Security Handbook

PowerChute Network Shutdown

990-91316-001

Publication Date: September, 2020

Schneider Electric

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.

Table of Contents

Appendix: Replacing the Default PowerChute SSL Certificate.....10

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 and uses the SHA-256 Signature Hash Algorithm. See **Appendix** 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 need to enable “Accept Untrusted SSL Certificates” to allow PowerChute to establish communication with the NMC if a self-signed cert is being used by the NMC.

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 Application Note #20 **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
- One symbol or special character
- The username also cannot be part of the password.

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-128-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** on the APC website.

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 acess.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.

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 Notes #180 **PowerChute Network Shutdown for VMware**, and #186 **PowerChute Network Shutdown in Advanced Redundant Setups.**

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.

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 **Hardening Guidelines** for more information.

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” 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. One of the configurable settings is the password for the root user – configuring this 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. For more information, see the PowerChute **Installation Guide** on the APC website.

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 Application Note #180 "**PowerChute Network Shutdown for VMware**."

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.

If connecting to a Nutanix cluster that requires a 256-bit cipher, the Java Cryptography Extension Policy Files must be installed. See Knowledge Base article **FA361427** available on the APC website for more information.

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.

All user credentials are stored in PowerChute using AES-128 bit encryption.

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 **https://www.apc.com/wp/?um=200**).

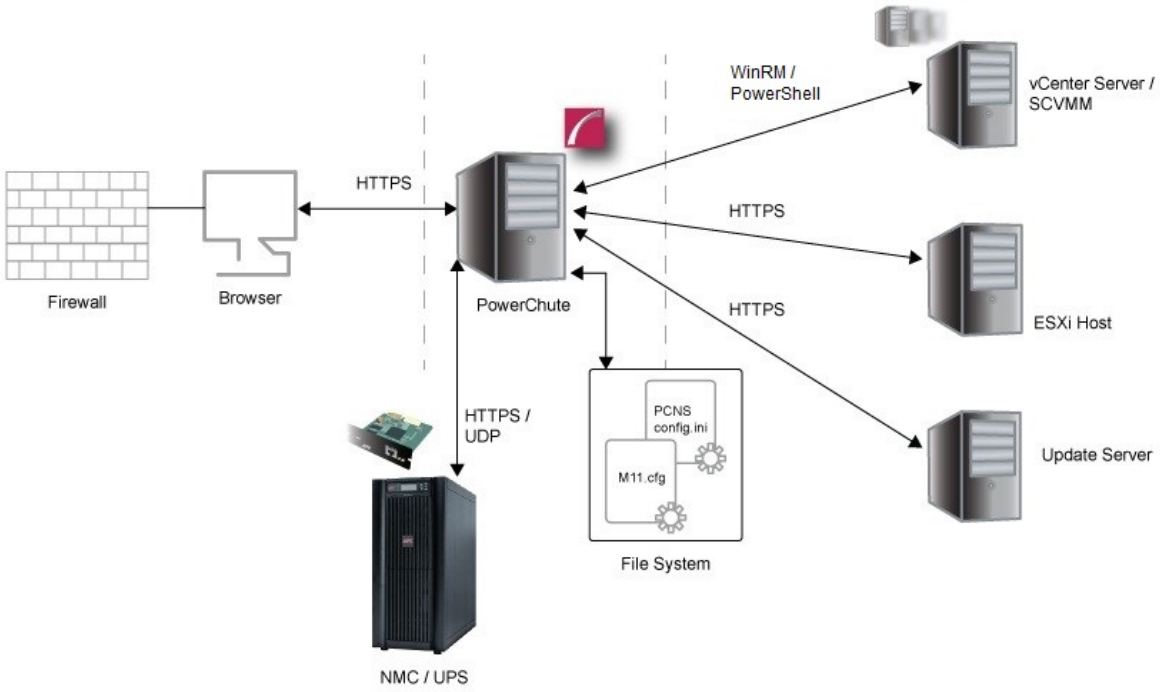
PowerChute also communicates with external VMware components using a secure HTTPS connection.

PowerChute uses a self-signed SSL Certificate by default that has a 2048-bit RSA public key and uses the SHA-1 Signature Hash Algorithm. The default self-signed cert can be replaced (see **Appendix** 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 using 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.



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** on the APC website 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**.

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, and backed up using the m11.bk file. User credentials can be restored 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

Product Center Page

The Product Center page is accessible via the Help menu in the PowerChute UI and contains links to important Knowledge Base articles.

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** on the APC website. 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 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.
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 these **manuals** 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 Guides 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. Import the Network Management Card SSL certificate to the PowerChute Keystore using the command: `<path_to_jre>\bin\keytool.exe -import -trustcacerts -alias root -file nmc.crt -keystore PowerChute-keystore`. Re-start the PowerChute service after importing the NMC SSL certificate.
3. During the Setup Wizard, on the Network Management Card connection page, ensure that the protocol used is HTTPS and port is 443. Ensure that the “Accept Untrusted SSL Certs” option is disabled.
4. Replace the default self-signed SSL certificate for the PowerChute UI using the instructions in **Appendix**.
5. 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`
6. It is recommended that Command files and SSH Action scripts are stored in a folder with appropriate security restrictions. Set permissions on the folder to allow PowerChute to run scripts in reaction to UPS events, but deny editing or deletion by non-administrative users.
7. Ensure that the file permissions set for the group1 folder and its contents allow read/write access only for trusted users and LocalSystem account on Windows and root account on Linux/Unix.
8. 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

9. 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** on the APC website for more information.
10. 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** on the APC website for more information.
11. 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. Please refer to APC Knowledge Base Article **FA290630** for more information on how to enable support for AES-192 and AES-256. Access Control should also be configured to restrict access to PowerChute via SNMP.
12. 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.
13. 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 follow **this guide** 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.

14. 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** on the APC website.

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: 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 displays 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 2048`” and press Enter.
5. Use the same password that was specified in step 3 in section “Changing the password for the Java Keystore”.
6. 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.scr`" and press Enter.
2. 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 option. This depends on the CA configuration.
3. 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`
   b. `configopenssl.cfg -infiles newpowerchute.csr`
   c. `rootca.crt` – This is the root CA certificate created when creating the CA.
   d. `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.
   e. `Openssl.cfg` – This is the OpenSSL configuration file.
   f. `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 PowerChute-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 PowerChute-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/pcnsconfig.ini/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 “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 “`<path_to_jre>/bin/keytool -list -v -keystore keystore`”
   c. Enter the password you specified in step 3 when prompted.
   d. Verify the keystore contents are displays 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 “`<path_to_jre>\bin\keytool -genkey -alias securekey -keyalg RSA -keystore keystore - keysize 2048`” and press Enter.
5. Use the same password that was specified in step 3 in section “Changing the password for the Java Keystore”.
6. 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 -certreq -alias securekey -keystore keystore -file newpowerchute.scr`” and press Enter.
2. 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 option. This depends on the CA configuration.
3. 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: `<path_to_jre>\bin\keytool -import –trustcacerts -alias root -file rootca.crt -keystore keystore`
5. Import the Web Server SSL cert using the command: `<path_to_jre>\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.

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.

990-91316-001 **9/2020**