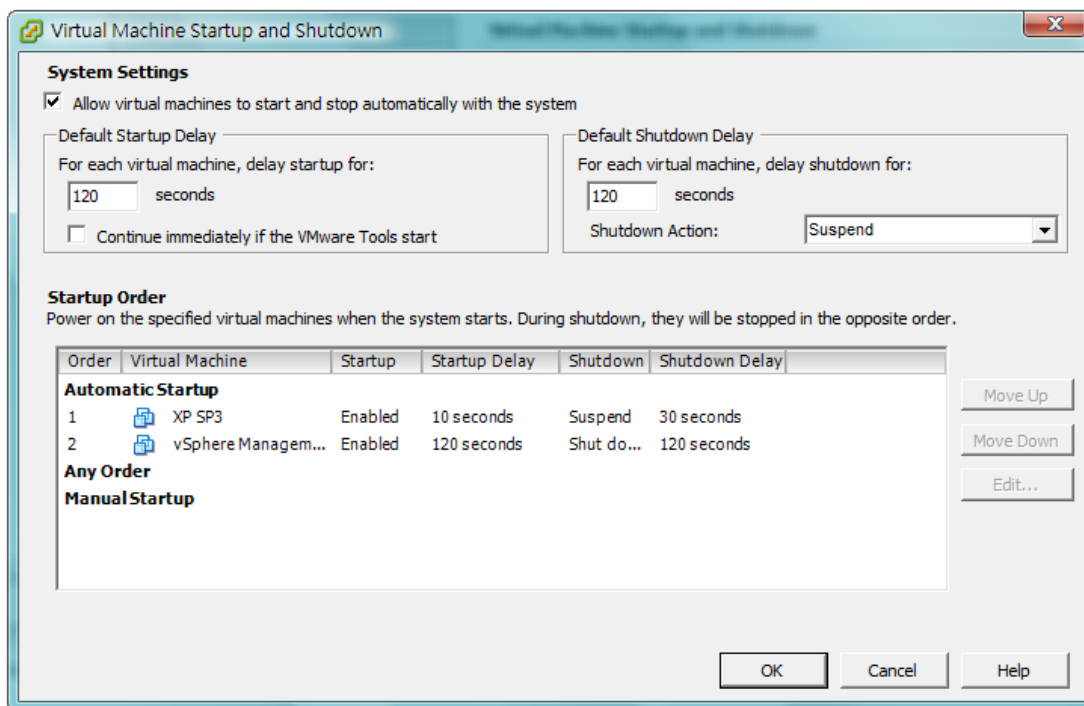
Configure Command Execution for VMWare ESXi 4

*(**Note:** Settings described in this section are not required on VMWare ESX 4)*

In order to assure the ESXi host and all virtual machines can be shut down correctly in case of power events, users have to edit the command script files for specific event to shutdown ESXi host from vMA. Refer to the examples of **shutdown.sh** in the **extcmd** directory of installation folder. Then configure the command file fields to have **shutdown.sh** selected on events which are configured with shutdown action in the Event Action/Events page. These events include *Shutdown time is insufficient* event. That ensures the command able to be executed when these events occur.

Fill in the **$host_username** and **$host_password** with actually username and password for the ESXi host in the **shutdownHostViaSOAPAPICall.pl** of the **/extcmd/etc** directory:

> *…. (snippet)…*
>
> *my $host_username = 'your_username';*
>
> *my $host_password = 'your_password';*
>
> *…. (snippet)…*

And add a line of the VMWare ESXi 4 installed computer (ESXi host) address in the **hostlist** file of the **/extcmd/etc** directory:

> *192.168.1.2*

Proper Operation in PDU

Once a computer running the Client connects to a PDU outlet, users must use a sequenced off/reboot command and not an immediate off/reboot command to control outlets in PDU web interface. A sequenced

off/reboot command provides sufficient time for the Client to shut the computer down properly.