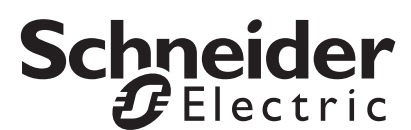


Security Handbook

PowerChute Network Shutdown

990-91316D-001

Publication Date: May, 2024



Schneider Electric IT Corporation Legal Disclaimer

The information presented in this manual is not warranted by the Schneider Electric IT Corporation 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 IT Corporation 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 IT Corporation. 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 IT CORPORATION, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC IT CORPORATION 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 IT CORPORATION HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC IT CORPORATION 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 IT Corporation 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.

Table of Contents

Overview	1
Content and Purpose of this Guide	1
Connectivity	1
PowerChute Access	1
Network Management Card Connection	1
Authentication	2
Password Requirements	2
Account Lock-Out	2
User Control	2
NMC Connection	3
Firewalls	3
External PowerChute Environment	3
The PowerChute Virtual Appliance	3
External User Credentials	4
PowerChute Network Shutdown - Communication/Access Model	4
PowerChute License	6
License Information	6
Connectivity & Authentication	6
Java Runtime Environment (JRE)	6
JRE Utilization	6
Disabled and Restricted Cryptographic Algorithms	7
Secure Backup Recommendations	8
INI File	8
Vulnerability Reporting and Management	8
How to report a Vulnerability	8
Security Updates and Notifications	8
Update Notifications	8
Knowledge Base	8
Software Integrity	8
Security Hardening and Removal Guidelines	9
Security Hardening Guidelines	9
Network Management Card	9
PowerChute Network Shutdown	9

Secure Removal Guidelines	10
---------------------------------	----

Appendix 1: Replacing the Default PowerChute SSL Certificate 11

Windows	11
Changing the password for the Java Keystore	11
Create a new Keystore for the trusted SSL cert	11
Create a certificate signing request and a new SSL cert signed by a Trusted CA	12
Import the Root CA and Web Server SSL certs to the PowerChute Keystore	12
Linux/Unix	13
Changing the password for the Java Keystore	13
Create a new Keystore for the trusted SSL cert	13
Create a certificate signing request and a new SSL cert signed by a Trusted CA	13
Import the Root CA and Web Server SSL certs to the PowerChute Keystore	14

Appendix 2: Adding a Trusted Certificate to PowerChute for NMC Communication15

Windows	15
Validate the Certificate in PowerChute-keystore	15
Linux	16
Validate the Certificate in PowerChute-keystore	16

Appendix 3: Adding the VxRail Manager Root CA Cert to PowerChute17

Change the PowerChute-keystore Password	17
Import Trusted Certificate	17

Appendix 4: Adding the VxRail Manager SSL Certificate to PowerChute18

Appendix 5: Creating Certificates with Subject Alternate Name (SAN) Entries19

Windows	19
Linux	20

Appendix 6: Reset the PowerChute virtual appliance root password.....22

Overview

Content and Purpose of this Guide

This guide documents the security features in PowerChute Network Shutdown including connectivity and authentication, as well as information on secure deployment and hardening guidelines.

Connectivity

PowerChute Access

The PowerChute user interface (UI) is accessible via a web browser and supports TLS v1.2 or 1.3 which provides authentication and encrypted communication for sensitive communications.

NOTE: When TLS is enabled, your browser displays a small lock icon.

PowerChute provides secured browser access via HTTPS as default to ensure that communication via the web interface is secure and cannot be intercepted. You have the option to select HTTP but this is not recommended for secure deployment.

PowerChute uses a self-signed SSL Certificate by default that has a 2048-bit RSA public key in PowerChute v4.4.1 and 4096-bit RSA public key in v5.1, and uses the SHA-1 Signature Hash Algorithm in PowerChute v4.4.1 and SHA-256 in v5.1. See [Appendix 1: Replacing the Default PowerChute SSL Certificate](#) for details on how to replace SSL certificates for Windows and Linux.

If enabled and configured, PowerChute can be accessed via SNMP v1 or v3. It is recommended to use SNMPv3 which provides authentication and encryption. In SNMPv1, the community name is transferred over the network in plain text; it is not encrypted.

Network Management Card Connection

The UPS Network Management Card (NMC) provides an interface between your APC UPS and your network. To establish communications between PowerChute and the NMC, PowerChute access and the chosen communication protocol (HTTP/HTTPS) must be enabled on the NMC.

In NMC firmware version 6.8.0 and higher, the NMC uses the HTTPS protocol by default. For firmware versions prior to v6.8.0, HTTP is the default protocol and it is recommended you use HTTPS for secure communications.

The User Name and Authentication Phrase specified in the NMC Web UI must also match the credentials provided in the PowerChute Setup wizard. The default port is 80 for HTTP, and 443 for HTTPS. Do not change this number unless you changed the port being used by your NMC.

The NMC uses a self-signed SSL certificate by default when HTTPS is enabled. You must add the NMC certificate to the PowerChute-keystore, see [Appendix 2: Adding a Trusted Certificate to PowerChute for NMC Communication](#).

NOTE: PowerChute does not validate certificates added to the PowerChute-keystore. PowerChute will continue to trust certificates in the PowerChute-keystore after they have expired or been revoked. It is your responsibility to remove these certificates from the PowerChute-keystore once they are no longer needed.

The NMC sends UPS status updates and information to PowerChute Network Shutdown via UDP packets on port 3052.

For a detailed description on how UPS information is sent over the network and how PowerChute receives NMC updates, see [The Communications Process of PowerChute Network Shutdown](#).

Authentication

During the initial PowerChute setup using the PowerChute Setup Wizard, you must enter a Username, Password and Authentication Phrase. The Username and Password will be used to log on to the PowerChute UI.

The Username and Authentication Phrase are used for authentication between PowerChute and the Network Management Card (NMC) and therefore they must match. The passwords used in PowerChute and the NMC can be different.

Password Requirements

Upon launching the PowerChute Setup Wizard, the Username, Password and Authentication Phrase can be set via the Security Details page. The password requires:

- Minimum 8 and maximum 128 characters in length
- One upper and lower case letter
- One number and special character
- Leading and trailing whitespace is removed from password
- White space within the passwords is permitted

No password or passphrase is stored in PowerChute in plain text. The Username, Password, and Authentication Phrase used to connect with PowerChute are stored in the `m11.cfg` file using AES-256-bit encryption.

The Username and Password can be reset via the `pcnconfig.ini` file, and the Authentication Phrase can be reset via the PowerChute UI. For information on how to reset your credentials, see the [PowerChute Network Shutdown User Guide](#).

Administrator access is required on all operating systems to open and edit the `pcnsconfig.ini` file.

Account Lock-Out

PowerChute will automatically “lock out” after three unsuccessful login attempts (incorrect Username and/or Password) to prevent brute force password cracking. The unsuccessful login attempts are tracked in the `access.log` file in the `group1` directory.

The account lock-out is isolated to the IP address of the machine where the unsuccessful login attempts originated. Users on a different machine with a different IP address can still attempt to log in to the PowerChute UI.

The account lock-out duration is set to two minutes by default. The lock-out duration and number of invalid login attempts can be modified using the `pcnsconfig.ini` file. The settings are in the Networking section:

LockoutDuration = 120

LockoutFailCount = 3

User Control

PowerChute allows you to create one administrator account only. This account has a unique log-in username and password enabling full read/write access. Only one session of PowerChute can be active at any time, therefore, users will not be able to log on to the same PowerChute Agent from multiple machines simultaneously.

It is strongly recommended that PowerChute is not made available on a public-facing network segment. This is to ensure secure user control.

To further restrict access, TCP port 6547 (HTTPS) can be blocked using firewall settings to prevent remote access to the UI. The UI can still be accessed locally via `https://localhost:6547`

NMC Connection

The communications mechanism between the NMC and PowerChute Network Shutdown provides the following security measures:

- Ensuring that user credentials are never sent in plain text.
- PowerChute will only process UDP packets from a trusted Network Management Card.
- Detecting if a UDP packet has been tampered with in transit.
- Detecting if a UDP packet has been replayed.

Firewalls

It is recommended you use a well-configured firewall in conjunction with an intrusion prevention system (IPS) to help protect PowerChute against Denial of Service attacks and unauthorized access.

- The firewall can be used to block access from untrusted/external networks and allow access only from trusted subnets.
- The IPS can be used to detect patterns of behavior associated with Denial of Service attacks.

External PowerChute Environment

PowerChute supports single, redundant, parallel and advanced UPS configurations. For more information on supported UPS configurations, please refer to the User Guides available on the [APC website](#), and Application Note #186 [PowerChute Network Shutdown in Advanced Redundant Setups](#).

The PowerChute Virtual Appliance

The PowerChute virtual appliance is a virtual machine image with AlmaLinux 9.3 (Shamrock Pampas Cat) OS running PowerChute Network Shutdown v5.1 pre-installed.

It 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. See the [Security Hardening and Removal Guidelines](#) section for more information.

It is strongly recommended to regularly update the AlmaLinux OS libraries of the Virtual Appliance to obtain the latest security updates. See “How to update the Virtual Appliance libraries” in the [PowerChute Installation Guide](#) for more information.

When using the PowerChute virtual appliance, you have the option to specify some settings for the appliance using the OVF Deployment Wizard. Some of the configurable settings are the password for the root user and the PowerChute Web UI username and password – configuring these may expose the virtual appliance to VMware vulnerabilities.

NOTE: Setting the PowerChute Web UI username and password via the OVF Deployment Wizard is mandatory. This prevents an unauthorized user from accessing the PowerChute Configuration Wizard without entering valid credentials.

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. For more information, see the [PowerChute Installation Guide](#).

On first launch of the appliance, the Virtual Appliance First-Time Configuration Wizard opens if you did not set the root password, network settings, and other settings during the OVF deployment. If you do not provide a password for the root user, or create an alternative user via the Wizard, the root account is disabled and you cannot log into the virtual appliance. It is highly recommended that you set the root password at this step to prevent lockout of the virtual appliance.

NOTE: The OVF properties are not available for deployment directly to an ESXi host. As a result, the PowerChute service is disabled when the virtual appliance is booted because the required PowerChute username and password are not specified pre-deployment. To resolve this issue, follow the steps outlined in [FAQ000261450](#).

External User Credentials

VMware

When VMware support is enabled and PowerChute is configured to protect Hosts that are managed by vCenter Server, a username and password are required. The VMware user account requires certain permissions in order to execute Virtualization Tasks – for a listing of the required permissions for this account, refer to Knowledge Base article [FA177822](#). A service account can be created in vSphere with only the required permissions instead of assigning the Administrator Role to this account – this is considered more secure. For more information on configuring vCenter Server accounts in PowerChute, refer to the [VMware User Guide](#).

Nutanix

When Nutanix support is enabled, to authenticate your connection to the Nutanix Controller Virtual Machine or Cluster, an IP address, Controller VM/Cluster password and AHV Host password are required, or an SSH key file path and its passphrase are required.

NOTE: To connect PowerChute to the Nutanix Controller VM/Cluster, the “nutanix” user account credentials must be used. You cannot use the “admin” user account credentials as this account does not have the necessary permissions for shutdown tasks.

SimpliVity/HyperFlex

When SimpliVity/HyperFlex support is enabled, a username and password are required to authenticate the connection.

NOTES:

- The default username for SimpliVity is “svtcli”.
- For HyperFlex, 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.

Dell VxRail

When VxRail support is enabled, PowerChute connects to VxRail Manager using the same credentials used for vCenter Server.

NOTE: All user credentials are stored in PowerChute using AES-128 bit encryption in PowerChute v4.4.1 and AES-256 bit encryption in v5.1.

PowerChute Network Shutdown - Communication/Access Model

The diagram below represents the access points to PowerChute Network Shutdown and its communication paths with external components such as VMware vCenter Server and VMware Hosts. PowerChute is primarily accessed via a secure HTTPS connection using a supported web browser (for the latest browser details, see the [Operating System, Processor, JRE and Browser Compatibility Chart](#)).

PowerChute uses a self-signed SSL Certificate by default that has a 2048-bit RSA public key in PowerChute v4.4.1 and 4096-bit RSA public key in v5.1, and uses the SHA-1 Signature Hash Algorithm in PowerChute v4.4.1 and SHA-256 in v5.1. The default self-signed cert can be replaced (see [Appendix 4](#) for detailed instructions).

PowerChute communicates with the Network Management Card using HTTPS for registration and control tasks. It receives UDP status updates from the NMC via UDP packets sent to port 3052. For more information on how to harden security for PowerChute and the NMC, refer to [Security Hardening Guidelines](#).

PowerChute stores configuration information on the local file system using the `pcnsconfig.ini` file and user credentials are stored encrypted in the `m11.cfg` file. Administrator access is required on all operating systems to access these files.

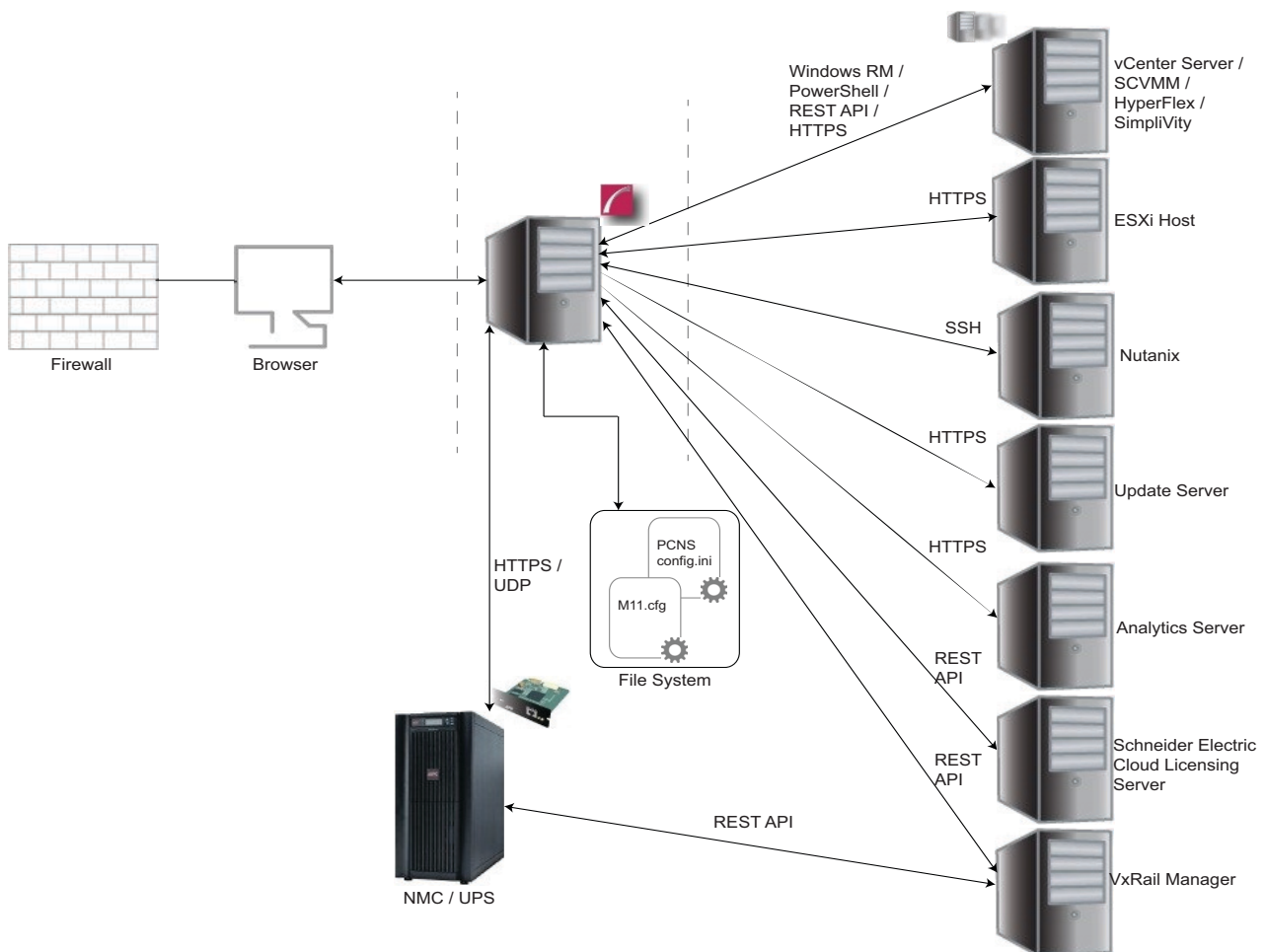
The Software Updates Notification feature is enabled by default and PowerChute communicates with the Update Server using a secure HTTPS connection. The Updates Server uses an SSL cert that has been signed using a Trusted Third Party Root Certification Authority.

The PowerChute Customer Experience Improvement Program (CEIP), if enabled, sends anonymous configuration and usage data to an Analytics Server using a secure HTTPS connection. This connection is outbound only to TCP port 443 and the Analytics Server uses an SSL cert that has been signed using a Trusted Third Party Root Certification Authority.

PowerChute communicates with the Schneider Licensing Server via HTTPS to validate license information.

PowerChute communicates with Hyper-V/SCVMM via Windows RM, and external VMware components using a secure HTTPS connection, including HyperFlex and SimpliVity. PowerChute communicates with Nutanix using SSH.

PowerChute communicates with VxRail Manager via a REST API over HTTPS to gather version information. The NMC communicates with VxRail Manager via a REST API over HTTPS to shut down the Dell VxRail Cluster.



PowerChute License

License Information

PowerChute Network Shutdown v4.5 and later are licensed products. A license can be purchased through your Schneider Electric IT Partner and is required for PowerChute to function and to perform graceful system shutdown.

Once purchased, you can activate your license in the PowerChute Setup wizard online using the Schneider Electric Cloud Licensing Server or offline using the [Schneider Electric Licensing Portal](#). For more information on how to activate your PowerChute license, see the [PowerChute Network Shutdown User Guide](#).

In PowerChute v5.1, you can avail of a trial license which enables all PowerChute functionalities for a period of 30 days. For more information, see the [PowerChute Network Shutdown User Guide](#). You can activate your license via the Local Licensing Server for PowerChute v5.0+. For more information, see the [Local Licensing Server User Guide](#).

Connectivity & Authentication

The 3 documented URLs are secured using HTTPS with TLS 1.2, and are signed using a trusted third-party root certificate authority. If you are presented with SSL-related security warnings when attempting to access these websites, you should not enter any login details or proceed.

If you activate your license via the online method, you can provide proxy information if required. The proxy username and password are stored in PowerChute using AES-256 bit encryption. The provided Activation ID is also stored using AES-256 bit encryption.

Java Runtime Environment (JRE)

JRE Utilization

PowerChute Network Shutdown installs a custom JRE to operate. PowerChute is shipped with the latest version of [OpenJDK](#) Java at the time of release.

PowerChute uses the following Java modules:

java.base	java.compiler
java.desktop	java.naming
java.rmi	java.management
java.scripting	java.instrument
java.security.jgss	java.sql
java.xml	java.logging
jdk.crypto.cryptoki	jdk.zipfs
jdk.jdwp.agent	

The OpenJDK version can be updated via the Java Update feature in the PowerChute UI when new versions containing security fixes are released. See the [PowerChute Network Shutdown User Guide](#) for more information.

For more information on JRE versions included with and supported by PowerChute Network Shutdown, refer to the [Operating System, Processor, JRE and Browser Compatibility Chart](#).

Disabled and Restricted Cryptographic Algorithms

In PowerChute v5.0, the `ssl_protocol` was removed from the INI configuration as it is more suitably configured by Java Runtime Environment. The purpose of this configuration value was to allow users to specify their preferred SSL Protocol when creating secure connections with collaborating systems.

Restrictions on cryptographic algorithms are configured by editing the `<java-home>/conf/security/java.security` file within the application JRE folder. This is more efficient for users to manage permitted cryptographic algorithms, and security protocols by PowerChute. For more information on the values and features of JRE security including the use of the `java.security` file, see the [Java Secure Socket Extension \(JSSE\) Reference Guide](#).

Secure Backup Recommendations

INI File

All configuration settings applied via the PowerChute Setup Wizard and User Interface are stored on the local file system using the `pcnsconfig.ini` file. It is recommended to save a copy of this file as a backup.

User credentials are stored using the `m11.cfg` file and are encrypted using AES-128 bit encryption in PowerChute v4.4.1 and AES-256 bit encryption in v5.1, and backed up using the `m11.bak` file. User credentials can be reset via the `pcnsconfig.ini` file. Administrator access is required on Windows and Linux operating systems to access these files.

Vulnerability Reporting and Management

How to report a Vulnerability

Cybersecurity incidents and potential vulnerabilities can be reported via the Schneider Electric website – [Report a Vulnerability](#).

Security Updates and Notifications

Update Notifications

If a security vulnerability is detected in PowerChute that requires a software update, a notification will be sent via the Update Notifications feature providing a web link from where the update can be downloaded. Software updates must be applied manually.

Knowledge Base

Security Bulletins in relation to known vulnerabilities are published on the Schneider Electric Knowledge Base.

Software Integrity

All PowerChute Network Shutdown web downloads include a list of SHA-256 hash values that can be validated for authenticity using the [SHA-256 Hash Signature Reference Guide](#). In addition, the Windows installer is digitally signed.

Security Hardening and Removal Guidelines

This section includes recommended configuration changes to increase security for PowerChute communication with the Network Management Card.

Security Hardening Guidelines

Network Management Card

1. Change the default Authentication Phrase via **Configuration > Shutdown > PowerChute Shutdown Parameters**. If you are running NMC 2 firmware version v6.8.0+, you are required to set an Authentication Phrase before PowerChute access can be enabled.
2. Disable HTTP and enable HTTPS via **Configuration > Network > Web > Access**. **NOTE:** HTTPS is required for Dell VxRail support.
3. Create a new SSL certificate for the Network Management Card using the **APC Network Management Card Security Wizard v1.0.4**, or the **NMC Security Wizard CLI Utility**. Please refer to the [NMC 3 Security Handbook](#) for more information.
4. Replace the default self-signed SSL certificate with the new one in **Configuration > Network > Web > SSL Certificate**.
5. Ensure that NMC firmware updates are installed to apply the latest security updates and bug fixes.
6. Please see the Security Handbooks for the Network Management Cards for more information on how to secure them – available [here](#).

PowerChute Network Shutdown

1. Change the credentials for the PowerChute-keystore via the `pcnsconfig.ini` file. See [Changing the password for the Java Keystore](#).
2. During the Setup Wizard, on the Network Management Card connection page, ensure that the protocol used is HTTPS and port is 443.
3. Replace the default self-signed SSL certificate for the PowerChute UI using the instructions in [Appendix 4](#).
4. Change the default password for the CACERTS keystore located in the group1 folder using the command: `keytool.exe -storepasswd -new <new password> -keystore cacerts -storepass changeit`
5. Prevent Remote Access to the Web UI if this is not required using a firewall rule for TCP ports 3052 and 6547. To prevent Denial of Service attacks such as the SSL/TLS resource exhaustion attack, these ports should be blocked and we do not recommend allowing access to PowerChute

on a public facing network interface. Additionally, the firewall should prevent inbound communication with UDP port 3052 except for the Network Management Card that PowerChute is communicating with. The PowerChute UI can still be accessed locally via <https://localhost:6547>

6. Use the Java Update feature in PowerChute to update the JRE regularly as software updates and security fixes are released. See the [PowerChute Network Shutdown User Guide](#) for more information.
7. Ensure that the Enable Automatic Updates feature is enabled to be informed when PowerChute software updates are available. See the [PowerChute Network Shutdown User Guide](#) for more information.
8. If using SNMP with PowerChute, it is recommended to only use SNMPv3 and to choose SHA-2 and AES-128 or higher for Authentication and Privacy. It is also recommended to change the default port of 161. Access Control should also be configured to restrict access to PowerChute via SNMP.
9. It is recommended you do not use untrusted third-party repositories to download software for the virtual appliance, and to use DNF in preference to YUM when updating system libraries as this is the most recent package management tool.
10. If you do not require remote SSH access to the virtual appliance, it is recommended you disable this service. To disable/enable SSH services, issue the following commands as the root user:

```
systemctl stop sshd

systemctl disable sshd


systemctl start sshd

systemctl stop sshd
```

Where access is required, it is recommended that you visit [AlmaLinux Security Guides](#) to harden the SSH service. The PowerChute virtual appliance can also be accessed via the VMware Remote Console.

NOTE: Technical Support may require you to copy configuration files and logs for troubleshooting purposes. In this case, you can temporarily enable SSH services to allow secure file transfer via SCP.

11. If you do require remote SSH access to the virtual appliance, it is strongly recommended you perform the following actions:
 - a. `update-crypto-policies --set FUTURE`
 - b. Create a backup of the crypto-policies file, for example `cp /etc/crypto-policies/back-ends/opensshserver.config /etc/crypto-policies/back-ends/opensshserver.config.old`
 - c. Edit `/etc/crypto-policies/back-ends/opensshserver.config` and delete `aes256-cbc`. Save the file.
 - d. Edit `/etc/ssh/sshd_config` and change `AllowTcpForwarding` to `No`. Save the file.
 - e. Re-start SSH – `systemctl restart sshd`

Secure Removal Guidelines

For information on how to uninstall PowerChute Network Shutdown, please refer to the [Installation Guide](#).

If the uninstallation does not successfully complete on Windows operating systems, you must manually delete folders, files and registry keys to completely uninstall PowerChute. For more information, refer to Knowledge Base article [FA159895](#).

Appendix 1: Replacing the Default PowerChute SSL Certificate

Windows

Changing the password for the Java Keystore

PowerChute stores the Web Interface SSL certs in a Java keystore file located in `C:\Program Files\APC\PowerChute\group1\keystore`.

To change the password for the keystore:

1. Stop the PowerChute service via the services console or using the command “net stop pcns1”.
2. Open `C:\Program Files\APC\PowerChute\group1\pcnsconfig.ini`
3. In the section `[NetworkManagementCard]` add the line `KeystorePassword = your_password` (`your_password` can be replaced with a password of your choice. It must be at least 6 characters).
4. Start the PowerChute service via the services console or using the command “net start pcns1”.
5. Verify that the keystore password has been changed:
 - a. Open a command prompt window and change directory to `C:\Program Files\APC\PowerChute\group1`
 - b. Type “`<path_to_jre>\bin\keytool.exe -list -v -keystore keystore`”
 - c. Enter the password you specified in step 3 when prompted.
 - d. Verify the keystore contents are displayed without error. (`<path_to_jre>` is the location of the private JRE).

Create a new Keystore for the trusted SSL cert

1. Stop the PowerChute service.
2. Delete the existing keystore file – `C:\Program Files\APC\PowerChute\group1\keystore`
3. Open a command prompt and change the directory to `C:\Program Files\APC\PowerChute\group1`
4. Type “`<path_to_jre>\bin\keytool.exe -genkey -alias securekey -keyalg RSA -keystore keystore -keysize 4096`” and press Enter.
5. Use the same password that was specified in step 3 in section “Changing the password for the Java Keystore”.
6. Enter the required values when prompted - the file value must match the hostname or FQDN (Fully Qualified Domain Name) of the server where PowerChute is installed. The other values you enter may need to match the values present on the CA. Some values are required by the CA, whereas others may be optional. This depends on the CA configuration.
7. Verify that the file keystore now exists in the group1 folder.

Create a certificate signing request and a new SSL cert signed by a Trusted CA

1. Type the command "`<path_to_jre>\bin\keytool.exe -certreq -alias securekey -keystore keystore -file newpowerchute.csr`" and press Enter.
2. Use the .CSR file to create a new certification signed by the Trusted CA. This process will depend on the Trusted CA software being used, e.g. for OpenSSL on Windows:
 - a. `openssl.exe ca -cert rootca.crt -keyfile rootca.key -out newpowerchute.crt -config openssl.cfg -infile newpowerchute.csr`
 - b. `rootca.crt` – This is the root CA certificate created when creating the CA.
 - c. `rootca.key` – Private key file created when setting up the CA
`newpowerchute.crt` – This is the new SSL cert that will be created and signed for use on the PowerChute Web interface.
 - d. `openssl.cfg` – This is the OpenSSL configuration file.
 - e. `newpowerchute.csr` – This is the file created in step 1.

NOTE: The `openssl` command used to generate the new signed cert is an example based on OpenSSL-Win32.

Import the Root CA and Web Server SSL certs to the PowerChute Keystore

1. Copy `rootca.crt` and `newpowerchute.crt` to the machine where PowerChute is installed.
2. Stop the PowerChute service.
3. Open a command prompt and change the directory to `C:\Program Files\APC\PowerChute\group1`
4. Import the root CA cert using the command: `<path_to_jre>\bin\keytool.exe -import -trustcacerts -alias root -file rootca.crt -keystore keystore`
5. Import the Web Server SSL cert using the command: `<path_to_jre>\bin\keytool.exe -import -trustcacerts -alias securekey -file newpowerchute.crt -keystore keystore`
6. Import the root CA cert to the internet browser on all machines that will be used to access the PowerChute user interface (UI).
7. Start the PowerChute service.
8. PowerChute should be using the new signed certificate and there should not be a SSL Cert security warning displayed by the browser when the PowerChute UI is launched.

NOTE: If using Microsoft Active Directory Certificate Services and you see error "keytool error: java.lang.Exception: Incomplete certificate chain in replay," see the following post [What do I do when keytool.exe can't establish a certificate chain from my certs?](#)

Linux/Unix

Changing the password for the Java Keystore

PowerChute stores the Web Interface SSL certs in a Java keystore file located in `/opt/APC/PowerChute/group1/keystore`.

To change the password for the keystore:

1. Stop the PowerChute service via the services console or using the command “service PowerChute stop”.
2. Open `/opt/APC/PowerChute/group1/pconsconfig.ini`
3. In the section `[NetworkManagementCard]` add the line `KeystorePassword = your_password` (`your_password` can be replaced with a password of your choice. It must be at least 6 characters).
4. Start the PowerChute service via the services console or using the command “service PowerChute start”.
5. Verify that the keystore password has been changed:
 - a. Open a command prompt window and change directory to `/opt/APC/PowerChute/group1`
 - b. Type “`../jre_x64/bin/keytool -list -v -keystore keystore`”
 - c. Enter the password you specified in step 3 when prompted.
 - d. Verify the keystore contents are displayed without error. (`<path_to_jre>` is the location of the private JRE).

Create a new Keystore for the trusted SSL cert

1. Stop the PowerChute service.
2. Delete the existing keystore file – `/opt/APC/PowerChute/group1/keystore`
3. Open a command prompt and change the directory to `/opt/APC/PowerChute/group1`
4. Type “`../jre_x64/bin/keytool -genkey -alias securekey -keyalg RSA -keystore keystore -keysize 4096`” and press Enter.
5. Use the same password that was specified in step 3 in section “Changing the password for the Java Keystore”.
6. Enter the required values when prompted - the file value must match the hostname or FQDN (Fully Qualified Domain Name) of the server where PowerChute is installed. The other values you enter may need to match the values present on the CA. Some values are required by the CA, whereas others may be optional. This depends on the CA configuration.
7. Verify that the file keystore now exists in the group1 folder.

Create a certificate signing request and a new SSL cert signed by a Trusted CA

1. Type the command “`../jre_x64/bin/keytool -certreq -alias securekey -keystore keystore -file newpowerchute.csr`” and press Enter.
2. Use the .CSR file to create a new certification signed by the Trusted CA. This process will depend on the Trusted CA software being used.

Import the Root CA and Web Server SSL certs to the PowerChute Keystore

1. Copy `rootca.crt` and `newpowerchute.crt` to the machine where PowerChute is installed.
2. Stop the PowerChute service.
3. Open a command prompt and change the directory to `/opt/APC/PowerChute/group1`
4. Import the root CA cert using the command: `../jre_x64/bin/keytool -import -trustcacerts -alias root -file rootca.crt -keystore keystore`
5. Import the Web Server SSL cert using the command: `../jre_x64/bin/keytool -import -trustcacerts -alias securekey -file newpowerchute.crt -keystore keystore`
6. Import the root CA cert to the internet browser on all machines that will be used to access the PowerChute user interface (UI).
7. Start the PowerChute service.
8. PowerChute should be using the new signed certificate and there should not be a SSL Cert security warning displayed by the browser when the PowerChute UI is launched.

Appendix 2: Adding a Trusted Certificate to PowerChute for NMC Communication

When using the HTTPS protocol to communicate with the NMC, you must import the NMC certificate to the PowerChute-keystore. You can import the default self-signed SSL certificate or create a new certificate that has been signed by a Trusted Certificate Authority to upload to the NMC and import that. Your [NMC Security Handbook](#) has details on the Security Wizard used to create the Trusted Certificate file with an extension .CRT. This file is then used to create components that can be uploaded to the NMC to replace the default self-signed certificate.


For PowerChute versions prior to v5.1, you can import the NMC certificate to the PowerChute-keystore using the Java keytool application or in v5.1, via the "Certificate Management" feature in the Web UI during NMC registration. See "Certificate Management" under the **Network Management Card Connection** topic in the [PowerChute User Guide](#) for more information.

To proceed, ensure that the PowerChute-keystore password is updated. In the **Network Management Card** section, add the lines **PowerChuteKeystorePassword = <New password>**

NOTE: PowerChute does not validate certificates added to the PowerChute-keystore. PowerChute will continue to trust certificates in the PowerChute-keystore after they have expired or been revoked. It is your responsibility to remove these certificates from the PowerChute-keystore once they are no longer needed.

Windows

You can use the Java keytool application to import the NMC certificate to the PowerChute-keystore. To export the self-signed certificate from the NMC:

1. In a web browser, view the NMC certificate. For example, in Chrome, click  **> More tools > Developer tools** (CTRL+Shift+I). Click on the **Security** tab and click the **View Certificate** button.
2. Click on the **Details** tab and click the **Copy to File...** button.
3. Using the Certificate Export Wizard, export the certificate as a Base-64 Encoded X.509 .cer file.
4. Copy the .cer file to the group1 directory: C:\Program Files\APC\PowerChute\group1\
5. Import the certificate using `<path_to_jre>\bin\keytool.exe -importcert -alias <nmc_ip_address> -keystore PowerChute-keystore -storepass <keystore password> -file <nmc_.cer_file>`

Validate the Certificate in PowerChute-keystore


1. Launch a terminal or command prompt and change the directory to the group1 directory of where PowerChute is installed. If the default location was chosen during installation, this will be C:\Program Files\APC\PowerChute\group1\
2. Run the command: `<path_to_jre>\bin\keytool.exe -list -v -keystore PowerChuteKeystore -storepass <keystore_password> -alias <nmc_ip_address>`
3. Search for "Certificate fingerprints" and note the SHA-1 value. For example: SHA1: 2D:94:62:DC:07:61:54:B8:56:D7:B5:71:B0:4B:A0:0A:1D:A8:1D:F5
4. Login to your NMC Web UI and navigate to **Configuration > Network > Web > SSL Certificate**.
5. Click **Valid Certificate** to view the certificate details.
6. Verify that the SHA-1 fingerprint value matches the value for the certificate in the PowerChute-keystore.

If the SHA-1 values match, set "acceptCerts = false" in the [NetworkManagementCard] section of the pcnsconfig.ini file, and restart the PowerChute service.

If the SHA-1 values do not match, delete the certificate from the PowerChute-keystore using the following command: `<path_to_jre>\bin\keytool.exe -delete -alias <nmc_ip_address> -keystore PowerChute-keystore -storepass <keystore_password>`

Linux

You can use the Java keytool application to import the NMC certificate to the PowerChute-keystore. To export the self-signed certificate from the NMC:

1. In a web browser, view the NMC certificate. For example, in Chrome, click  **> More tools > Developer tools** (CTRL+Shift+I). Click on the **Security** tab and click the **View Certificate** button.
2. Click on the **Details** tab and click the **Copy to File...** button.
3. Using the Certificate Export Wizard, export the certificate as a Base-64 Encoded X.509 .cer file.
4. Copy the .cer file to the group1 directory: `opt/APC/PowerChute/group1`
5. Import the certificate using `../jre_x64/bin/keytool -importcert -alias <nmc_ip_address> -keystore PowerChute-keystore -storepass <keystore_password> -file <nmc_.cer_file>`

Validate the Certificate in PowerChute-keystore

1. Launch a terminal or command prompt and change the directory to the group1 directory of where PowerChute is installed. If the default location was chosen during installation, this will be `opt/APC/PowerChute/group1`
2. Run the command: `../jre_x64/bin/keytool -list -v -keystore PowerChuteKeystore -storepass <keystore_password> -alias <nmc_ip_address>`
3. Search for "Certificate fingerprints" and note the SHA-1 value. For example: SHA1:
2D:94:62:DC:07:61:54:B8:56:D7:B5:71:B0:4B:A0:0A:1D:A8:1D:F5
4. Login to your NMC Web UI and navigate to **Configuration > Network > Web > SSL Certificate**.
5. Click **Valid Certificate** to view the certificate details.
6. Verify that the SHA-1 fingerprint value matches the value for the certificate in the PowerChute-keystore.

If the SHA-1 values match, set "`acceptCerts = false`" in the `[NetworkManagementCard]` section of the `pcnsconfig.ini` file, and restart the PowerChute service.

If the SHA-1 values do not match, delete the certificate from the PowerChute-keystore using the following command: `../jre_x64/bin/keytool -delete -alias <nmc_ip_address> -keystore PowerChute-keystore -storepass <keystore_password>`

Appendix 3: Adding the VxRail Manager Root CA Cert to PowerChute

NOTES:

- These steps are only valid for PowerChute v4.5. In v5.1, you can add the VxRail Manager certificates via the PowerChute Setup wizard.
- For VxRail 7.0.320 and above, you only need to import the vCenter Root certificates and not the VxRail Manager certificates.

Change the PowerChute-keystore Password

You must change the PowerChute-keystore password before you can add trusted root certificates to the keystore:

1. Stop the PowerChute service.
2. Open the PowerChute configuration file (`pcnsconfig.ini`) located in the `group1` directory.
3. In the section `[NetworkManagementCard]`, add the line `"PowerChuteKeystorePassword = <your_password>"`.
4. Save the `pcnsconfig.ini` file and start the PowerChute service.

Import Trusted Certificate

Follow the steps below to download and import a trusted VxRail root CA certificate to PowerChute:

1. Copy the root CA certificate from `/etc/vmware-marvin/ssl/rootcert.crt` via SCP on the VxRail Manager appliance.
2. Export the VxRail Manager server certificate using the VxRail API interface: `https://<ip_address>/rest/vxm/api-doc.html`
3. Click **Not secure** on the upper left-hand side of the screen, click **Certificate**, click **Details**, and click **Copy to File...** to open a wizard to download the VxRail CA certificate.
4. Extract the downloaded files for your operating system.
5. Stop the PowerChute service.
6. Open a command file prompt and change the directory to `/opt/APC/PowerChute/group1`
7. Import the root CA certificate using the command: `../jre_x64/bin/keytool -importcert -file vxrail.crt -keystore PowerChute-keystore -trustcacerts`
8. Start the PowerChute service.

Appendix 4: Adding the VxRail Manager SSL Certificate to PowerChute

NOTE: These steps are only valid for PowerChute v4.5. In v5.1, you can add the VxRail Manager certificates via the PowerChute Setup wizard.

1. Copy the VxRail Manager SSL certificate (e.g. `vxrail.crt`) to the machine where PowerChute is installed.
2. Stop the PowerChute service.
3. Open a command prompt and change the directory to `/opt/APC/PowerChute/group1`
4. Import the Dell VxRail cert using the command: `../jre_x64/bin/keytool -import -alias vxrail -file vxrail.crt -keystore PowerChute-keystore -alias vxrail`

NOTE: The SSL certificate must be imported using the alias “vxrail” or the connection to VxRail will be unsuccessful.

5. Start the PowerChute service.
6. PowerChute should be using the new signed certificate and you should not be presented with error messages regarding unsigned certificates.

Appendix 5: Creating Certificates with Subject Alternate Name (SAN) Entries

NOTE: These steps are only valid for PowerChute v4.5 and above.

Windows

1. Stop the PowerChute service.
2. Open the PowerChute configuration file (`pcnsconfig.ini`) and add "KeystorePassword=<new_password>" to the [NetworkManagementCard] section.
3. Save the `pcnsconfig.ini` file.
4. Re-start the PowerChute service.
5. Open a command prompt and change the directory to `C:\Program Files\APC\PowerChute\group1\`
6. Verify that the keystore password was successfully changed using the command:
`<path_to_jre>\bin\keytool.exe -list -v -keystore keystore -storepass <new_password>`
7. Stop the PowerChute service.
8. Delete the existing self-signed certificate from the keystore using the command: `keytool.exe -delete -alias securekey -keystore keystore`
9. Create a root CA cert using the command: `openssl req -x509 -sha256 -days 1825 -newkey rsa:4096 -keyout rootCA.key -out rootCA.crt`
10. Create a configuration file for the certificate signing request (`req.conf`), for example:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
C = IE
ST = Galway
L = Galway
O = PCNS
OU = SANPCNS
CN = <computer_name / fully_qualified_domain_name>
[v3_req]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = <fully_qualified_domain_name>
DNS.2 = <host_name>
```

DNS.3 = localhost

11. Create the certificate signing request (CSR) using the command: `openssl req -new -out pcns_san.csr -newkey rsa:4096 -nodes -sha256 -keyout pcns_san.key -config req.conf`
12. Sign the CSR using the root certificate using the command: `openssl x509 -req -days 365 -in pcns_san.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out pcns_san.crt -extfile req.conf -extensions v3_req`
13. Import the private key to the keystore:
 - a. `openssl pkcs12 -export -in pcns_san.crt -inkey pcns_san.key -out pcns_san.p12 -name securekey`

NOTE: When prompted for the export password, enter the password set for the keystore in step 2. If the private key password and the keystore passwords do not match, the web service will be unable to start with the error "java.security.UnrecoverableKeyException: Cannot recover key".
 - b. `<path_to_jre>\bin\keytool.exe -importkeystore -deststorepass <password> -destkeystore keystore -srckeystore pcns_san.p12 -srcstoretype PKCS12`
14. Import the root certificate to the PowerChute-keystore using the command: `keytool.exe -importcert -alias root -file rootCA.crt -keystore keystore`
15. Add the rootCA.crt into the web browser.

Linux

1. Stop the PowerChute service.
2. Open the PowerChute configuration file (`pcnsconfig.ini`) and add "KeystorePassword=<new_password>" to the [NetworkManagementCard] section.
3. Save the `pcnsconfig.ini` file.
4. Re-start the PowerChute service.
5. Open a command prompt and change the directory to `/opt/APC/PowerChute/group1`
6. Verify that the keystore password was successfully changed using the command: `../jre_x64/bin/keytool -list -v -keystore keystore`
7. Stop the PowerChute service.
8. Delete the existing self-signed certificate from the keystore using the command: `keytool -delete -alias securekey -keystore keystore`
9. Create a root CA cert using the command: `openssl req -x509 -sha256 -days 1825 -newkey rsa:4096 -keyout rootCA.key -out rootCA.crt`
10. Create a configuration file to the certificate signing request (`req.conf`), for example:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
C = IE
ST = Galway
L = Galway
O = PCNS
OU = SANPCNS
CN = <computer_name / fully_qualified_domain_name>
```



```
[v3_req]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = <fully_qualified_domain_name>
DNS.2 = <host_name>
DNS.3 = localhost
```

11. Create the certificate signing request (CSR) using the command: `openssl req -new -out pcns_san.csr -newkey rsa:4096 -nodes -sha256 -keyout pcns_san.key -config req.conf`
12. Sign the CSR using the root certificate using the command: `openssl x509 -req -days 365 -in pcns_san.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out pcns_san.crt -extfile req.conf -extensions v3_req`
13. Import the private key to the keystore:
 - a. `openssl pkcs12 -export -in pcns_san.crt -inkey pcns_san.key -out pcns_san.p12 -name securekey`
NOTE: When prompted for the export password, enter the password set for the keystore in step 2. If the private key password and the keystore passwords do not match, the web service will be unable to start with the error “java.security.UnrecoverableKeyException: Cannot recover key”.
 - b. `../jre_x64/bin/keytool -importkeystore -deststorepass <password> -destkeystore keystore -srckeystore pcns_san.p12 -srcstoretype PKCS12`
14. Import the root certificate to the PowerChute-keystore using the command: `keytool -importcert -alias root -file rootCA.crt -keystore keystore`
15. Add the rootCA.crt into the web browser.

Appendix 6: Reset the PowerChute virtual appliance root password

Follow the steps below to reset the PowerChute virtual appliance (AlmaLinux) root password. **NOTE:** For screenshots of these steps, please refer to the “Reset PowerChute Virtual Appliance Root Password” section in the [User Guide](#).

1. Open the VMware console.
2. Reboot the virtual appliance.
3. Press "e" during the boot process on the grub menu to enter the grub editor.
4. Use the arrow keys to move to the end of the line that starts with "linux" and add the following at the end of the line: "rd.break enforcing=0".
5. Press `Ctrl + X` to boot to emergency mode.
6. Mount the `/sysroot` directory with read and write permissions with the command `mount -o rw,remount /sysroot`.
7. Change the directory environment to `/sysroot`.
8. Use the command `passwd root` to set a new password for the root user.
9. Exit `sysroot` by typing the command `exit` and make the file system read-only again by typing the command `mount -o ro,remount /sysroot`.
10. Exit emergency mode and reboot the appliance.
11. Login using the new root password.

APC by Schneider Electric Worldwide Customer Support

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

- Visit the APC by Schneider Electric web site, 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.