

Installation Guide

PowerChute™ Network Shutdown v4.2

Windows®

Linux®/Unix®

Mac OS® X

Hyper-V®/SCVMM®

VMware®

990-2838L-001

07/2016



Schneider Electric Legal Disclaimer

The information presented in this manual is not warranted by Schneider Electric to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Copyright, intellectual, and all other proprietary rights in the content (including but not limited to software, audio, video, text, and photographs) rests with Schneider Electric or its licensors. All rights in the content not expressly granted herein are reserved. No rights of any kind are licensed or assigned or shall otherwise pass to persons accessing this information.

This Publication shall not be for resale in whole or in part.

PowerChute™ Network Shutdown (PowerChute) works in conjunction with the UPS Network Management Card (NMC) to provide network-based shutdown of multiple computer systems.

In the case of a UPS critical event, the software performs a graceful, unattended system shutdown before the UPS battery is exhausted. The number of protected systems is limited only by the capacity of the UPS.

View these [Application Notes](#) for detailed information on using PowerChute in specific environments.



After installation, it is essential to configure the software using the PowerChute Setup wizard. This ensures that PowerChute is aware of UPS critical events in order to protect your system.

Product Center

The PowerChute [Product Center](#) page has many links to useful up-to-date information. This includes background information on virtualization, loss of communications, and application notes which discuss varied subject matter including possible UPS configurations.

Software and Hardware Requirements

To install PowerChute Network Shutdown (PowerChute), you must have the following:

- A supported **operating system** and web **browser**, as listed on the website, [Operating System and Compatibility Chart](#). For VMware®, a licensed version of ESXi is required. PowerChute does not support the free version of ESXi.

- **Disk space**

Task	Disk Space Required
Commence PowerChute Network Shutdown installation process	100 MB
Install PowerChute Network Shutdown using a virtual appliance - Disk format: thin provisioned	2 GB
Install PowerChute Network Shutdown using a virtual appliance - Disk format: thick provisioned	3 GB
Installing PowerChute Network Shutdown with a private JRE	135 MB
Installing PowerChute Network Shutdown when a public JRE is already installed	15 MB

- **JRE**

You must have a supported Java™ Runtime Environment (JRE), as seen for the different [operating systems](#)

PowerChute gives you the option of installing a “private” JRE.



If there is no supported public JRE present on the OS, then you have to choose the private JRE option to continue with the installation. The minimum supported JRE is Java 8.

For most operating systems, you can download a Java Runtime Environment from <http://java.com>.

Note: For Mac OS® X, JDK 8 or greater must be installed as the JRE does not contain the required files to run PowerChute. JDK 8 can be downloaded from the [Oracle website](#) - select the JDK download option.

- The **computer hardware** requirements are a 700 MHz processor and 256 MB of memory.
- On a graphical interface with PowerChute: A monitor with a minimum resolution of 800 x 600; however, 1024 x 768 or greater is recommended.

- A **UPS** with a Smart Slot and a **Network Management Card** (part number AP9617, AP9618, AP9619, AP9630, AP9631, AP9635) with a firmware version of 3.3.1 or later, or a Symmetra PX2 (which has an internal Network Management Card, OG-9354).
 - You can update your NMC firmware from the [APC website](#).
- PowerChute Network Shutdown cannot be used with PowerNet SNMP Adapters (cards). If your card has a part number of AP9605, AP9606, AP9205, or AP9603, it is not compatible with PowerChute Network Shutdown.
- You must know the **IP address** for each NMC.
- PowerChute can use IPv4 or IPv6 to communicate with the Network Management Card(s). IPv6 support is available only for Network Management Card firmware 6.0.X or higher.

- **Firewall**

PowerChute needs to be able to connect to the NMC Web Access port (default: TCP port 80) and receive data inbound to UDP port 3052. If SNMP is enabled, PowerChute needs to be able to receive data inbound on the SNMP port configured during installation (the default port is 161). You must also configure the firewall to allow traps to be sent to the port of the configured trap receiver.

When the Windows® Firewall is enabled, you can allow the PowerChute installation to configure the firewall automatically for the required ports.

- Windows **PowerShell 2.0** or higher is required for Hyper-V® support on PowerChute. For instructions on how to install PowerShell 2.0 on Windows Server 2008, see [http://msdn.microsoft.com/en-us/library/ff637750\(v=azure.10\).aspx](http://msdn.microsoft.com/en-us/library/ff637750(v=azure.10).aspx).
- You must have **administrator or root privileges** to run the installer.
- You must **uninstall** PowerChute Plus, PowerChute Business Edition, PowerChute Personal Edition, and PowerChute Server before installing PowerChute Network Shutdown.

- **SNMP MIB**

To access PowerChute Network Shutdown via SNMP using a Network Management System (NMS), it may be necessary to first install the APC PowerNet MIB on the NMS. To get the latest version of the PowerNet MIB:

1. Visit the APC Website at <http://www.apc.com/tools/download/index.cfm>
2. Select **Firmware Upgrades - MIB** from the **Software/Firmware** dropdown list.
3. Install the MIB on the NMS by following the instructions in the NMS User Guide.

The PowerNet MIB is also available in the `group1` folder of the PowerChute installation directory.

Preliminary Steps in Installing

To install and operate the PowerChute Network Shutdown software, perform the following steps first.

1. Install the Network Management Card (NMC) in your UPS and configure it with an IP address before beginning the PowerChute installation.

For installation instructions, see the Network Management Card installation guide.

2. Using the NMC user interface, configure the UPS and the Network Management Card. At a minimum, perform these tasks:
 - a. When configuring a shutdown, set the **Low Battery Duration** field value to at least five minutes.
 - b. Set the **authentication phrase** for the administrator.



The administrator authentication phrase and the administrator user name must be the same for the NMC and PowerChute.

In the NMC, the default administrator user name and password are both **apc**, while the default setting for the authentication phrase is **admin user phrase**. We recommend that you change the defaults for security reasons.

Different NMC account types and PowerChute

With firmware version 6.0.6 and above of the NMC, it is possible to add multiple users with different account types - Administrator, Device, Read-only, and Network-Only.

PowerChute can use an Administrator or Device account instead of the built-in "apc" account to communicate with the NMC.

To do this:

1. Create an account on the NMC, either an Administrator or Device account, using **Configuration - Security - Local Users - Management**.

You must log on using the superuser account ("apc") to add new users.

2. On the NMC user interface, go to the **Configuration - Shutdown** page.
3. Select the new account you created from the **User Name** drop-down under **PowerChute Shutdown Parameters**.
4. Use the same user name in PowerChute. The Authentication Phrase must also match.

Installation Guide

PowerChute Network Shutdown

Windows

Installing PowerChute Network Shutdown

See these sections:

- [Installing on Windows and Windows Server Core](#)
- [Upgrading the Software](#)
- [Uninstalling on Windows](#)
- [Silently Installing the Software](#)

Installing on Windows and Windows Server Core



To install on Windows in order to monitor a VMware host, see the [VMware](#) section of this help.

To install on Hyper-V or SCVMM, see the [Hyper-V/SCVMM](#) section of this help.

Follow these steps below.

1. Locate the PowerChute installation executable file, **Setup-x32.exe** or **Setup-x64.exe**, on the PowerChute CD or download it from the [APC website](#). You must have administrator rights to run the installer.

Double-click on the file.

(If you downloaded from the website, you need to extract the exe file from the zip file).

2. A warning dialog, below, displays if you downloaded the exe from the web: click the **Run** button.

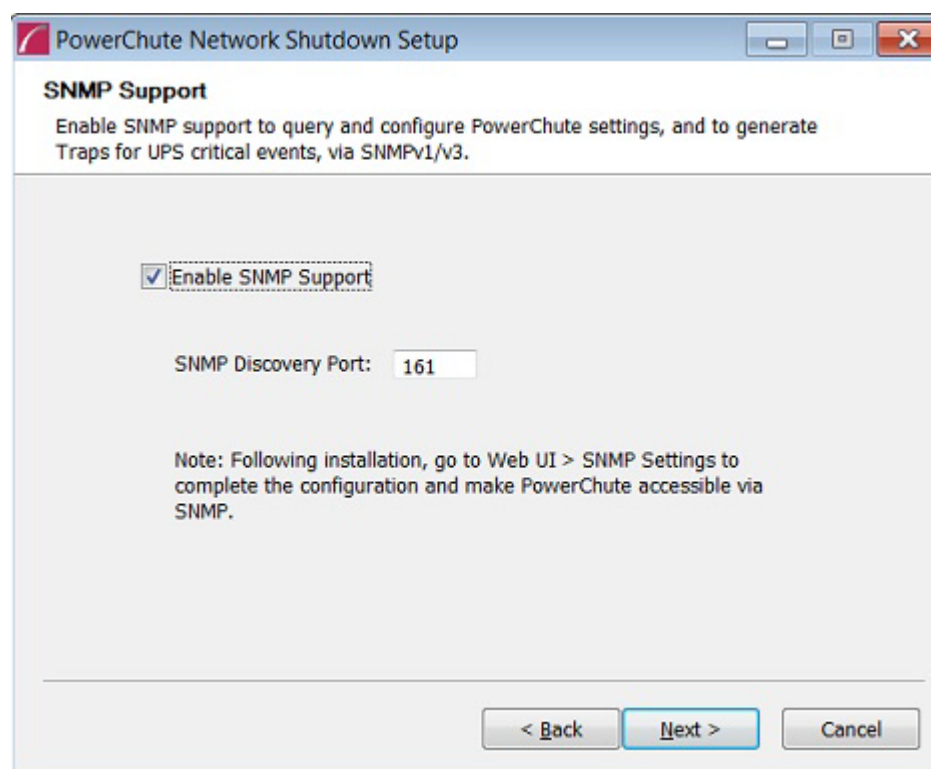


3. At the welcome dialog, click on **Next** to continue.
At the License Agreement dialog, if you agree with the terms, click **I Agree** to continue.
4. When configuring for a Java Runtime Environment (JRE), the PowerChute installer checks the Windows Registry to determine if a supported public JRE version is installed. If a valid public JRE is detected, you can choose between using it or the private JRE that is bundled with PowerChute.



See [JRE](#) for information on using a public or a private JRE installation.

5. The SNMP Support dialog is shown:



Select the checkbox to **Enable SNMP Support**.

NOTE: If SNMP support is not enabled during installation, it cannot be subsequently enabled through the PowerChute Configuration Wizard, and no options relating to SNMP will be available in the web user interface, or via the configuration INI file.

Enter the **SNMP Discovery Port**. The default value of 161 is automatically populated, but this can be edited if this port is already in use. The Port number availability is automatically checked, and if it is not available, a new port number must be entered to proceed.

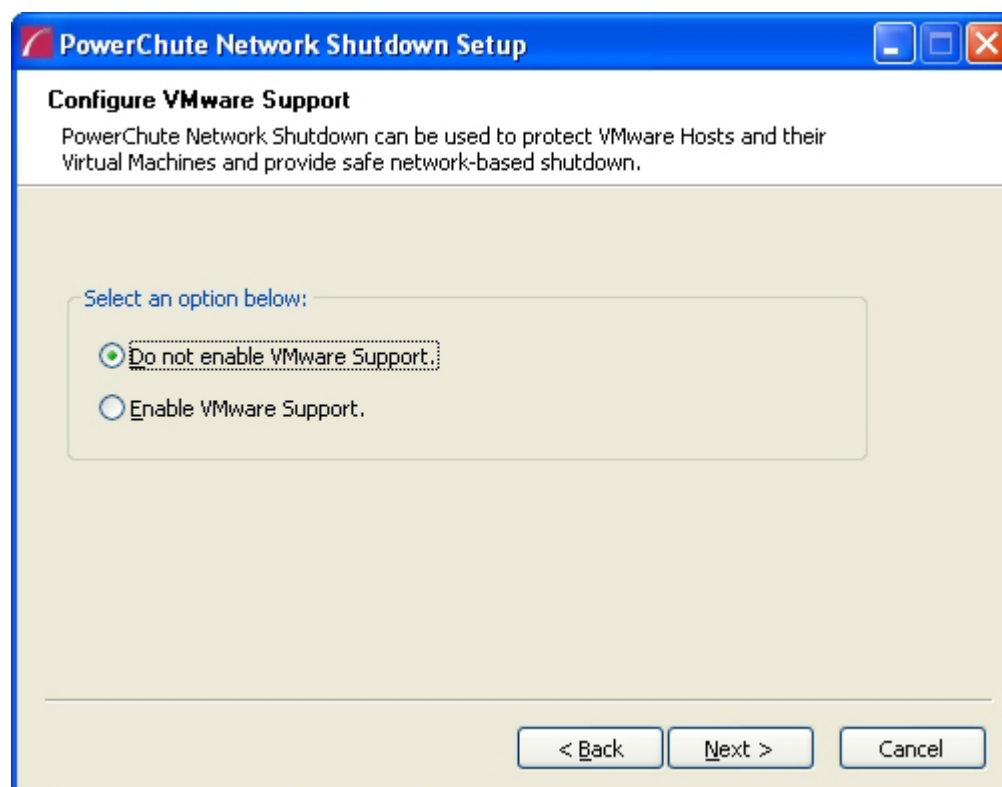
If the Windows firewall is enabled, make sure that PowerChute can receive inbound data to port 161. See [Firewall](#) for more information.



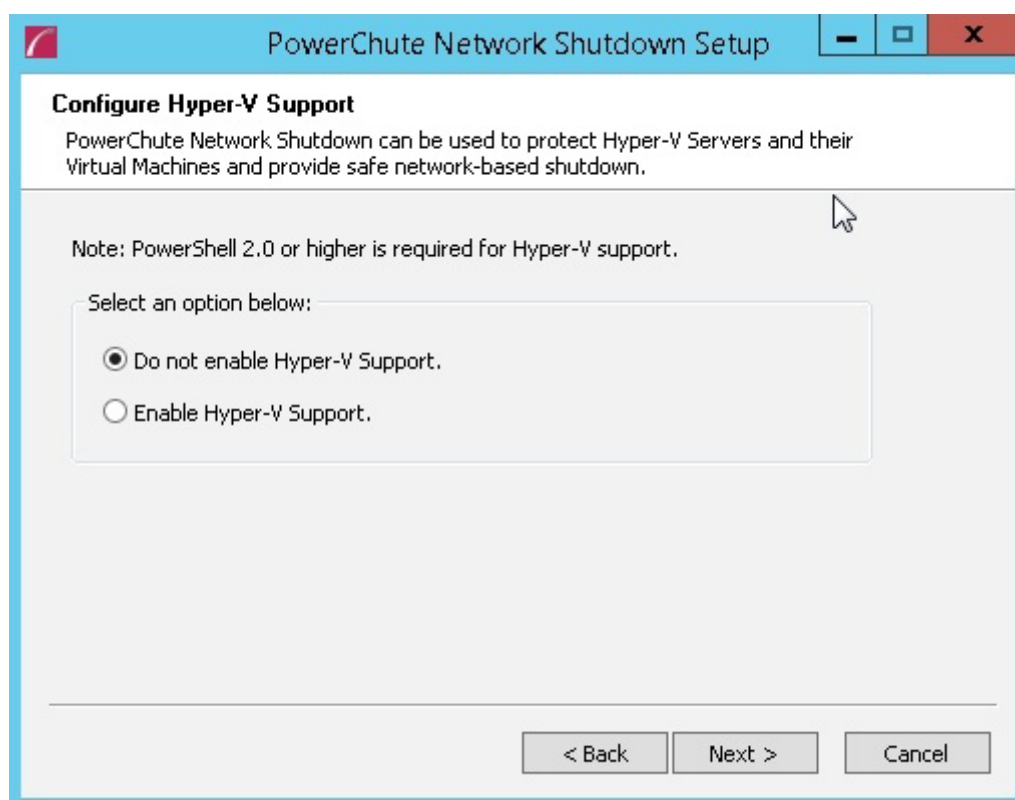
Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.

Click **Next** to continue.

6. If Hyper-V is not detected, you see the VMware Support dialog shown below; choose **Do not enable VMware Support**.



If Hyper-V is detected, you see the Hyper-V Support dialog shown below; choose **Do not enable Hyper-V Support** and click Next to proceed.



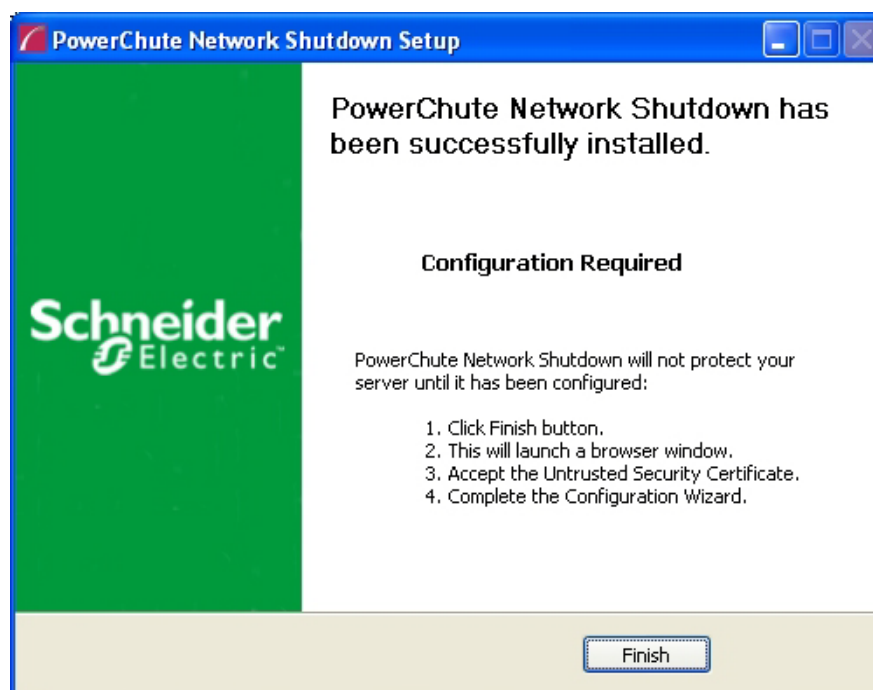
7. Enter an installation folder location or accept the default.

8. When your Windows Firewall is enabled, you can allow the PowerChute installation to configure the firewall automatically by choosing **Yes** when prompted:

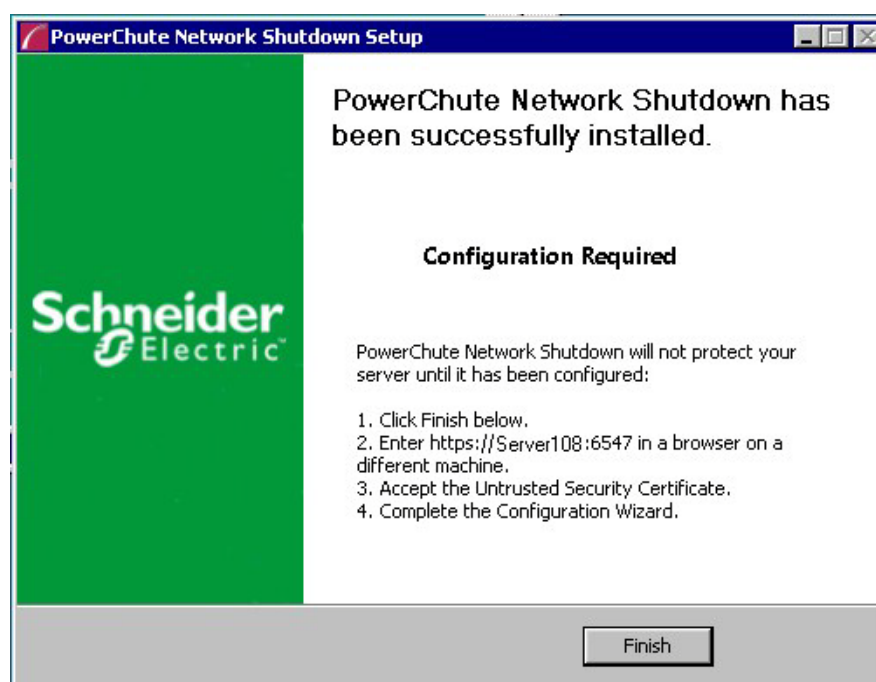
PowerChute Network Shutdown ports must be opened in the Windows Firewall to enable communication with the Network Management Card(s). Would you like this configuration to be performed automatically?

See [Firewall](#) for more information.

After installation, it is necessary to configure PowerChute in order to protect your system. On Windows, the PowerChute setup wizard opens automatically after you click the **Finish** button on this dialog:



On Windows Server Core, you see the following dialog, follow the steps there:



Upgrading the Software

If you have v3.1 or higher of PowerChute already installed on your target machine, the installation process asks you whether you want to perform an upgrade rather than a complete installation. Upgrading enables you to retain your existing configuration settings.

For earlier versions of PowerChute, you must uninstall the software before installing v4.2.

It is not necessary to run the PowerChute setup wizard after the upgrade on Windows.



You cannot upgrade from a 32-bit version to a 64-bit version of PowerChute, you must do a full installation. Also, you must manually uninstall the old version first.

Following the upgrade installation, to ensure that the PowerChute user interface enhancements are applied correctly, it is necessary to clear the browser history:

- In Internet Explorer - select **Tools > Safety > Delete browsing history**
- In Chrome - select **Settings > Show advanced settings > Privacy > Clear browsing data**
- In Firefox - select **Open Menu > History > Clear Recent History**

Uninstalling on Windows

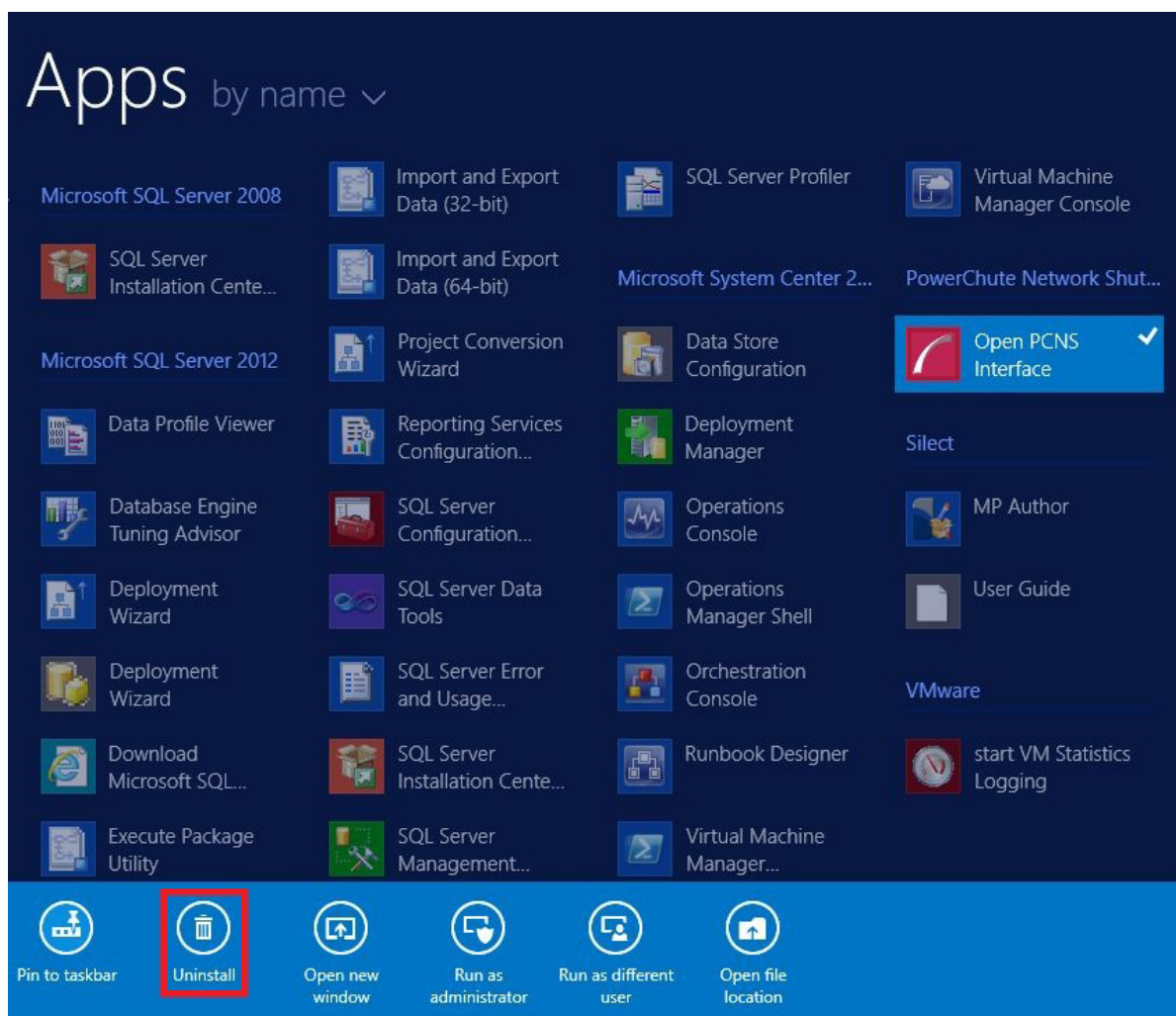
On Windows, use the **Uninstall** option under **PowerChute Network Shutdown** in the Windows Start menu.

On Windows Server Core, follow these steps.

1. Open a command prompt window.
2. Type `C:\Program Files\APC\PowerChute\uninstall.exe` and press Enter.

On Windows Server 2012, PowerChute must be uninstalled using Add/Remove Programs.

1. Right-click the PowerChute Network Shutdown menu option in the **Start** menu.
2. Click **Uninstall** in the options menu that displays on the bottom of the screen.



To uninstall in silent mode:

1. Open a command prompt.
2. Type `"C:\Program Files\APC\PowerChute\uninstall.exe" /S` and press return.

Silently Installing the Software

Installing silently means the installation is unattended or non-interactive.



It is not possible to roll out your event configurations or shutdown settings using a silent installation. You can however, use `pcnsconfig.ini` to do this. See the section on INI files in the online help.



PowerChute only supports silent installation in Single, Redundant and Parallel UPS configurations.

Silent Install on Windows

Perform the following steps:

Edit the silent installations file to set the required parameters; see [Editing your silent installation file](#).

1. Type the following on one line at the Windows command line:

```
Setup.exe /S /F silentInstall.ini
```



If a silent installation fails, see [Appendix A: Error codes for silent installations](#).

Editing your silent installation file

On Windows operating systems, the file that guides silent installations is named **silentInstall.ini**.

The file is a plain text file and can be edited with a standard text editor. Each field or line has a value that the installer needs in order to carry out the installation. The table below explains the fields available in the silent installation file.

Field name	Description
applicationDirectory=	Specifies the installation folder. Type the folder name after "=", ensuring it has valid characters for the operating system. Note: You can't use multiple-byte characters (Chinese for example) and some single byte high-ASCII characters, e.g. ß, é, à, in the installation path.
ACCEPT_EULA=yes	Yes signifies acceptance of the software licence agreement. The installation will not proceed unless yes is specified here.
*INSTALL_JAVA=System PCNS	The value <code>System</code> here signifies you want to use the public JRE for your PowerChute installation. The value <code>PCNS</code> here signifies you want to use the private JRE.
*The installation detects whether the JRE meets the requirements, see JRE .	
REGISTER_WITH_NMC=yes no	Using yes or no, specify whether PowerChute should be registered with the Network Management Card (NMC) or not.
MODE=single redundant parallel	Use single, redundant, or parallel to specify the UPS configuration mode. For detailed information, see "PowerChute Network Shutdown Operating Modes and supported UPS Configurations" here .
NETWORKCONFIG=IPv4 IPv6	Specify your Internet protocol with IPv4 or IPv6.
IPv6NETWORKCONFIG= unicast multicast	When you are using IPv6 only (you entered NETWORKCONFIG= IPv6 above) you must specify the communication mechanism here. See also UNICAST_ADDRESS= and MULTICAST_ADDRESS= . For detailed information, see "The Communications Process of PowerChute Network Shutdown" here .
IP_1= IP_2= IP_3= IP_4= IP_5= IP_6= IP_7= # IP_8= # IP_9=	On each line, specify the IP address of each NMC that will be communicating with this PowerChute installation. You can comment out unneeded entries by putting the # character at the beginning of the line (see examples 8 and 9).

Field name	Description
IP_1_Outlet= IP_2_Outlet= IP_3_Outlet= IP_4_Outlet= IP_5_Outlet= IP_6_Outlet= IP_7_Outlet= # IP_8_Outlet= # IP_9_Outlet=	<p>This applies only to UPS devices with outlet groups (for example, Smart-UPS SMX and SMT devices). Specify the outlet group that supplies power to the PowerChute installation.</p> <p>On a UPS that has only Switched Outlet Groups, "IP_1_Outlet" must be set to "1". If you enter "0", PowerChute may not correctly identify Outlet events associated with the first Outlet group.</p> <p>On a UPS that has both a Main Outlet Group (not switched) and Switched Outlet Groups, "IP_1_Outlet" must be set to "0".</p> <p>You can comment out entries not needed by putting the # character at the beginning of the line (see examples 8 and 9).</p>
PORT=	This is the NMC web port: 80 for HTTP; 443 for HTTPS.
PROTOCOL= HTTP HTTPS	Use HTTP or HTTPS to specify which protocol you are using.
ACCEPTCERTS= YES NO	<p>When using the HTTPS protocol, SSL certificates are used to secure the connection. By default the NMC use a self-signed certificate, which needs to be accepted.</p> <p>Select YES to automatically accept a self-signed certificate.</p> <p>Select NO to accept a connection only if the NMC is configured with a valid certificate.</p>
USERNAME= PASSWORD= AUTHENTICATION_PHRASE=	<p>Enter the user name, password, and authentication phrase to validate PowerChute communication with the NMC. (The authentication phrase reverts to the default if not specified).</p> <p>Note: We recommend that you change the defaults for security reasons.</p> <p>The acceptable characters for username and password are:</p> <ul style="list-style-type: none"> • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: _ ! \ " # \$ % & ' () * + , - . / : ; < = > ? @ ^ ` { } [] ~ <p>The password length must be from 3–32 characters, and the username from 3–10 characters. The authentication phrase must be 15–32 ASCII characters.</p>
LOCAL_IP_ADDRESS=	This information applies to a PowerChute server with multiple network cards. Use it to specify the IP address of the card that will communicate with PowerChute.
UNICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and unicast in IPV6NETWORKCONFIG= unicast multicast , you must specify your unicast host address here.
MULTICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and multicast in IPV6NETWORKCONFIG= unicast multicast , the Network Management card will send UDP packets to the multicast address you specify here.
SNMPv1	
ENABLE_SNMPV1_ACCESS = True False	Specify true to enable SNMPv1 access and false to disable SNMPv1 access.
NAME_COMMUNITY_N =	Enter the community name, up to 15 ASCII characters.
NMS_COMMUNITY_N=	Enter the IP address of the Network Management System.

Field name	Description
ACCESS_TYPE_COMMUNITY_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMP community string: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT =	Specify the SNMP Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMPv3	
ENABLE_SNMPV3_ACCESS = True False	Specify True to enable SNMPv3 access and false to disable SNMPv3 access.
USERNAME_PROFILE_N =	Specify the user name of the SNMPv3 user profile, up to 32 ASCII characters.
AUTH_PASSPHRASE_PROFILE_N =	Enter the Authentication passphrase of 8-32 ASCII characters.
PRIV_PASSPHRASE_PROFILE_N =	Enter the Privacy passphrase of 8-32 ASCII characters.
AUTH_PROTOCOL_PROFILE_N = MD5 SHA1 SHA256 SHA512 NONE	Specify the Authentication protocol of the SNMPv3 user profile.
PRIV_PROTOCOL_PROFILE_N = AES128 AES192 AES192EX AES256EX AES256 DES NONE	Specify the Privacy protocol of the SNMPv3 user profile. See the “ <i>SNMP Troubleshooting</i> ” topic of the <i>PowerChute Network Shutdown User Guide</i> available on www.apc.com for more information on JRE requirements for AES-192/Ex and AES-256/Ex.
ACCESS_TYPE_PROFILE_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMPv3 user profile: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT=	Specify the SNMP discovery Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMP Traps	
UPSCriticalEvents_Enabled = True False	Specify True to enable SNMP Traps for UPS Critical Events.
UPSCriticalEvents_SendClearingTrap = True False	Enter True to send a Trap once a UPS Critical Event has cleared.
UPSCriticalEvents_Delay =	Specify the length of time in seconds that the UPS Critical Event must persist before a trap is sent.
UPSCriticalEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
UPSCriticalEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the UPS Critical Event is cleared.
UPSCriticalEvents_RepeatTimes =	Specify the number of times the trap is sent when the UPS Critical Event occurs.
LostCommsEvents_Enabled = True False	Specify True to enable SNMP Traps for Lost Communication Events.
LostCommsEvents_SendClearingTrap = True False	Enter True to send a Trap once a Lost Communication Event has cleared.

Field name	Description
LostCommsEvents_Delay =	Specify the length of time in seconds that the Lost Communication Event must persist before a trap is sent.
LostCommsEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
LostCommsEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the Lost Communication Event is cleared.
LostCommsEvents_RepeatTimes =	Specify the number of times the trap is sent when the Lost Communication Event occurs.
Enabled_TrapReceiver_N = True False	Enter True to enable the Trap Receiver.
NMS_TrapReceiver_N =	Enter the IP address of the Network Management System that will receive traps.
Port_TrapReceiver_N =	Enter the port number of the Trap Receiver.
Type_TrapReceiver_N = v1 v3	Enter the version of SNMP used to send the traps.
ProfileName_TrapReceiver_N =	Enter the User Name of the SNMPv3 User Profile used to send the traps.
Note: N indicates an integer (0-N)	

Installation Guide

PowerChute Network Shutdown

Linux/UNIX

Installing PowerChute Network Shutdown

See these sections:

- [Installation Steps on Linux and UNIX](#)
- [Upgrading the Software](#)
- [Uninstalling on Linux and UNIX](#)
- [Silently Installing the Software](#)

Installation Steps on Linux and UNIX

These instructions also apply when installing on Solaris, AIX and HP-UX. You must have root privileges to perform the installation.



When installing on Solaris:

- Java 7 is bundled with the 32-bit version of PowerChute
- Java 8 is bundled only with the 64-bit version of PowerChute

1. If you are installing from the CD, locate your installation files in one of the following directories on the CD: Linux_x32 or Linux_x64. Copy them to a temporary directory on your server.
2. If you are installing from the website, locate the file `pcns420Linux.tar.gz` on the APC website and copy it to a temporary directory on your server.

Change your working directory to the temporary directory. Then type the following commands:

```
gunzip pcns420Linux.tar.gz
tar -xf pcns420Linux.tar
```

3. If you are not logged on as the root user, you need to run the installer using `sudo`, or switch to root user context using the `su` command and then run the installer.

```
./install.sh
```



After a web download you need to grant execute permissions:

```
chmod +x install.sh
```

On HP-UX type the command `su - root` before running

```
./install.sh
```

4. At the License Agreement, if you agree with the terms, type Yes and press the Enter key to continue. Type No to exit.
5. When configuring for a Java Runtime Environment (JRE), if a valid public JRE is detected, you can choose between using it or the private JRE that is bundled with PowerChute (see [JRE](#)). The private JRE is not available for AIX or HP-UX.

If using the public JRE, you must enter its path. Enter an installation folder location or accept the default.

You cannot specify a directory name that contains a space, either for the installation or the Java directory. If you do not specify an installation directory, it will be installed to the default: `/opt/APC`.

6. Enter **Yes to Enable SNMP Support** and enter the **SNMP discovery port**. If the default port number 161 is unavailable, enter another available port number.

If a firewall is configured, make sure that PowerChute can receive inbound data to port 161. See [Firewall](#) for more information.

NOTE: If SNMP support is not enabled during installation, it cannot be subsequently enabled through the PowerChute Configuration Wizard, and no options relating to SNMP will be available in the web user interface, or via the configuration INI file.



Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.

After installation, it is necessary to configure your system in order to protect it. You must open the browser and enter the PowerChute URL:

`https://<your_machine_name>/IP:6547`

Follow the steps in the PowerChute setup wizard to complete your configuration.

Upgrading the Software

If you have v3.1 or higher of PowerChute already installed on your target machine, the installation process asks you whether you want to perform an upgrade rather than a complete installation. Upgrading enables you to retain your existing configuration settings.

After an Linux upgrade, it is not necessary to run the PowerChute setup wizard.



You cannot upgrade from a 32-bit version to a 64-bit version of PowerChute, you must do a full installation. Also, you must manually uninstall the old version first.

Following the upgrade installation, to ensure that the PowerChute user interface enhancements are applied correctly, it is necessary to clear the browser history:

- In Internet Explorer - select **Tools > Safety > Delete browsing history**
- In Chrome - select **Settings > Show advanced settings > Privacy > Clear browsing data**
- In Firefox - select **Open Menu > History > Clear Recent History**

Uninstalling on Linux and UNIX

On Linux:

- Run the uninstall script located in the PowerChute directory from a terminal prompt.

```
/opt/APC/PowerChute/uninstall
```

- To uninstall in **silent mode**, run the uninstall script located in the PowerChute directory, with the `-q` option.

```
/opt/APC/PowerChute/uninstall -q
```

- On UNIX, when the daemon starts, the script adds 1024 file handles. Delete `ulimit -n 1024` from the PCNS startup script if you do not need them at:

```
/opt/APC/PowerChute/group1/powerchute.sh.
```


Silently Installing the Software

Installing silently means the installation is unattended or non-interactive.



It is not possible to roll out your event configurations or shutdown settings using a silent installation. You can however, use `pcnsconfig.ini` to do this. See the section on INI files in the online help.



PowerChute only supports silent installation in Single, Redundant and Parallel UPS configurations.

Silent Install on Linux

Edit the `silentInstall.sample` file to set the required parameters; see [Editing your silent installation file](#).

Type the following command to start the installation, as an administrator:

```
./install.sh -f silentInstall.sample
```



If a silent installation fails, see [Appendix A: Error codes for silent installations](#).

Editing your silent installation file

On the Linux operating system, the file that guides silent installations is named `silentInstall.sample`.

The file is a plain text file and can be edited with a standard text editor. Each field or line has a value that the installer needs in order to carry out the installation. The table below explains the fields available in the silent installation file.

Field name	Description
INSTALL_DIR=	Specifies the installation directory. Type the directory name after "=", ensuring it has valid characters for the operating system. Note: You can't use multiple-byte characters (Chinese for example) and some single byte high-ASCII characters, e.g. ß, é, ä, in the installation path.
JAVA_DIR=	Specifies the JRE directory. Type the path where the public JRE is installed on the system e.g. <code>/usr/local/bin/jre/jre1.X.X_XX</code> . If this value is blank or absent, the private JRE is installed.
ACCEPT_EULA=yes	Yes signifies acceptance of the software licence agreement. The installation will not proceed unless yes is specified here.
REGISTER_WITH_NMC= yes no	Using yes or no, specify whether PowerChute should be registered with the Network Management Card (NMC) or not.
MODE= single redundant parallel	Use single, redundant, or parallel to specify the UPS configuration mode. For detailed information, see "PowerChute Network Shutdown Operating Modes and supported UPS Configurations" here .
NETWORKCONFIG= IPv4 IPv6	Specify your Internet protocol with IPv4 or IPv6.
IPv6NETWORKCONFIG= unicast multicast	When you are using IPv6 only (you entered NETWORKCONFIG= IPv6 above) you must specify the communication mechanism here. See also UNICAST_ADDRESS= and MULTICAST_ADDRESS= . For detailed information, see "The Communications Process of PowerChute Network Shutdown" here .
IP_1= IP_2= IP_3= IP_4= IP_5= IP_6= IP_7= # IP_8= # IP_9=	On each line, specify the IP address of each NMC that will be communicating with this PowerChute installation. You can comment out unneeded entries by putting the # character at the beginning of the line (see examples 8 and 9).

Field name	Description
IP_1_Outlet= IP_2_Outlet= IP_3_Outlet= IP_4_Outlet= IP_5_Outlet= IP_6_Outlet= IP_7_Outlet= # IP_8_Outlet= # IP_9_Outlet=	<p>This applies only to UPS devices with outlet groups (for example, Smart-UPS SMX and SMT devices). Specify the outlet group that supplies power to the PowerChute installation.</p> <p>On a UPS that has only Switched Outlet Groups, "IP_1_Outlet" must be set to "1". If you enter "0", PowerChute may not correctly identify Outlet events associated with the first Outlet group.</p> <p>On a UPS that has both a Main Outlet Group (not switched) and Switched Outlet Groups, "IP_1_Outlet" must be set to "0".</p> <p>You can comment out entries not needed by putting the # character at the beginning of the line (see examples 8 and 9).</p>
PORT=	This is the NMC web port: 80 for HTTP; 443 for HTTPS.
PROTOCOL= HTTP HTTPS	Use HTTP or HTTPS to specify which protocol you are using.
ACCEPTCERTS= YES NO	<p>When using the HTTPS protocol, SSL certificates are used to secure the connection. By default the NMC use a self-signed certificate, which needs to be accepted.</p> <p>Select YES to automatically accept a self-signed certificate.</p> <p>Select NO to accept a connection only if the NMC is configured with a valid certificate.</p>
USERNAME= PASSWORD= AUTHENTICATION_PHRASE=	<p>Enter the user name, password, and authentication phrase to validate PowerChute communication with the NMC. (The authentication phrase reverts to the default if not specified).</p> <p>Note: We recommend that you change the defaults for security reasons.</p> <p>The acceptable characters for username and password are:</p> <ul style="list-style-type: none"> • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: _ ! \ " # \$ % & ' () * + , - . / : ; < = > ? @ ^ ` { } [] ~ <p>The password length must be from 3–32 characters, and the username from 3–10 characters. The authentication phrase must be 15–32 ASCII characters.</p>
LOCAL_IP_ADDRESS=	This information applies to a PowerChute server with multiple network cards. Use it to specify the IP address of the card that will communicate with PowerChute.
UNICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and unicast in IPV6NETWORKCONFIG= unicast multicast , you must specify your unicast host address here.
MULTICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and multicast in IPV6NETWORKCONFIG= unicast multicast , the Network Management card will send UDP packets to the multicast address you specify here.
SNMPv1	
ENABLE_SNMPV1_ACCESS = True False	Specify true to enable SNMPv1 access and false to disable SNMPv1 access.
NAME_COMMUNITY_N =	Enter the community name, up to 15 ASCII characters.
NMS_COMMUNITY_N=	Enter the IP address of the Network Management System.

Field name	Description
ACCESS_TYPE_COMMUNITY_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMP community string: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT =	Specify the SNMP Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMPv3	
ENABLE_SNMPV3_ACCESS = True False	Specify True to enable SNMPv3 access and false to disable SNMPv3 access.
USERNAME_PROFILE_N =	Specify the user name of the SNMPv3 user profile, up to 32 ASCII characters.
AUTH_PASSPHRASE_PROFILE_N =	Enter the Authentication passphrase of 8-32 ASCII characters.
PRIV_PASSPHRASE_PROFILE_N =	Enter the Privacy passphrase of 8-32 ASCII characters.
AUTH_PROTOCOL_PROFILE_N = MD5 SHA1 SHA256 SHA512 NONE	Specify the Authentication protocol of the SNMPv3 user profile.
PRIV_PROTOCOL_PROFILE_N = AES128 AES192 AES192EX AES256EX AES256 DES NONE	Specify the Privacy protocol of the SNMPv3 user profile. See the “ <i>SNMP Troubleshooting</i> ” topic of the <i>PowerChute Network Shutdown User Guide</i> available on www.apc.com for more information on JRE requirements for AES-192/Ex and AES-256/Ex.
ACCESS_TYPE_PROFILE_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMPv3 user profile: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT=	Specify the SNMP discovery Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMP Traps	
UPSCriticalEvents_Enabled = True False	Specify True to enable SNMP Traps for UPS Critical Events.
UPSCriticalEvents_SendClearingTrap = True False	Enter True to send a Trap once a UPS Critical Event has cleared.
UPSCriticalEvents_Delay =	Specify the length of time in seconds that the UPS Critical Event must persist before a trap is sent.
UPSCriticalEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
UPSCriticalEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the UPS Critical Event is cleared.
UPSCriticalEvents_RepeatTimes =	Specify the number of times the trap is sent when the UPS Critical Event occurs.
LostCommsEvents_Enabled = True False	Specify True to enable SNMP Traps for Lost Communication Events.
LostCommsEvents_SendClearingTrap = True False	Enter True to send a Trap once a Lost Communication Event has cleared.

Field name	Description
LostCommsEvents_Delay =	Specify the length of time in seconds that the Lost Communication Event must persist before a trap is sent.
LostCommsEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
LostCommsEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the Lost Communication Event is cleared.
LostCommsEvents_RepeatTimes =	Specify the number of times the trap is sent when the Lost Communication Event occurs.
Enabled_TrapReceiver_N = True False	Enter True to enable the Trap Receiver.
NMS_TrapReceiver_N =	Enter the IP address of the Network Management System that will receive traps.
Port_TrapReceiver_N =	Enter the port number of the Trap Receiver.
Type_TrapReceiver_N = v1 v3	Enter the version of SNMP used to send the traps.
ProfileName_TrapReceiver_N =	Enter the User Name of the SNMPv3 User Profile used to send the traps.
Note: N indicates an integer (0-N)	

Installation Guide

PowerChute Network Shutdown

Mac OS X

Installing PowerChute Network Shutdown

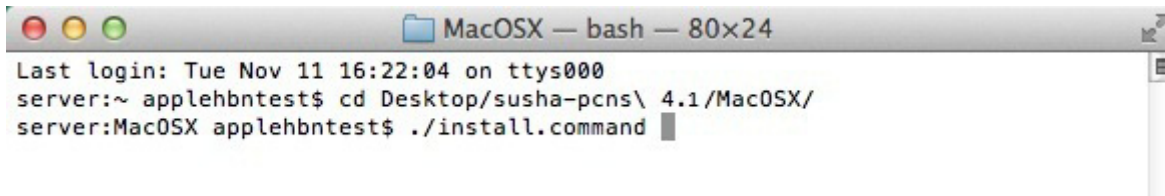
See these sections:

- [Installing on Mac OS X](#)
- [Upgrading the Software](#)
- [Uninstalling on Mac OS X](#)
- [Silently Installing the Software](#)

Installing on Mac OS X

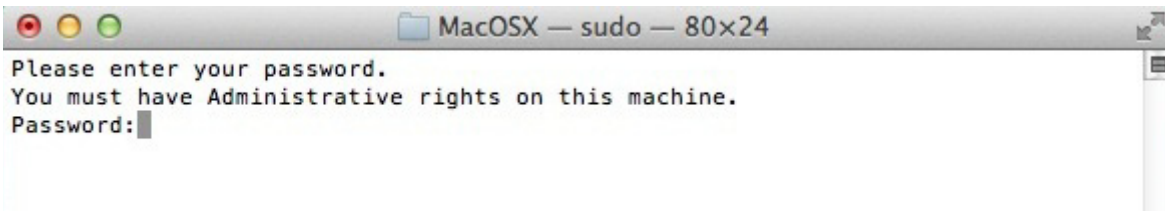
PowerChute must be installed on the machine to be protected. Perform the following steps:

1. Locate the PowerChute installation files on the PowerChute CD, or download it from the [APC website](#). Copy the installation files from the Mac OS X folder to a folder on the Mac.
2. Open a terminal and navigate to the folder containing the installation script.
3. Run `./install.command`



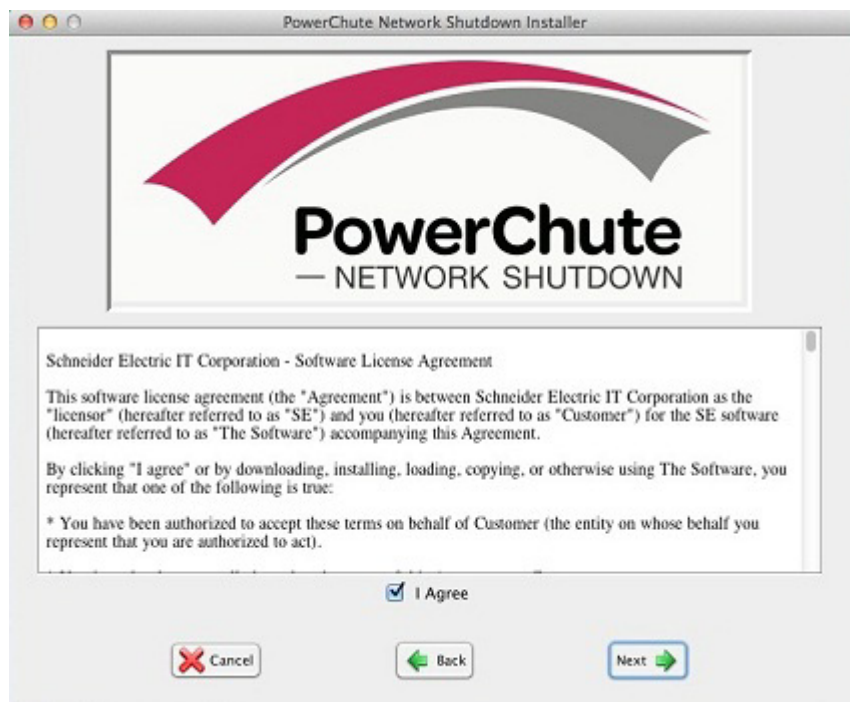
```
MacOSX — bash — 80x24
Last login: Tue Nov 11 16:22:04 on ttys000
server:~ applehbntest$ cd Desktop/susha-pcns\ 4.1/MacOSX/
server:MacOSX applehbntest$ ./install.command
```

4. In the terminal window you will be prompted to enter your password.

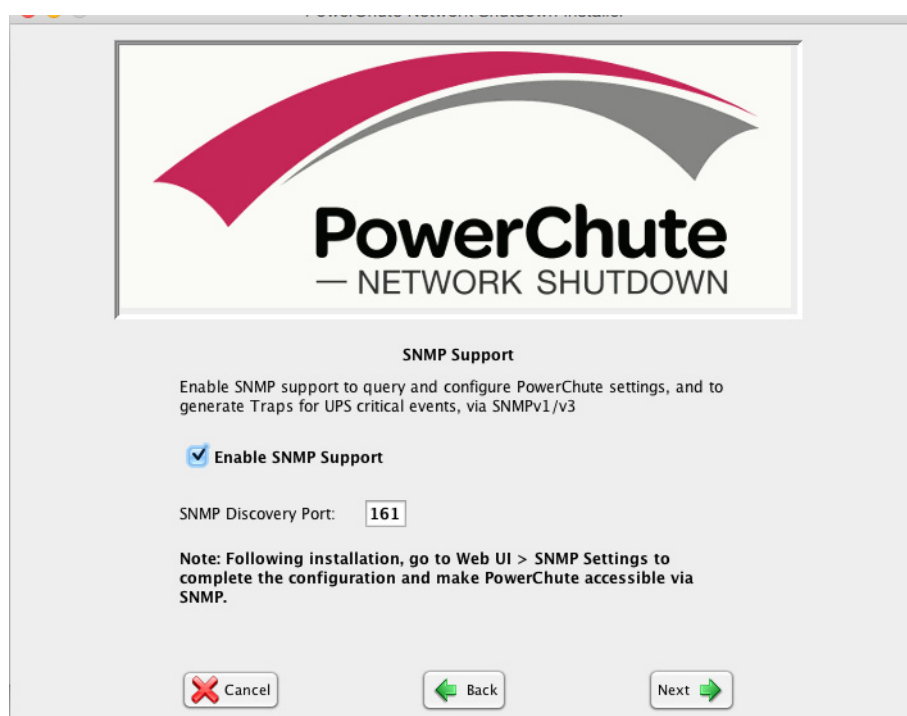


```
MacOSX — sudo — 80x24
Please enter your password.
You must have Administrative rights on this machine.
Password:
```

5. The PowerChute installer will display, click next to accept the License Agreement.



6. Enter the path to the directory in which you want to install PowerChute.
7. The SNMP Support dialog is shown:



Select the checkbox to **Enable SNMP Support**.

NOTE: If SNMP support is not enabled during installation, it cannot be subsequently enabled through the PowerChute Configuration Wizard, and no options relating to SNMP will be available in the web user interface, or via the configuration INI file.

Enter the **SNMP Discovery Port**. The default value of 161 is automatically populated, but this can be edited if this port is already in use. The Port number availability is automatically checked, and if it is not available, a new port number must be entered to proceed.

If a firewall is configured, make sure that PowerChute can receive inbound data to port 161. See [Firewall](#) for more information.



Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.

8. Click **Next** to proceed with the installation. The installation cannot be canceled once it has begun.



9. The installation progress bar will display.



10. When the installation is successful, a window displays to prompt server configuration.



11. Click **Open PCNS in browser** to complete the PowerChute Configuration wizard.



After installation, it is necessary to configure your system in order to protect it. Follow the setup wizard to specify your configuration.

Upgrading the Software

PowerChute cannot be upgraded during installation on Mac OS X. To install a new version of PowerChute, you must manually uninstall the previous version and do a full installation of the latest version PowerChute v4.2.

Uninstalling on Mac OS X

To uninstall PowerChute on Mac OS X:

1. Go to the folder where the installation files have been placed:
`/Users/Shared/Applications/APC/PowerChute`
2. Double click on the file called `uninstall.command`
3. A terminal window opens to prompt you to enter your password.
4. A window opens to confirm the uninstall - click **Yes** to uninstall.



5. A window displays to confirm that uninstallation is complete.



To uninstall in silent mode:

1. In a terminal window, navigate to the folder in which the PowerChute files are installed.
2. Enter the command `./uninstall.command -q`

Silently Installing the Software

Installing silently means the installation is unattended or non-interactive.



It is not possible to roll out your event configurations or shutdown settings using a silent installation. You can however, use `pcnsconfig.ini` to do this. See the section on INI files in the online help.



PowerChute only supports silent installation in Single, Redundant and Parallel UPS configurations.

Silent Install on Mac OS X

Edit the silent installations file to set the required parameters; see [Editing your silent installation file](#).

For an installation on Mac OS X, navigate to the temporary folder on the new server, and type the following command on one line:

```
Install.command -s silentinstall.ini
```



Using `sudo` will always prompt the user to enter a password. To do this completely silently, you could use this command:
`Echo password | sudo -S ./install.command -s`

The `applicationDirectory` should be the first line in the INI file. See [Editing your silent installation file](#).



If a silent installation fails, see [Appendix A: Error codes for silent installations](#).

Editing your silent installation file

The file that guides silent installations in Mac OS X is named **silentInstall.ini**.

Each field or line has a value that the installer needs in order to carry out the installation. The table below explains the fields available in the silent installation file.

Field name	Description
applicationDirectory=	Specifies the installation folder. Type the folder name after "=", ensuring it has valid characters for the operating system. Note: You can't use multiple-byte characters (Chinese for example) and some single byte high-ASCII characters, e.g. ß, é, ä, in the installation path.
ACCEPT_EULA=yes	Yes signifies acceptance of the software licence agreement. The installation will not proceed unless yes is specified here.
REGISTER_WITH_NMC= yes no	Using yes or no, specify whether PowerChute should be registered with the Network Management Card (NMC) or not.
MODE= single redundant parallel	Use single, redundant, or parallel to specify the UPS configuration mode. For detailed information, see "PowerChute Network Shutdown Operating Modes and supported UPS Configurations" here .
NETWORKCONFIG= IPv4 IPv6	Specify your Internet protocol with IPv4 or IPv6.
IPv6NETWORKCONFIG= unicast multicast	When you are using IPv6 only (you entered NETWORKCONFIG= IPv6 above) you must specify the communication mechanism here. See also UNICAST_ADDRESS= and MULTICAST_ADDRESS= . For detailed information, see "The Communications Process of PowerChute Network Shutdown" here .
IP_1= IP_2= IP_3= IP_4= IP_5= IP_6= IP_7= # IP_8= # IP_9=	On each line, specify the IP address of each NMC that will be communicating with this PowerChute installation. You can comment out unneeded entries by putting the # character at the beginning of the line (see examples 8 and 9).
IP_1_Outlet= IP_2_Outlet= IP_3_Outlet= IP_4_Outlet= IP_5_Outlet= IP_6_Outlet= IP_7_Outlet= # IP_8_Outlet= # IP_9_Outlet=	This applies only to UPS devices with outlet groups (for example, Smart-UPS SMX and SMT devices). Specify the outlet group that supplies power to the PowerChute installation. On a UPS that has only Switched Outlet Groups, "IP_1_Outlet" must be set to "1". If you enter "0", PowerChute may not correctly identify Outlet events associated with the first Outlet group. On a UPS that has both a Main Outlet Group (not switched) and Switched Outlet Groups, "IP_1_Outlet" must be set to "0". You can comment out entries not needed by putting the # character at the beginning of the line (see examples 8 and 9).
PORT=	This is the NMC web port: 80 for HTTP; 443 for HTTPS.
PROTOCOL= HTTP HTTPS	Use HTTP or HTTPS to specify which protocol you are using.

Field name	Description
ACCEPTCERTS= YES NO	<p>When using the HTTPS protocol, SSL certificates are used to secure the connection. By default the NMC use a self-signed certificate, which needs to be accepted.</p> <p>Select YES to automatically accept a self-signed certificate.</p> <p>Select NO to accept a connection only if the NMC is configured with a valid certificate.</p>
USERNAME= PASSWORD= AUTHENTICATION_PHRASE=	<p>Enter the user name, password, and authentication phrase to validate PowerChute communication with the NMC. (The authentication phrase reverts to the default if not specified).</p> <p>Note: We recommend that you change the defaults for security reasons.</p> <p>The acceptable characters for username and password are:</p> <ul style="list-style-type: none"> • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: _!\"#\$%&'()*+,-./:;<=>?@^`{ }[]~ <p>The password length must be from 3–32 characters, and the username from 3–10 characters. The authentication phrase must be 15–32 ASCII characters.</p>
LOCAL_IP_ADDRESS=	This information applies to a PowerChute server with multiple network cards. Use it to specify the IP address of the card that will communicate with PowerChute.
UNICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and unicast in IPV6NETWORKCONFIG= unicast multicast , you must specify your unicast host address here.
MULTICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and multicast in IPV6NETWORKCONFIG= unicast multicast , the Network Management card will send UDP packets to the multicast address you specify here.
SNMPv1	
ENABLE_SNMPV1_ACCESS = True False	Specify true to enable SNMPv1 access and false to disable SNMPv1 access.
NAME_COMMUNITY_N =	Enter the community name, up to 15 ASCII characters.
NMS_COMMUNITY_N=	Enter the IP address of the Network Management System.
ACCESS_TYPE_COMMUNITY_N = READONLY READWRITE DISABLED	<p>Specify the Access type of the SNMP community string:</p> <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT =	Specify the SNMP Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMPv3	
ENABLE_SNMPV3_ACCESS = True False	Specify True to enable SNMPv3 access and false to disable SNMPv3 access.
USERNAME_PROFILE_N =	Specify the user name of the SNMPv3 user profile, up to 32 ASCII characters.
AUTH_PASSPHRASE_PROFILE_N =	Enter the Authentication passphrase of 8-32 ASCII characters.
PRIV_PASSPHRASE_PROFILE_N =	Enter the Privacy passphrase of 8-32 ASCII characters.

Field name	Description
AUTH_PROTOCOL_PROFILE_N = MD5 SHA1 SHA256 SHA512 NONE	Specify the Authentication protocol of the SNMPv3 user profile.
PRIV_PROTOCOL_PROFILE_N = AES128 AES192 AES192EX AES256EX AES256 DES NONE	Specify the Privacy protocol of the SNMPv3 user profile. See the “ <i>SNMP Troubleshooting</i> ” topic of the <i>PowerChute Network Shutdown User Guide</i> available on www.apc.com for more information on JRE requirements for AES-192/Ex and AES-256/Ex.
ACCESS_TYPE_PROFILE_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMPv3 user profile: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT=	Specify the SNMP discovery Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMP Traps	
UPSCriticalEvents_Enabled = True False	Specify True to enable SNMP Traps for UPS Critical Events.
UPSCriticalEvents_SendClearingTrap = True False	Enter True to send a Trap once a UPS Critical Event has cleared.
UPSCriticalEvents_Delay =	Specify the length of time in seconds that the UPS Critical Event must persist before a trap is sent.
UPSCriticalEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
UPSCriticalEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the UPS Critical Event is cleared.
UPSCriticalEvents_RepeatTimes =	Specify the number of times the trap is sent when the UPS Critical Event occurs.
LostCommsEvents_Enabled = True False	Specify True to enable SNMP Traps for Lost Communication Events.
LostCommsEvents_SendClearingTrap = True False	Enter True to send a Trap once a Lost Communication Event has cleared.
LostCommsEvents_Delay =	Specify the length of time in seconds that the Lost Communication Event must persist before a trap is sent.
LostCommsEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
LostCommsEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the Lost Communication Event is cleared.
LostCommsEvents_RepeatTimes =	Specify the number of times the trap is sent when the Lost Communication Event occurs.
Enabled_TrapReceiver_N = True False	Enter True to enable the Trap Receiver.
NMS_TrapReceiver_N =	Enter the IP address of the Network Management System that will receive traps.
Port_TrapReceiver_N =	Enter the port number of the Trap Receiver.
Type_TrapReceiver_N = v1 v3	Enter the version of SNMP used to send the traps.
ProfileName_TrapReceiver_N =	Enter the User Name of the SNMPv3 User Profile used to send the traps.

Note: N indicates an integer (0-N)

Installation Guide

PowerChute Network Shutdown

Hyper-V/SCVMM

Installing PowerChute Network Shutdown

See these sections:

- [PowerChute Hyper-V Installation](#)
- [Installing on Windows Hyper-V/SCVMM](#)
- [PowerChute SCVMM Installation](#)
- [Hyper-V and SCVMM Configuration](#)
- [Upgrading the Software](#)
- [Uninstalling on Hyper-V and SCVMM](#)
- [Silently Installing the Software](#)

Using PowerChute in the Hyper-V environment

The Hyper-V server can be part of a Windows failover cluster or a standalone host. If it is part of a cluster, then PowerChute can perform a migration of the virtual machines to any available Hyper-V hosts in the same cluster during a shutdown.

Remote Server Administration Tools

The Remote Server Administration Tools must be installed for Hyper-V and Failover Clustering (Windows Server 2012). The PowerChute powershell scripts will not work correctly (for either VM migration or VM shutdown) if these are not installed.

To verify:

1. Launch Powershell.
2. Run the command `Get-Module -ListAvailable`.
3. Check that Hyper-V and FailoverClusters are shown:

```
PS C:\Users\administrator.SCUMMGAL> Get-Module -ListAvailable
Directory: C:\Windows\system32\WindowsPowerShell\v1.0\Modules

ModuleType Version      Name                               ExportedCommands
-----
Manifest    2.0.0.0      AppLocker                         {Get-AppLockerFile...
Manifest    2.0.0.0      Appx                              {Add-AppxPackage, ...
Manifest    1.0          BestPractices                     {Get-BpaModel, Get...
Manifest    1.0.0.0      BitsTransfer                      {Add-BitsFile, Com...
Manifest    1.0.0.0      BranchCache                      {Add-BCDataCacheEx...
Manifest    1.0.0.0      CimCmdlets                       {Get-CimAssociated...
Binary      2.0.0.0      ClusterAwareUpdating             {Get-ClusterPlugin, Re...
Manifest    1.0.0.0      DirectAccessClientComponents     {Disable-DAManualE...
Script      2.0          Disn                             {Add-AppxProvision...
Manifest    1.0.0.0      DnsClient                       {Resolve-DnsName, ...
Manifest    2.0.0.0      FailoverClusters                 {Add-ClusterCheckp...
Manifest    1.0.0.0      GroupPolicy                     {Backup-GPO, Block...
Binary      1.1          Hyper-V                         {Add-VMHardDrive, A...
```

Installing on Windows Hyper-V/SCVMM

Follow these steps below.

1. Locate the PowerChute installation executable file, **Setup-x64.exe**, on the PowerChute CD or download it from the [APC website](#). You must have administrator rights to run the installer.

Double-click on the file.

(If you downloaded from the website, you need to extract the exe file from the zip file).

2. A warning dialog, below, displays if you downloaded the exe from the web: click the **Run** button.



3. At the welcome dialog, click on **Next** to continue.

At the License Agreement dialog, if you agree with the terms, click **I Agree** to continue.

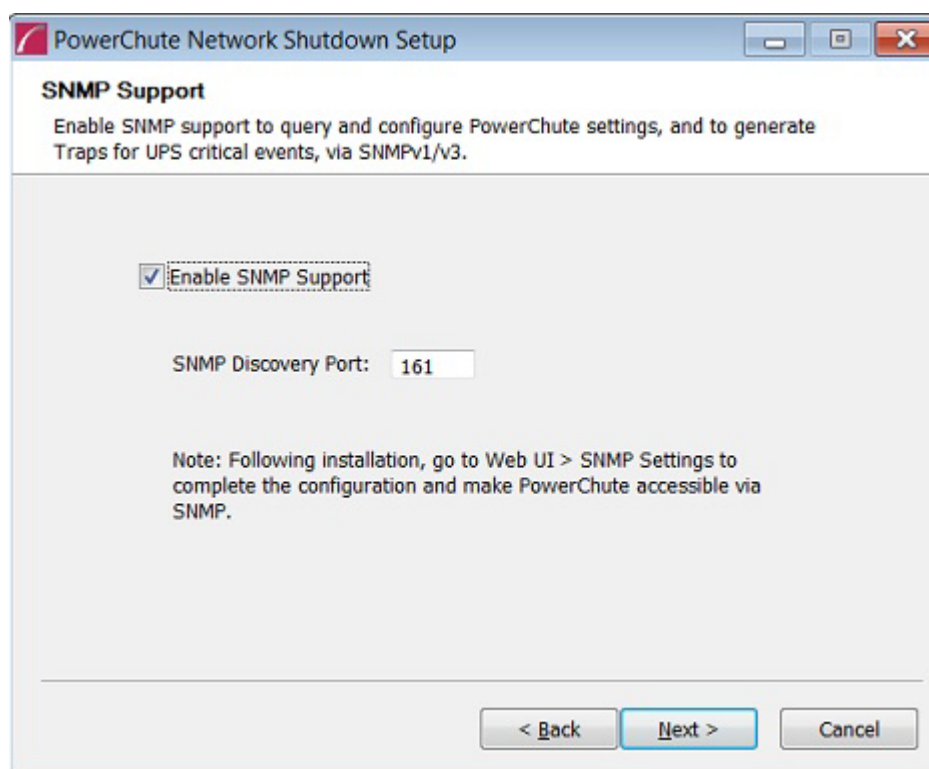
Enter an installation folder location or accept the default.

4. When configuring for a Java Runtime Environment (JRE), if a valid public JRE is detected, you can choose between using it or the private JRE that is bundled with PowerChute.



See [JRE](#) for information on using a public or a private JRE installation.

5. The SNMP Support dialog is shown:



Select the checkbox to **Enable SNMP Support**.

NOTE: If SNMP support is not enabled during installation, it cannot be subsequently enabled through the PowerChute Configuration Wizard, and no options relating to SNMP will be available in the web user interface, or via the configuration INI file.

Enter the **SNMP Discovery Port**. The default value of 161 is automatically populated, but this can be edited if this port is already in use. The Port number availability is automatically checked, and if it is not available, a new port number must be entered to proceed.

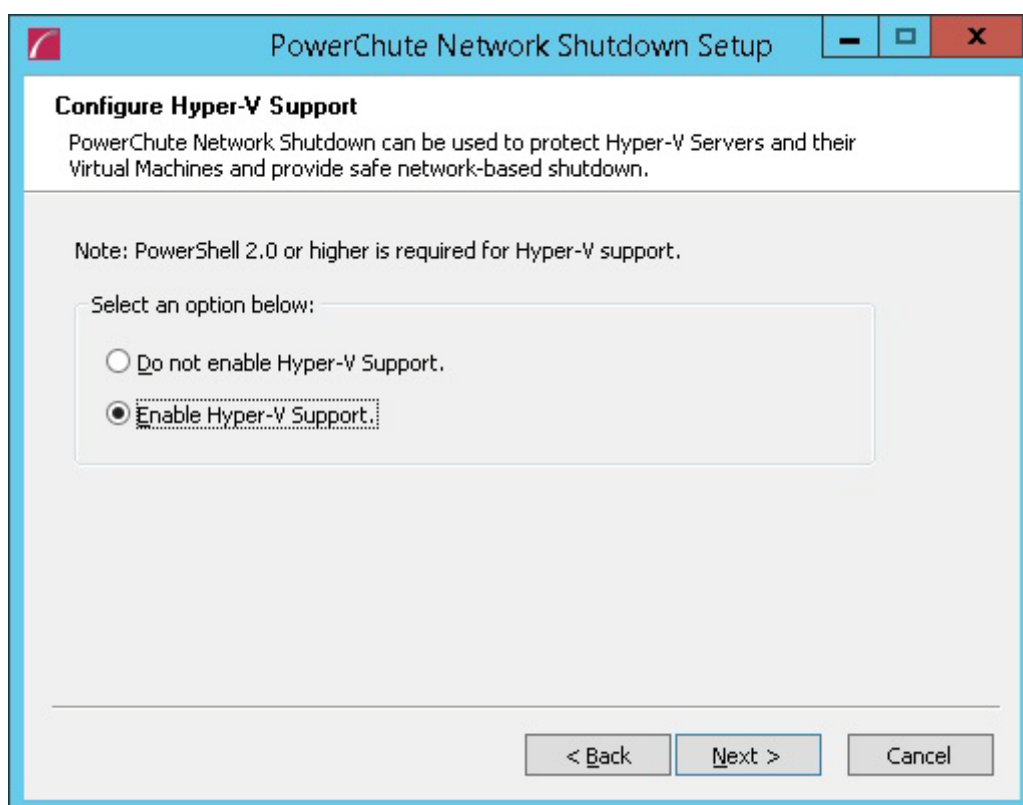
If the Windows firewall is enabled, make sure that PowerChute can receive inbound data to port 161. See [Firewall](#) for more information.



Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.

Click **Next** to continue.

6. At the dialog below, choose **Enable Hyper-V Support** and your installation proceeds.



A dialog will appear to note the following:

- a. PowerChute does not support environments where SCVMM is running on a Virtual Machine.
- b. PowerChute must be installed on a physical machine.

Click **OK** to proceed.

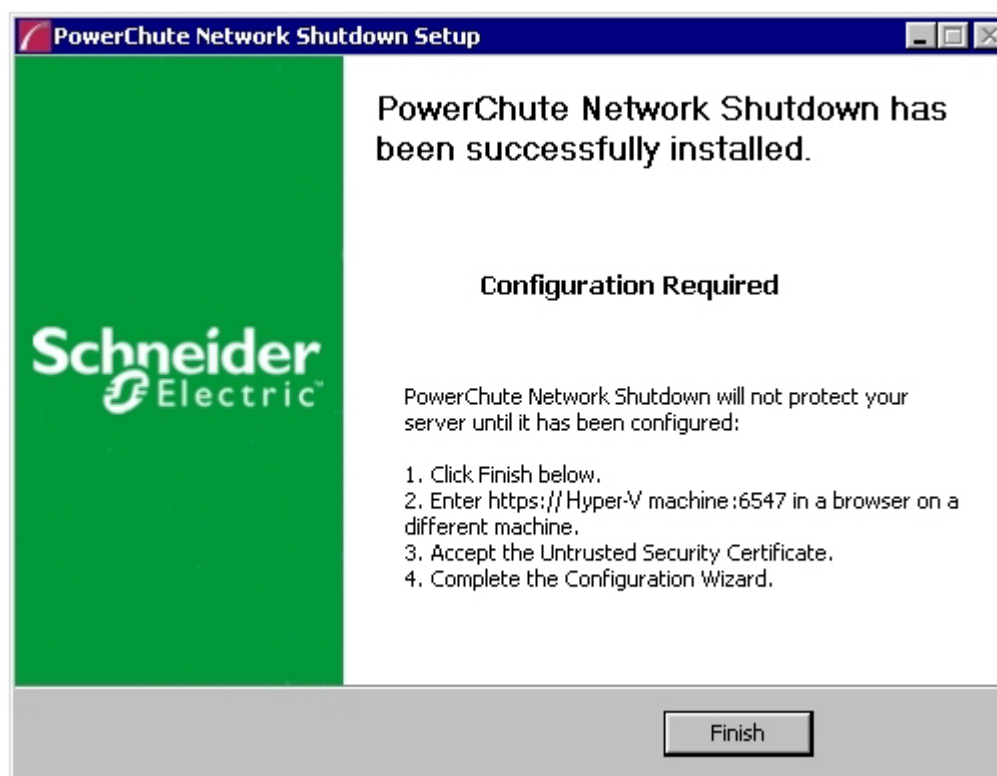
3. When your Windows Firewall is enabled, you can allow the PowerChute installation to configure the firewall automatically by choosing **Yes** when prompted:

PowerChute Network Shutdown ports must be opened in the Windows Firewall to enable communication with the Network Management Card(s). Would you like this configuration to be performed automatically?

See [Firewall](#) for more information.

After installation, it is necessary to configure PowerChute in order to protect your system.

If you installed on Hyper-V server, you have to go to another machine in order to configure this installation of PowerChute. In the graphic below, **Hyper-V machine** at step 2 represents the machine name or the IP address of your Hyper-V machine.



On a standard Windows machine when you have enabled Hyper-V in this installation process, the PowerChute setup wizard opens automatically after you click the **Finish** button.



PowerChute SCVMM Installation

PowerChute can protect Hyper-V hosts that are managed by System Center Virtual Machine Manager (SCVMM). SCVMM should be configured on a physical machine. SCVMM configured on a virtual machine is not supported by PowerChute.

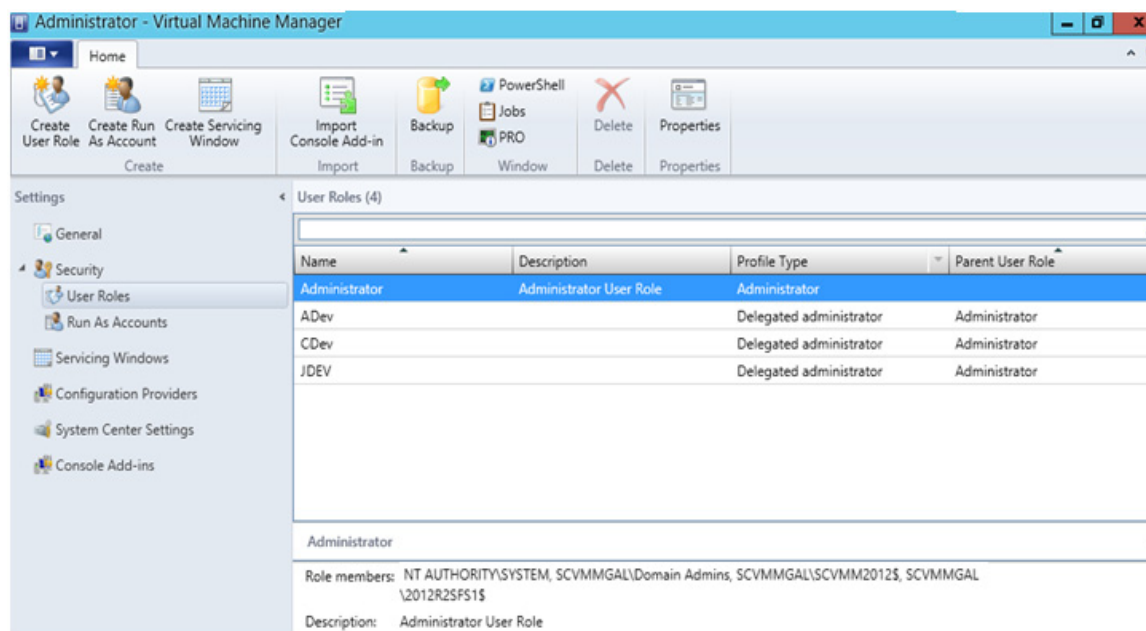
PowerChute can be installed on the same server as SCVMM, or on a remote server.

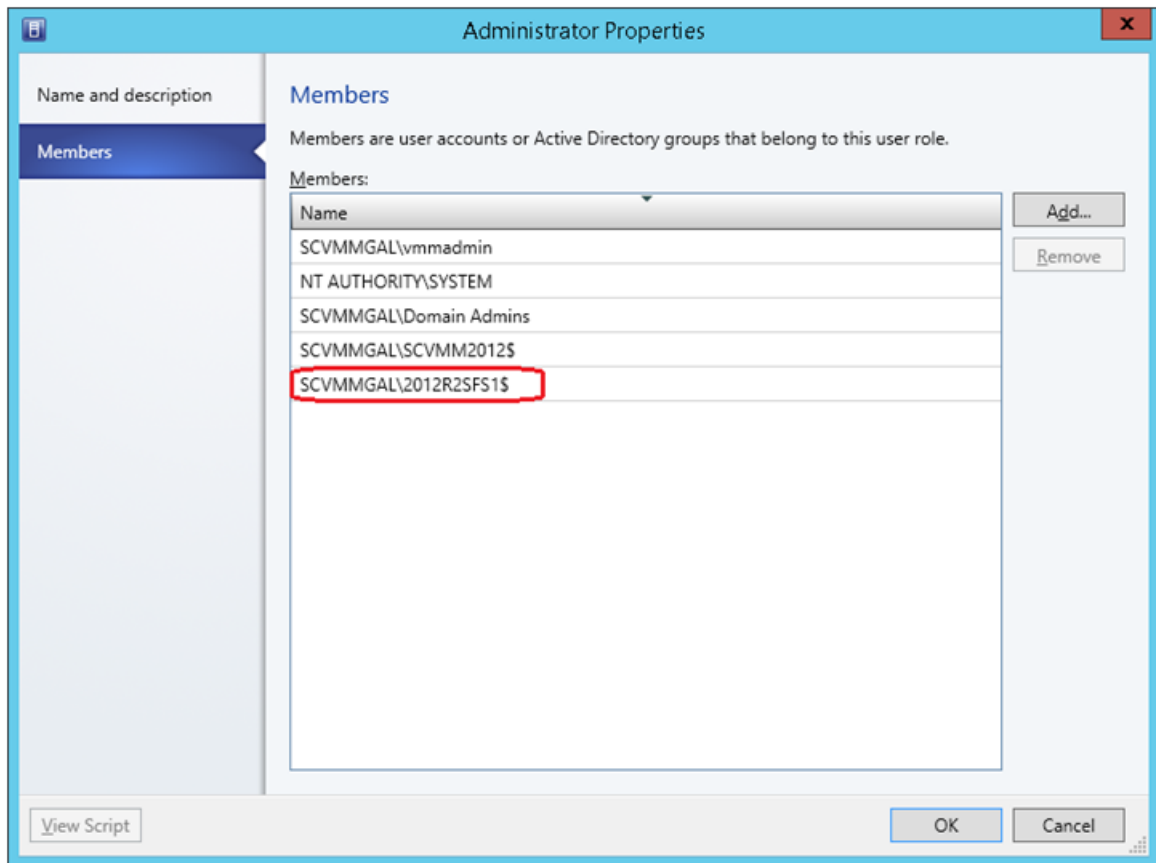
If PowerChute is installed on a remote server:

- It is necessary to also install the SCVMM console on that server to provide the Powershell modules used by PowerChute.
- It is necessary to add the machine account on which PowerChute is installed to the Administrator User Role in SCVMM settings.
- It is necessary to use a remote shut down command to shut down the SCVMM machine. The remote shut down command is not part of PowerChute.

To add the machine account on which PowerChute is installed to the Administrator User Role in SCVMM:

1. In SCVMM Console, Click **Settings**.
2. Expand **Security** and select **User Roles**.
3. Right click on the Administrator role in the right hand pane and select **Properties**.
4. In the **Administrator Properties** dialog click **Members**.
5. Click the **Add** button and enter the machine name on which PowerChute is installed.
6. Click OK twice.
7. The PowerChute machine account should be listed under **Role Members**.





Hyper-V and SCVMM Configuration

Powershell scripts are used to perform Live Migration of VMs and Graceful VM shutdown for Hyper-V and Maintenance Mode/Host Shutdown in SCVMM. By default, Windows prevents the execution of Powershell scripts. The PowerChute installation program will automatically detect if Powershell script execution is enabled and provide an option to enable it if it is not. To verify that the Execution Policy has been changed, open a new command prompt window and

enter the command:

```
powershell Get-ExecutionPolicy
```

Verify that it has been set to `remotesigned`.

If it is not set to `remotesigned`, open a command prompt and type the following

```
powershell Set-ExecutionPolicy remotesigned
```



For more information on the Execution Policy settings, see [Microsoft Technet](#).

Upgrading the Software

If you have v3.1 or higher of PowerChute already installed on your target machine, the installation process asks you whether you want to perform an upgrade rather than a complete installation. Upgrading enables you to retain your existing configuration settings.

Following the upgrade installation, to ensure that the PowerChute user interface enhancements are applied correctly, it is necessary to clear the browser history:

- In Internet Explorer - select **Tools > Safety > Delete browsing history**
- In Chrome - select **Settings > Show advanced settings > Privacy > Clear browsing data**
- In Firefox - select **Open Menu > History > Clear Recent History**

Uninstalling on Hyper-V and SCVMM

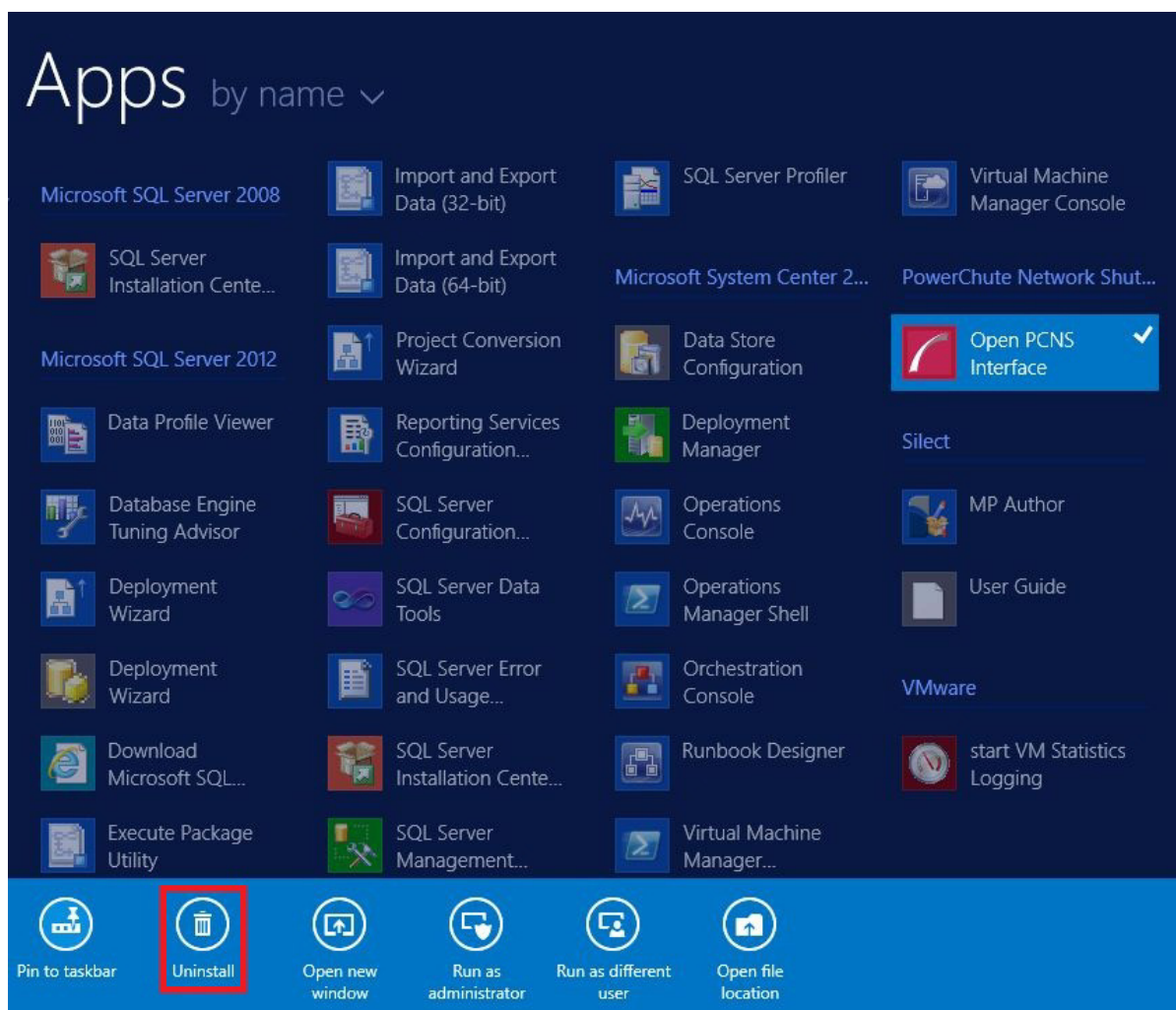
On Windows, use the **Uninstall** option under **PowerChute Network Shutdown** in the Windows Start menu.

On Windows Server Core, follow these steps.

1. Open a command prompt window.
2. Type `C:\Program Files\APC\PowerChute\uninstall.exe` and press Enter.

On Windows Server 2012, PowerChute must be uninstalled using Add/Remove Programs.

1. Right-click the PowerChute Network Shutdown menu option in the **Start** menu.
2. Click **Uninstall** in the options menu that displays on the bottom of the screen.



To uninstall in silent mode:

1. Open a command prompt.
2. Type `"C:\Program Files\APC\PowerChute\uninstall.exe" /S` and press return.

Silently Installing the Software

Installing silently means the installation is unattended or non-interactive.



It is not possible to roll out your event configurations or shutdown settings using a silent installation. You can however, use `pcnsconfig.ini` to do this. See the section on INI files in the online help.



PowerChute only supports silent installation in Single, Redundant and Parallel UPS configurations.

Silent Install on Hyper-V

Perform the following steps:

Edit the silent installations file to set the required parameters; see [Editing your silent installation file](#).

1. Type the following on one line at the Windows command line:

```
Setup.exe /S /F silentInstall.ini
```



If a silent installation fails, see [Appendix A: Error codes for silent installations](#).

Editing your silent installation file

On Hyper-V, the file that guides silent installations is named `silentInstall.ini`

The file is a plain text file and can be edited with a standard text editor. Each field or line has a value that the installer needs in order to carry out the installation. The table below explains the fields available in the silent installation file.

Field name	Description
applicationDirectory=	Specifies the installation folder. Type the folder name after "=", ensuring it has valid characters for the operating system. Note: You can't use multiple-byte characters (Chinese for example) and some single byte high-ASCII characters, e.g. ß, é, à, in the installation path.
ACCEPT_EULA=yes	Yes signifies acceptance of the software licence agreement. The installation will not proceed unless yes is specified here.
*INSTALL_JAVA= System PCNS	The value <code>System</code> here signifies you want to use the public JRE for your PowerChute installation. The value <code>PCNS</code> here signifies you want to use the private JRE.
*The installation detects whether the JRE meets the requirements, see JRE .	
REGISTER_WITH_NMC= yes no	Using yes or no, specify whether PowerChute should be registered with the Network Management Card (NMC) or not.
MODE= single redundant parallel	Use single, redundant, or parallel to specify the UPS configuration mode. For detailed information, see "PowerChute Network Shutdown Operating Modes and supported UPS Configurations" here .
NETWORKCONFIG= IPv4 IPv6	Specify your Internet protocol with IPv4 or IPv6.
IPv6NETWORKCONFIG= unicast multicast	When you are using IPv6 only (you entered NETWORKCONFIG= IPv6 above) you must specify the communication mechanism here. See also UNICAST_ADDRESS= and MULTICAST_ADDRESS= . For detailed information, see "The Communications Process of PowerChute Network Shutdown" here .
IP_1= IP_2= IP_3= IP_4= IP_5= IP_6= IP_7= # IP_8= # IP_9=	On each line, specify the IP address of each NMC that will be communicating with this PowerChute installation. You can comment out unneeded entries by putting the # character at the beginning of the line (see examples 8 and 9).

Field name	Description
IP_1_Outlet= IP_2_Outlet= IP_3_Outlet= IP_4_Outlet= IP_5_Outlet= IP_6_Outlet= IP_7_Outlet= # IP_8_Outlet= # IP_9_Outlet=	<p>This applies only to UPS devices with outlet groups (for example, Smart-UPS SMX and SMT devices). Specify the outlet group that supplies power to the PowerChute installation.</p> <p>On a UPS that has only Switched Outlet Groups, "IP_1_Outlet" must be set to "1". If you enter "0", PowerChute may not correctly identify Outlet events associated with the first Outlet group.</p> <p>On a UPS that has both a Main Outlet Group (not switched) and Switched Outlet Groups, "IP_1_Outlet" must be set to "0".</p> <p>You can comment out entries not needed by putting the # character at the beginning of the line (see examples 8 and 9).</p>
PORT=	This is the NMC web port: 80 for HTTP; 443 for HTTPS.
PROTOCOL= HTTP HTTPS	Use HTTP or HTTPS to specify which protocol you are using.
ACCEPTCERTS= YES NO	<p>When using the HTTPS protocol, SSL certificates are used to secure the connection. By default the NMC use a self-signed certificate, which needs to be accepted.</p> <p>Select YES to automatically accept a self-signed certificate.</p> <p>Select NO to accept a connection only if the NMC is configured with a valid certificate.</p>
USERNAME= PASSWORD= AUTHENTICATION_PHRASE=	<p>Enter the user name, password, and authentication phrase to validate PowerChute communication with the NMC. (The authentication phrase reverts to the default if not specified).</p> <p>Note: We recommend that you change the defaults for security reasons.</p> <p>The acceptable characters for username and password are:</p> <ul style="list-style-type: none"> • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: <code>_!\"#\$%&'()*+,-./:;<=>?@^`{ }[]~</code> <p>The password length must be from 3–32 characters, and the username from 3–10 characters. The authentication phrase must be 15–32 ASCII characters.</p>
LOCAL_IP_ADDRESS=	This information applies to a PowerChute server with multiple network cards. Use it to specify the IP address of the card that will communicate with PowerChute.
UNICAST_ADDRESS=	When you have specified IPv6 in <code>NETWORKCONFIG= IPv4 IPv6</code> and unicast in <code>IPV6NETWORKCONFIG= unicast multicast</code> , you must specify your unicast host address here.
MULTICAST_ADDRESS=	When you have specified IPv6 in <code>NETWORKCONFIG= IPv4 IPv6</code> and multicast in <code>IPV6NETWORKCONFIG= unicast multicast</code> , the Network Management card will send UDP packets to the multicast address you specify here.
VIRTUALINSTALL= VMware Hyper-V	Specify <code>Hyper-V</code> to enable the Hyper-V/SCVMM virtualization features.
CONFIGURATION_MODE = Managed Unmanaged	Specify <code>Managed</code> for configurations managed by SCVMM. Specify <code>Unmanaged</code> for unmanaged Hyper-V configurations.
SCVMMSERVER_ADDRESS=	Specify the IP Address or the host name or the FQDN (Fully Qualified Domain Name) of the SCVMM Server.
SNMPv1	

Field name	Description
ENABLE_SNMPV1_ACCESS = True False	Specify true to enable SNMPv1 access and false to disable SNMPv1 access.
NAME_COMMUNITY_N =	Enter the community name, up to 15 ASCII characters.
NMS_COMMUNITY_N=	Enter the IP address of the Network Management System.
ACCESS_TYPE_COMMUNITY_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMP community string: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT =	Specify the SNMP Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMPv3	
ENABLE_SNMPV3_ACCESS = True False	Specify True to enable SNMPv3 access and false to disable SNMPv3 access.
USERNAME_PROFILE_N =	Specify the user name of the SNMPv3 user profile, up to 32 ASCII characters.
AUTH_PASSPHRASE_PROFILE_N =	Enter the Authentication passphrase of 8-32 ASCII characters.
PRIV_PASSPHRASE_PROFILE_N =	Enter the Privacy passphrase of 8-32 ASCII characters.
AUTH_PROTOCOL_PROFILE_N = MD5 SHA1 SHA256 SHA512 NONE	Specify the Authentication protocol of the SNMPv3 user profile.
PRIV_PROTOCOL_PROFILE_N = AES128 AES192 AES192EX AES256EX AES256 DES NONE	Specify the Privacy protocol of the SNMPv3 user profile. See the “ <i>SNMP Troubleshooting</i> ” topic of the <i>PowerChute Network Shutdown User Guide</i> available on www.apc.com for more information on JRE requirements for AES-192/Ex and AES-256/Ex.
ACCESS_TYPE_PROFILE_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMPv3 user profile: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT=	Specify the SNMP discovery Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMP Traps	
UPSCriticalEvents_Enabled = True False	Specify True to enable SNMP Traps for UPS Critical Events.
UPSCriticalEvents_SendClearingTrap = True False	Enter True to send a Trap once a UPS Critical Event has cleared.
UPSCriticalEvents_Delay =	Specify the length of time in seconds that the UPS Critical Event must persist before a trap is sent.
UPSCriticalEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
UPSCriticalEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the UPS Critical Event is cleared.
UPSCriticalEvents_RepeatTimes =	Specify the number of times the trap is sent when the UPS Critical Event occurs.

Field name	Description
LostCommsEvents_Enabled = True False	Specify True to enable SNMP Traps for Lost Communication Events.
LostCommsEvents_SendClearingTrap = True False	Enter True to send a Trap once a Lost Communication Event has cleared.
LostCommsEvents_Delay =	Specify the length of time in seconds that the Lost Communication Event must persist before a trap is sent.
LostCommsEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
LostCommsEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the Lost Communication Event is cleared.
LostCommsEvents_RepeatTimes =	Specify the number of times the trap is sent when the Lost Communication Event occurs.
Enabled_TrapReceiver_N = True False	Enter True to enable the Trap Receiver.
NMS_TrapReceiver_N =	Enter the IP address of the Network Management System that will receive traps.
Port_TrapReceiver_N =	Enter the port number of the Trap Receiver.
Type_TrapReceiver_N = v1 v3	Enter the version of SNMP used to send the traps.
ProfileName_TrapReceiver_N =	Enter the User Name of the SNMPv3 User Profile used to send the traps.
Note: N indicates an integer (0-N)	

Installation Guide

PowerChute Network Shutdown

VMware

Installing PowerChute Network Shutdown with VMware Support

You have three different ways of deploying or installing PowerChute in order to monitor VMware hosts:

- [Installing on Windows to Monitor VMware Hosts](#)
- [Deploying the PowerChute Virtual Appliance](#)
- [Installing on vSphere Management Assistant \(vMA\)](#)

See also [Upgrading the software](#), [Silently Installing the Software](#), [Uninstalling](#).

Recommendations on Deploying/ Installing PowerChute

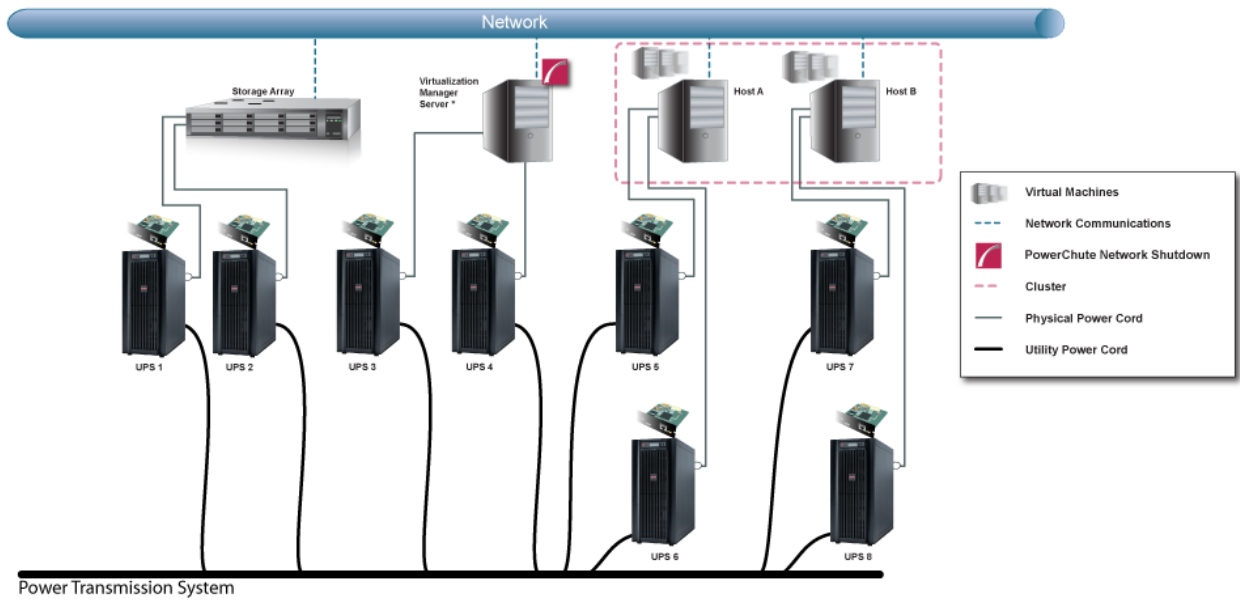
We recommend the following in a VMware environment:

VMware Setup	Recommended Deployment/ Installation of PowerChute
VMware Hosts in multiple clusters	PowerChute installed on a physical Windows machine
Single VMware host that is not managed by vCenter Server	PowerChute virtual appliance
VMware hosts in one cluster for Single, Redundant or Parallel UPS configurations	PowerChute virtual appliance or PowerChute installed on a physical Windows machine
VMware hosts managed by vCenter Server which is running on a physical machine	PowerChute installed on a physical Windows machine
Using vCenter Server running on a VM or vCenter Server Virtual Appliance (VCSA) for Single, Redundant or Parallel UPS configurations	PowerChute virtual appliance or PowerChute installed on a physical Windows machine
Advanced UPS configuration, see graphic below. See application notes for background information.	PowerChute installed on a physical Windows machine



If PowerChute is installed on a host that is part of a vSAN enabled cluster, that host cannot be placed into Maintenance Mode.

Advanced UPS Configuration: PowerChute can monitor both Single UPS's and groups of Redundant UPS's protecting your virtualization environment. If using Redundant UPS groups, redundancy levels can be set on a per group basis e.g. N+1, N+2.



Installing on Windows to Monitor VMware Hosts

PowerChute Network Shutdown can be installed on a physical Windows machine in order to remotely monitor VMware hosts. Follow these steps below.

1. Locate the PowerChute installation executable file for Windows, **Setup-x32.exe** or **Setup-x64.exe**, on the PowerChute CD or download it from the [APC website](#). You must have administrator rights to run the installer.

Double-click on the file.

(If you downloaded from the website, you need to extract the exe file from the zip file).

2. A warning dialog, below, displays if you downloaded the exe from the web: click the **Run** button.



3. At the welcome dialog, click on **Next** to continue.

At the License Agreement dialog, if you agree with the terms, click **I Agree** to continue.

4. When configuring for a Java Runtime Environment (JRE), if a valid public JRE is detected, you can choose between using it or the private JRE that is bundled with PowerChute.



See [JRE](#) for information on using a public or a private JRE installation.

5. Enter **Yes** to **Enable SNMP Support** and enter the **SNMP discovery port**. If the default port number 161 is unavailable, enter another available port number.

NOTE: If SNMP support is not enabled during installation, it cannot be subsequently enabled through the PowerChute Configuration Wizard, and no options relating to SNMP will be available in the web user interface, or via the configuration INI file.



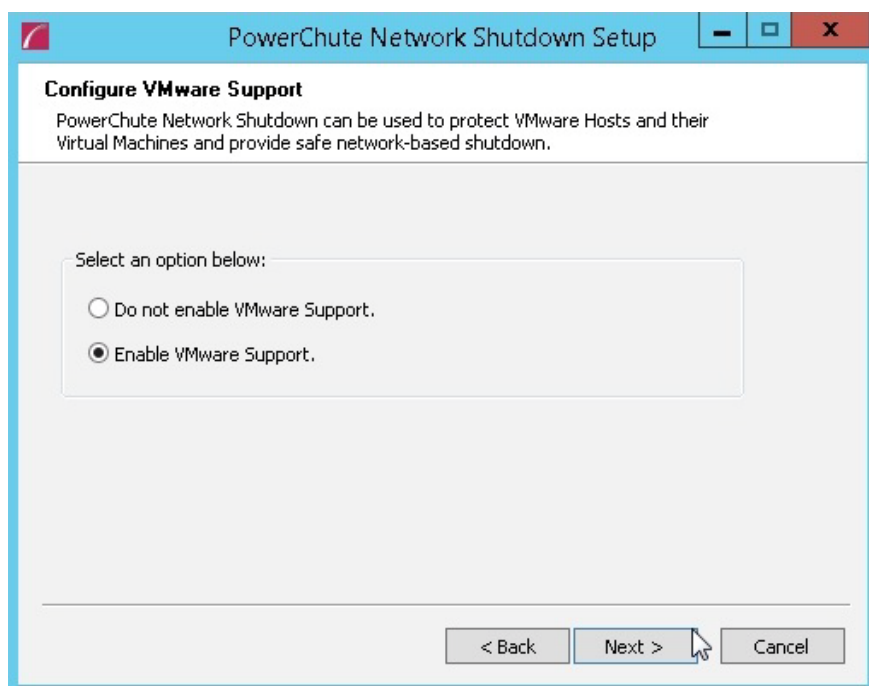
Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.

6. Choose **Enable VMware Support** at the dialog below.



On a physical Windows machine with Hyper-V enabled or SCVMM console/server installed, PowerChute cannot monitor VMware hosts, and the configure VMware Support option screen is not shown.

Please install PowerChute on a physical Windows machine that does not have Hyper-V enabled or SCVMM server/console installed.



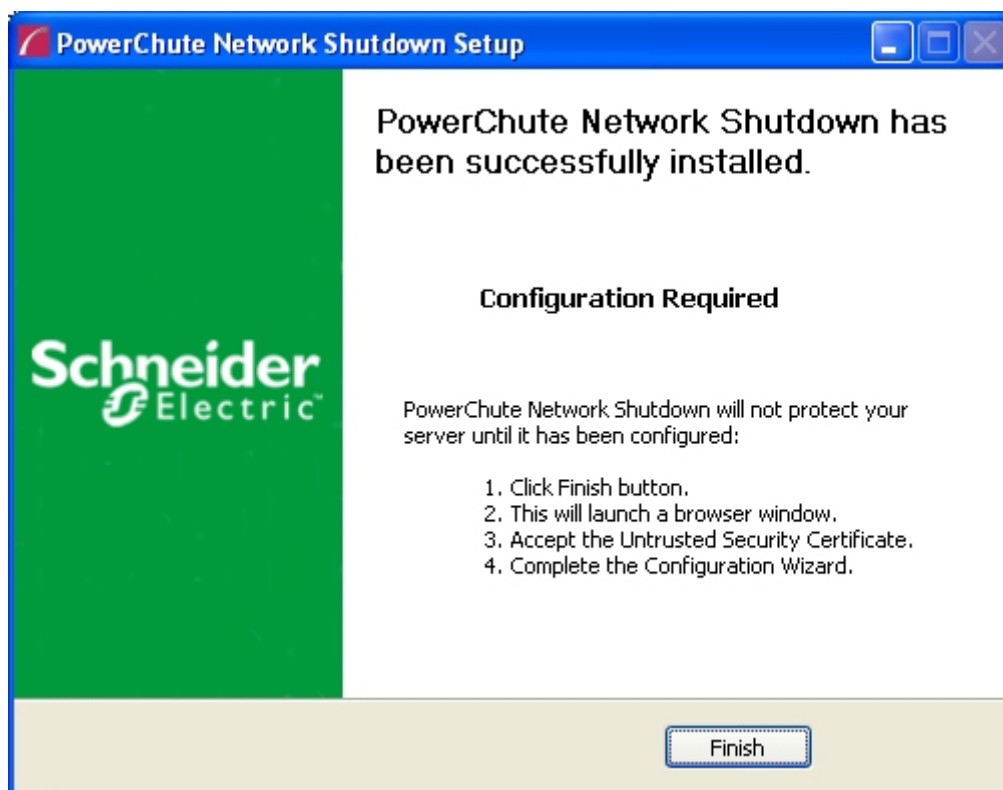
A dialog displays to note that Advanced UPS Configuration is not supported if PowerChute is installed on a Virtual Machine. Click **OK** proceed.

7. Enter an installation folder location or accept the default and your installation proceeds.
8. When your Windows Firewall is enabled, you can allow the PowerChute installation to configure the firewall automatically by choosing **Yes** when prompted:

PowerChute Network Shutdown ports must be opened in the Windows Firewall to enable communication with the Network Management Card(s). Would you like this configuration to be performed automatically?

See [Firewall](#) for more information.

After installation, it is necessary to configure PowerChute in order to protect your system. The PowerChute setup wizard opens automatically after you click the **Finish** button.



Deploying the PowerChute Virtual Appliance

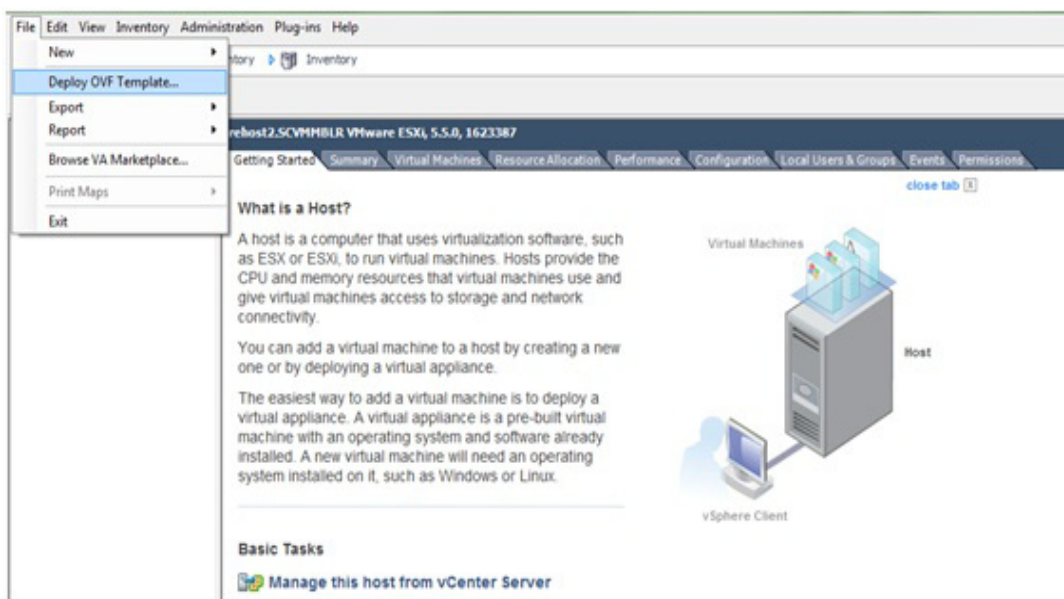
The PowerChute Virtual Appliance is a virtual machine image with CentOS Linux 5.11 running PowerChute Network Shutdown v4.2 pre-installed.



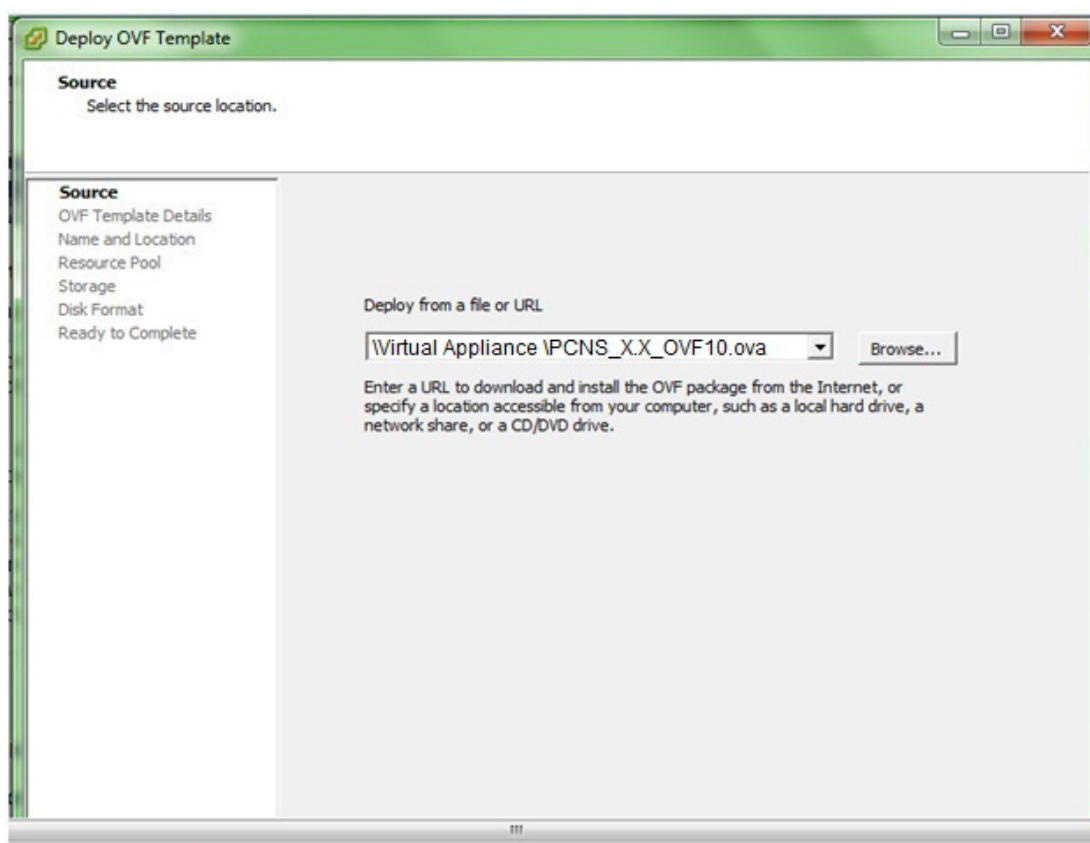
The Schneider Electric KBase <http://www.apc.com/site/support/index.cfm/faq/index.cfm> (FAQ ID is FA159775), provides information on installing the vSphere Client.

To deploy the virtual appliance using the vSphere Desktop client:

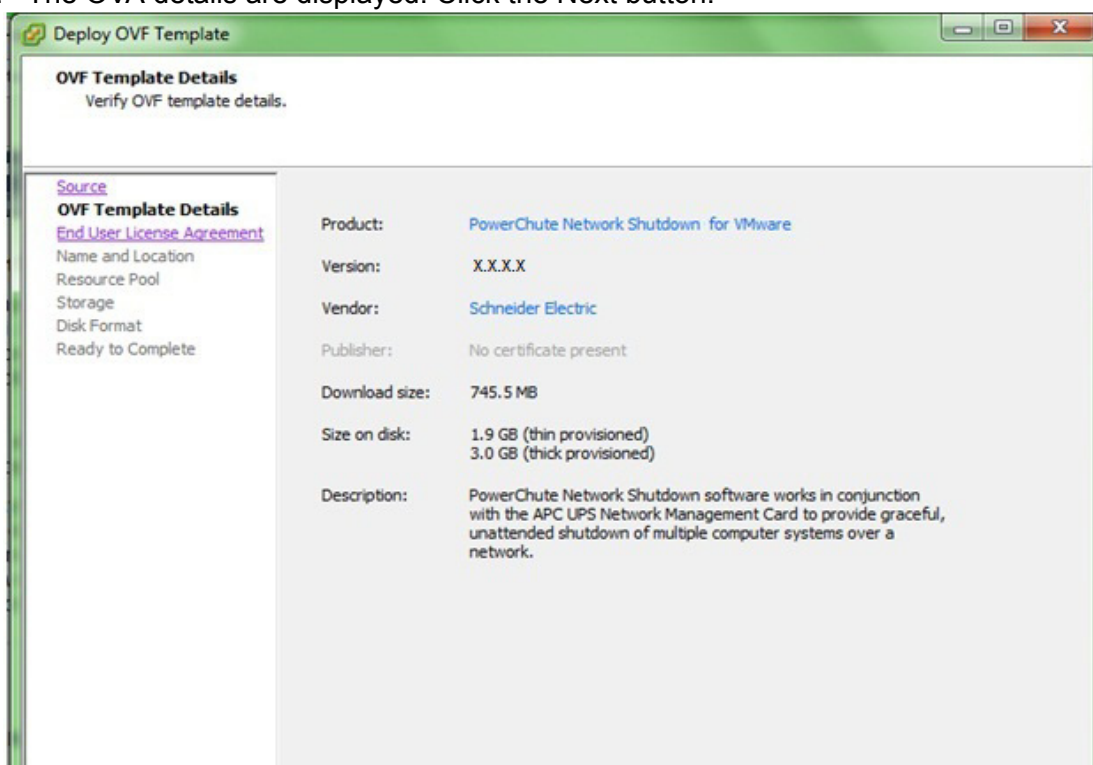
1. Download the PowerChute virtual appliance file, **PCNS_4.2_OVF10.ova** from the [APC website](#).
2. Log on to the VMware host or vCenter Server using your vSphere Client.
3. Select **File - Deploy OVF Template** from the menu.



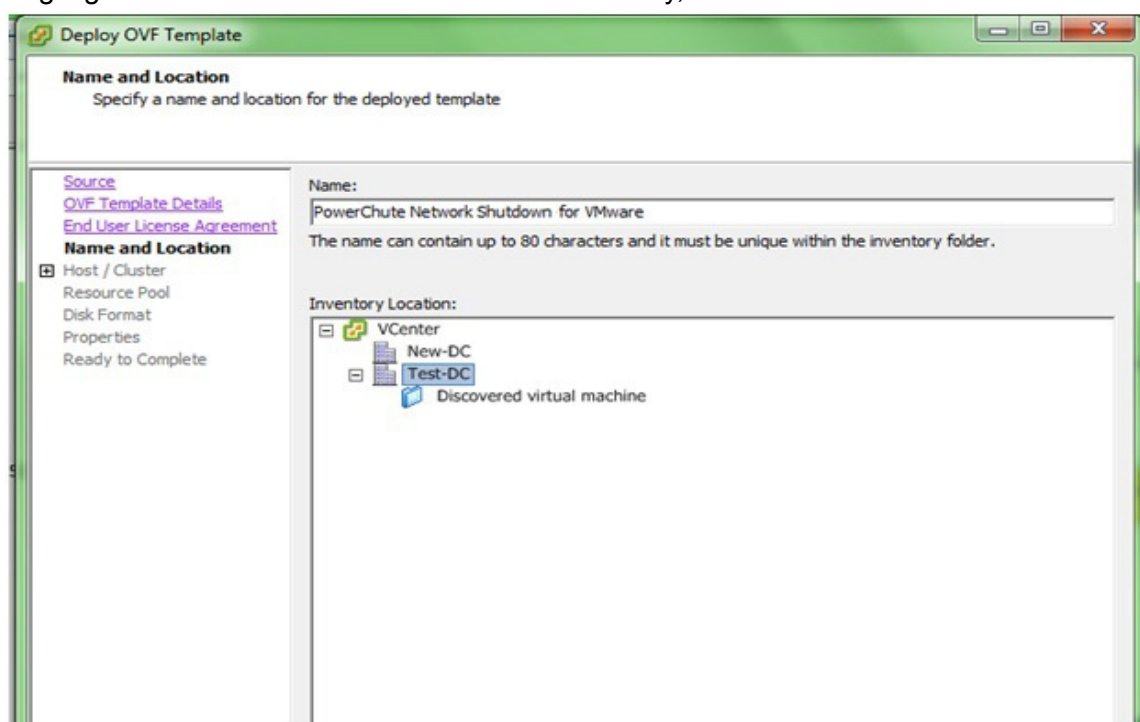
4. At the **Deploy from a file or URL** field, enter the path to the .OVA file.



5. The OVA details are displayed. Click the Next button.

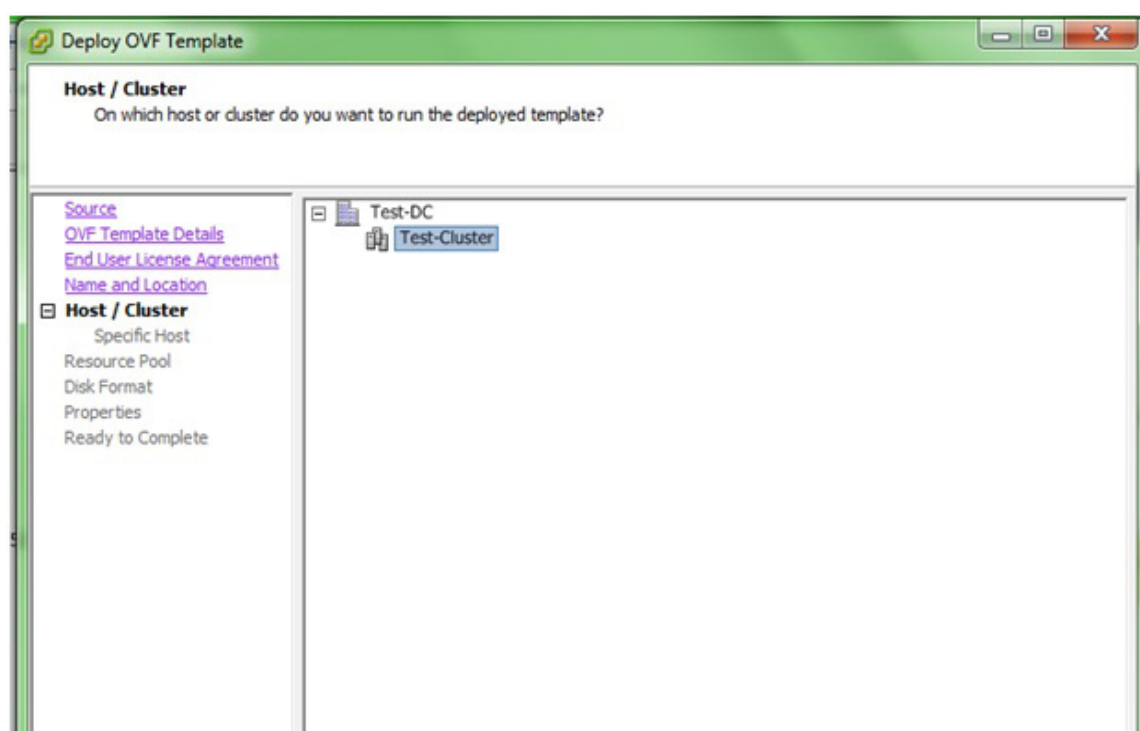


6. When the End User License Agreement (EULA) is displayed, click **Accept** and then Next.
7. Accept the default name and specify the datacenter and then click on the + sign and highlight **Discovered virtual machine** if necessary, and click Next.



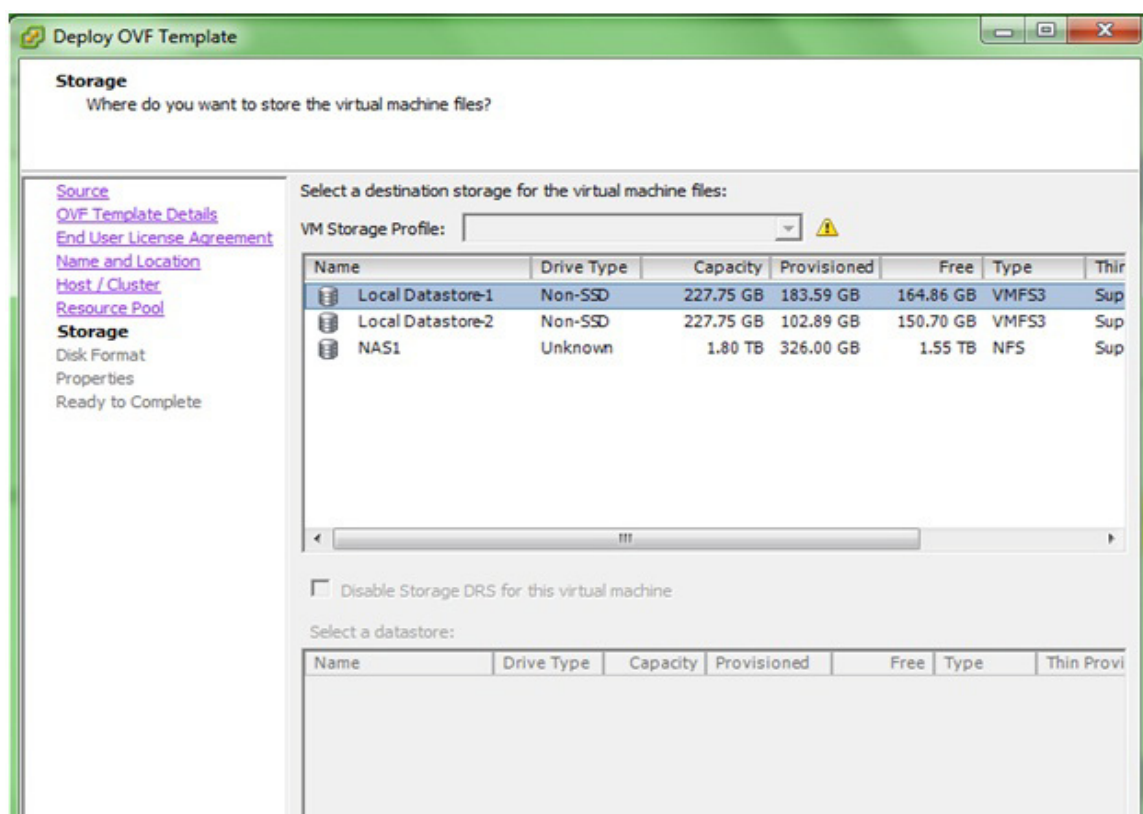
8. This step is not relevant if you are deploying to a standalone host.

Specify a host or a cluster and click Next. If you specify a cluster, you will be asked to specify a host within that cluster.

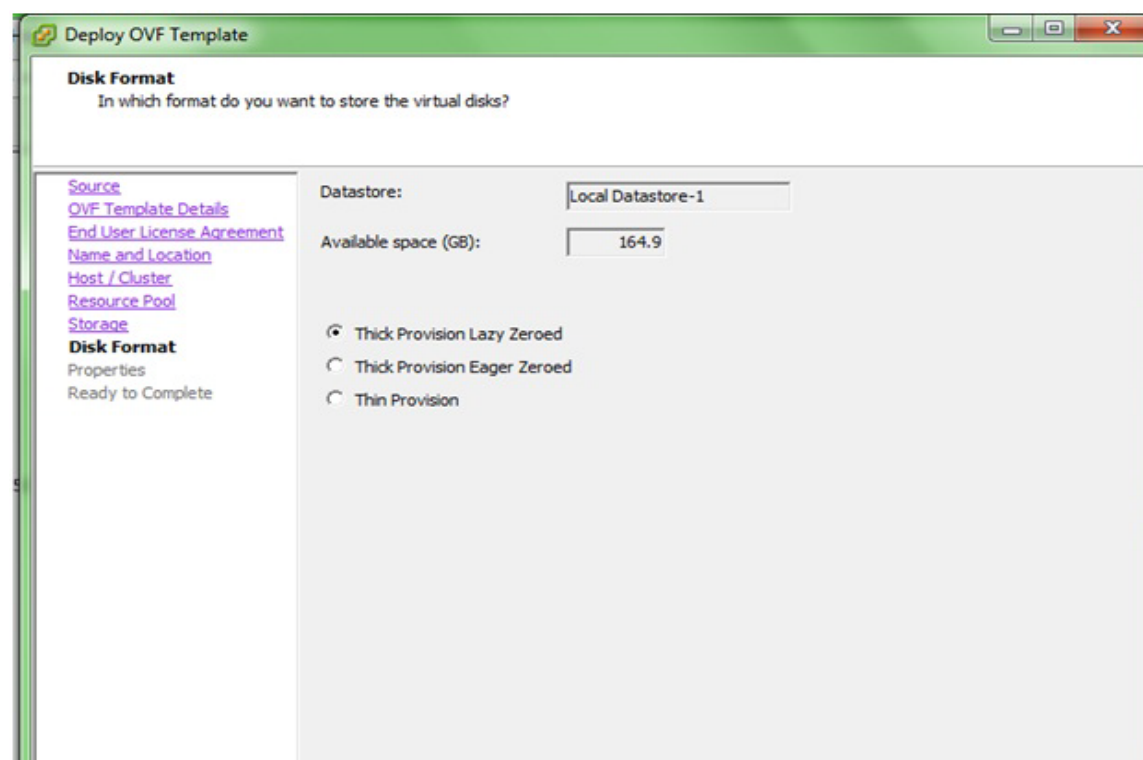


9. This step is not relevant if you are deploying to a standalone host.

Specify a configured datastore on your system that has sufficient disk space to deploy the virtual appliance. Click Next.



10. At Disk Format, choose the default disk layout option by clicking Next.



11. This step is not relevant if you are deploying to a standalone host - to configure a static IP address when deploying to a standalone host, use the Network configuration menu displayed at first boot of the appliance - see [Step 14](#).

At **Networking Properties**, if you want to use fixed IP-addressing, then fill in these field values as necessary. If you are using DHCP, you do not need to fill in the fields, so just click Next.

The screenshot shows the 'Deploy OVF Template' window. On the left, a sidebar lists navigation options: Source, OVF Template Details, End User License Agreement, Name and Location, Host / Cluster, Resource Pool, Storage, Disk Format, Properties (selected), and Ready to Complete. The main area is titled 'Networking Properties' and contains four sections with input fields: 'Default Gateway' (The default gateway address for this VM. Leave blank if DHCP is desired.), 'DNS' (The domain name servers for this VM (comma separated). Leave blank if DHCP is desired.), 'Network 1 IP Address' (The IP address for this interface. Leave blank if DHCP is desired.), and 'Network 1 Netmask' (The netmask or prefix for this interface. Leave blank if DHCP is desired.).

12. The options you have chosen display again, click **Finish** to commence the installation. The time taken to deploy the appliance depends on your network speed.

The screenshot shows the 'Deploy OVF Template' window at the 'Ready to Complete' stage. The sidebar on the left now highlights 'Ready to Complete'. The main area has a heading 'Ready to Complete' with the question 'Are these the options you want to use?'. Below this, it states 'When you click Finish, the deployment task will be started.' and lists the 'Deployment settings:' in a table-like format.

Deployment settings:	
OVF file:	C:\Virtual Appliance\PCNS_XX_OVF10.ovf
Download size:	745.5 MB
Size on disk:	3.0 GB
Name:	PowerChute Network Shutdown for VMware
Folder:	Test-DC
Host/Cluster:	Test-Cluster
Datastore:	Local Datastore-1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"Network 1" to "VM Network"
Property:	gateway =
Property:	DNS =
Property:	ip0 =
Property:	netmask0 =

This message box below displays when the installation has completed successfully and **PowerChute Network Shutdown 4.2 for VMware** displays as a VM in the inventory:



13. Power on your PowerChute virtual machine.

14. The Network Configuration options will display.

To set a static IP address choose **6) IP Address allocation for eth0**.

To view the DHCP Assigned IP address choose **0) Show Current Configuration**.

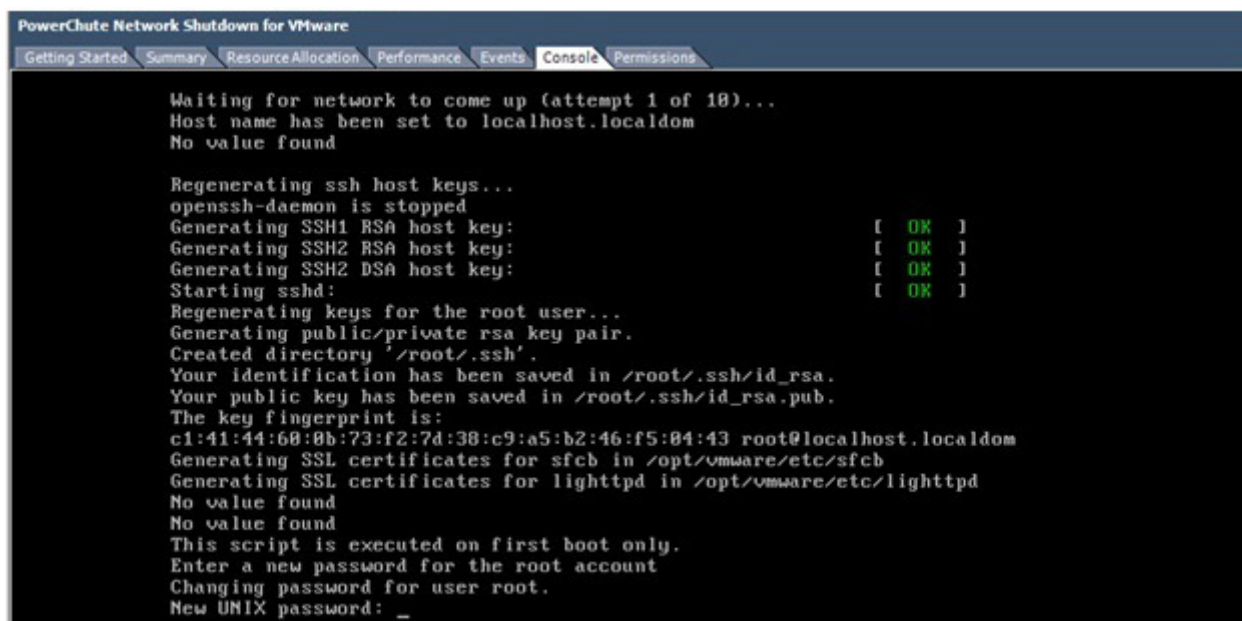
To proceed with the setup choose **1) Exit this program**.

```
Network Configuration for eth0
IPv4 Address:
Netmask:
IPv6 Address:
Prefix:

Global Configuration
IPv4 Gateway:
IPv6 Gateway:
Hostname:      localhost
DNS Servers:
Proxy Server:

Main Menu
0) Show Current Configuration (scroll with Shift-PgUp/PgDown)
1) Exit this program
2) Default Gateway
3) Hostname
4) DNS
5) Proxy Server
6) IP Address Allocation for eth0
Enter a menu number [0]: _
```

15. On the first boot of the appliance you will be prompted to create a password for the root user.



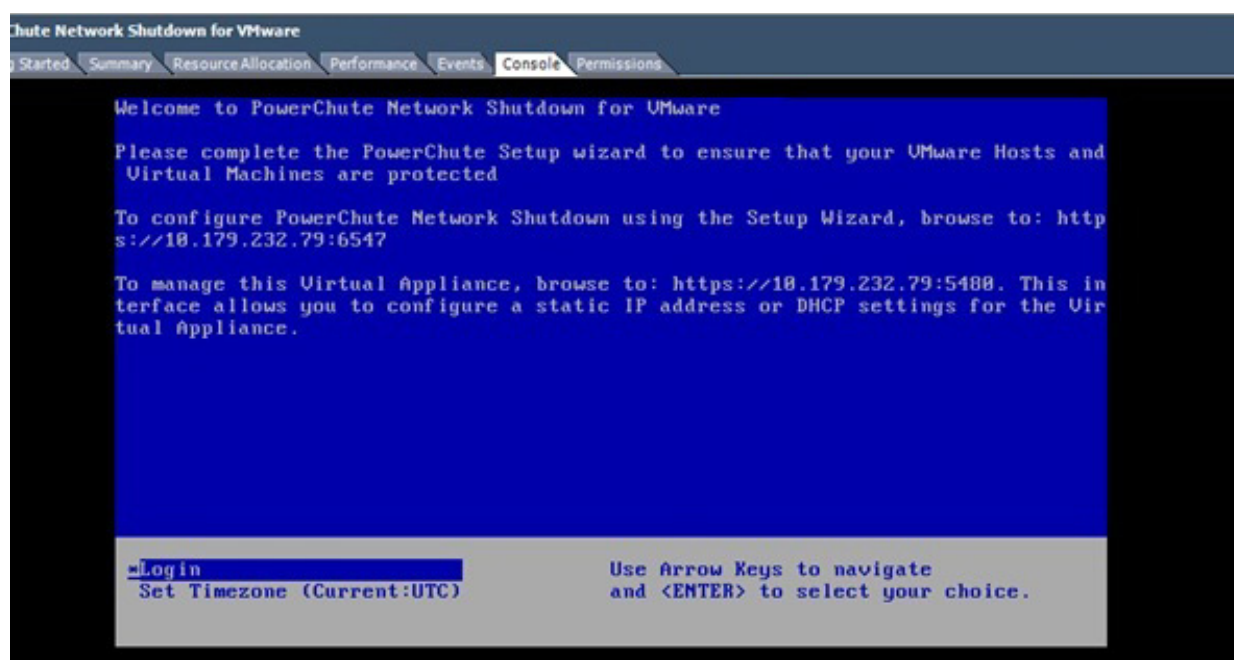
```
PowerChute Network Shutdown for VMware
Getting Started Summary Resource Allocation Performance Events Console Permissions

Waiting for network to come up (attempt 1 of 18)...
Host name has been set to localhost.localdom
No value found

Regenerating ssh host keys...
openssh-daemon is stopped
Generating SSH1 RSA host key: [ OK ]
Generating SSH2 RSA host key: [ OK ]
Generating SSH2 DSA host key: [ OK ]
Starting sshd: [ OK ]
Regenerating keys for the root user...
Generating public/private rsa key pair.
Created directory '/root/.ssh'.
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
c1:41:44:60:0b:73:f2:7d:38:c9:a5:b2:46:f5:04:43 root@localhost.localdom
Generating SSL certificates for sfcb in /opt/vmware/etc/sfcb
Generating SSL certificates for lighttpd in /opt/vmware/etc/lighttpd
No value found
No value found
This script is executed on first boot only.
Enter a new password for the root account
Changing password for user root.
New UNIX password: _
```

16. To access the PowerChute Network Shutdown user interface, you need to find out its URL. Click on the **Console** tab or right-click on the VM in the left-hand pane and select **Open Console**.

The welcome screen displays. The URL of the new installation of PowerChute will display following the sentence “**To configure PowerChute Network Shutdown, browse to:**”.



```
PowerChute Network Shutdown for VMware
Getting Started Summary Resource Allocation Performance Events Console Permissions

Welcome to PowerChute Network Shutdown for VMware

Please complete the PowerChute Setup wizard to ensure that your VMware Hosts and
Virtual Machines are protected

To configure PowerChute Network Shutdown using the Setup Wizard, browse to: http
s://10.179.232.79:6547

To manage this Virtual Appliance, browse to: https://10.179.232.79:5480. This in
terface allows you to configure a static IP address or DHCP settings for the Vir
tual Appliance.

Login
Set Timezone (Current:UTC)

Use Arrow Keys to navigate
and <ENTER> to select your choice.
```

17. Browse to https://<IP_Address>:6547 to launch the PowerChute setup wizard.

18. **Note:** SNMP is enabled by default in the PowerChute Virtual Appliance.

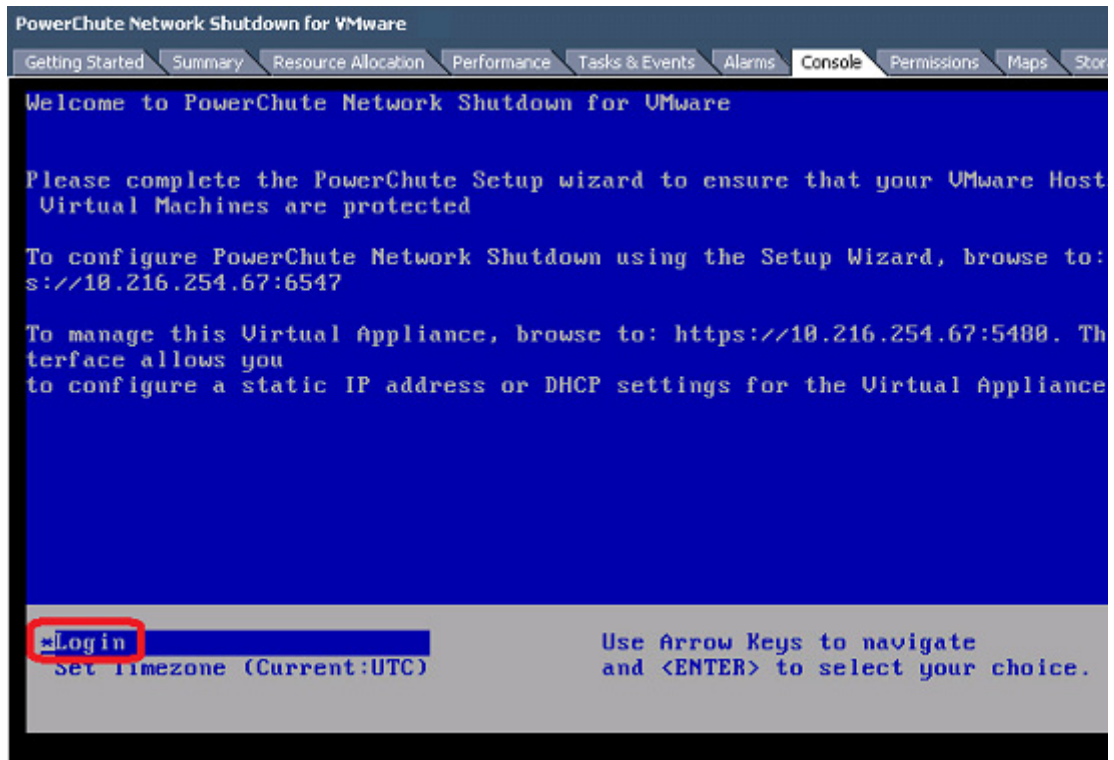
Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.



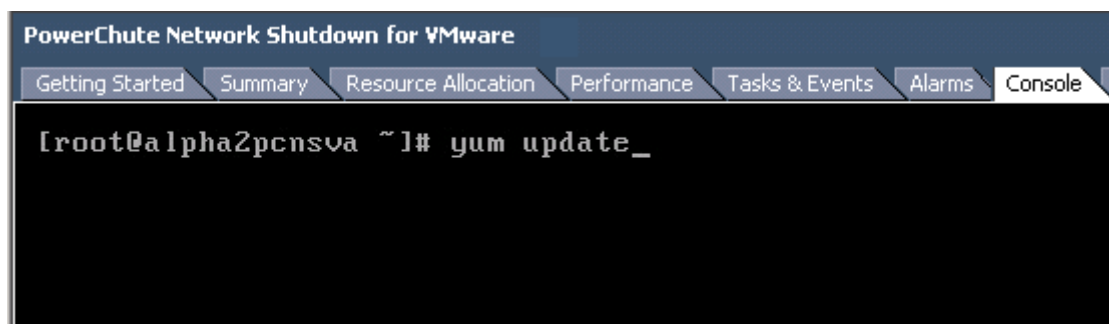
To obtain the latest security-related updates, it is recommended to update the libraries installed on the Virtual Appliance.

To update the Virtual Appliance libraries:

- Log in to the PowerChute virtual appliance



- Run the command `yum update`



- Install the updates

```

PowerChute Network Shutdown for VMware
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views

sudo x86_64 1.7.2p1-29.el5_10 base 364 k
tar x86_64 2:1.15.1-32.el5_8 base 748 k
tcl x86_64 8.4.13-6.el5 base 1.3 M
tzdata x86_64 2014i-1.el5 updates 788 k
udev x86_64 095-14.32.el5 base 2.4 M
util-linux x86_64 2.13-0.59.el5_8 base 1.9 M
vim-minimal x86_64 2:7.0.109-7.2.el5 base 334 k
vsftpd x86_64 2.0.5-28.el5 base 143 k
wget x86_64 1.11.4-3.el5_8.2 base 583 k
yum noarch 3.2.22-40.el5.centos base 1.0 M
yum-metadata-parser x86_64 1.1.2-4.el5 base 25 k
zlib i386 1.2.3-7.el5 base 51 k
zlib x86_64 1.2.3-7.el5 base 52 k
Installing for dependencies:
binutils x86_64 2.17.50.0.6-26.el5 base 2.9 M
readline i386 5.1-3.el5 base 223 k
sqlite i386 3.3.6-7 base 213 k

Transaction Summary
=====
Install      4 Package(s)
Upgrade    109 Package(s)

Total download size: 143 M
Is this ok [y/N]: _

```

- If a proxy server is used to connect to the Internet then the yum settings need to be updated to download the updates successfully. To do this edit /etc/yum.conf and add proxy details as shown:

```

PowerChute Network Shutdown for VMware
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions

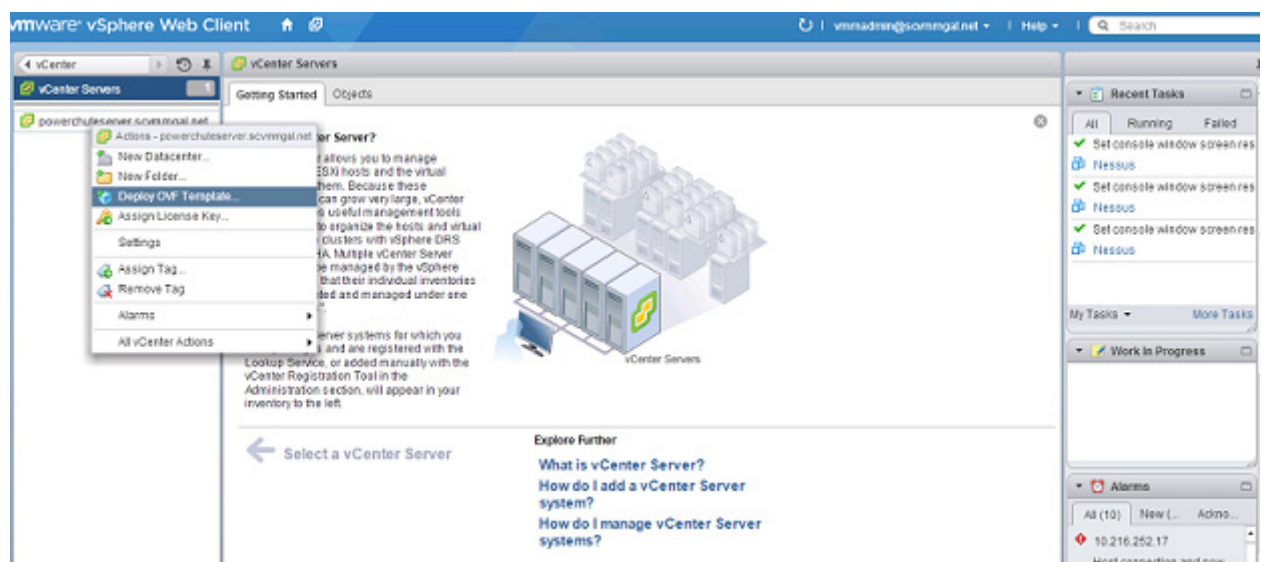
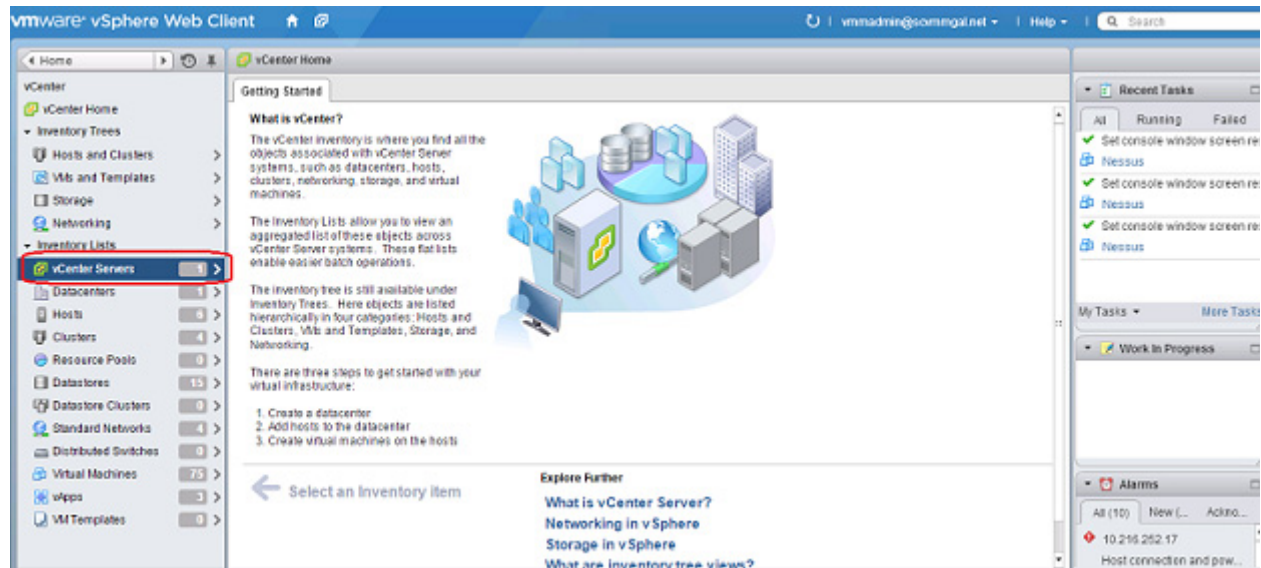
[main]
cachedir=/var/cache/yum
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
bugtracker_url=http://bugs.centos.org/yum
proxy=http://205.167.7.126:80
proxy_username=
proxy_password=

```

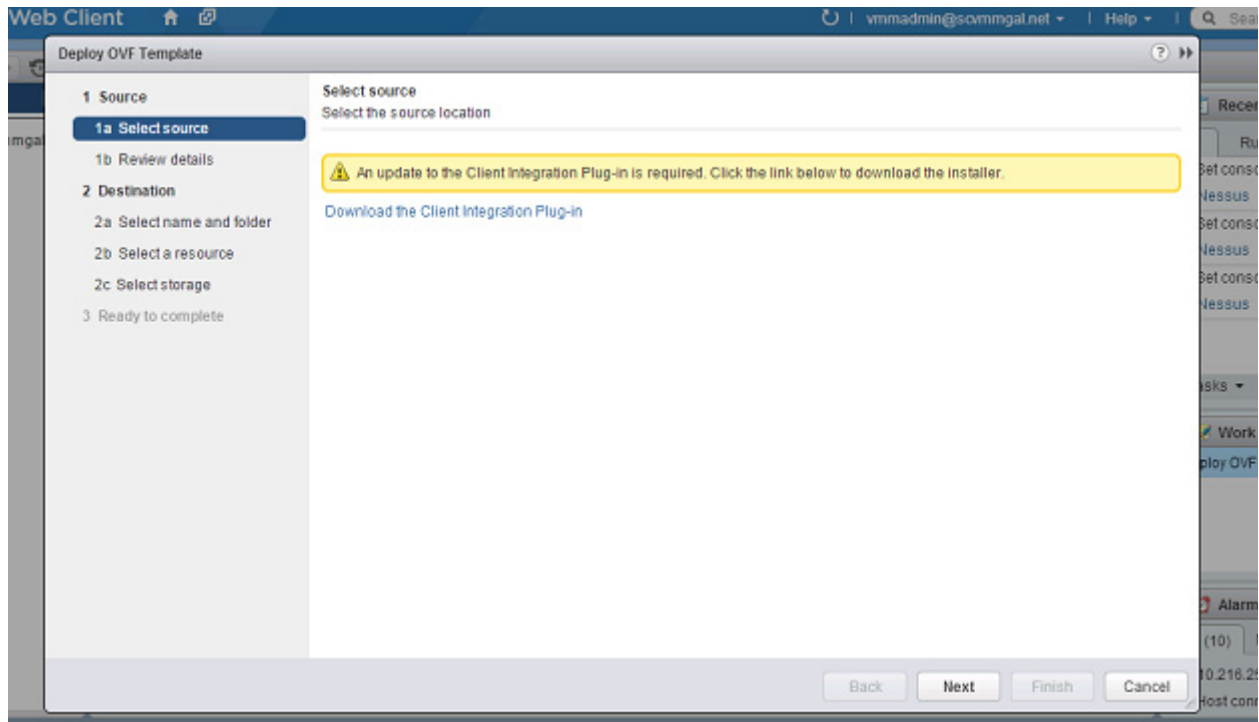
If you do not have Internet Connectivity and wish to update any of the libraries on the Virtual Appliance, the updated RPMs must be manually copied to the Virtual Appliance and installed using the RPM command as outlined in [Knowledge Base FA234757](#).

To deploy the virtual appliance using the vSphere Web client:

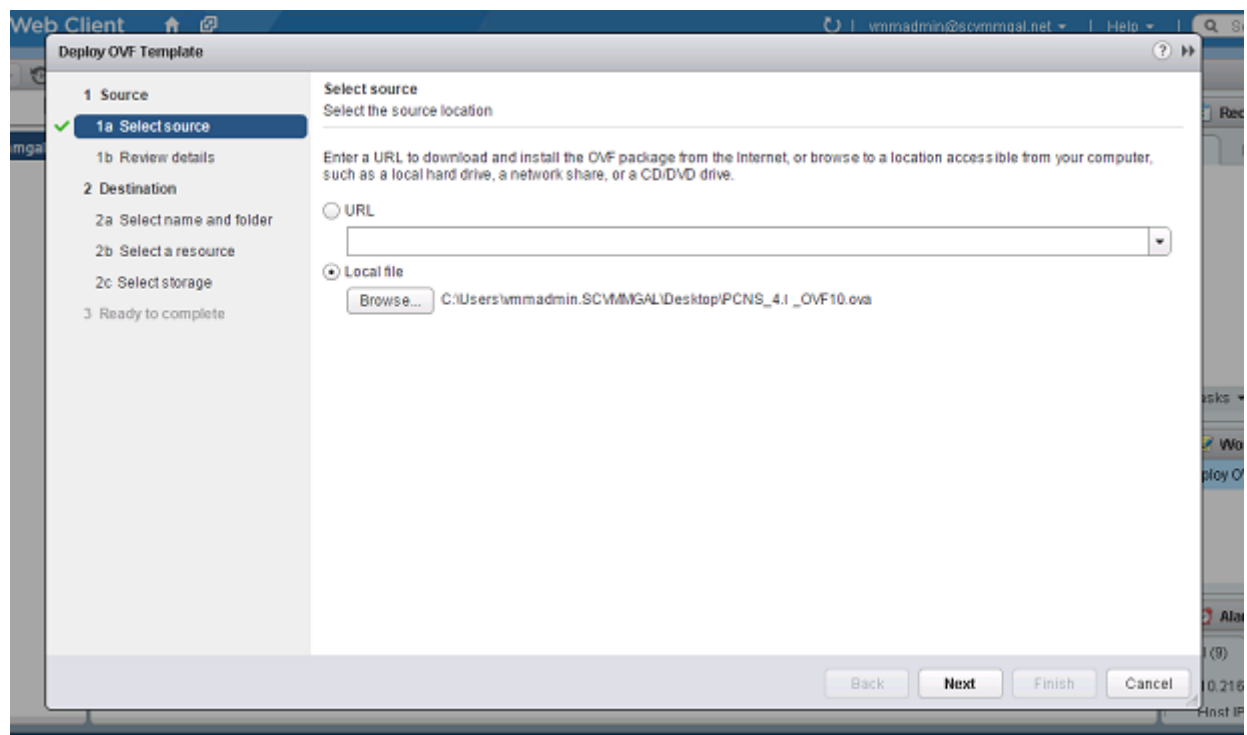
1. Download the PowerChute virtual appliance file, **PCNS_4.2_OVF10.ova** from the [APC website](#).
2. Log on to the VMware host or vCenter Server using your vSphere Client.
3. Select **vCenter Servers > Deploy OVF Template...** from the menu.



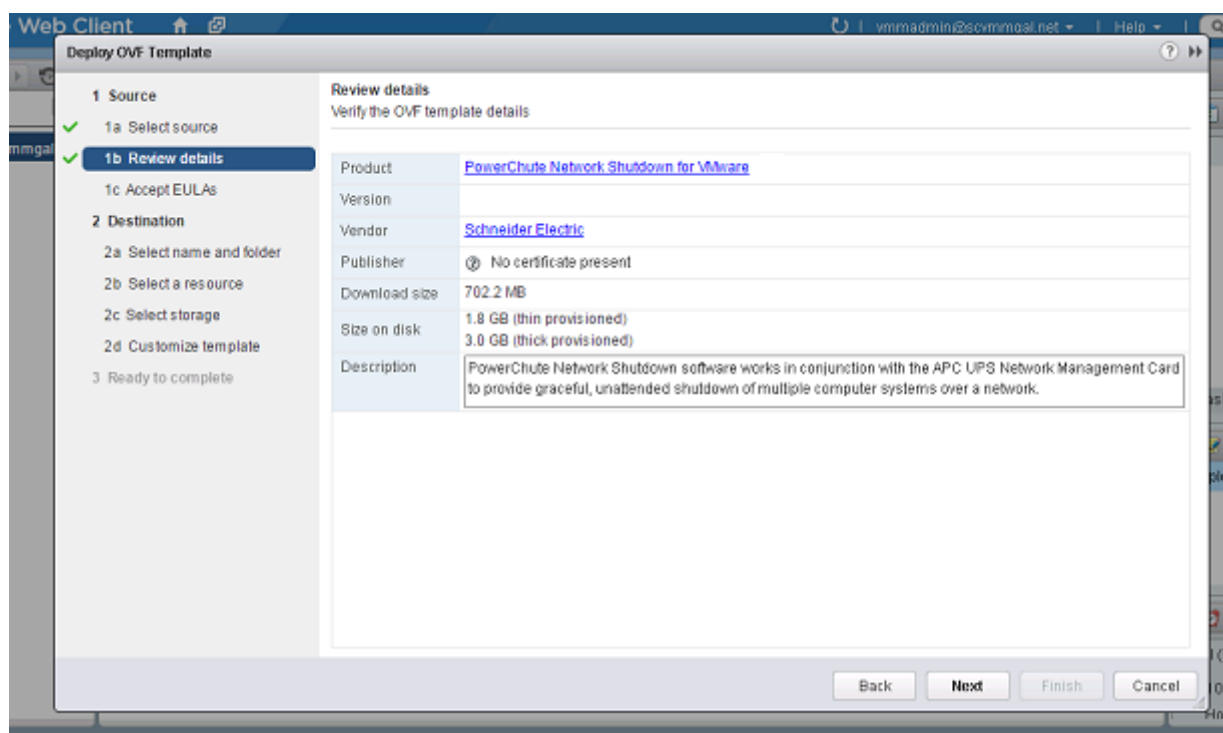
4. If the web client displays an error message to state that an update to the Client Integration Plug-in is required, download the Integration Plugin installer, close the web browser, run the installer and begin again at step 1.



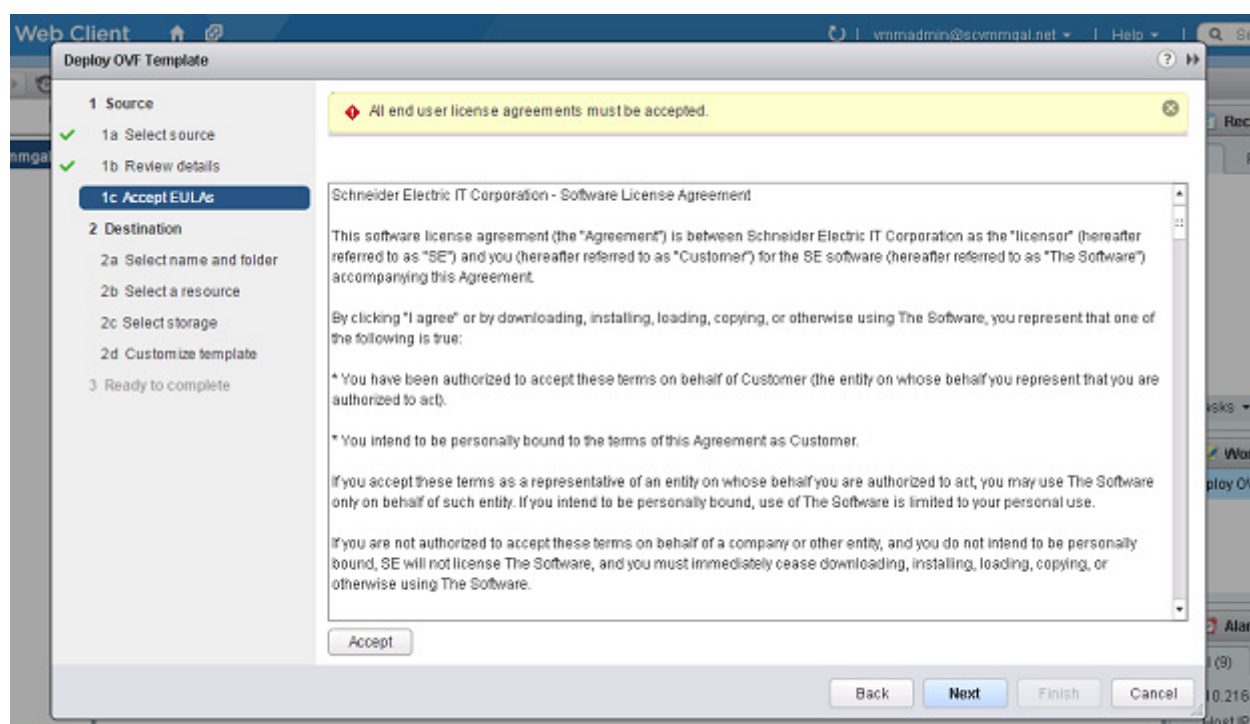
At the **Deploy OVF Template** choose **Select Source > Local file** and browse to the .OVA file.



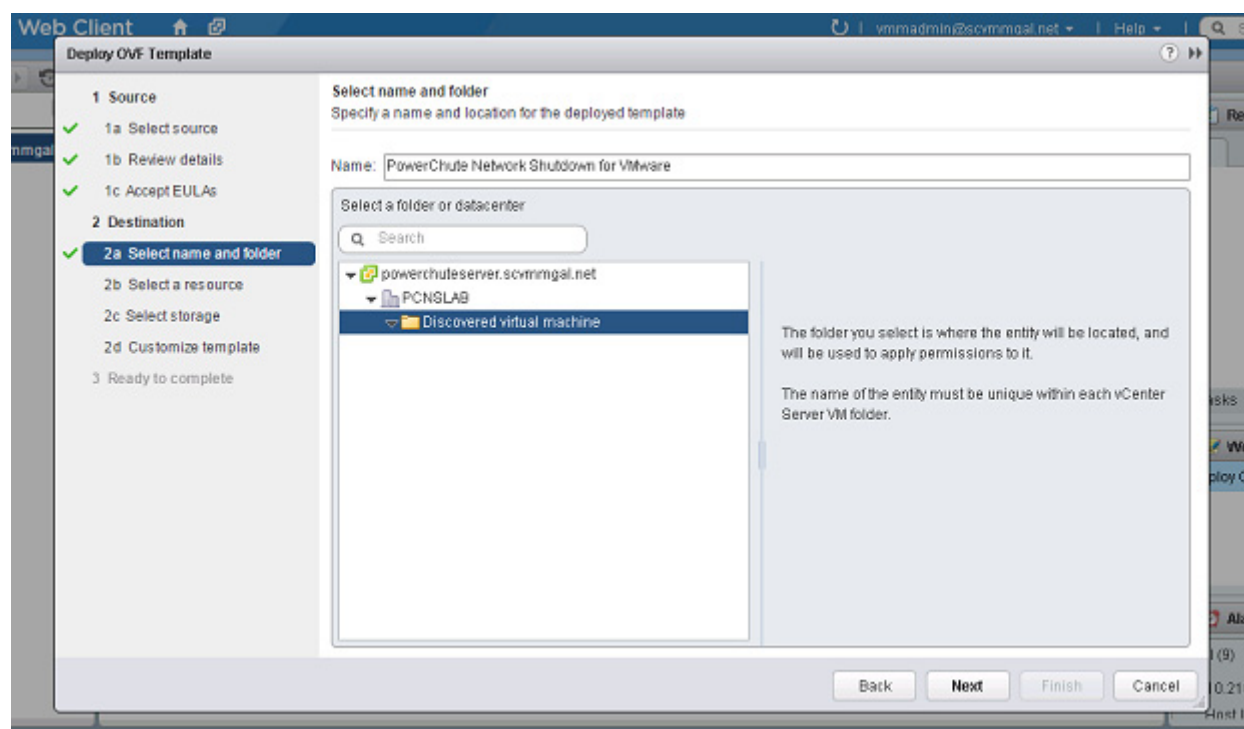
5. The OVA details are displayed. Click the Next button.



6. When the End User Licence Agreement (EULA) is displayed, click **Accept** and then **Next**.

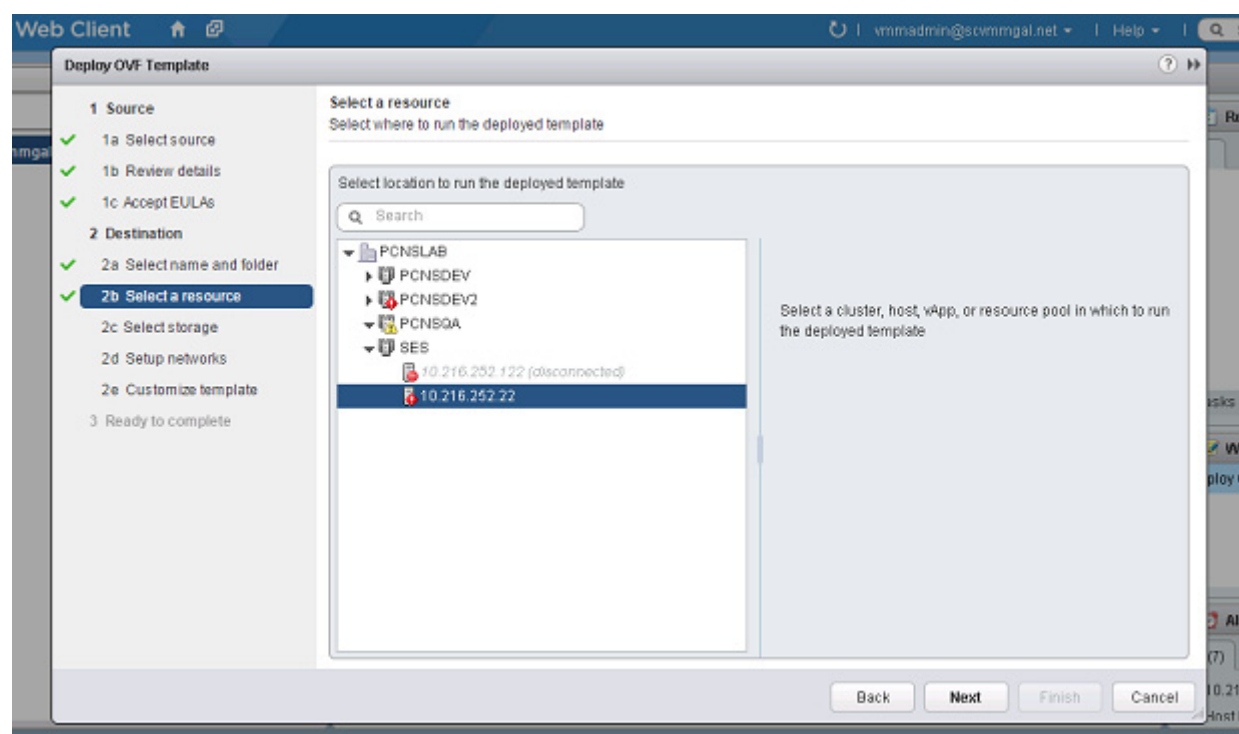


7. Specify a name for the deployed template, navigate to the datacenter, click to expand and highlight **Discovered virtual machine**, and click Next.



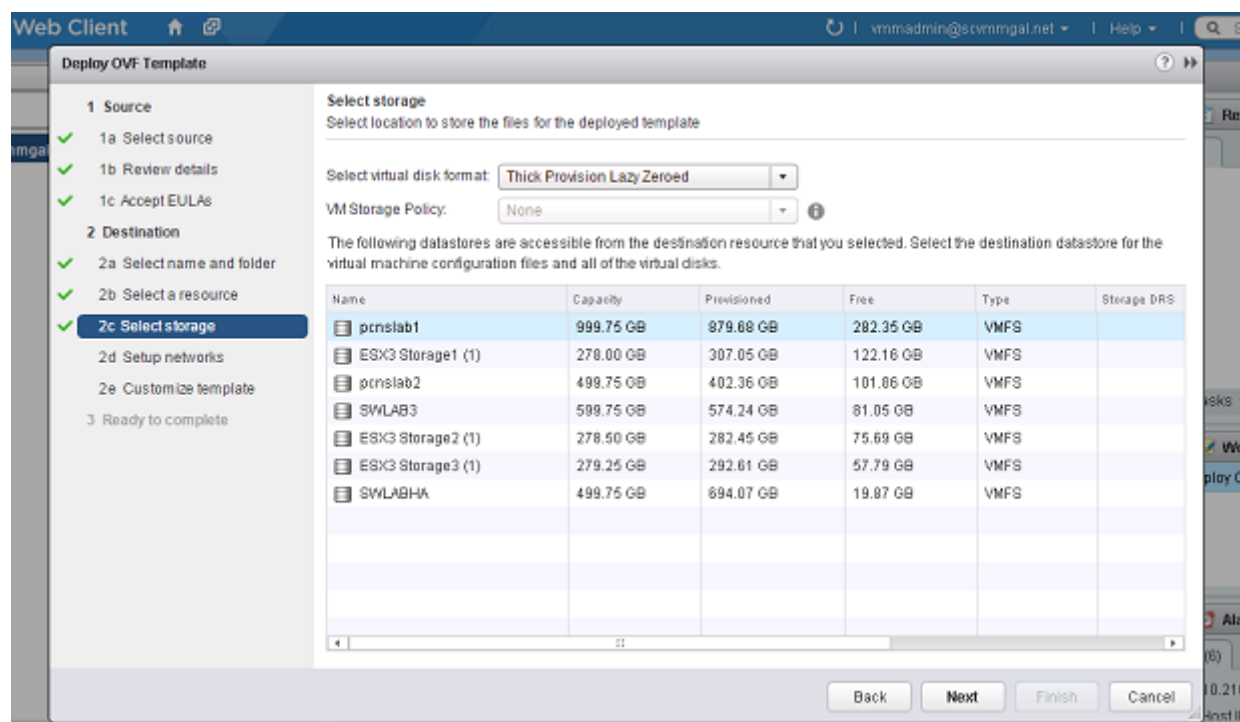
8. This step is not relevant if you are deploying to a standalone host.

Select a resource - specify a host or a cluster and click Next. If you specify a cluster, you will be asked to specify a host within that cluster.

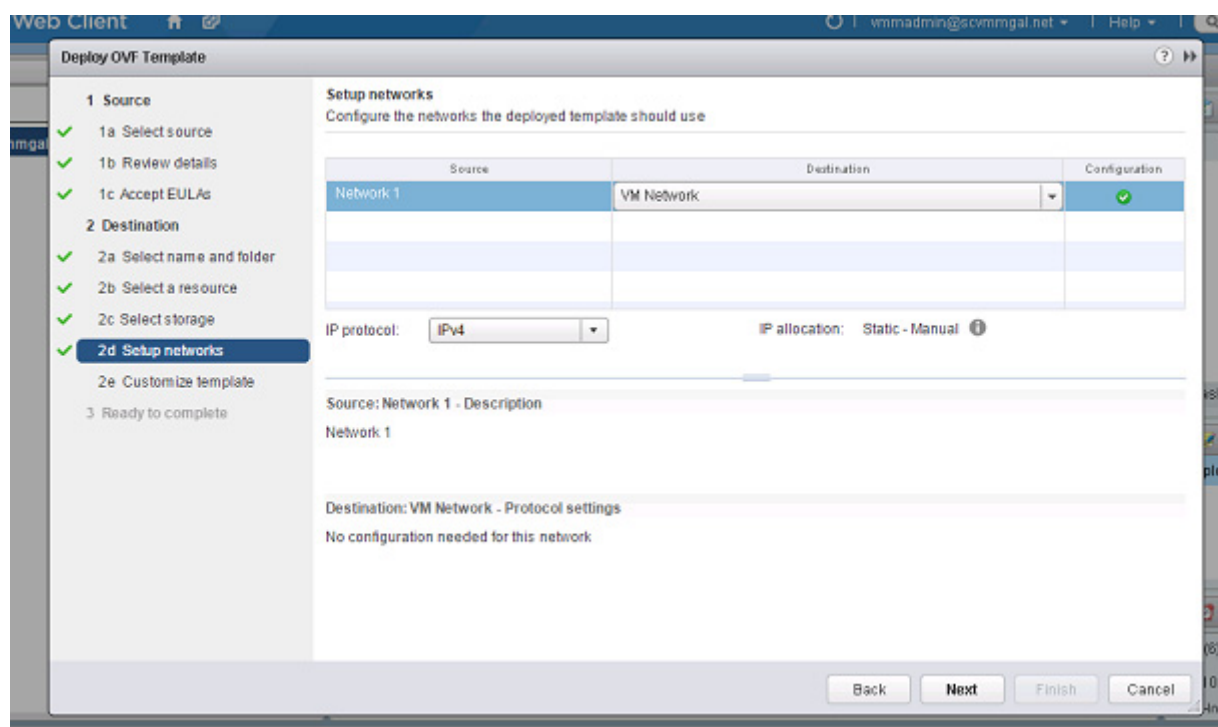


9. This step is not relevant if you are deploying to a standalone host.

Select storage - specify a configured datastore on your system that has sufficient disk space to deploy the virtual appliance. Click Next.



10. **Setup networks** - if using static IP allocation, fill in these field values as necessary. If you are using DHCP, you do not need to fill in the fields, so just click Next.



11. This step is not relevant if you are deploying to a standalone host - to configure a static IP address when deploying to a standalone host, use the Network configuration menu displayed at first boot of the appliance - see [Step 14](#) of Deploying the Virtual appliance using the vSphere Desktop Client.

Customize template - the option is presented to customize the deployment properties. Leave the option blank to choose the default options.

Web Client | vmadmin@scvmmgal.net | Help

Deploy OVF Template

1 Source

- 1a Select source
- 1b Review details
- 1c Accept EULAs

2 Destination

- 2a Select name and folder
- 2b Select a resource
- 2c Select storage
- 2d Setup networks
- 2e Customize template**

3 Ready to complete

Customize template

Customize the deployment properties of this software solution

All properties have valid values [Show next...](#) [Collapse all...](#)

Networking Properties 4 settings

Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired.
DNS	The domain name servers for this VM (comma separated). Leave blank if DHCP is desired.
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired.
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired.

Back Next Finish Cancel

12. Review the options that have been chosen and click **Finish** to commence the installation. The time taken to deploy the appliance depends on your network speed.

Web Client | vmadmin@scvmmgal.net | Help

Deploy OVF Template

1 Source

- 1a Select source
- 1b Review details
- 1c Accept EULAs

2 Destination

- 2a Select name and folder
- 2b Select a resource
- 2c Select storage
- 2d Setup networks
- 2e Customize template

3 Ready to complete

Ready to complete

Review your settings selections before finishing the wizard.

OVF file	C:\Users\vmadmin\SCVMMGAL\Desktop\PCNS_OVF10.ovf
Download size	702.2 MB
Size on disk	3.0 GB
Name	PowerChute Network Shutdown for VMware
Datastore	pcnslab1
Target	10.216.252.22
Folder	Discovered virtual machine
Disk storage	Thick Provision Lazy Zeroed
Network mapping	Network 1 to VM Network
IP allocation	Static - Manual, IPv4
Properties	Default Gateway = DNS = Network 1 IP Address = Network 1 Netmask =

☒ Power on after deployment

Back Next Finish Cancel

When the installation has completed successfully **PowerChute Network Shutdown 4.2 for VMware** displays as a VM in the inventory. To complete the configuration, continue from step 13 of Deploying the Virtual Appliance using the vSphere Desktop client - Power on your PowerChute virtual machine.

Installing on vSphere Management Assistant (vMA)

PowerChute Network shutdown can also be installed on the vSphere Management Assistant (vMA).

There are two steps, see [Deploying vMA on a VMware Host](#). and [Installing PowerChute on the vMA](#).

Deploying vMA on a VMware Host.

The web page [vSphere Management Assistant](#) provides more information. Alternatively, you can call VMware customer support.

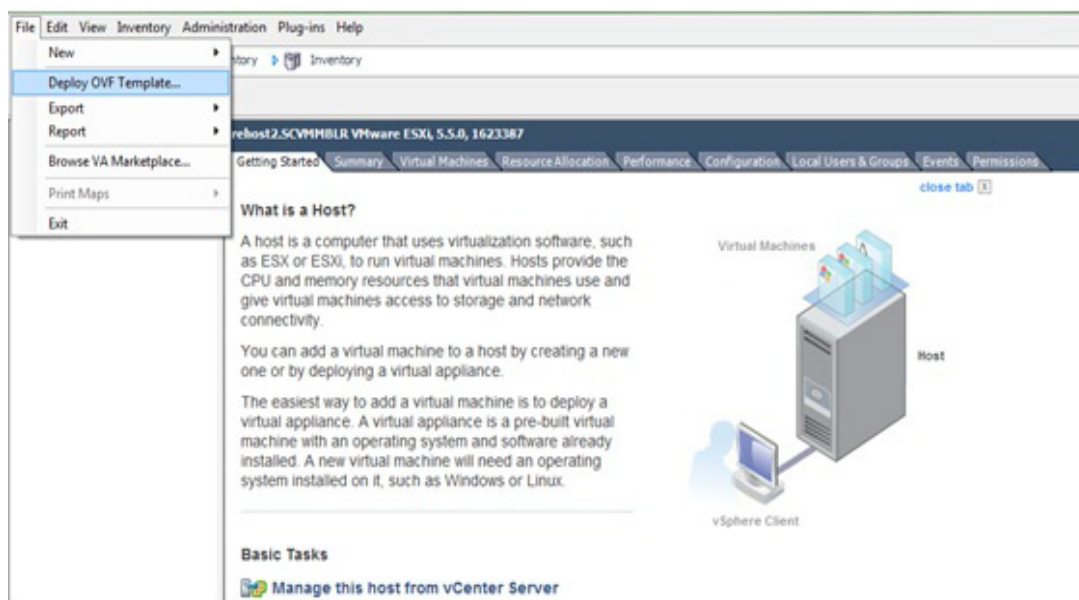
The Schneider Electric KBase <http://www.apc.com/site/support/index.cfm/faq/index.cfm> (FAQ ID is FA159775), has some information on installing the vSphere Client.



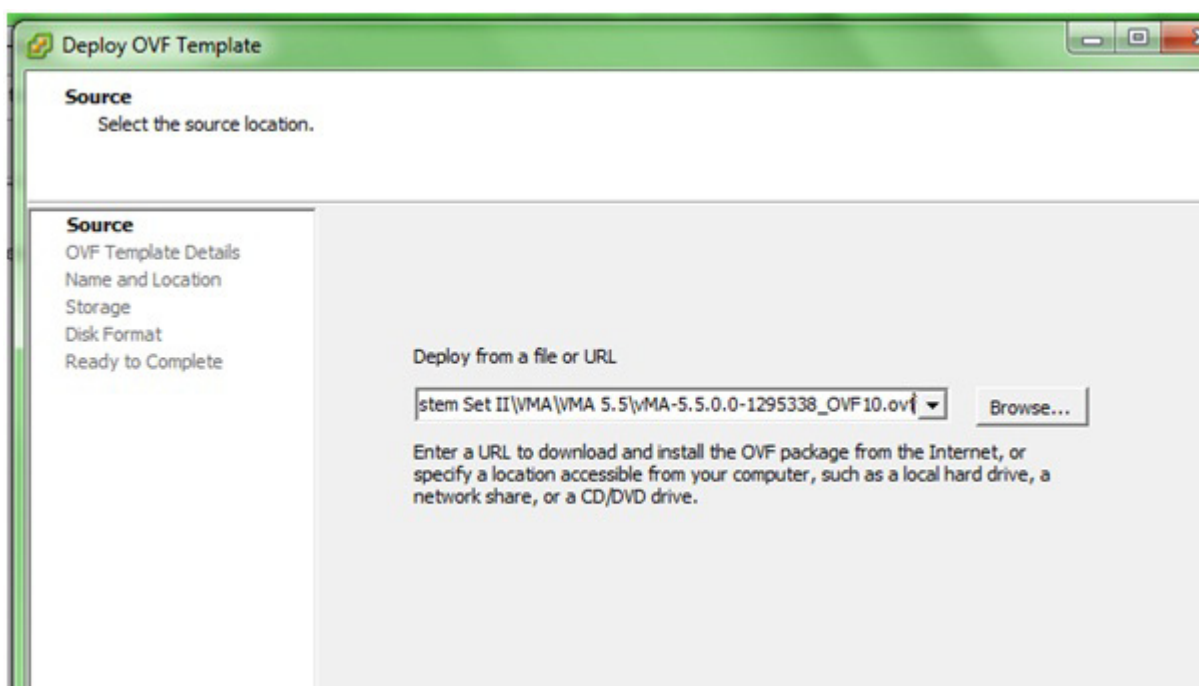
vSphere Management Assistant (vMA) was previously known as VMware Infrastructure Management Assistant (VIMA).

Follow these steps to install vMA.

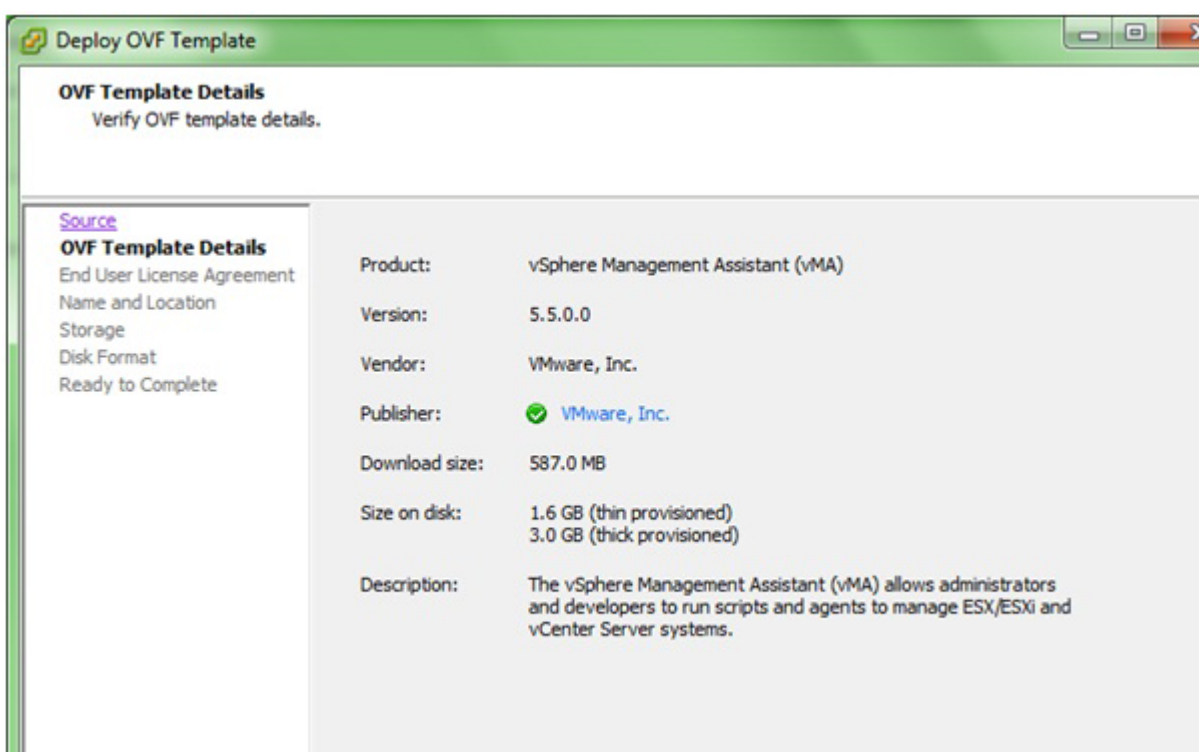
1. Download the vMA installation files from [vSphere Management Assistant](#), and extract the files.
2. Log on to the VMware host or vCenter server using your vSphere Client.
3. Select **File - Deploy OVF Template** from the menu.



- At the **Deploy from a file or URL** field, enter the path to the .OVF file you extracted at step 1 above.



- The vMA and OVF details are displayed. Click the Next button.



- When the End User Licence Agreement (EULA) is displayed, click **Accept** and then Next.

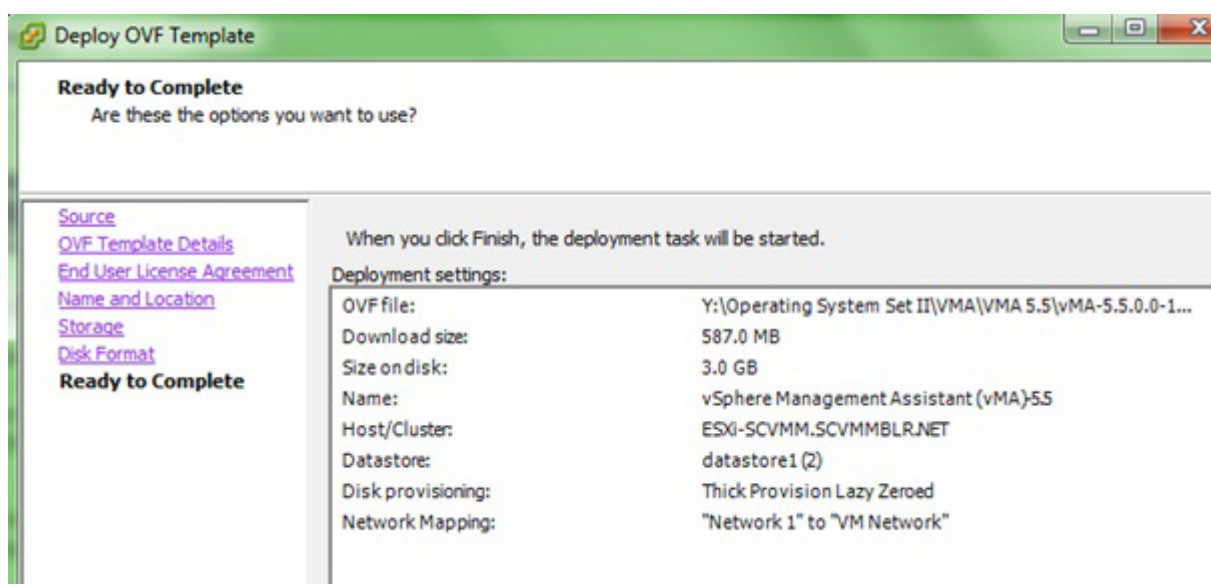
7. Accept the default vMA name (and location) or enter alternatives, and click Next.

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar is green with the text 'Deploy OVF Template'. The main window has a green header bar with the same text. Below the header, the title 'Name and Location' is displayed in bold, followed by the instruction 'Specify a name and location for the deployed template'. On the left side, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location' (which is highlighted), 'Storage', 'Disk Format', and 'Ready to Complete'. The main area on the right has a 'Name:' label and a text input field containing 'vSphere Management Assistant (vMA)'. Below the input field, a note states: 'The name can contain up to 80 characters and it must be unique within the inventory folder.'

8. At Disk Format, choose the default disk layout option by clicking Next.

The screenshot shows the 'Deploy OVF Template' wizard window at the 'Disk Format' step. The title bar is green with the text 'Deploy OVF Template'. The main window has a green header bar with the same text. Below the header, the title 'Disk Format' is displayed in bold, followed by the instruction 'In which format do you want to store the virtual disks?'. On the left side, there is a navigation pane with links: 'Source', 'OVF Template Details', 'End User License Agreement', 'Name and Location', 'Storage', 'Disk Format' (which is highlighted), and 'Ready to Complete'. The main area on the right has a 'Datastore:' label and a text input field containing 'datastore1 (2)'. Below this, there is a label 'Available space (GB):' and a text input field containing '89.2'. At the bottom, there are three radio button options: 'Thick Provision Lazy Zeroed' (which is selected), 'Thick Provision Eager Zeroed', and 'Thin Provision'.

9. The options you have chosen display again, click **Finish**.



The vMA software is now installed, and it should be displaying in the left-hand pane.

10. Select the vMA in the left-hand pane.
11. Power on the vMA virtual machine, then follow the instructions on configuring the IP address, setting vi-admin password, etc.

```
Network Configuration for eth0
IPv4 Address:
Netmask:
IPv6 Address:
Prefix:

Global Configuration
IPv4 Gateway:
IPv6 Gateway:
Hostname:      localhost
DNS Servers:
Proxy Server:

Main Menu
0) Show Current Configuration (scroll with Shift-PgUp/PgDown)
1) Exit this program
2) Default Gateway
3) Hostname
4) DNS
5) Proxy Server
6) IP Address Allocation for eth0
Enter a menu number [0]: _
```

```
Starting password configuration ...
The root account is disabled in this vMA virtual machine, which means no one can
log in as root. The administrator account for vMA is called "vi-admin". In orde
r to log in to vMA, you need to log in as this user. This user has been pre-crea
ted in the vMA, and its password needs to be set now. Please enter a secure pass
word for the account now.

Please provide a password for the vi-admin user. If you are prompted for an old
password for this user, press <enter>.
Old Password:
New password:
Retype new password: _
```

Installing PowerChute on the vMA

You must have root privileges to perform the installation.

1. If you are installing from the CD, locate your installation files in the ESXi directory on the CD. Copy them to a temporary directory on your server.
2. If you are installing from the website, locate this file on the [APC website](#) and copy it to a temporary directory on your server:

`pcns420ESXi.tar.gz`

3. Change your working directory to the temporary directory. Then type the following commands:

```
sudo gunzip pcns420ESXi.tar.gz
sudo tar -xf pcns420ESXi.tar
```

4. Type: `sudo ./install.sh`



After a web download you need to grant execute permissions:

```
sudo chmod +x install.sh
```

5. At the License Agreement, if you agree with the terms, type Yes and press the Enter key to continue. Type No to exit.
6. When configuring for a Java Runtime Environment (JRE), if a valid public JRE is detected, you can choose between using it or the private JRE that is bundled with PowerChute (see [JRE](#)).

If using the public JRE, you must enter its path. Enter an installation folder location or accept the default.

You cannot specify a directory name that contains a space, either for the installation or the Java directory. If you do not specify an installation directory, it will be installed to the default: `/opt/APC`.



The PowerChute Network Shutdown service starts automatically when the installation is completed. You can then delete the installation files.

7. Enter **Yes** to **Enable SNMP Support** and enter the **SNMP discovery port**. If the default port number 161 is unavailable, enter another available port number.

If a firewall is configured, make sure that PowerChute can receive inbound data to port 161. See [Firewall](#) for more information.

NOTE: If SNMP support is not enabled during installation, it cannot be subsequently enabled through the PowerChute Configuration Wizard, and no options relating to SNMP will be available in the web user interface, or via the configuration INI file.



Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.

8. Go to a computer that has a browser and open the PowerChute user interface with:

```
https://<server_ip_address>:6547
```

Follow the steps in the PowerChute setup wizard to complete your configuration.

Upgrading the software

Upgrading enables you to retain your existing configuration settings. Upgrades are only possible if your existing version of PowerChute is 3.1 or greater.

If you have v3.1 or higher of PowerChute already installed on your target machine, the installation process asks you whether you want to perform an upgrade rather than a complete installation.

See the table below for information on upgrades:

PowerChute Install Type	Upgrade possible?
Installing on Windows to Monitor VMware Hosts	Yes
Deploying the PowerChute Virtual Appliance	No
Installing on vSphere Management Assistant (vMA)	Yes

Following the upgrade installation, to ensure that the PowerChute user interface enhancements are applied correctly, it is necessary to clear the browser history:

- In Internet Explorer - select **Tools > Safety > Delete browsing history**
- In Chrome - select **Settings > Show advanced settings > Privacy > Clear browsing data**
- In Firefox - select **Open Menu > History > Clear Recent History**

Upgrading the Virtual Appliance

To upgrade the Virtual Appliance, you do not need to deploy a new copy of the Appliance and run the Setup Wizard. You can now upgrade the version of PowerChute running on the Virtual Appliance using the ESXi installation files:

1. Copy the ESXi installation files to the Virtual Appliance.
2. Run `./install.sh`

Uninstalling

Uninstalling PowerChute on a vMA:

- Run the uninstall script located in the PowerChute directory from a terminal prompt.

```
/opt/APC/PowerChute/uninstall
```

- To uninstall in **silent mode**, run the uninstall script located in the PowerChute directory, with the `-q` option.

```
/opt/APC/PowerChute/uninstall -q
```

For a virtual appliance installation, you should delete the appliance from inventory:

- Right-click on the virtual appliance and choose **Delete from disk**.

Silently Installing the Software

Installing silently means the installation is unattended or non-interactive.



It is not possible to roll out your event configurations or shutdown settings using a silent installation. You can however, use `pcnsconfig.ini` to do this. See the section on INI files in the online help.



PowerChute only supports silent installation in Single, Redundant and Parallel UPS configurations.

Silent Install on VMware



You cannot install silently using the virtual appliance method, see [Deploying the PowerChute Virtual Appliance](#).

Edit the silent installation file `silentInstall.sample` to set the required parameters; see [Editing your silent installation file](#).

Type the following command to start the installation:

```
sudo ./install.sh -f silentInstall.sample
```



If a silent installation fails, see [Appendix A: Error codes for silent installations](#).

Editing your silent installation file

When monitoring a VMware host with PowerChute Network Shutdown, your silent installation file is named `silentInstall.ini`. For Linux installations, the file is named `silentInstall.sample`.

These are plain text files and can be edited with a text editor. The table below described the fields in the silent installation file to be configured:

Field name	Description
The fields directly below, <code>applicationDirectory</code> and <code>INSTALL_JAVA</code> , are used when you are monitoring a VMware host from a Windows machine with PowerChute Network Shutdown (see Installing on Windows to Monitor VMware Hosts).	
<code>applicationDirectory=</code>	Specifies the installation folder. Type the folder name after "=", ensuring it has valid characters for the operating system. Note: You can't use multiple-byte characters (Chinese for example) and some single byte high-ASCII characters, e.g. ß, é, ä, in the installation path.
<code>ACCEPT_EULA=yes</code>	Yes signifies acceptance of the software licence agreement. The installation will not proceed unless yes is specified here.
<code>INSTALL_JAVA=</code> <code>System PCNS</code>	The value <code>System</code> here signifies you want to use the public JRE for your PowerChute installation. The value <code>PCNS</code> here signifies you want to use the private JRE. The installation detects whether the public JRE meets the requirements.
The fields directly below, <code>INSTALL_DIR</code> and <code>JAVA_DIR</code> , are used when you are monitoring a VMware host from a VM with PowerChute Network Shutdown (see Installing PowerChute Network Shutdown with VMware Support).	
<code>INSTALL_DIR=</code>	Specifies the installation directory. Type the path where the public JRE is installed on the system e.g. <code>\usr\bin</code> . Note: You can't use multiple-byte characters (Chinese for example) and some single byte high-ASCII characters, e.g. ß, é, ä, in the installation path.
<code>JAVA_DIR=</code>	Specifies the JRE directory. Type the directory name after "=", ensuring it has valid characters for the operating system. If this value is blank or absent, the private JRE is installed. Specify a public JRE for PowerChute by setting the path to the JRE executable. See JRE .
<code>REGISTER_WITH_NMC=</code> <code>yes no</code>	Using yes or no, specify whether PowerChute should be registered with the Network Management Card (NMC) or not.
<code>MODE=</code> <code>single redundant parallel</code>	Use single, redundant, or parallel to specify the UPS configuration mode. See the online help, UPS Configuration Options , for more information.
<code>NETWORKCONFIG=</code> <code>IPv4 IPv6</code>	Specify your internet protocol with IPv4 or IPv6.
<code>IPv6NETWORKCONFIG=</code> <code>unicast multicast</code>	When you are using IPv6 only (having entered <code>NETWORKCONFIG= IPv6</code> above) you must specify the communication mechanism here. See also UNICAST_ADDRESS= and MULTICAST_ADDRESS= . For detailed information, see "The Communications Process of PowerChute Network Shutdown" here .

Field name	Description
IP_1= IP_2= IP_3= IP_4= IP_5= IP_6= IP_7= # IP_8= # IP_9=	On each line, specify the IP address of each NMC that will be communicating with this PowerChute installation. You can comment out unneeded entries by putting the # character at the beginning of the line (see examples 8 and 9).
IP_1_Outlet= IP_2_Outlet= IP_3_Outlet= IP_4_Outlet= IP_5_Outlet= IP_6_Outlet= IP_7_Outlet= # IP_8_Outlet= # IP_9_Outlet=	This applies only to UPS devices with Outlet Groups (for example, Smart-UPS SMX and SMT devices). Specify the outlet group that supplies power to the PowerChute installation. On a UPS that has only Switched Outlet Groups, "IP_1_Outlet" must be set to "1". If you enter "0", PowerChute may not correctly identify Outlet events associated with the first Outlet group. On a UPS that has both a Main Outlet Group (not switched) and Switched Outlet Groups, "IP_1_Outlet" must be set to "0". You can comment out unneeded entries by putting the # character at the beginning of the line (see examples 8 and 9).
PORT=	This is the NMC web port: 80 for HTTP; 443 for HTTPS.
PROTOCOL= HTTP HTTPS	Use HTTP or HTTPS to specify which protocol you are using.
ACCEPTCERTS= YES NO	When using the HTTPS protocol, SSL certificates are used to secure the connection. By default the NMC use a self-signed certificate, which needs to be accepted. Select YES to automatically accept a self-signed certificate. Select NO to accept a connection only if the NMC is configured with a valid certificate
USERNAME= PASSWORD= AUTHENTICATION_PHRASE=	Enter the user name, password, and authentication phrase to validate PowerChute communication with the NMC. (The authentication phrase reverts to the default if not specified). Note: We recommend that you change the defaults for security reasons. The acceptable characters for username and password are: <ul style="list-style-type: none"> • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: _!\"#\$%&'()*+,-./:;<=>?@^`{ }[]~ The password length must be from 3–32 characters, and the username from 3–10 characters. The authentication phrase must be 15–32 ASCII characters.
LOCAL_IP_ADDRESS=	This information applies to a PowerChute server with multiple network cards. Use it to specify the IP address of the card that will communicate with PowerChute.
UNICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and unicast in IPV6NETWORKCONFIG= unicast multicast , you must specify your unicast host address here.
MULTICAST_ADDRESS=	When you have specified IPv6 in NETWORKCONFIG= IPv4 IPv6 and multicast in IPV6NETWORKCONFIG= unicast multicast , the Network Management card will send UDP packets to the multicast address you specify here.

Field name	Description
CONFIGURATION_MODE= Managed Unmanaged	Specify the mode in which your ESXi servers are configured. See the online help for more information on this.
VCENTERSERVER_ADDRESS=	When the CONFIGURATION_MODE= field above is “managed”, specify the IP Address or the host name or the FQDN (Fully Qualified Domain Name) of the vCenter server.
VCENTERSERVER_USERNAME=	When the CONFIGURATION_MODE= field above is “managed”, specify the user name of the vCenter server.
VCENTERSERVER_PASSWORD=	When the CONFIGURATION_MODE= field above is “managed”, specify the password of the vCenter server.
VCENTERSERVER_PROTOCOL = http https	Specify the protocol by which vCenter Server communicates with PowerChute.
VCENTERSERVER_PORT = 80 443	Specify the vCenter Server Port.
ESXHOST_ADDRESS=	When the CONFIGURATION_MODE= field above is “unmanaged”, specify the IP Address or the host name or the FQDN (Fully Qualified Domain Name) of the ESXi host to be managed.
ESXHOST_USERNAME=	When the CONFIGURATION_MODE= field above is “unmanaged”, specify the user name of the ESXi host.
ESXHOST_PASSWORD=	When the CONFIGURATION_MODE= field above is “unmanaged”, specify the password of the ESXi host
ESXHOST_PROTOCOL = http https	Specify the protocol by which the ESXi Host communicates with PowerChute.
ESXHOST_PORT = 80 443	Specify the port of the ESXi Host.
SNMPv1	
ENABLE_SNMPV1_ACCESS = True False	Specify true to enable SNMPv1 access and false to disable SNMPv1 access.
NAME_COMMUNITY_N =	Enter the community name, up to 15 ASCII characters.
NMS_COMMUNITY_N=	Enter the IP address of the Network Management System.
ACCESS_TYPE_COMMUNITY_ N = READONLY READWRITE DISABLED	Specify the Access type of the SNMP community string: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT =	Specify the SNMP Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMPv3	
ENABLE_SNMPV3_ACCESS = True False	Specify True to enable SNMPv3 access and false to disable SNMPv3 access.
USERNAME_PROFILE_N =	Specify the user name of the SNMPv3 user profile, up to 32 ASCII characters.
AUTH_PASSPHRASE_PROFILE _N =	Enter the Authentication passphrase of 8-32 ASCII characters.
PRIV_PASSPHRASE_PROFILE_ N =	Enter the Privacy passphrase of 8-32 ASCII characters.

Field name	Description
AUTH_PROTOCOL_PROFILE_N = MD5 SHA1 SHA256 SHA512 NONE	Specify the Authentication protocol of the SNMPv3 user profile.
PRIV_PROTOCOL_PROFILE_N = AES128 AES192 AES192EX AES256EX AES256 DES NONE	Specify the Privacy protocol of the SNMPv3 user profile. See the “ <i>SNMP Troubleshooting</i> ” topic of the <i>PowerChute Network Shutdown User Guide</i> available on www.apc.com for more information on JRE requirements for AES-192/Ex and AES-256/Ex.
ACCESS_TYPE_PROFILE_N = READONLY READWRITE DISABLED	Specify the Access type of the SNMPv3 user profile: <ul style="list-style-type: none"> • DISABLED: No SNMP GET or SET requests are permitted. • READONLY: Only SNMP GET requests are permitted. • READWRITE: SNMP GET and SET requests are permitted.
SNMP_PORT=	Specify the SNMP discovery Port. 161 is the default.
Note: N indicates an integer (0-N)	
SNMP Traps	
UPSCriticalEvents_Enabled = True False	Specify True to enable SNMP Traps for UPS Critical Events.
UPSCriticalEvents_SendClearingTrap = True False	Enter True to send a Trap once a UPS Critical Event has cleared.
UPSCriticalEvents_Delay =	Specify the length of time in seconds that the UPS Critical Event must persist before a trap is sent.
UPSCriticalEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
UPSCriticalEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the UPS Critical Event is cleared.
UPSCriticalEvents_RepeatTimes =	Specify the number of times the trap is sent when the UPS Critical Event occurs.
LostCommsEvents_Enabled = True False	Specify True to enable SNMP Traps for Lost Communication Events.
LostCommsEvents_SendClearingTrap = True False	Enter True to send a Trap once a Lost Communication Event has cleared.
LostCommsEvents_Delay =	Specify the length of time in seconds that the Lost Communication Event must persist before a trap is sent.
LostCommsEvents_RepeatInterval =	Specify the time interval in seconds that the trap is re-sent.
LostCommsEvents_RepeatUntilCleared = True False	Specify True if you want the trap to be sent at the repeat interval until the Lost Communication Event is cleared.
LostCommsEvents_RepeatTimes =	Specify the number of times the trap is sent when the Lost Communication Event occurs.
Enabled_TrapReceiver_N = True False	Enter True to enable the Trap Receiver.
NMS_TrapReceiver_N =	Enter the IP address of the Network Management System that will receive traps.
Port_TrapReceiver_N =	Enter the port number of the Trap Receiver.

Field name	Description
Type_TrapReceiver_N = v1 v3	Enter the version of SNMP used to send the traps.
ProfileName_TrapReceiver_N =	Enter the User Name of the SNMPv3 User Profile used to send the traps.
Note: N indicates an integer (0-N)	

Appendix A: Error codes for silent installations

When using silent installations (and upgrades), you can use the list of error codes in the table below to understand what's going wrong when the installation fails.

For silent install using the shell script `install.sh` the error message is written to the terminal standard output. The error code can be retrieved using the `$?` variable.

For Windows, the error code is written to a file called **PCNSinstall.log**.

Error Code	Error Message	Description
0		Success: Indicates that installation succeeded.
1	Usage: <code>install.sh [-f <config file>]</code> : Silent install with configuration file. <code>install.sh [-h -H]</code> : Print help.	Usage: Indicates that unrecognized parameters were passed to the installer.
4	Error: <code>install.sh</code> must be run with root privileges!	Administrator Only: Indicates that a non-administrator has tried to run the installer.
5	Error: Unknown OS.	Unsupported OS: The installer has detected an Operating System it cannot support.
6	PowerChute Network Shutdown is already installed. Upgrade is not supported for this version. Please uninstall the existing PowerChute to continue with installation of PowerChute v.4.2. Installation cancelled.	Upgrade Not Supported: Indicates that PowerChute cannot support upgrade from a previous installation of PowerChute. This can be due to the versioning being too old, or an attempted upgrade of a previous multiple install.
7	Installation cancelled.	User Abort: Indicates that the user has aborted installation.
8	You must remove the installed version of PowerChute Plus.	PC Plus Detected: Indicates that the installer has aborted due to the detection of a version of PowerChute Plus.
9	You must remove the installed version of PowerChute Business Edition Server.	PowerChute Business Edition Detected: Indicates that the installer has aborted due to the detection a version of PowerChute Business Edition.
10	You must remove the installed version of PowerChute Server.	PowerChute Server Detected: Indicates that the installer has aborted due to the detection of a version of PowerChute Server.

Error Code	Error Message	Description
12	<p>One of:</p> <p>Error: Too many INSTALL_DIR in silentConfiguration.ini.</p> <p>Error: INSTALL_DIR must start with '/'. Installation directory must start with '/'. Error: INSTALL_DIR must not contain white space.</p> <p>Error: INSTALL_DIR must not contain back slash "\".</p> <p>Error: INSTALL_DIR is not configured. Installation directory must not contain white space " ".</p> <p>Installation directory must not contain back slash "\".</p> <p>Failed to create directory <install directory>.</p>	Invalid Install Directory: Indicates that the installer has aborted due to an invalid target directory.
13	Installation cancelled.	Invalid Java Version: Invalid version of Java specified in configuration file.
14	This version of PowerChute Network Shutdown does not support the Japanese language. Please consult www.apc.com for the required version of PowerChute Network Shutdown.	Unsupported Locale: The installer has detected an attempt to install an English build on a Japanese system.
15	Can't find <zip filename>	Zipfile Missing: Indicates that the installer cannot find the zipfile, from which to extract the PowerChute install.
16	Error: Invalid file <filename>	Silent Configuration Missing: Indicates that the installer has aborted because the specified silent configuration file could not be read.
17	Error: EULA must be accepted by setting ACCEPT_EULA=YES in config file	EULA Not Accepted: Indicates that the installer has aborted because the End User Licence Agreement was not accepted.
18	[Error]: <configuration value> is not defined in <configuration file>.	Silent Configuration Missing Parameter: Indicates that required parameters are missing from the silent configuration file.
19	[Error]: Too many <configuration value> in <configuration file>	Silent Configuration Multiple Parameters: Indicates that a parameter is duplicated in the silent configuration file.
20	<p>One of:</p> <p>Error: Too many JAVA_DIR in <configuration file>.</p> <p>Error: JAVA_DIR must start with '/'. Error: JAVA_DIR must not contain white space " ".</p> <p>Error: JAVA_DIR must not contain back slash "\".</p> <p>Error: Invalid JAVA_DIR. <directory> does not exist.</p> <p>Java is not available on the path. Please specify a java directory.</p>	Invalid Java Directory: Indicates that the installer has aborted due to an invalid Java directory specified in the silent configuration file.
21	[Error]: <21> Installation cancelled.	Registry Failure: Indicates the installer has aborted due to an inability to write registry entries.

Error Code	Error Message	Description
22	[Error]: <22> Installation cancelled.	Service Failure: The installer failed to register the PCNS service.
23	[Error]: <23> Installation cancelled.	M11 Backup Failure: The installer has failed to back up the m11.cfg data store during an upgrade.
24	ERROR: Invalid value for LOCAL_IP_ADDRESS specified in silent configuration file. Aborting with error code <error code>.	The IP address was not specified: The installer cannot determine the host IP address, due to multiple network adapters. Invalid Localhost specified in the silent install configuration file. The IP address specified is not associated with the target server.
25	ERROR: Cannot write to specified ini configuration file: <ini file>	Invalid INI. The silent installer cannot write to the pcnsconfig.ini file in the installation directory.
28	ERROR: Invalid value for mode specified in silent configuration file.	Invalid Mode. Silent install configuration file specifies an invalid value for MODE.
29	ERROR: Invalid value for port specified in silent configuration file.	Invalid Port. Silent install configuration file specifies an invalid value for PORT.
30	ERROR: Invalid value for protocol specified in silent configuration file.	Invalid Protocol. Silent installation configuration file specifies an invalid value for PROTOCOL. The valid values are HTTP and HTTPS.
31	ERROR: Not enough UPS Network Management Card addresses specified in silent configuration file for specified mode.	A minimum of 2 IP addresses are required for Redundant, Parallel, and Advanced UPS Configurations.
32	UPS Network Management Card has not responded to registration attempt. Registration has failed due to a timeout.	Registration failed with NMC due to timeout. The NMC host address and the connection attempt were both fine, but the NMC failed to respond.
33	Bad UPS Network Management Card host address supplied. Registration has failed.	The registration failed with NMC due to a bad host address.
34	Could not connect to UPS Network Management Card. Registration has failed.	Registration failed with NMC because incorrect security information - user name, password, authentication phrase - was sent.
35	Could not register with UPS Network Management Card. Please check your configuration.	Registration failed with NMC for a reason other than those cited in the error codes directly above.
36	Incorrect security details given. Registration has failed.	Bad Security Values. Registration failed with NMC due to incorrect security credentials.
37	UPS Network Management Cards specified are not part of a parallel setup.	Not Parallel: Parallel registration attempted, but the NMCs are not part of a parallel configuration.
40	UPS Network Management Cards are not of the same family. Registration has failed.	Not Same Models. Registration failed due to one or more NMCs not having the same model type.
41	Registration has failed due to untrusted SSL certificates presented from the UPS Network Management Card.	SSL Error. Registration failed due to one or more NMCs presenting an untrusted SSL Certificate.
42	ERROR: Invalid value for <outlet group> specified in silent configuration file.	Invalid outlet group. Silent installation configuration file specifies an invalid value for IP_<n>_Outlet
43	ERROR: Invalid value for username specified in silent configuration file.	Invalid User Name specified in the silent install configuration file. The username has failed to pass the regex.

Error Code	Error Message	Description
44	ERROR: Invalid value for password specified in silent configuration file.	Invalid Password specified in the silent install configuration file. The password given has failed to pass the regex.
45	ERROR: Invalid value for authentication phrase specified in silent configuration file.	Invalid Authentication Phrase specified in the silent install configuration file. The authentication phrase has failed to pass the regex.
47	Failed to establish an SSL connection to the UPS Network Management Card. Please verify the address and port specified.	There was an SSL handshake error.
48	A valid JRE has not been detected. Please go to www.java.com (http://www.java.com) and install java, or change INSTALL_JAVA in the silentInstall.ini file.	You need to install a supported public JRE or use the private JRE.
49	Silent configuration file contains multiple UPS Network Management Card addresses. Only one is required for single mode.	There are too many NMC addresses set up: The silent installation configuration file specifies too many NMC addresses for the specified mode.
50	ERROR: Invalid value for NetworkConfig specified in silent configuration file.	The NetworkConfig field value is invalid in the INI silent configuration file.
51	ERROR: Invalid value for IPv6NetworkConfig specified in silent configuration file.	The IPv6NetworkConfig field value is invalid in the INI silent configuration file.
59	ERROR: Network mode is <IPv4/IPv6>.Please enter valid <IPv4/IPv6> address for <NMC_IP/ IP_1/LOCAL_IP_ADDRESS>key.	You have entered an IPv4 address instead of an IPv6 address or vice versa.
Error codes 52–56 only apply in a VMware environment.		
52	ERROR: Invalid value for ESXiConfigurationMode specified in silent configuration file.	The ESXiConfigurationMode field value is invalid in the INI silent configuration file.
53	ERROR: Connection to VCenter Server <vCenter Server IP/Hostname> failed.	There was a vCenter Server connection error.
54	ERROR: Connection to ESXi Host <ESXi IP/ Hostname> failed.	There was a VMware Host connection error.
55	Invalid vCenter Server address.	You have entered an invalid vCenter Server hostname.
56	Invalid ESXi Host address.	You have entered an invalid VMware hostname.
64	Invalid SNMP Port.	You have entered an invalid SNMP Port, or the port may be in use.
65	Invalid SNMP NMS.	You have entered an invalid IP address for the Network Management System.
66	Invalid SNMP Access Type.	You have entered an invalid SNMP Access Type. Options are Disable, Read or Write.
67	Invalid SNMP Authentication protocol.	You have entered an invalid SNMP Authentication Protocol. Options are MD5, SHA1, SHA256, or SHA512.
68	Invalid SNMP Privacy Protocol.	You have entered an invalid SNMP Privacy Protocol. Options are AES-128, AES-192/Ex, AES-256/Ex or DES.

Error Code	Error Message	Description
69	Invalid SNMP Authentication passphrase.	You have entered an invalid Authentication passphrase. The Authentication passphrase must be 8-32 ASCII characters in length.
70	Invalid SNMP Privacy passphrase.	You have entered an invalid Privacy passphrase. The Privacy passphrase must be 8-32 ASCII characters in length.
71	Invalid SNMP Delay.	You have entered an invalid SNMP Delay. Enter a positive number of seconds.
72	Invalid SNMP Repeat Times.	You have entered invalid Repeat Times. Enter a positive whole number.
73	Invalid SNMP Repeat Interval.	You have entered an invalid SNMP Repeat Interval. Enter a positive whole number of seconds.
74	Invalid SNMP Trap Receiver Name.	You have entered an invalid SNMP Trap Receiver Name.
75	Invalid SNMP Trap Receiver NMS.	You have entered an invalid IP address for SNMP Trap Receiver NMS.
76	Invalid SNMP Trap Receiver Port.	You have entered an invalid port number for SNMP Trap Receiver Port.
77	Invalid SNMP Trap Receiver Type.	You have entered an invalid SNMP Trap Receiver Type. Options are v1 or v3.

APC by Schneider Electric Worldwide Customer Support

Customer support for this or any other APC by Schneider Electric product is available at no charge in any of the following ways:

- Visit the APC by Schneider Electric web site, www.apc.com to access documents in the APC Knowledge Base and to submit customer support requests.
 - **www.apc.com** (Corporate Headquarters)
Connect to localized APC by Schneider Electric web site for specific countries, each of which provides customer support information.
 - **www.apc.com/support/**
Global support searching APC Knowledge Base and using e-support.
- Contact the APC by Schneider Electric Customer Support Center by telephone or e-mail.
 - Local, country specific centers: go to **www.apc.com/support/contact** for contact information.
 - For information on how to obtain local customer support, contact the APC by Schneider Electric representative or other distributor from whom you purchased your APC by Schneider Electric product.

© 2016 APC by Schneider Electric. APC, the APC logo, and PowerChute are owned by Schneider Electric Industries S.A.S., or their affiliated companies. All other trademarks are property of their respective owners.