Installation Guide

PowerChute™ Network Shutdown v4.4

Windows®

Linux®/Unix®

Hyper-V®/SCVMM®

VMware® (Nutanix™, SimpliVity, HyperFlex)

Nutanix™

990-2838Q-001

11/2020

PowerChute™
— NETWORK SHUTDOWN

Schneider Electric

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.

Introduction

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.

  NOTE: PowerChute v4.3+ is a 64-bit only application and cannot be installed on a 32-bit operating system.
- **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	1.8 GB
Install PowerChute Network Shutdown using a virtual appliance - Disk format: thick provisioned	10 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 v4.4 installs the Java 13 JRE.

  NOTE: PowerChute only supports OpenJDK Java.
- 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 2** (part number AP9630, AP9631, AP9635) with a firmware version of 5.0.3 or later, a **Network Management Card 3** (part number AP9640, AP9641) with a firmware version of 1.1.0.16 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 2 (NMC 2) firmware 6.0.X or higher, and Network Management Card 3 (NMC 3) firmware 1.1.0.16 or higher.

- **Firewall**
  PowerChute needs to be able to connect to the NMC Web Access port (default: TCP port 80 (NMC 2), TCP port 443 (NMC 3)) 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.

- You must have **administrator or root privileges** to run the installer.

- All hostnames must be resolvable on the machine/virtual machine where PowerChute is installed for the shutdown sequence to proceed as expected. To do this, add the hosts to the hosts file using an ASCII text editor. This file can be found in the below locations:

  - On **Windows**: `C:\Windows\system32\drivers\etc\hosts`
  - On **Linux**: `/etc/hosts`

- 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.

- **Virtual Appliance**
  The PowerChute virtual appliance should be used only for running the PowerChute application – do not modify it or use it for any other purpose. Ensure that SSH access to the appliance is disabled, unless it is needed to gather log files or for the purposes of scripting the deployment of the Appliance.
  It is strongly recommended to regularly update the CentOS libraries of the Virtual Appliance to obtain the latest security updates. See How to update the Virtual Appliance libraries.

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.

   For installation instructions, see the Network Management Card Installation Guide.
2. Using the NMC user interface (UI), set the **Low Battery Duration** field value to at least five minutes when configuring a shutdown.
3. Navigate to **Configuration** > **Shutdown** in the NMC UI to enable and configure PowerChute. **NOTE:** The below steps are relevant for NMC 2 firmware version 6.8.0 and above, and NMC 3 firmware version 1.1.0.16 and above.
   a. Select the communication protocol to be used: HTTPS, HTTP, or none. **NOTE:** The chosen protocol must be enabled on your NMC before PowerChute communications can be established.
   b. Specify a user name and authentication phrase.
   c. Enable PowerChute.

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.

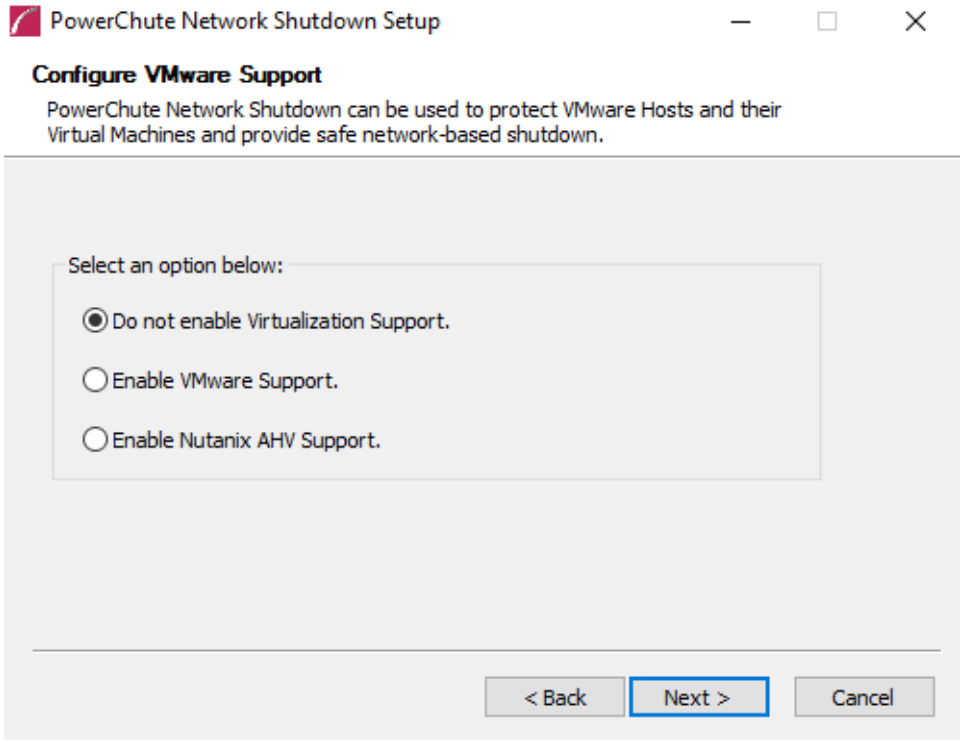
Follow these steps below.

1. Download the PowerChute installation executable file, **Setup-x64.exe**, from the APC website. You must have administrator rights to run the installer.
   Extract the file, and double-click on the file.
2. A warning dialog, below, displays if you downloaded the exe from the web: click the **Run** button.

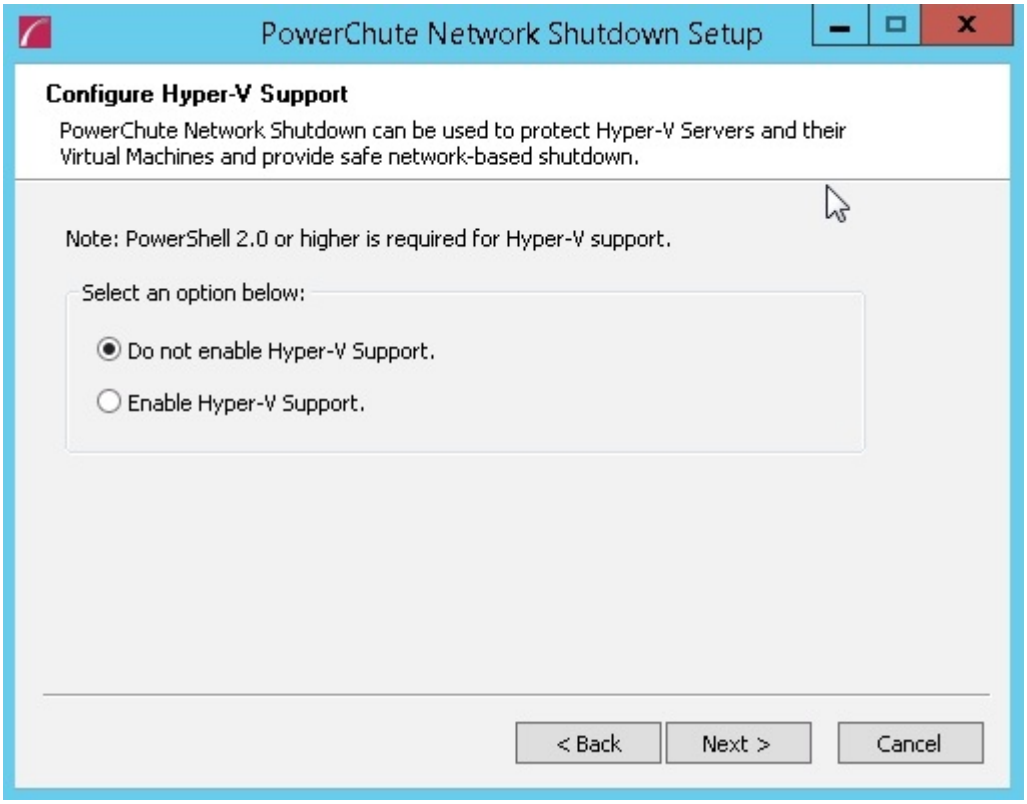
3. At the welcome dialog, click on **Next** to continue.

   At the License Agreement dialog, if you agree with the terms, click **I Agree** to continue.
4. PowerChute includes a private Java Runtime Environment (JRE) that is bundled with the software. In this step, PowerChute installs this bundled JRE on your Windows operating system.

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



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

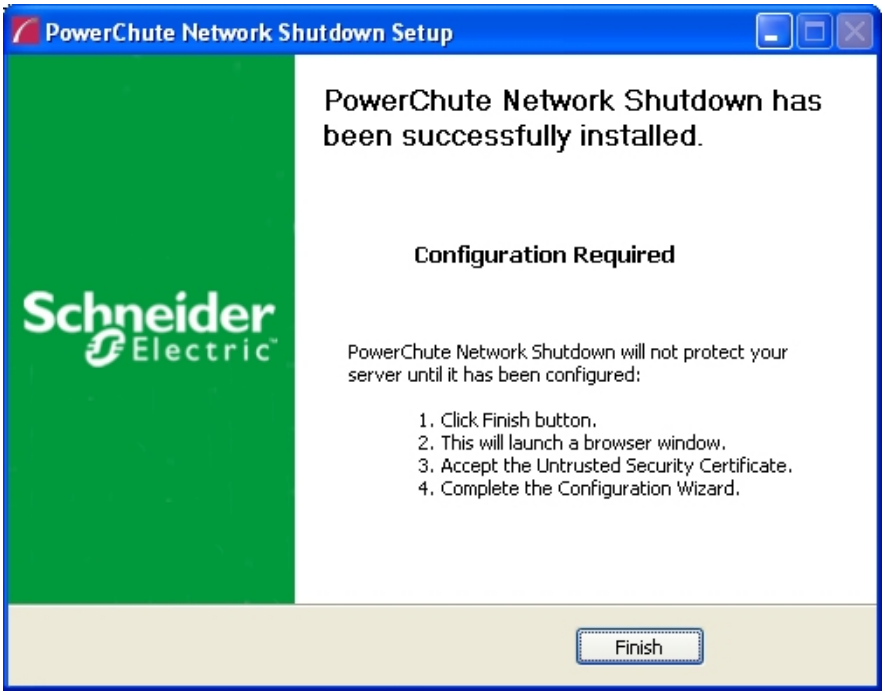
   Do not copy unsigned DLLS, .jar files, executable files, or any files from an untrusted source to the PowerChute installation folder.

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

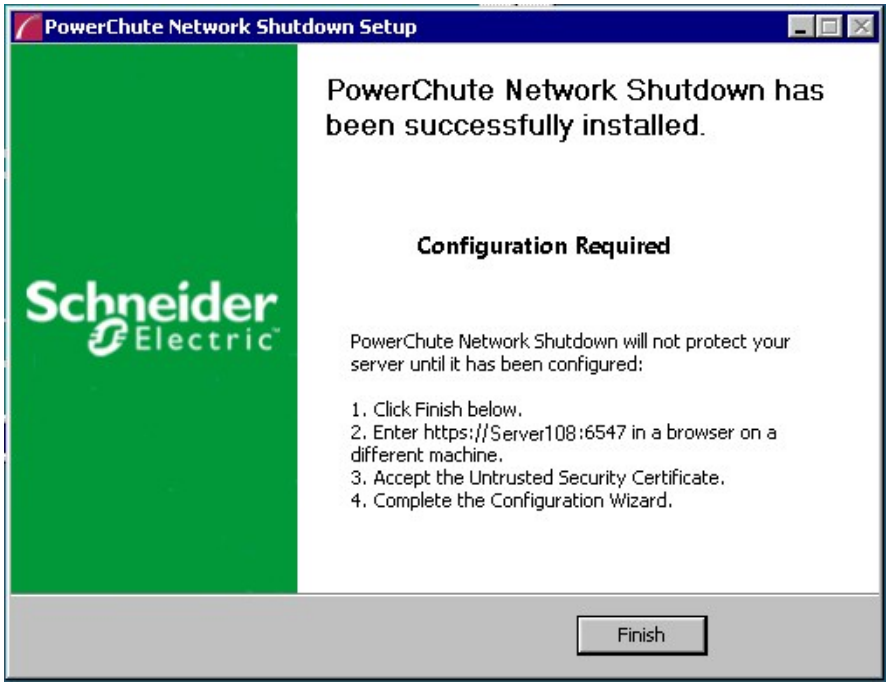
   ```
   PowerChute Network Shutdown ports must be opened in the Windows
   Firewall to enable communication with the Network Management
   Card(s). Would you like this configuration to be performed
   automatically?
   ```

   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 v4.2 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 v4.4.

It is not necessary to run the PowerChute Setup wizard after the upgrade.

PowerChute v4.3+ is a 64-bit only application and cannot be installed on a 32-bit operating system. If you have a 32-bit operating system, you cannot upgrade to v4.3+.

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

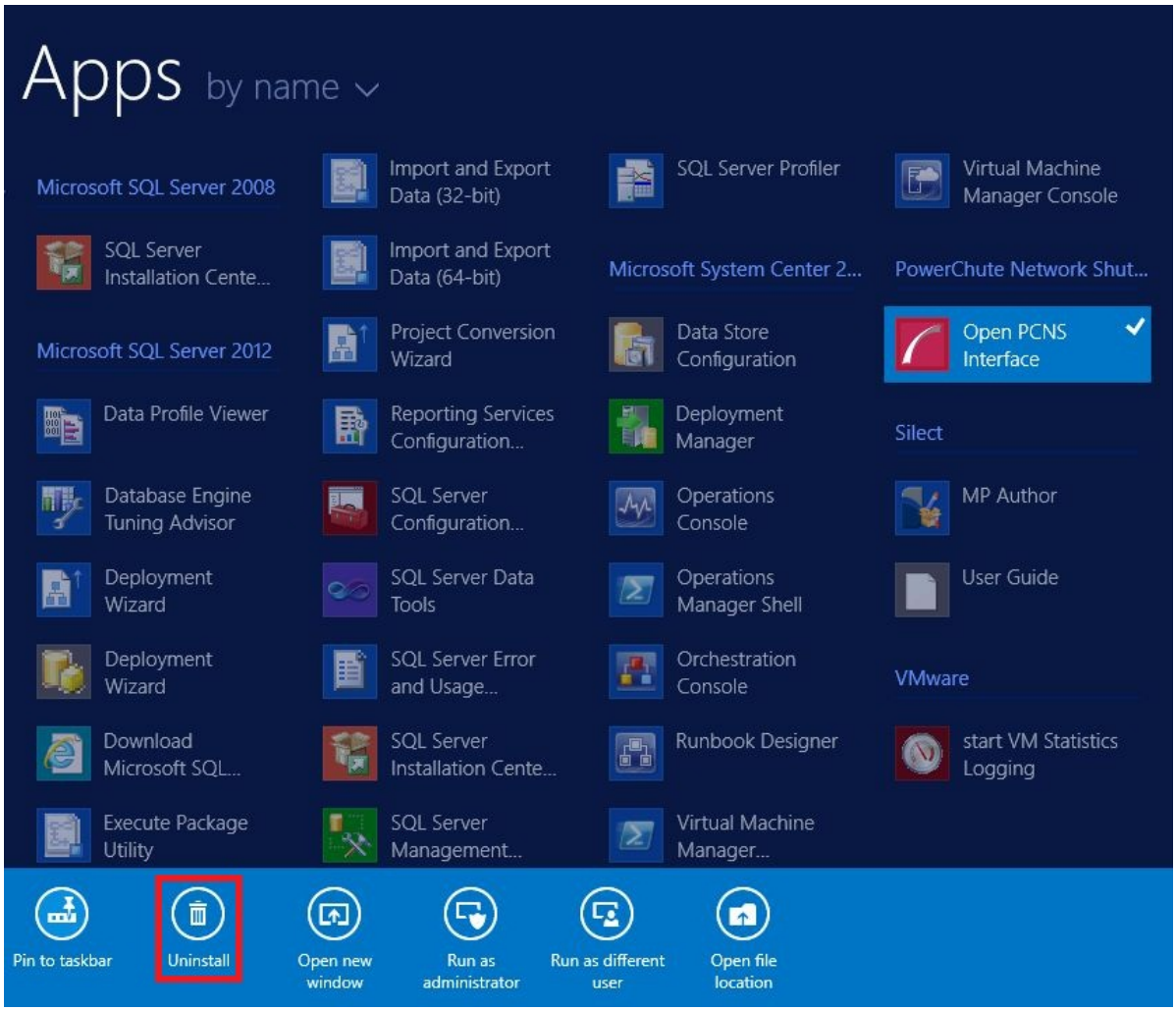
On Windows, use the **Uninstall** option under **PowerChute Network Shutdown** in the Windows Start menu.

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, 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 is unsuccessful, 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, ä, in the installation path.
ACCEPT_EULA=yes	Yes signifies acceptance of the software license agreement. The installation will not proceed unless yes is specified here.
*INSTALL_JAVA= System | PCNS	The value `System` here signifies you want to use the public JRE for your PowerChute installation. The value `PCNS` 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=	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.
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 acceptable characters for username and password are: • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: _ ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ ^ ` { | } [ ] ~ The password requires: • Minimum 8 and maximum 128 characters in length • One upper and one lower case letter • One number and special character • The username also cannot be part of the password The username must be between 1–10 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.
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: • 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 "*SNMP Troubleshooting*" topic of the *PowerChute Network Shutdown User Guide* 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: • 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

You must have root privileges to perform the installation.

1. Download the `pcns440Linux.tar.gz` file from the APC website, extract the file, and copy it to a temporary directory on your server.
   Change your working directory to the temporary directory. Then type the following commands:
   ```
   gunzip pcns440Linux.tar.gz
   tar -xf pcns440Linux.tar
   ```
2. 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
   ```

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).

   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`.

   Do not copy unsigned .jar files, executable files, or any files from an untrusted source to the PowerChute installation folder.

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 v4.2 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.

It is not necessary to run the PowerChute Setup wizard after an upgrade.

PowerChute v4.3+ is a 64-bit only application and cannot be installed on a 32-bit operating system. If you have a 32-bit operating system, you cannot upgrade to v4.3+.

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.

Perform the following steps:

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 is unsuccessful, 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. `/usr/local/bin/jre/jre1.X.X_XX`. If this value is blank or absent, the private JRE is installed.
ACCEPT_EULA=yes	Yes signifies acceptance of the software license 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=	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.
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 acceptable characters for username and password are: • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: _ ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ ^ ` { | } [ ] ~ The password requires: • Minimum 8 and maximum 128 characters in length • One upper and one lower case letter • One number and special character • The username also cannot be part of the password The username must be between 1–10 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.
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: • 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 "*SNMP Troubleshooting*" topic of the *PowerChute Network Shutdown User Guide* 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: • 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

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

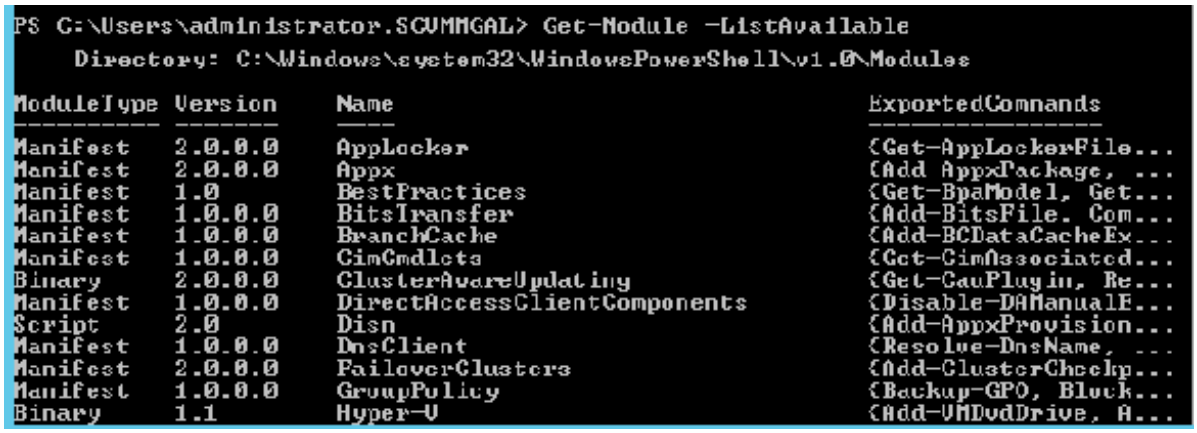
The Hyper-V server can be part of a Windows failover cluster or a standalone host. If it is part of a cluster, then PowerChute can perform a migration of the virtual machines to any available Hyper-V hosts in the same cluster during a shutdown.

Remote Server Administration Tools

The Remote Server Administration Tools must be installed for Hyper-V and Failover Clustering. 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:



Installing on Windows Hyper-V/SCVMM

Follow these steps below.

1. Download the PowerChute installation executable file, **Setup-x64.exe**, from the APC website. You must have administrator rights to run the installer.
   Extract the file, and double-click on the 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.

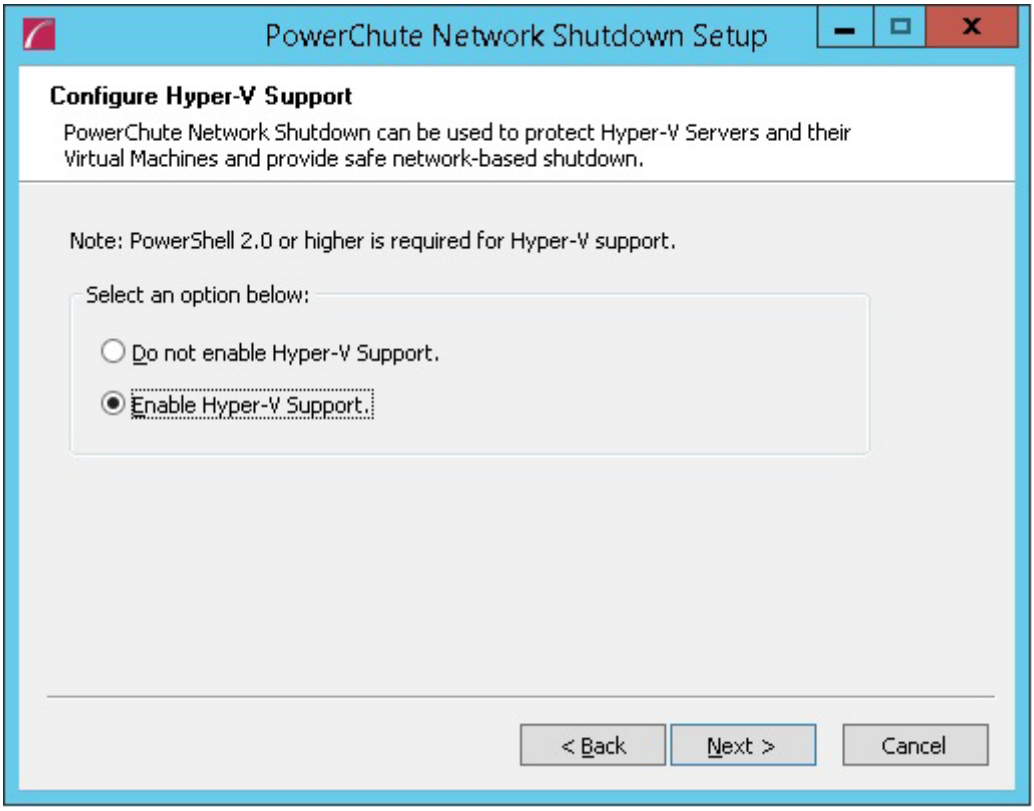
   At the License Agreement dialog, if you agree with the terms, click **I Agree** to continue.

   Enter an installation folder location or accept the default.

   Do not copy unsigned DLLS, .jar files, executable files, or any files from an untrusted source to the PowerChute installation folder.

4. PowerChute includes a private Java Runtime Environment (JRE) that is bundled with the software. In this step, PowerChute installs this bundled JRE on your operating system.

5. 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 within the cluster.

   b. PowerChute must be installed on a physical machine.

   Click **OK** to proceed.

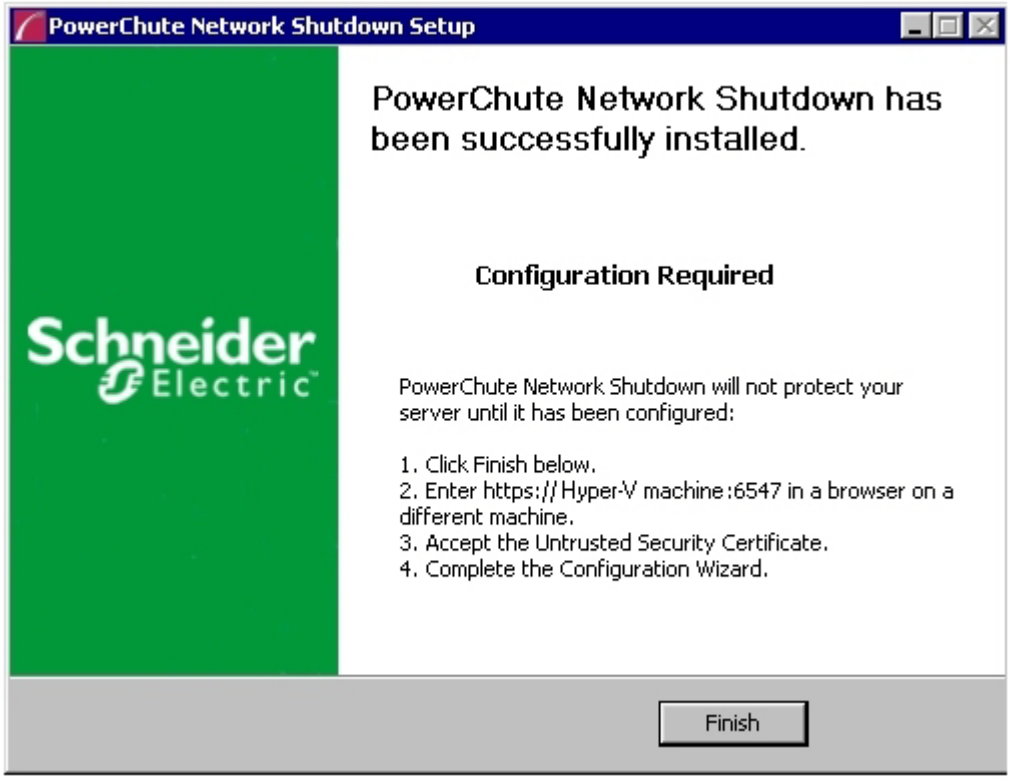
6. When your Windows Firewall is enabled, you can allow the PowerChute installation to configure the firewall automatically by choosing **Yes** when prompted:

   ```
   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?
   ```

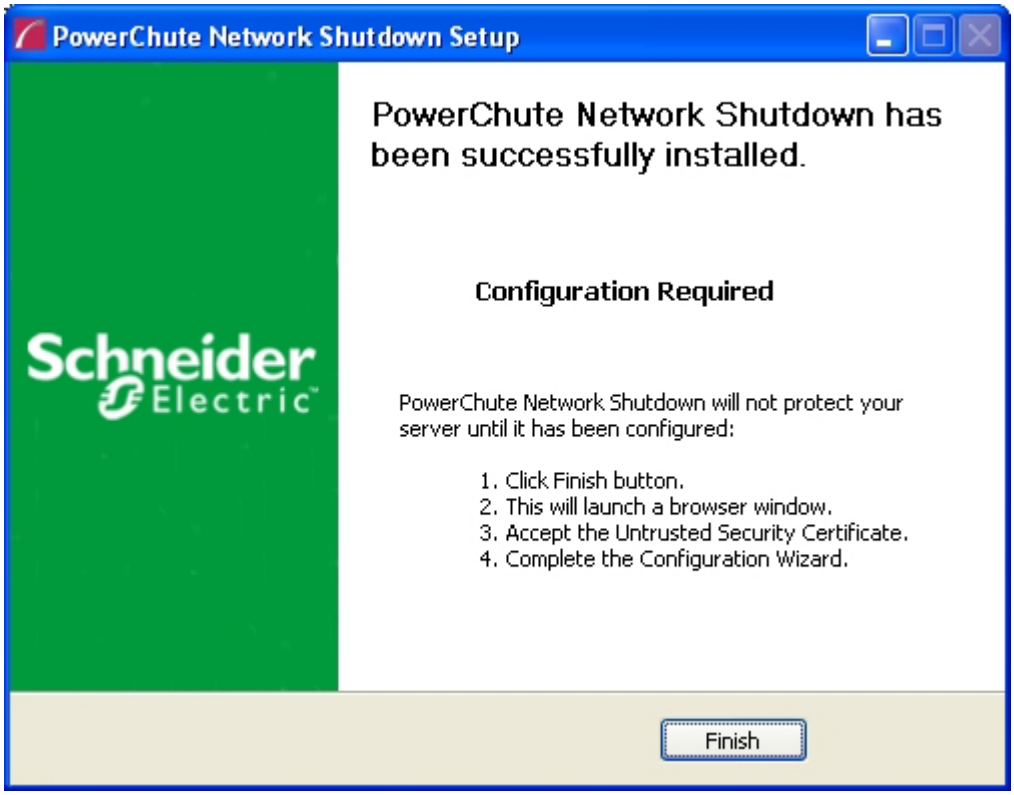
   See Firewall for more information.

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.

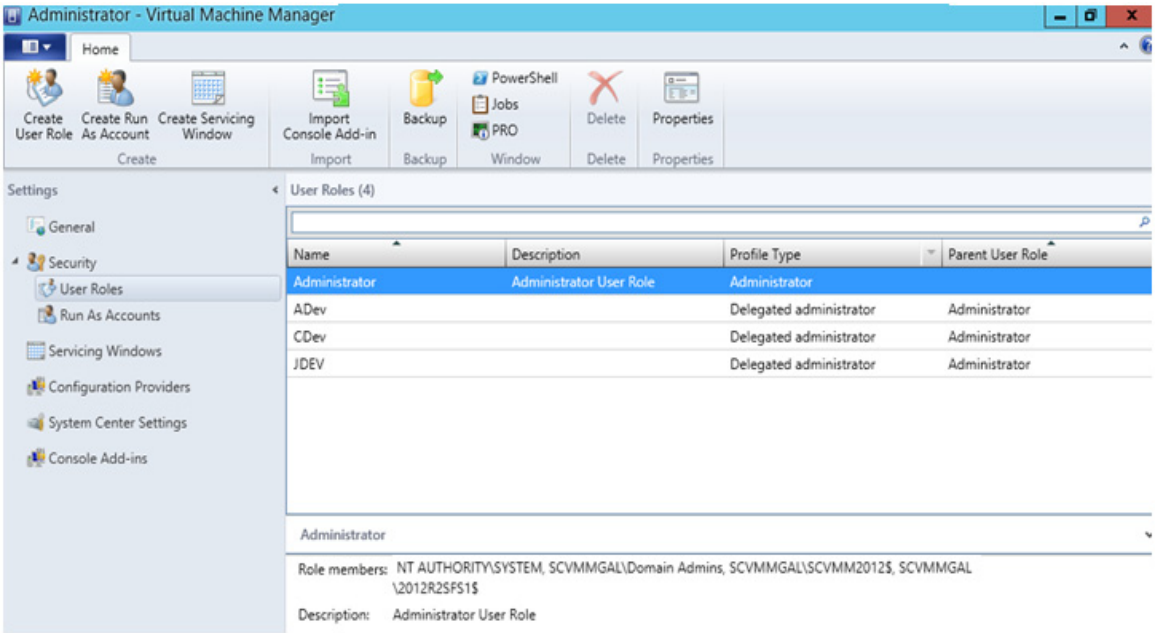
PowerChute can be installed on the same server as SCVMM, or on a remote server.

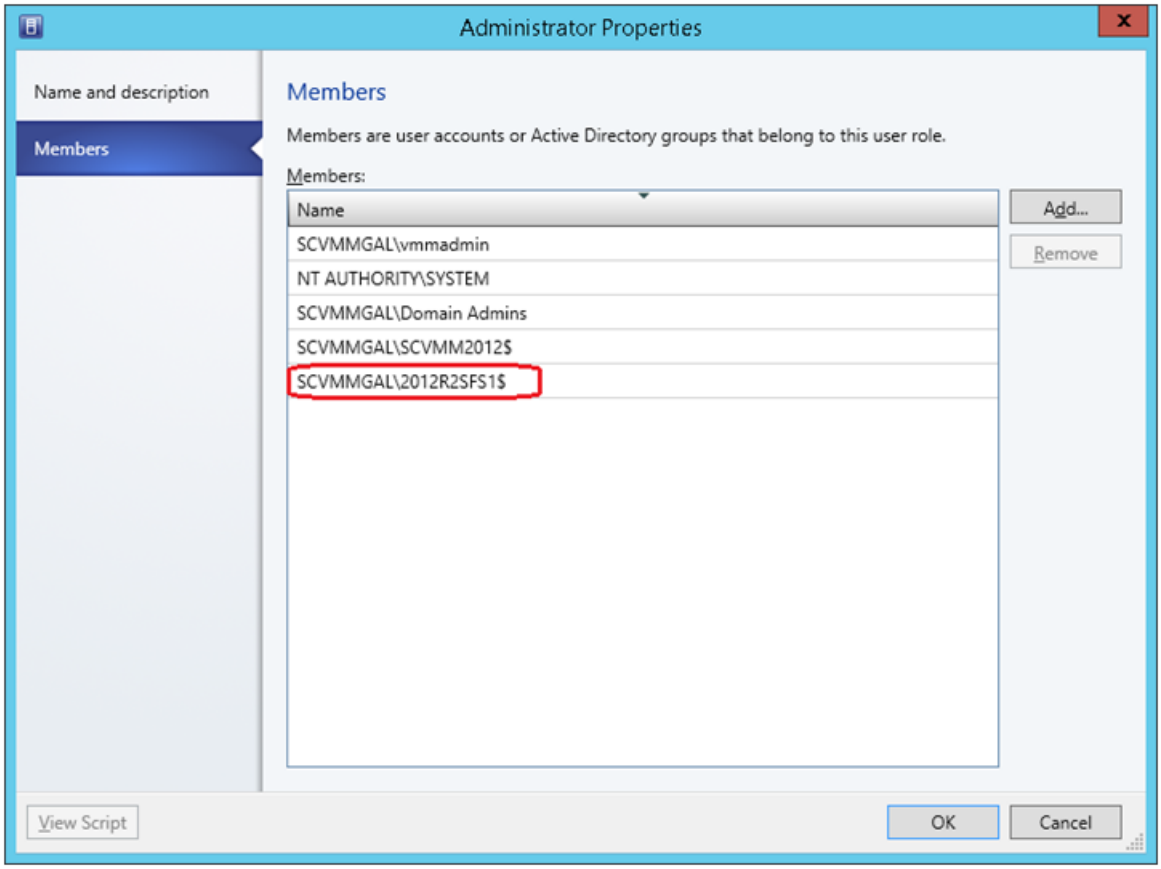
If PowerChute is installed on a remote server:

- 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 v4.2 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.

It is not necessary to run the PowerChute Setup wizard after an upgrade.

PowerChute v4.3+ is a 64-bit only application and cannot be installed on a 32-bit operating system. If you have a 32-bit operating system, you cannot upgrade to v4.3+.

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

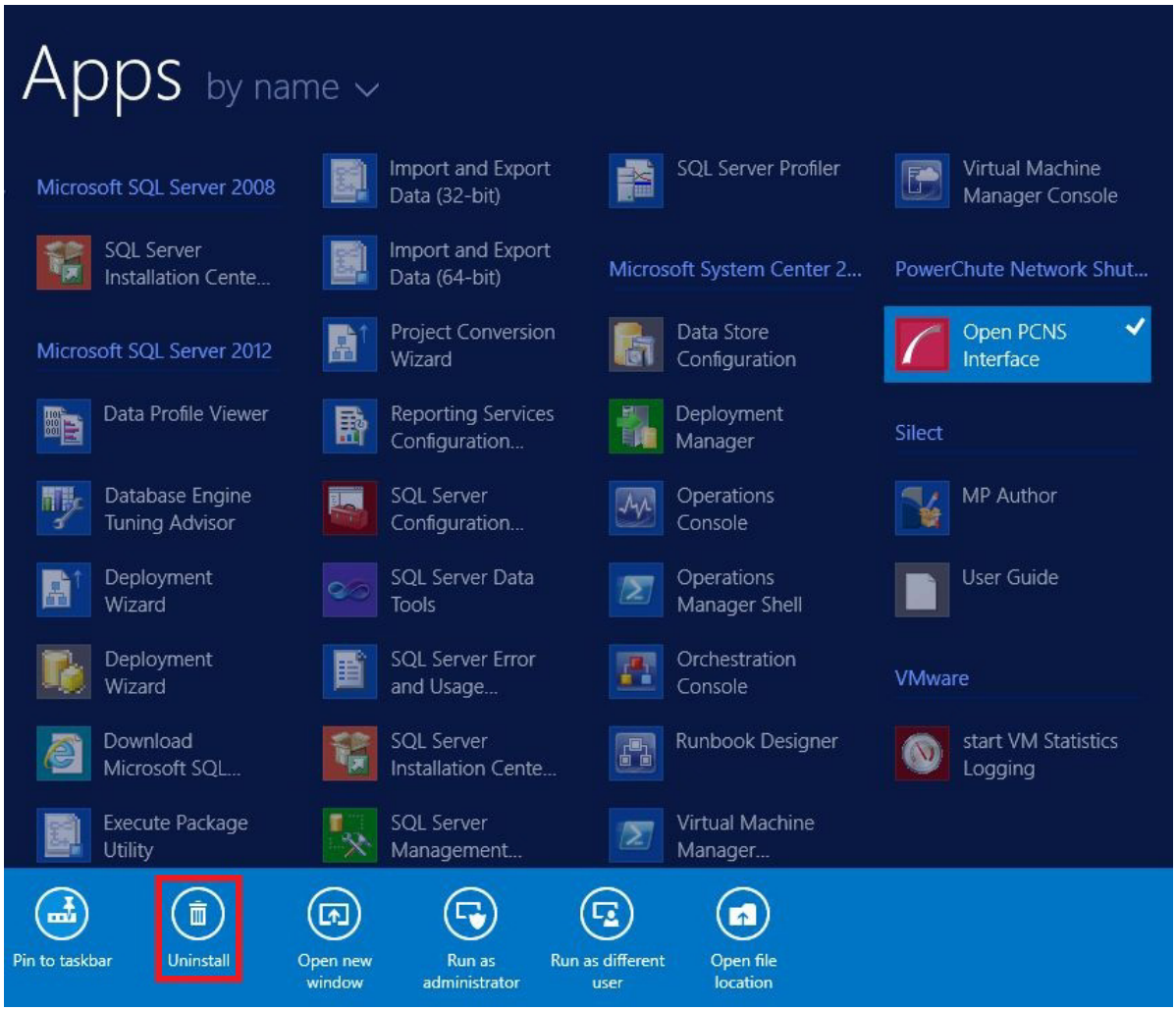
On Windows, use the **Uninstall** option under **PowerChute Network Shutdown** in the Windows Start menu.

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, 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 is unsuccessful, 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, ä, in the installation path.
ACCEPT_EULA=yes	Yes signifies acceptance of the software license agreement. The installation will not proceed unless yes is specified here.
*INSTALL_JAVA= System | PCNS	The value `System` here signifies you want to use the public JRE for your PowerChute installation. The value `PCNS` 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=	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.
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 acceptable characters for username and password are: • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: `_!\"#$%&'()*+,-./:;<=>?@^`{|}[]~` The password requires: • Minimum 8 and maximum 128 characters in length • One upper and one lower case letter • One number and special character • The username also cannot be part of the password The username must be between 1–10 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.
VIRTUALINSTALL= VMware | Hyper-V	Specify `Hyper-V` to enable the Hyper-V/SCVMM virtualization features.
CONFIGURATION_MODE = Managed |Unmanaged	Specify `Managed` for configurations managed by SCVMM. Specify `Unmanaged` 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.

Field name	Description
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: • 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 "*SNMP Troubleshooting*" topic of the *PowerChute Network Shutdown User Guide* 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: • 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.

Field name	Description
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

VMware

Installing PowerChute Network Shutdown with VMware Support

You have two 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

See also Hyperconverged Infrastructure Support, 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 or Deploy one PowerChute virtual appliance per cluster
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 same physical machine as vCenter Server
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 virtual appliance or PowerChute installed on a physical Windows machine

We recommend the following in a **vSAN environment**:

The below recommendations are also applicable to a vSAN environment, e.g. Dell VxRail.

VMware Setup	Recommended Deployment/ Installation of PowerChute
VMware Hosts in multiple clusters	PowerChute installed on a physical Windows machine or PowerChute installed on a Host outside of the cluster or PowerChute virtual appliance *
VMware hosts in one cluster for Single, Redundant or Parallel UPS configurations	PowerChute installed on a physical Windows machine or PowerChute installed on a Host outside of the cluster or PowerChute virtual appliance *
VMware hosts managed by vCenter Server which is running on a physical machine	PowerChute installed on same physical machine as vCenter Server or PowerChute installed on a Host outside of the cluster or PowerChute virtual appliance *
Using vCenter Server running on a VM or vCenter Server Virtual Appliance (VCSA) for Single, Redundant or Parallel UPS configurations	PowerChute installed on a physical Windows machine or PowerChute installed on a Host outside of the cluster or PowerChute virtual appliance *
Advanced UPS configuration, see graphic below. See application notes for background information.	PowerChute virtual appliance or PowerChute installed on a physical Windows machine
vSAN Stretched Cluster	PowerChute virtual appliance deployed on Host outside the cluster that is running the Witness Appliance or PowerChute installed on a physical machine

* If the PowerChute virtual appliance is deployed to a vSAN host, the **Skip Maintenance Mode** checkbox in the PowerChute UI must be selected. In a Dell VxRail environment, the virtual appliance must be deployed to cluster storage; it cannot be deployed to local storage.

We recommend the following in a **Nutanix environment**:

VMware Setup	Recommended Deployment/ Installation of PowerChute
VMware hosts in one cluster for Single, Redundant or Parallel UPS configurations	PowerChute installed on a physical Windows machine
VMware hosts managed by vCenter Server which is running on a physical machine	PowerChute installed on same physical machine as vCenter Server
Using vCenter Server running on a VM or vCenter Server Virtual Appliance (VCSA) for Single, Redundant or Parallel UPS configurations	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

We recommend the following in an **HPE SimpliVity environment**:

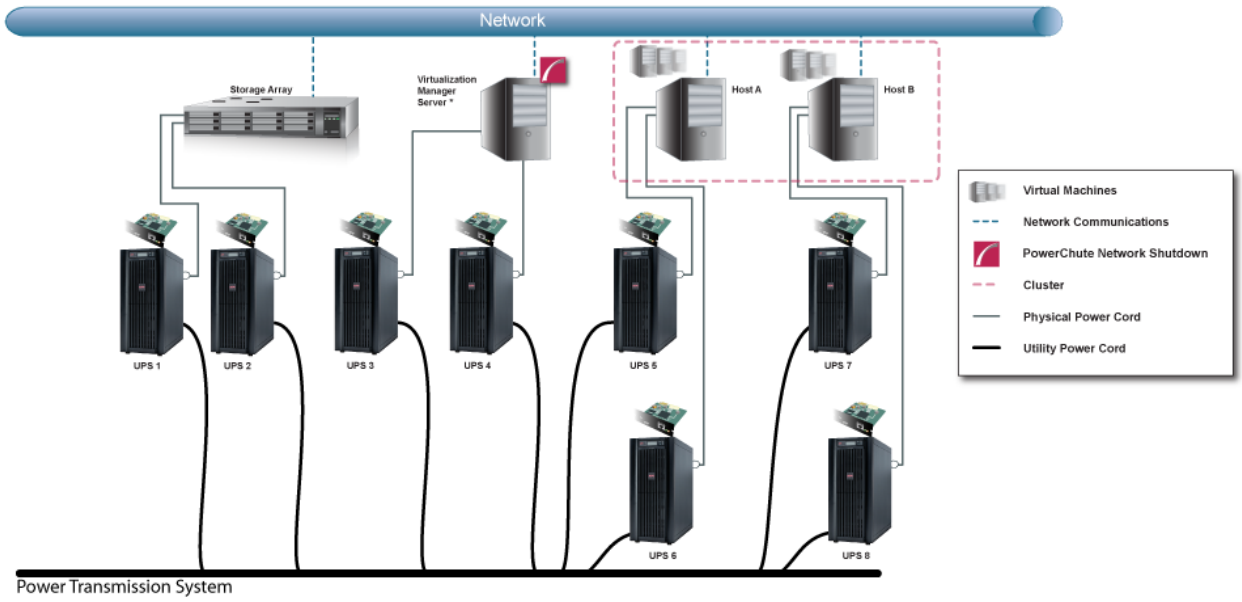
VMware Setup	Recommended Deployment/ Installation of PowerChute
VMware Hosts in multiple clusters	PowerChute installed on a physical Windows machine or PowerChute virtual appliance with one instance of PowerChute per cluster
VMware hosts in one cluster for Single, Redundant or Parallel UPS configurations	PowerChute installed on a physical Windows machine or PowerChute virtual appliance deployed on local datastore on a node in the cluster
VMware hosts managed by vCenter Server which is running on a physical machine	PowerChute installed on same physical machine as vCenter Server or PowerChute virtual appliance deployed on local datastore on a node in the cluster
Using vCenter Server running on a VM or vCenter Server Virtual Appliance (VCSA) for Single, Redundant or Parallel UPS configurations	PowerChute installed on a physical Windows machine or PowerChute virtual appliance deployed on local datastore on a node in the cluster
Advanced UPS configuration, see graphic below. See application notes for background information.	PowerChute installed on a physical Windows machine with HPE SimpliVity Arbiter or PowerChute virtual appliance deployed on local datastore

We recommend the following in a **HyperFlex environment**:

VMware Setup	Recommended Deployment/ Installation of PowerChute
VMware Hosts in multiple clusters	PowerChute installed on a physical Windows machine or PowerChute virtual appliance with one instance of PowerChute per cluster
VMware hosts in one cluster for Single, Redundant or Parallel UPS configurations	PowerChute installed on a physical Windows machine or PowerChute virtual appliance deployed on local datastore on a node in the cluster *
VMware hosts managed by vCenter Server which is running on a physical machine	PowerChute installed on a physical Windows machine or PowerChute virtual appliance deployed on local datastore on a node in the cluster *
Using vCenter Server running on a VM or vCenter Server Virtual Appliance (VCSA) for Single, Redundant or Parallel UPS configurations	PowerChute installed on a physical Windows machine or PowerChute virtual appliance deployed on local datastore on a node in the cluster *
Advanced UPS configuration, see graphic below. See application notes for background information.	PowerChute installed on a physical Windows machine or PowerChute virtual appliance deployed on local datastore *

* If the PowerChute virtual appliance is deployed to local datastore, the virtual appliance must be powered off before attempting to upgrade the HyperFlex Cluster. If the appliance is not powered off, the upgrade will be blocked while waiting for the host to enter 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.

These steps are also applicable for installing PowerChute in a vSAN or Dell VxRail environment.

1. Download the PowerChute installation executable file for Windows, **Setup-x64.exe**, from the APC website. You must have administrator rights to run the installer.
   Extract the file, and double-click on the file.
2. A warning dialog, below, displays if you downloaded the exe from the web:
   click the **Run** button.

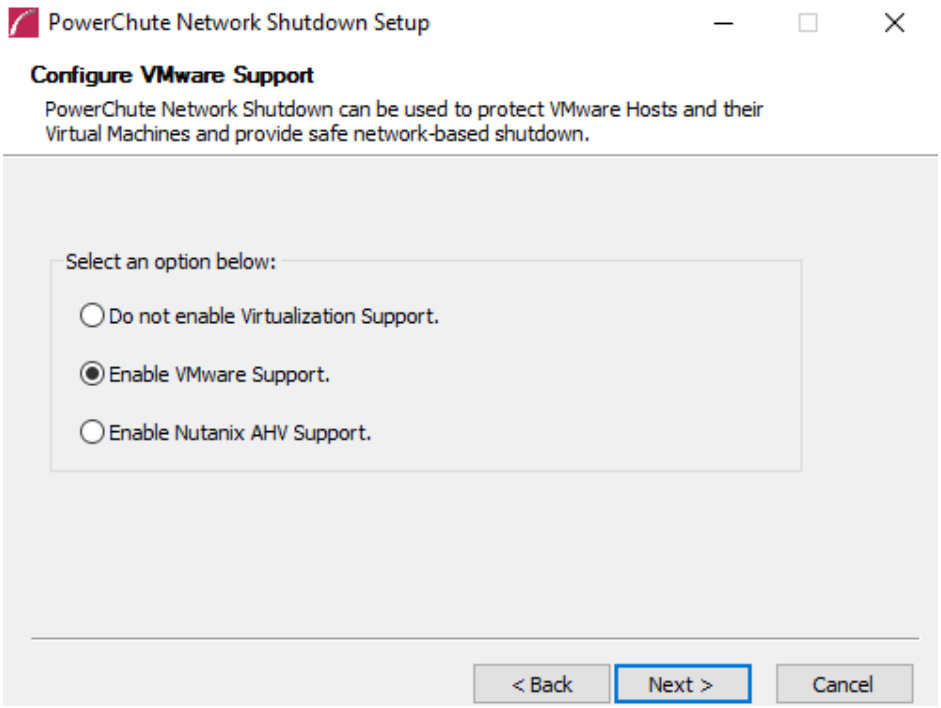
3. At the welcome dialog, click on **Next** to continue.

   At the License Agreement dialog, if you agree with the terms, click **I Agree** to continue.
4. PowerChute includes a private Java Runtime Environment (JRE) that is bundled with the software. In this step, PowerChute installs this bundled JRE on your operating system.

5. 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.



6. Enter an installation folder location or accept the default and your installation proceeds.

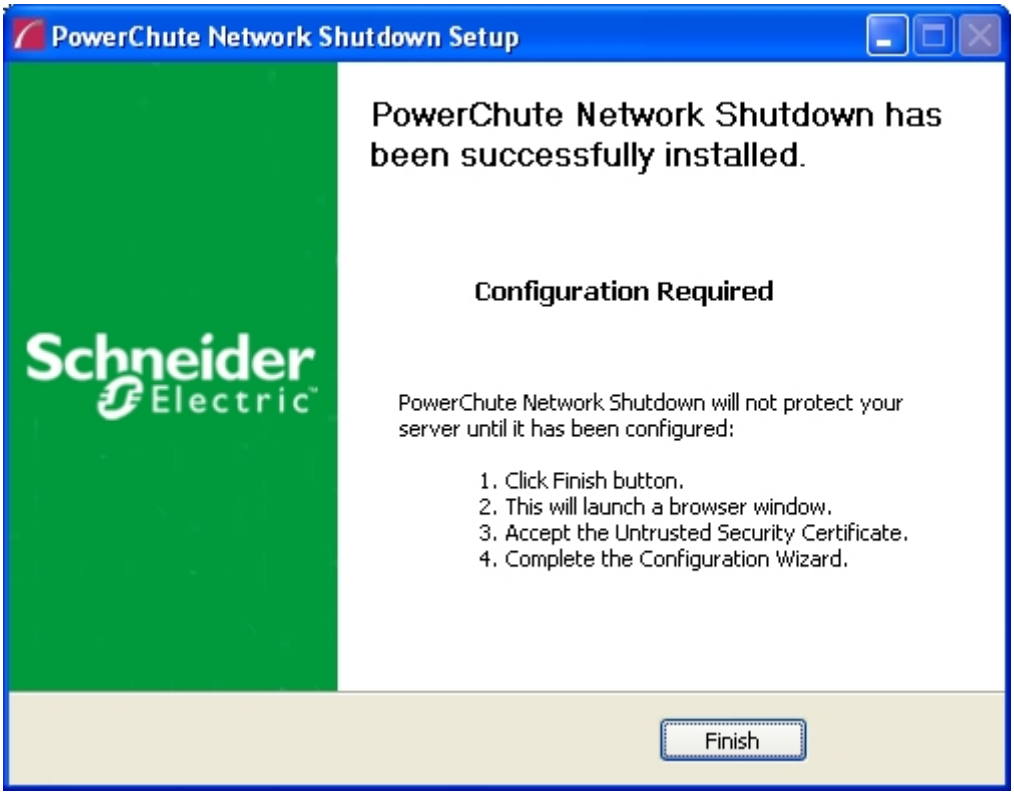
   Do not copy unsigned DLLS, .jar files, executable files, or any files from an untrusted source to the PowerChute installation folder.

7. 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.



In the **vCenter Server Details** screen in the PowerChute Setup wizard, the username specified to connect to ESXi hosts must be in lowercase.

Deploying the PowerChute Virtual Appliance

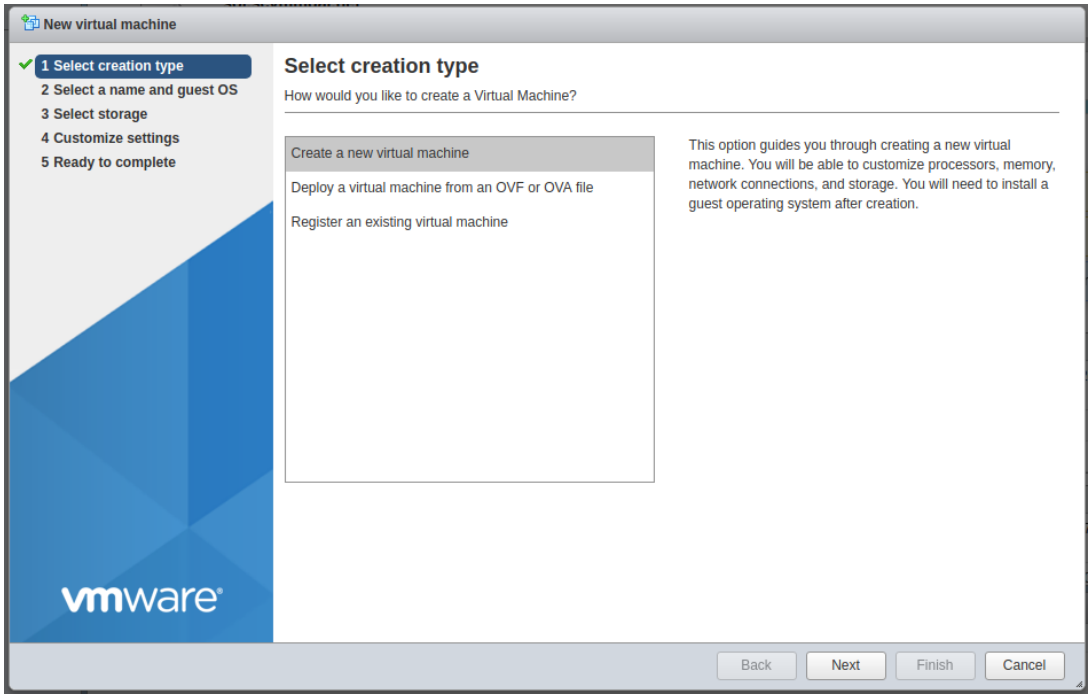
The PowerChute Virtual Appliance is a virtual machine image with CentOS Linux 8.1 running PowerChute Network Shutdown v4.4 pre-installed.

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

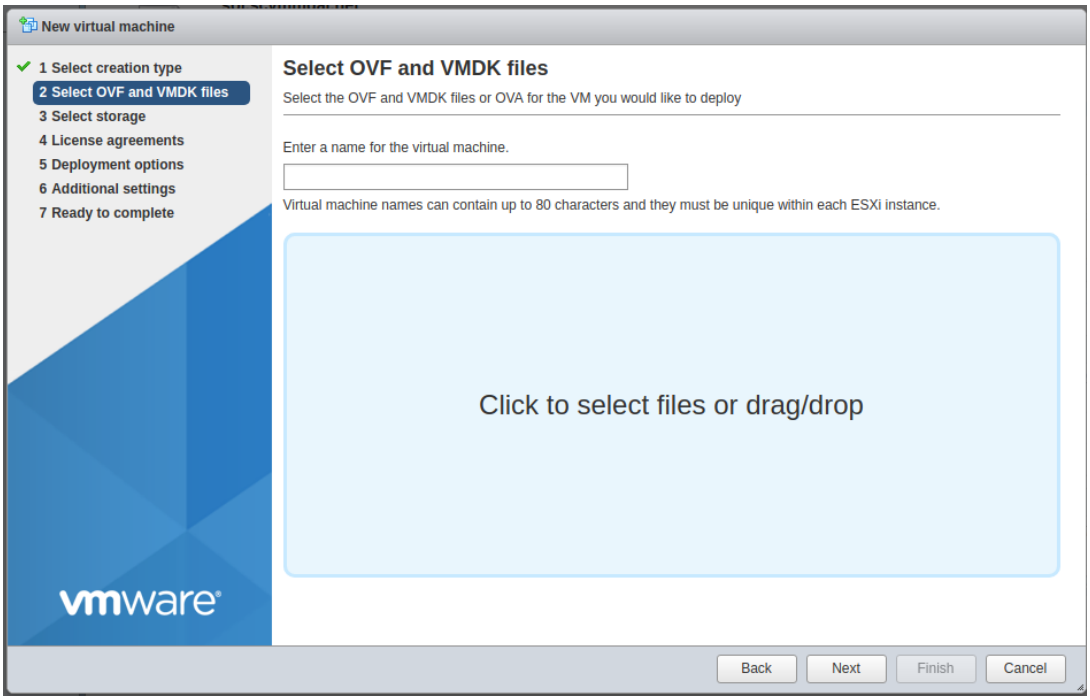
To deploy the virtual appliance using the vSphere Web client:

The screens shown below (vSphere Web Client v6.5) may differ from the version of vSphere you are using. Consult the vSphere documentation for more information.

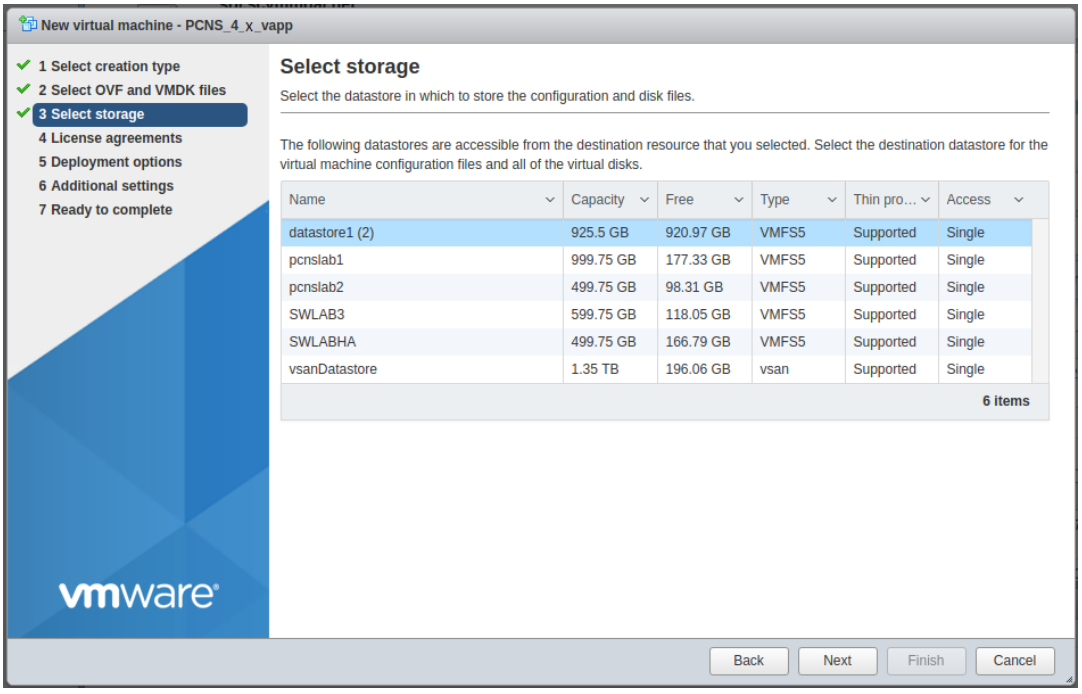
1. Download the PowerChute virtual appliance file from the APC website.
2. Log on to the VMware host using your vSphere Web Client.
3. On the Host view, select **Create/Register VM**.
4. In Step 1 of the **New virtual machine** wizard, select the **Deploy a virtual machine from an OVF or OVA file** option, and click Next.



5. Insert a name into the **Enter a name for the virtual machine field** and select the OVF file you extracted in Step 1.

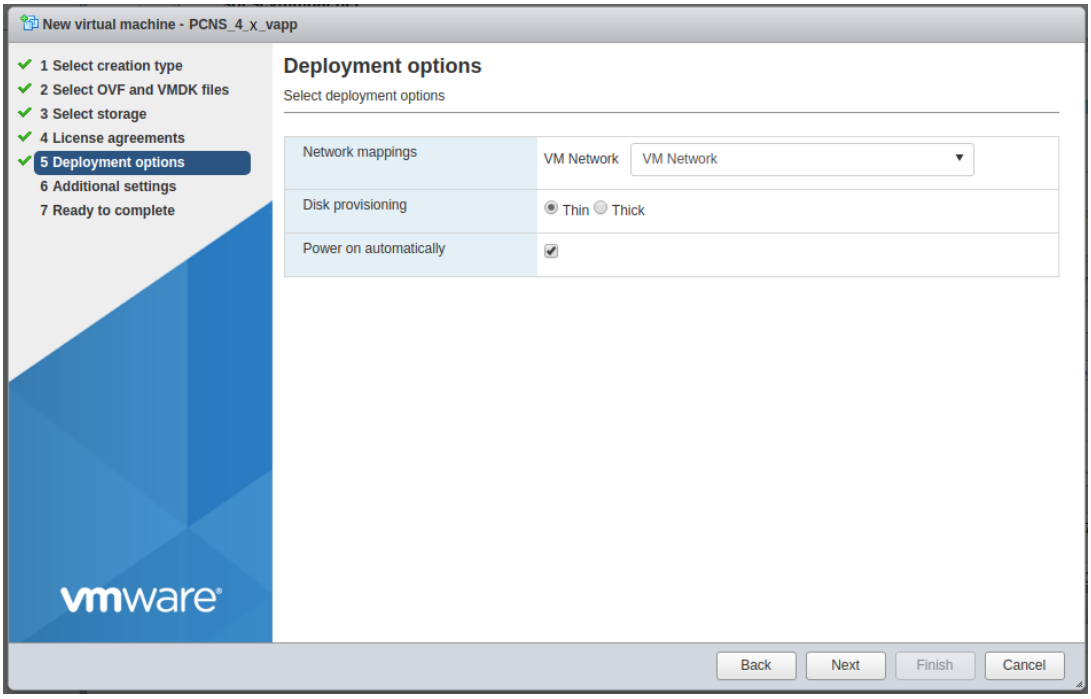


6. Select a configured datastore on your system that has sufficient disk space to deploy the virtual appliance, and click Next.

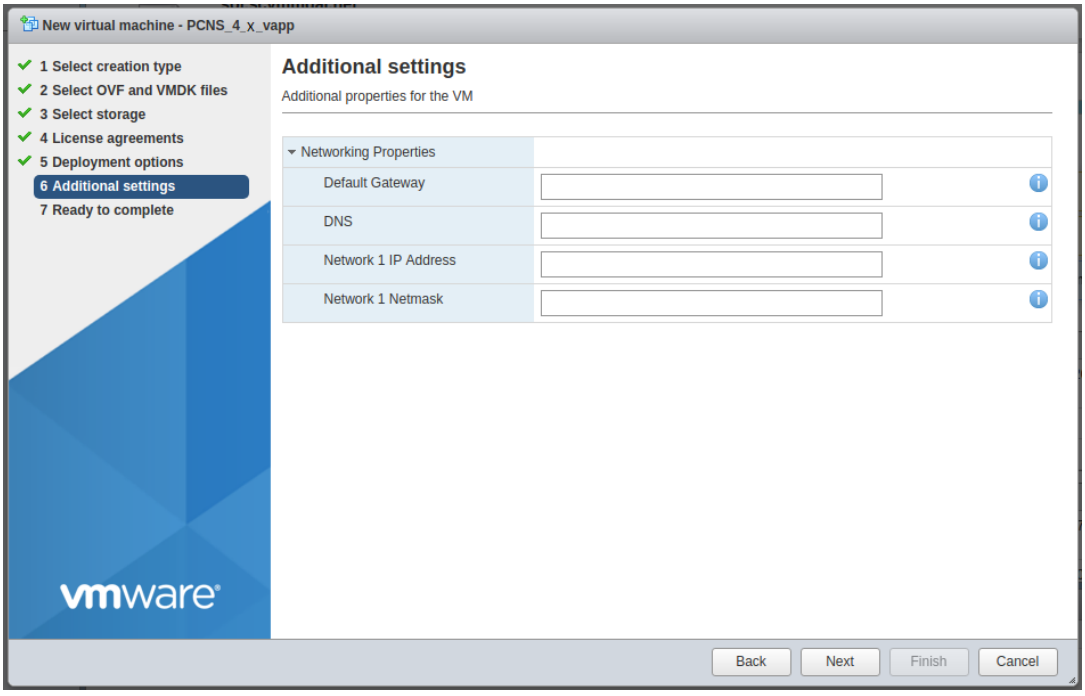


7. When the End User License Agreement (EULA) is displayed, click **I agree** and then Next.

8. Review your deployment options. Select **Network mappings**, **Disk provisioning**, and **Power on automatically** as required, and click Next.



9. This step is not relevant when you are deploying to a standalone host. Any settings made here are ignored.

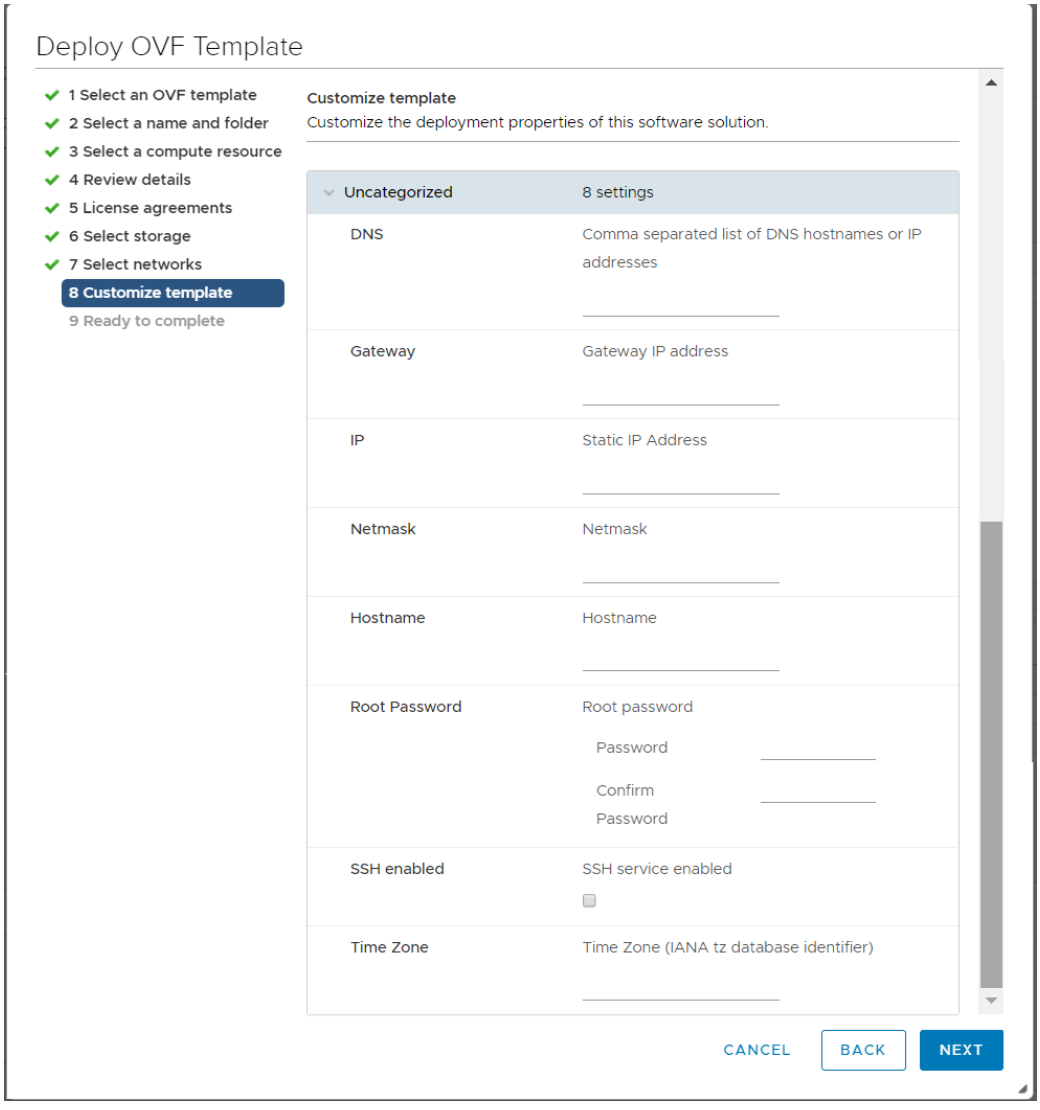


NOTE: To configure a static IP address when deploying to a standalone host, use the Network configuration menu displayed at first boot of the appliance - see Step 14.

10. You can specify certain settings for the virtual appliance before deployment if the virtual appliance is deployed via the vCenter UI:

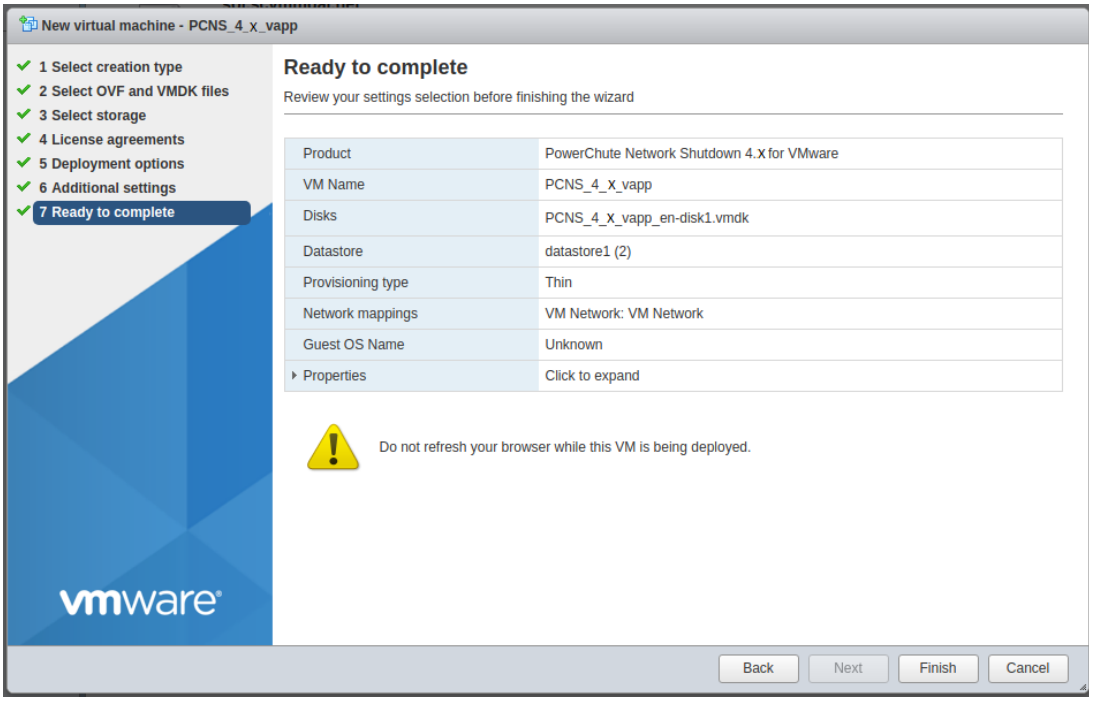
    - **DNS:** The DNS server hostnames or IP addresses, separated by commas.
    - **Gateway:** The gateway IP address.
    - **IP:** The virtual appliance's static IP address.
    - **Netmask:** The virtual appliance's netmask, for example: 255.255.255.0
    - **Hostname:** The virtual appliance's hostname.
    - **Root Password:** The password for the root user.

      Configuring the root password before deployment may expose the virtual appliance to VMware vulnerabilities.
      IMPORTANT: Before configuration and deployment of the PowerChute virtual appliance, **review VMware Security Advisory 0013.1 3c and 3d and update vSphere and vCenter accordingly**.
      If you are using an affected vCenter/vSphere version, it is recommended to change the root password **after** the virtual appliance has deployed - see Step 14.
    - **SSH enabled:** Select this checkbox to enable SSH on the virtual appliance. **NOTE:** Ensure that SSH access to the appliance is disabled, unless it is needed to gather log files or for the purposes of scripting the deployment of the appliance.
    - **Time Zone:** The time zone of the virtual appliance. This value must be in IANA tz database format, e.g. "Europe/Dublin".



NOTE: This screenshot is from vSphere Web Client 6.7.

11. The options you have chosen are displayed, verify them and click Finish to commence the installation. The time taken to deploy the virtual appliance depends on your network speed.



12. When the installation has successfully completed, the PowerChute Network Shutdown Virtual Appliance displayed as a virtual machine in your inventory.

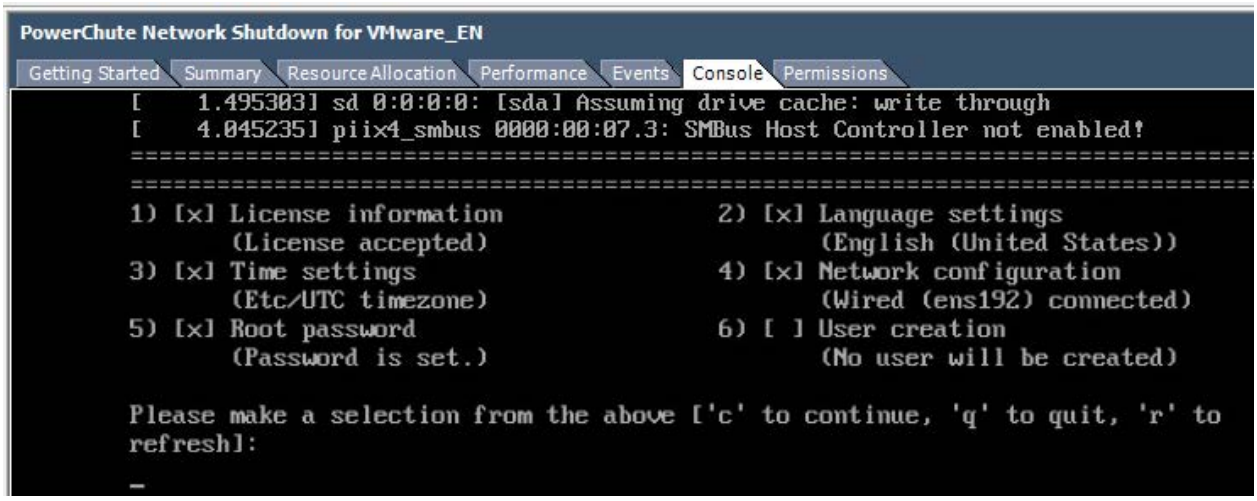
13. Power on your PowerChute virtual machine.

If the root password, time zone, etc. were provided in Step 10, Step 14 below is not required.

14. On first launch of the appliance, the Virtual Appliance First-Time Configuration Wizard opens. Select the option to create a password for the root user.
NOTE: There is no default password for the root user. You must provide a root password during the CentOS initial setup, or at first log in.

The CentOS end user license agreement is automatically accepted during the virtual appliance deployment.

NOTE: When using the first-time configuration wizard, navigate between screens by pressing ‘c’ on your keyboard. If you press ‘q’ to quit, your configuration changes will not be applied, and will be discarded.



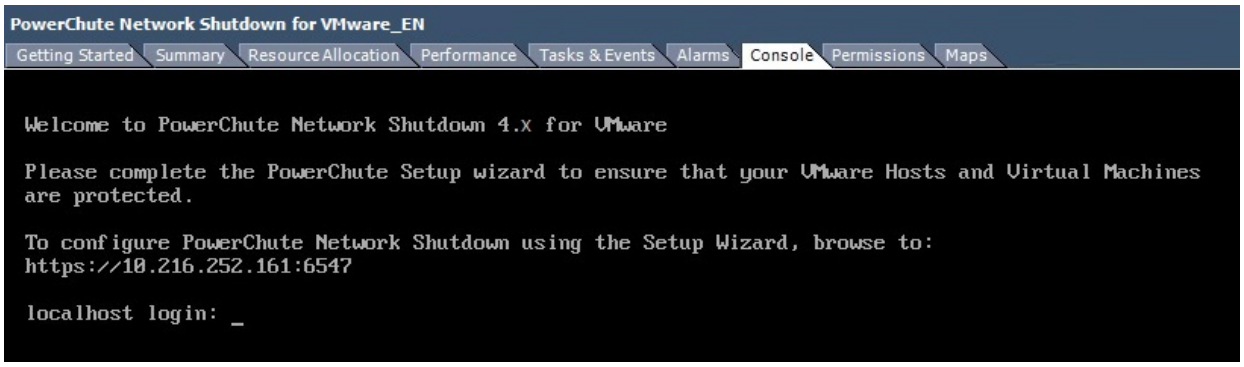
NOTES: If networking properties are not supplied, the first connected network adapter is enabled by default, and a DHCP IP address is allocated by the network.

If multiple network adapters are added to the Virtual Machine, only the first connected adapter is enabled. To enable further network adapters, log in to the Virtual Machine and use standard CentOS network management tools to configure your networking.

OVF Environment settings are persisted across reboots by Network Manager. If OVF Environment Transport is enabled, the OVF Environment settings are applied at each start up.To prevent this, disable OVF Environment Transport.

15. 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:”**.

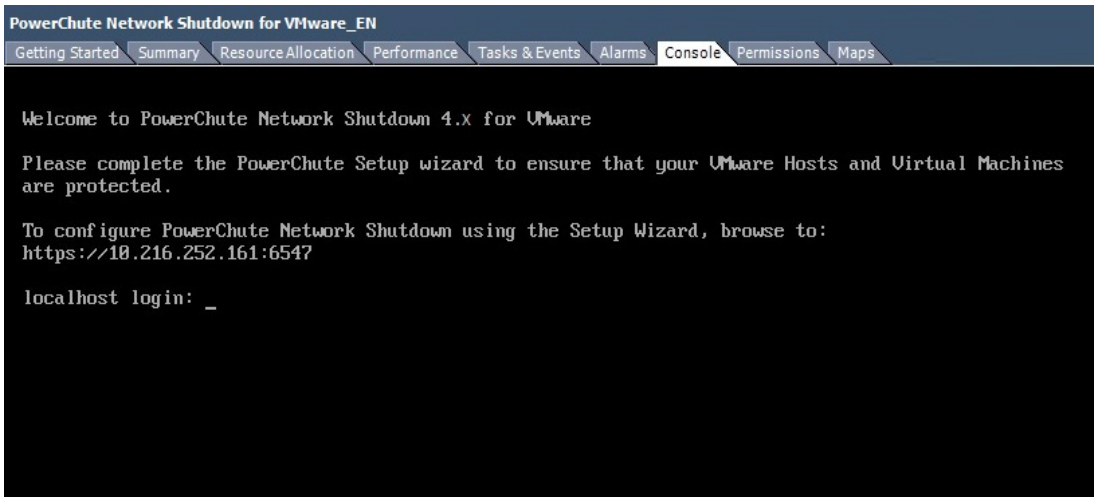


16. Browse to `https://<IP_Address>:6547` to launch the PowerChute Setup wizard.
17. **NOTE:** SNMP is disabled by default in the PowerChute Virtual Appliance.
    Following installation, it is necessary to enable SNMP settings in the web user interface to make PowerChute accessible via SNMP.
    NOTE: To reconfigure for a static IP Address, log in and use the CentOS networking tools.

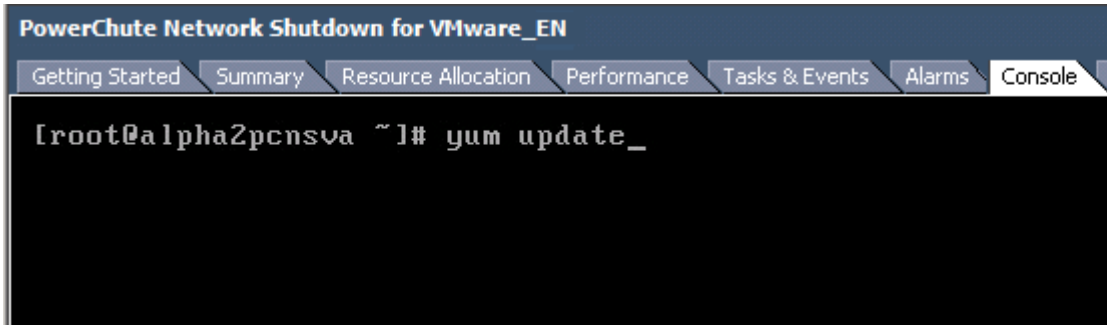
It is strongly recommended to update the CentOS libraries installed on the virtual appliance to obtain the latest security updates.

Howto update the Virtual Appliance libraries:

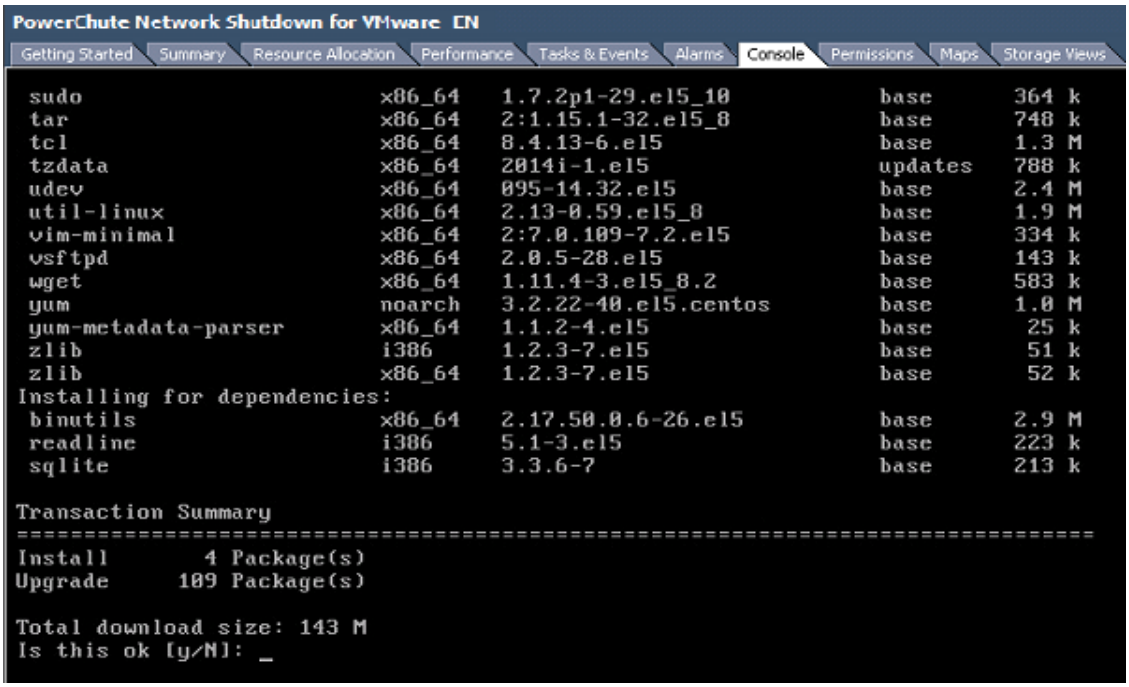
- Log in to the PowerChute virtual appliance



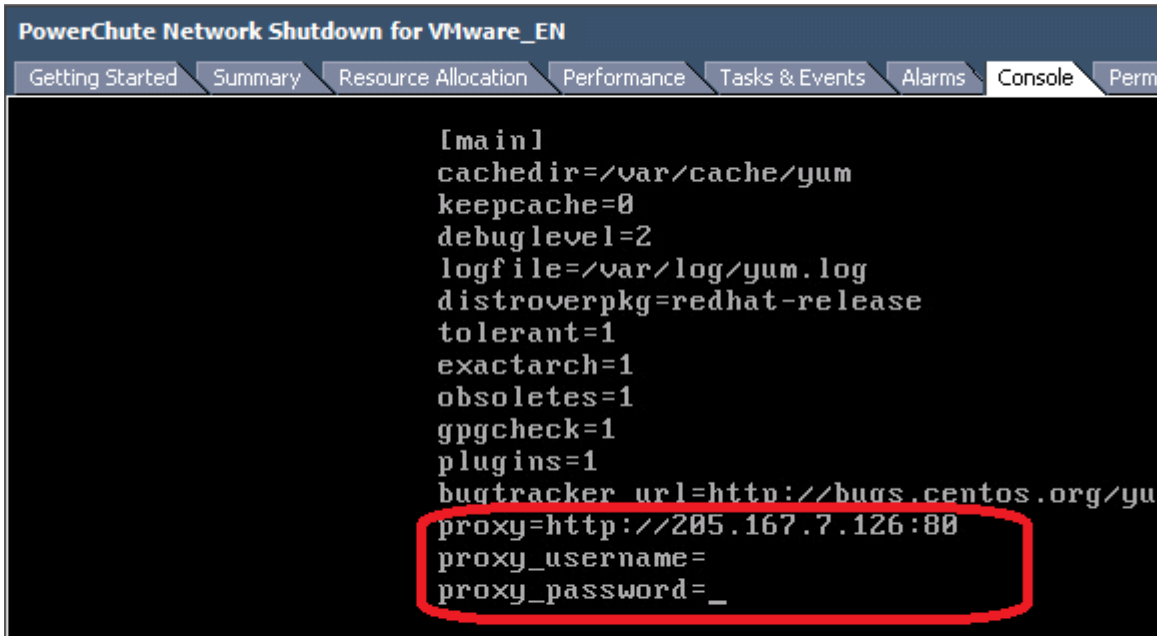
- Run the command **yum update**



- Install the updates



- 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:



Hyperconverged Infrastructure Support

If you have a supported hyperconverged infrastructure support (HCI) solution, you can enable HCI support for VMware in the PowerChute Setup wizard. PowerChute v4.4 supports the following HCI solutions:

- Nutanix
- HPE SimpliVity
- HyperFlex
- vSAN
- Dell VxRail

NOTE: To install PowerChute in a vSAN or Dell VxRail environment, follow the steps outlined in Installing on Windows to Monitor VMware Hosts.

Nutanix Support

PowerChute provides support for shutting down and starting up virtual machines running on a single Nutanix Cluster with ESXi as your hypervisor. PowerChute also supports shutting down and starting up the Nutanix Controller Virtual Machines, Acropolis File (Nutanix File) Services, and the Nutanix Cluster.

NOTES:

- One or more Nutanix blocks are supported. However, all nodes in the blocks must be part of the same Cluster.
- In an advanced configuration, all Hosts in the Cluster must be protected by the same UPS or UPS group.

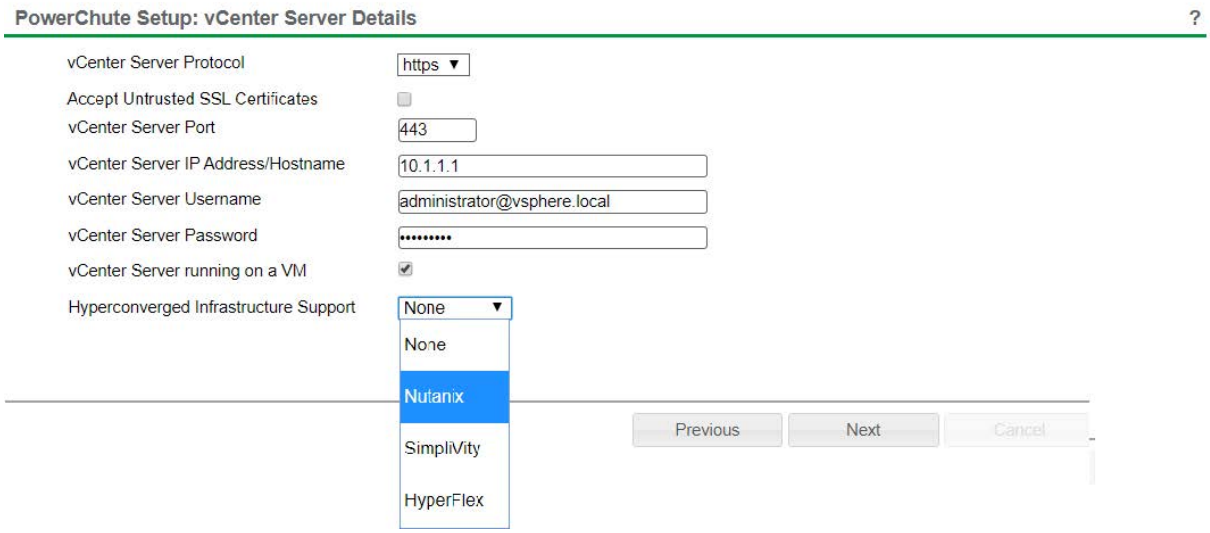
Install PowerChute

PowerChute must be installed on a physical Windows machine outside of the Nutanix Cluster in a Nutanix configuration. Follow the installation steps detailed in Installing on Windows to Monitor VMware Hosts to successfully install PowerChute with VMware support.

Configure Nutanix

When PowerChute is successfully installed, the PowerChute Setup wizard opens automatically after you click the **Finish** button. Follow the steps below to complete your Nutanix configuration:

1. In the **vCenter Server Details** screen, select Nutanix from the **Hyperconverged Infrastructure Support** drop-down list and click **Next**.



The **Accept Untrusted SSL Certificates** checkbox is unselected by default. If left unselected, only SSL certificates signed by a trusted CA will be accepted when connecting to vCenter Server and ESXi hosts. By default, these certificates are self-signed and this will cause a cause connection error. This is for increased security and to prevent man-in-the-middle (MITM) type attacks. Select this checkbox if you want to use untrusted/self-signed SSL certificates to connect to vCenter Server and ESXi hosts.

Alternatively, you can add the vCenter Server root CA certificate to the PowerChute-keystore by following the steps detailed in the vCenter Server Settings topic in the User Guide.

2. Enter your Nutanix connection details in the **CVM/Cluster Details** screen to connect to your Controller Virtual Machine or Cluster and click **Next**. The recommended configuration is to connect to your Nutanix Cluster.

You can authenticate the connection by entering either the Controller VM/Cluster IP address and a password, or a SSH key file. If both authentication options are specified, PowerChute will use the password.

NOTE: You must use the “nutanix” user account credentials to connect to the Controller VM/Cluster. You cannot use Prism user account credentials to connect.

The SSH key file, if configured, must be located in the user_files folder, or a sub-folder, in the PowerChute installation directory. If the default installation directory was chosen during installation, this location will be:

- C:\Program Files\APC\PowerChute\user_files for Windows systems
- /opt/APC/PowerChute/user_files/ for Linux systems

NOTE: If you are upgrading to PowerChute v4.4, any SSH key files used in a previous version of PowerChute must be manually added to the user_files folder. If the key files are not added to the directory, you will see the below error in the Event Log:

```
ERROR: The ini contains an invalid value for SSH_Key_Path in
section NutanixClusterDetails.
```

It is strongly recommended you validate your configuration after an upgrade.

For more information on Nutanix configuration options, refer to the *PowerChute VMware User Guide* available on the APC website.

HPE SimpliVity Support

PowerChute provides support for shutting down and starting up virtual machines running on an HPE SimpliVity Cluster with ESXi as your hypervisor. PowerChute also supports shutting down and starting up the OmniStack Virtual Controllers in the cluster(s).

NOTES:

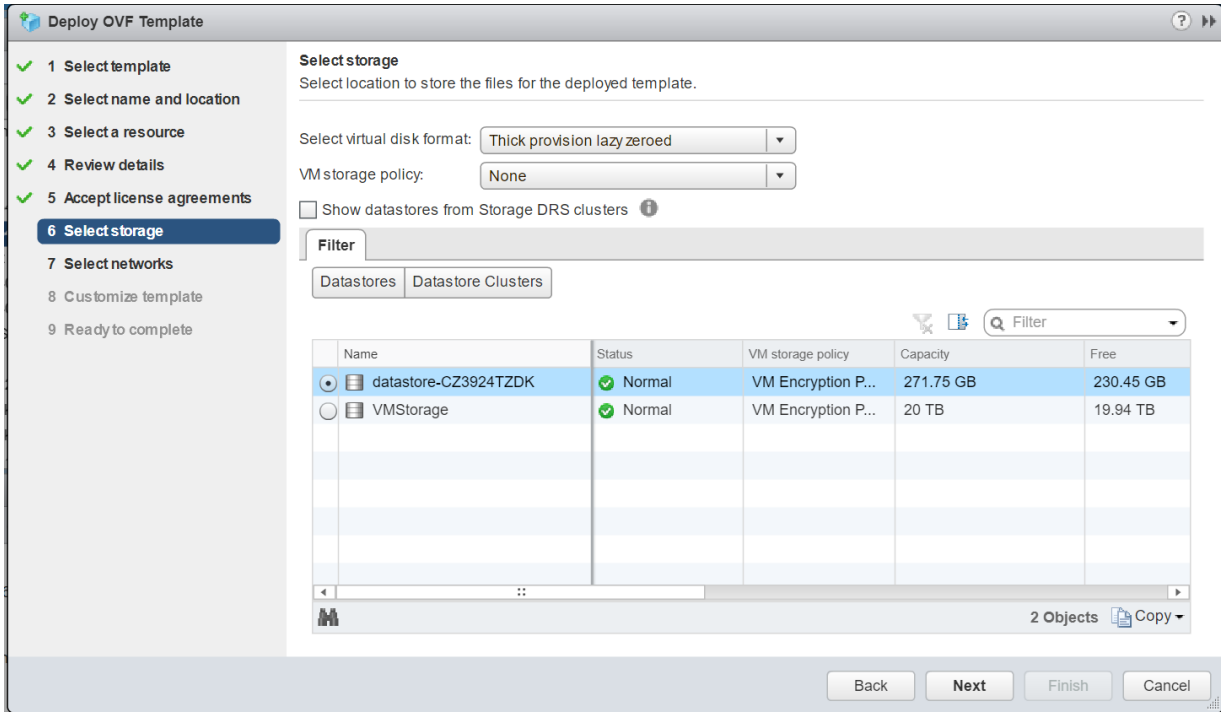
- In an advanced configuration, there must be one UPS setup protecting the HPE SimpliVity Cluster, and one UPS setup protecting the external physical Windows machine with HPE SimpliVity Arbiter and PowerChute.
- In an advanced configuration, vCenter Server may be deployed as a VM on the HPE SimpliVity Cluster or on the same physical machine as the Arbiter service and PowerChute.
- In an HPE SimpliVity Federation with multiple clusters, it is recommended to have one instance of PowerChute per cluster.

Install PowerChute

For HPE SimpliVity, PowerChute can be installed on a physical Windows machine outside of the cluster, or deployed as a VM in the cluster.

- **PowerChute on physical Windows machine:** Follow the installation steps detailed in the Installing on Windows to Monitor VMware Hosts section.
- **PowerChute deployed as VM in the cluster:** Follow the installation steps detailed in the Deploying the PowerChute Virtual Appliance section.

When deploying the virtual appliance OVA file, you cannot deploy the OVA file on the HPE SimpliVity Cluster datastore. You must deploy the OVA file to a local datastore.

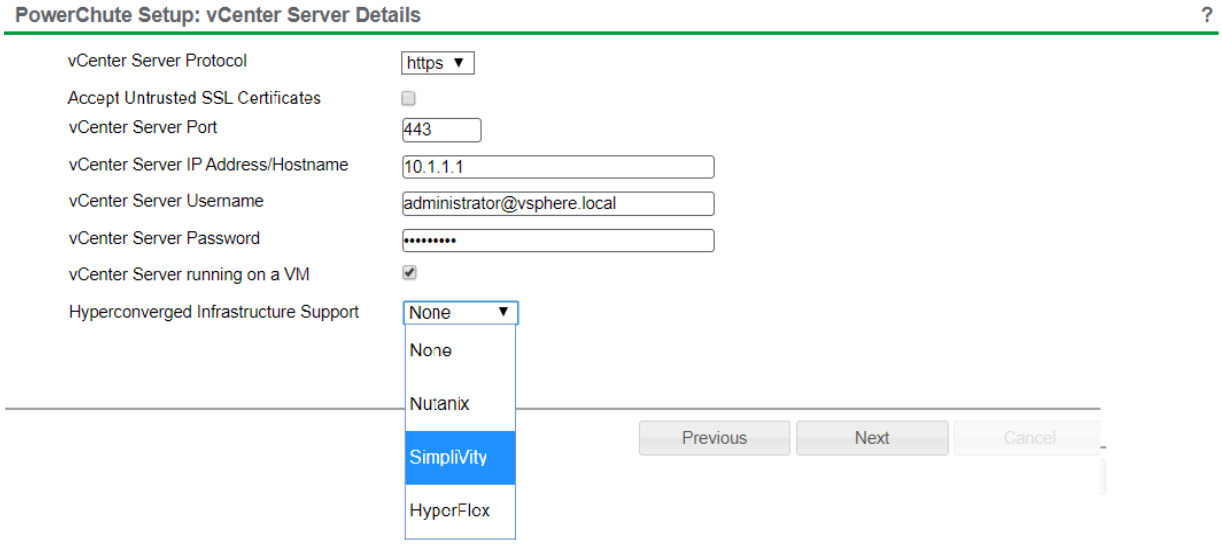


Configure HPE SimpliVity

When PowerChute is successfully installed on Windows, the PowerChute Setup wizard opens automatically after you click the **Finish** button. The PowerChute UI can be accessed at `https://<IP_Address>:6547`.

Follow the steps below to complete your HPE SimpliVity configuration:

1. In the **vCenter Server Details** screen, select SimpliVity from the **Hyperconverged Infrastructure Support** drop-down list and click **Next**.



The **Accept Untrusted SSL Certificates** checkbox is unselected by default. If left unselected, only SSL certificates signed by a trusted CA will be accepted when connecting to vCenter Server and ESXi hosts. By default, these certificates are self-signed and this will cause a cause connection error. This is for increased security and to prevent man-in-the-middle (MITM) type attacks. Select this checkbox if you want to use untrusted/self-signed SSL certificates to connect to vCenter Server and ESXi hosts.

Alternatively, you can add the vCenter Server root CA certificate to the PowerChute-keystore by following the steps detailed in the vCenter Server Settings topic in the User Guide.

2. Enter your HPE SimpliVity connection details in the **SimpliVity Details** screen to connect to your Virtual Controller and click **Next**. The default user name is “svtcli”. It is not recommended to change the HPE SimpliVity user name used by PowerChute.

For more information on HPE SimpliVity configuration options, refer to the *PowerChute VMware User Guide* available on the APC website.

Cisco HyperFlex Support

PowerChute provides support for shutting down and starting up virtual machines running on a HyperFlex Cluster with ESXi as your hypervisor. PowerChute also supports shutting down and starting up the Controller Virtual Machines and the HyperFlex Cluster.

NOTES:

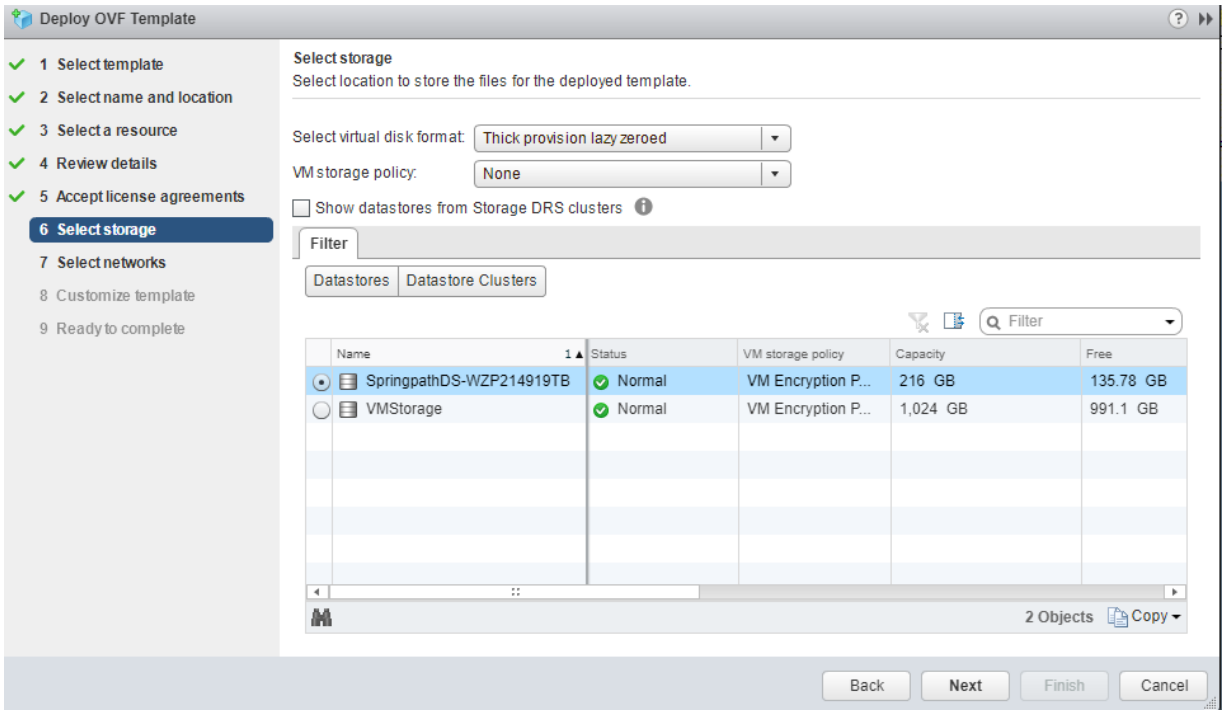
- In an advanced configuration, all hosts in the HyperFlex Cluster must be protected by the same UPS Setup.
- If there are multiple HyperFlex Edge Clusters, it is recommended to have one instance of PowerChute per cluster.

Install PowerChute

For HyperFlex, PowerChute can be installed on a physical Windows machine outside of the cluster, or deployed as a VM in the cluster.

- **PowerChute on physical Windows machine:** Follow the installation steps detailed in the Installing on Windows to Monitor VMware Hosts section.
- **PowerChute deployed as VM in the cluster:** Follow the installation steps detailed in the Deploying the PowerChute Virtual Appliance section.

When deploying the virtual appliance OVA file, you cannot deploy the OVA file on the HyperFlex Cluster datastore. You must deploy the OVA file to a local datastore.

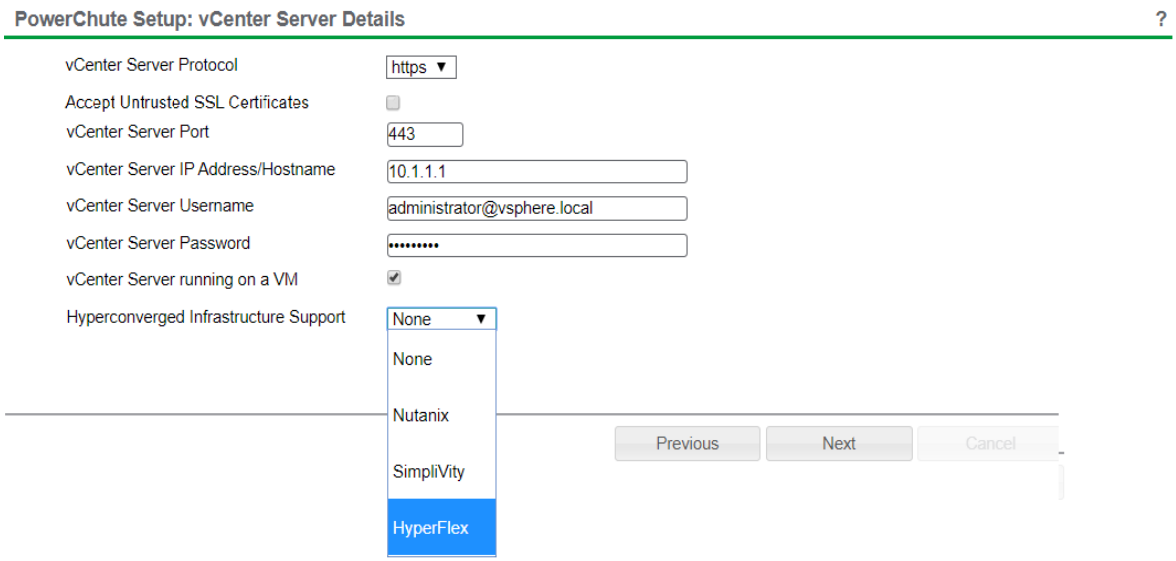


Configure HyperFlex

When PowerChute is successfully installed on Windows, the PowerChute Setup wizard opens automatically after you click the **Finish** button. The PowerChute UI can be accessed at `https://<IP_Address>:6547`.

Follow the steps below to complete your HyperFlex configuration:

1. In the **vCenter Server Details** screen, select HyperFlex from the **Hyperconverged Infrastructure Support** drop-down list and click **Next**.



The **Accept Untrusted SSL Certificates** checkbox is unselected by default. If left unselected, only SSL certificates signed by a trusted CA will be accepted when connecting to vCenter Server and ESXi hosts. By default, these certificates are self-signed and this will cause a cause connection error. This is for increased security and to prevent man-in-the-middle (MITM) type attacks. Select this checkbox if you want to use untrusted/self-signed SSL certificates to connect to vCenter Server and ESXi hosts.

Alternatively, you can add the vCenter Server root CA certificate to the PowerChute-keystore by following the steps detailed in the vCenter Server Settings topic in the User Guide.

2. Enter your HyperFlex connection details in the **HyperFlex Details** screen to connect to your Cluster and click **Next**.

The local admin account credentials must be provided and not the VMware account credentials to allow graceful shutdown in the event that vCenter Server is unavailable.

For more information on HyperFlex configuration options, refer to the *PowerChute VMware User Guide* available on the APC website.

Upgrading the Software

If you have v4.2 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 v4.4.

It is not necessary to run the PowerChute Setup wizard after an upgrade

PowerChute v4.3+ is a 64-bit only application and cannot be installed on a 32-bit operating system. If you have a 32-bit operating system, you cannot upgrade to v4.3+.

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

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

For a virtual appliance installation, you should manually power off the virtual appliance and 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
```

It is not supported to set custom SSL certificates during a silent installation. In the `silentInstall` file, set ACCEPTCERTS=YES, and import SSL certificates if needed after the installation.

For more information on importing SSL certificates, see the **vCenter Server Settings** topic in the User Guide.

If a silent installation is unsuccessful, 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, applicationDirectory and INSTALL_JAVA, 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).	
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 license agreement. The installation will not proceed unless yes is specified here.
INSTALL_JAVA= System | PCNS	The value `System` here signifies you want to use the public JRE for your PowerChute installation. The value `PCNS` here signifies you want to use the private JRE. The installation detects whether the public JRE meets the requirements.
The fields directly below, INSTALL_DIR and JAVA_DIR, are used when you are monitoring a VMware host from a VM with PowerChute Network Shutdown (see Installing PowerChute Network Shutdown with VMware Support).	
INSTALL_DIR=	Specifies the installation directory. Type the path where the public JRE is installed on the system e.g. `\usr\bin`. **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 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 Disk space.
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. See the online help, **UPS Configuration Options,** for more information.
NETWORKCONFIG= IPv4 | IPv6	Specify your internet protocol with IPv4 or IPv6.
IPV6NETWORKCONFIG= unicast | multicast	When you are using IPv6 only (having 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.

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: • the alphabet in both lowercase and uppercase (a to z and A to Z) • numbers from 0 to 9 • these characters: _ ! \ " # $ % & ' ( ) * + , - . / : ; < = > ? @ ^ ` { | } [ ] ~ The password requires: • Minimum 8 and maximum 128 characters in length • One upper and one lower case letter • One number and special character • The username also cannot be part of the password The username must be between 1–10 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.

Field name	Description
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, he Network Management card will send UDP packets to the multicast address you specify here.
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.
ESXIHOST_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.
ESXIHOST_USERNAME=	When the CONFIGURATION_MODE= field above is “unmanaged”, specify the user name of the ESXi host.
ESXIHOST_PASSWORD=	When the CONFIGURATION_MODE= field above is “unmanaged”, specify the password of the ESXi host
ESXIHOST_PROTOCOL = http | https	Specify the protocol by which the ESXi Host communicates with PowerChute.
ESXIHOST_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: • 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	

Field name	Description
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 "*SNMP Troubleshooting*" topic of the *PowerChute Network Shutdown User Guide* 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: • 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.

Field name	Description
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

Nutanix

Installing PowerChute Network Shutdown with Nutanix Support

See these sections:

- Installing on Windows to Monitor Nutanix Hosts
- Upgrading the Software
- Uninstalling the Software

Using PowerChute in a Nutanix environment

PowerChute provides support for shutting down and starting up virtual machines running on a single Nutanix Cluster directly with Nutanix Acropolis Hypervisor (AHV). PowerChute also supports the shutting down and starting up of a Nutanix Cluster with VMware as your hypervisor.

NOTES:

- One or more Nutanix blocks are supported. However, all nodes in the blocks must be part of the same Cluster. **NOTE:** A block contains 4 or 8 nodes depending on your Nutanix model.
- In an advanced configuration, all blocks in the Cluster must be protected by the same UPS or UPS group.

Installing on Windows to Monitor Nutanix Hosts

To install PowerChute with Nutanix AHV:

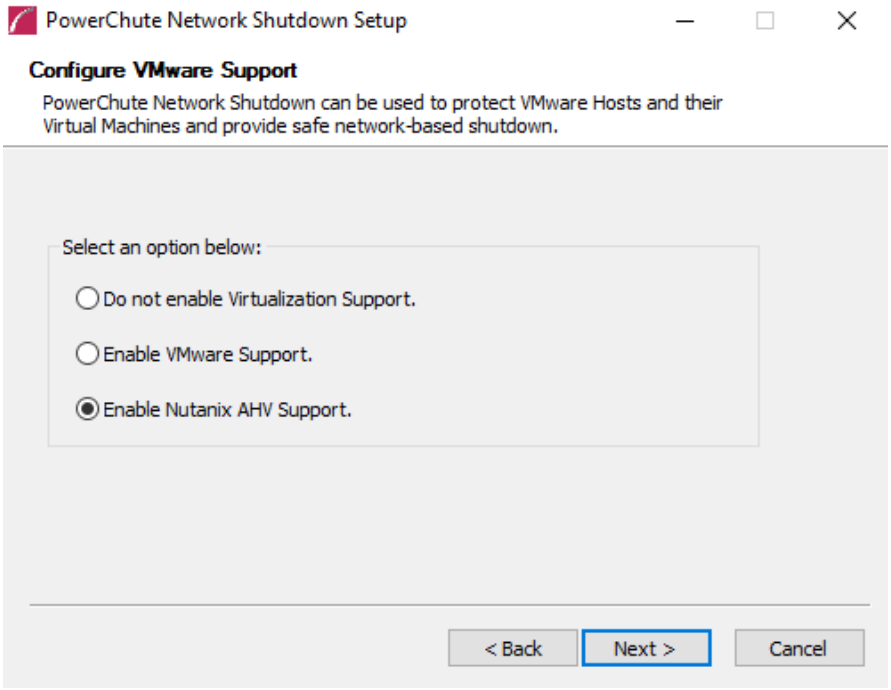
Follow these steps below.

1. Download the PowerChute installation executable file, **Setup-x64.exe**, from the APC website. You must have administrator rights to run the installer.
   Extract the file, and double-click on the 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. PowerChute includes a private Java Runtime Environment (JRE) that is bundled with the software. In this step, PowerChute installs this bundled JRE on your operating system.

6. Choose **Enable Nutanix AHV Support** at the dialog below.



7. Enter an installation folder location or accept the default and your installation proceeds.

   Do not copy unsigned DLLS, .jar files, executable files, or any files from an untrusted source to the PowerChute installation folder.

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.

Upgrading the Software

If you have v4.3 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 v4.4.

It is not necessary to run the PowerChute Setup wizard after the upgrade.

PowerChute v4.3+ is a 64-bit only application and cannot be installed on a 32-bit operating system. If you have a 32-bit operating system, you cannot upgrade to v4.3+.

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 the Software

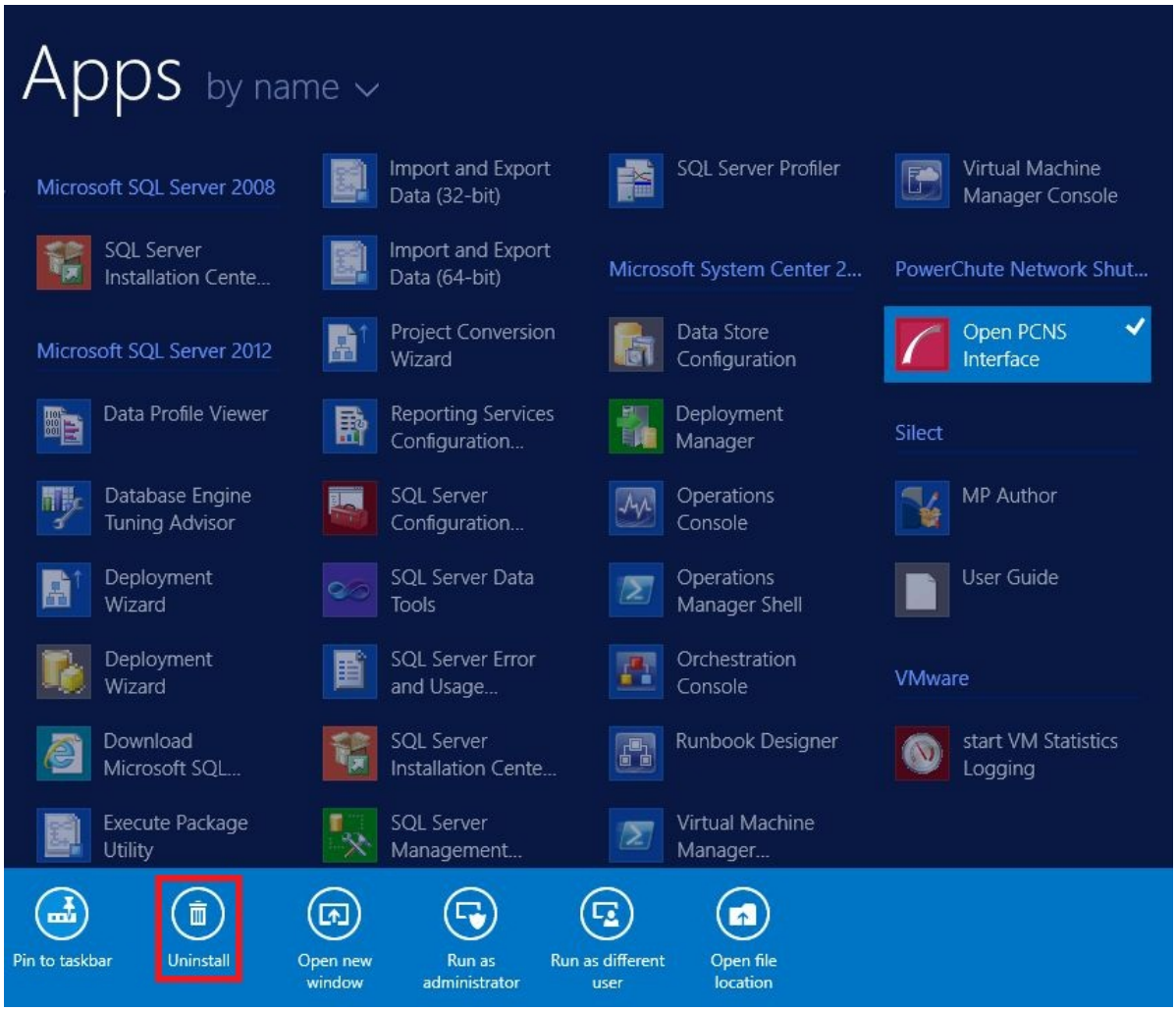
On Windows, use the **Uninstall** option under **PowerChute Network Shutdown** in the Windows Start menu.

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, 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.

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 is unsuccessful.

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: install.sh [-f <config file>]: Silent install with configuration file. install.sh [-h|-H]: Print help.	Usage: Indicates that unrecognized parameters were passed to the installer.
4	Error: install.sh 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 v4.4. 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	One of: Error: Too many INSTALL_DIR in silentConfiguration.ini. Error: INSTALL_DIR must start with '/'. Installation directory must start with "/". Error: INSTALL_DIR must not contain white space. Error: INSTALL_DIR must not contain back slash "\". Error: INSTALL_DIR is not configured. Installation directory must not contain white space " ". Installation directory must not contain back slash "\". Failed to create directory <install directory>.	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 License 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	One of: Error: Too many JAVA_DIR in <configuration file>. Error: JAVA_DIR must start with "/". Error: JAVA_DIR must not contain white space " ". Error: JAVA_DIR must not contain back slash "\". Error: Invalid JAVA_DIR. <directory> does not exist. Java is not available on the path. Please specify a java directory.	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 was unable to register the PCNS service.
23	[Error]: <23> Installation cancelled.	M11 Backup Failure: The installer was unable 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 unsuccessful with NMC due to timeout. The NMC host address and the connection attempt were both fine, but the NMC did not respond.
33	Bad UPS Network Management Card host address supplied. Registration has failed.	Registration unsuccessful with NMC due to a bad host address.
34	Could not connect to UPS Network Management Card. Registration has failed.	Registration unsuccessful 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 unsuccessful 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 unsuccessful 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 unsuccessful 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 unsuccessful 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 did not 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 did not 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 did not 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, AES-256 or DES.

Error Code	Error Message	Description
69	Invalid SNMP Authentication passphrase.	You have entered an invalid Authentication passphrase. The Authentication passphrase must be 15-32 ASCII characters in length.
70	Invalid SNMP Privacy passphrase.	You have entered an invalid Privacy passphrase. The Privacy passphrase must be 15-32 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.

© 2020 Schneider Electric. All Rights Reserved. Schneider Electric, APC and PowerChute are trademarks and the property of Schneider Electric SE, its subsidiaries and affiliated companies. All other trademarks are property of their respective owners.

990-2838Q-001 **11/2020**