PowerChute™ Network Shutdown Security Features & Deployment

By David Grehan, Sarah Jane Hannon

ABSTRACT

PowerChute™ Network Shutdown (PowerChute) software works in conjunction with the UPS Network Management Card (NMC) to provide graceful, unattended shutdown of multiple IT systems over a network.

This Application Note provides an overview of the security features in PowerChute including connectivity and authentication as well as information on secure deployment.

Applications

IT Server Rooms, Data Centers, Remote Branch Offices, Distributed Networks.

Customer Benefits

- Graceful network-based shutdown
- Run command file capability
- Event logging
- Secure communications
- Browser accessible
- Redundant UPS configuration support
- Parallel UPS configuration support
- HTTPS communications
- IPv6 support

Introduction

All APC by Schneider Electric software products are developed in adherence with key security principles, to deliver secure products protecting IT equipment.

This Application Note contains the following information:

by Schneider Electric

Connectivity

PowerChute Access

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

If enabled and configured, PowerChute can be accessed via SNMP v1 or v3. It is recommended to use SNMP v3 only as this provides Authentication, Privacy and Access Control.

PowerChute supports MD5/SHA-1/SHA-2 for Authentication and DES/AES-128/AES-192/AES-256 for Privacy when using SNMP v3.

PowerChute Network Shutdown provides secured browser access via HTTPS as default to ensure that communication via the web interface is secure and cannot be interpreted. Users do 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-1 Signature Hash Algorithm.

Please see Appendix A for details on how to replace SSL certificates for Windows and Linux.

Connectivity Protocol Definitions

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and the pages returned by the Web server.

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet.

Network Management Card Connection

The UPS Network Management Card (NMC) provides an interface between your APC UPS and your network. The NMC uses the HTTP protocol by default. This can be changed to HTTPS through the NMC user interface. 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.

Based on the NMC protocol used, you can select either HTTP or HTTPS in PowerChute. This can be changed via the PowerChute setup wizard following installation if required on the UPS Details screen.

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 information to PowerChute Network Shutdown via UDP packets which are limited to a few hundred bytes.

For a detailed description on how UPS information is sent over the network and how PowerChute receives NMC updates, please see Application Note #20 “The Communications Process of PowerChute Network Shutdown”.

Authentication

PowerChute User Interface

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

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

Password Recommendations

Upon launching the PowerChute Setup Wizard, the Username, Password and Authentication Phrase can be set via the Security Details page. Password complexity is not enforced, though setting a password with a minimum of 8 characters comprising numbers, letters and at least one special character is recommended.

The Username, Password and Authentication phrase are all stored using AES-128-bit encryption. Prior to executing the Setup Wizard, the default Authentication Phrase should be changed on each Network Management Card that PowerChute will communicate with. The Username, Password and Authentication Phrase can be reset via the pcnconfig.ini file. Therefore, only trusted user accounts should be granted write-access to this file.

Account Lock-Out

PowerChute will automatically "lock out" after three unsuccessful log-in attempts (incorrect User ID and/or Password) to prevent remote password cracking. Each lockout is logged to the Event log and the UI is inaccessible for two minutes and displays "Account is locked out".

User Control

PowerChute allows you to create one administrator account only. This account has a unique log-in user name 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.

To ensure secure user control it is recommended that PowerChute is not available on a public-facing network segment.

NMC Connection

The communications mechanism between the NMC and PowerChute Network Shutdown uses an MD5-based authentication scheme (Hash-based Message Authentication Code), which has the goals of:

- Ensuring that the password is never sent in plain text.
- Proving that the sender of a message is an authentic user as only those with knowledge of the password phrase can send valid messages.
- Detecting if a message has been tampered with in transit.
- Detecting if a message is being replayed.

The Authentication Phrase must be between 15 and 32 ASCII characters.

A well configured firewall and solid security policy is integral to the security of any network as this does not guarantee:

- That all data is encrypted.
- That a brute-force attack will fail to determine the password phrase.
- Prevention of most Denial of Service attacks

External User Credentials

When VMware support is enabled and PowerChute is configured to protect Hosts that are managed by vCenter Server a username and password are required. These details are stored in PowerChute using AES-128 bit encryption. The VMware user account requires certain permissions in order to execute Virtualization Tasks – for a listing of the required permissions for this account please refer to FA177822 in the Schneider Electric Knowledge Base. 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 please refer to the Application Note #180 – "PowerChute Network Shutdown for VMware"

When Nutanix support is enabled, to authenticate your connection to the Nutanix Controller Virtual Machine or Cluster, an IP address, CVM/Cluster password and AHV Host password are required, or an SSH key file path and its passphrase are required. These details are stored in PowerChute using AES-128 bit encryption. **Note**: To connect PowerChute to the Nutanix Cluster/CVM, the 'Nutanix' user account credentials must be used. You cannot use the 'admin' user account credentials.

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.

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, please see http://www.apc.com/whitepaper/?um=200).

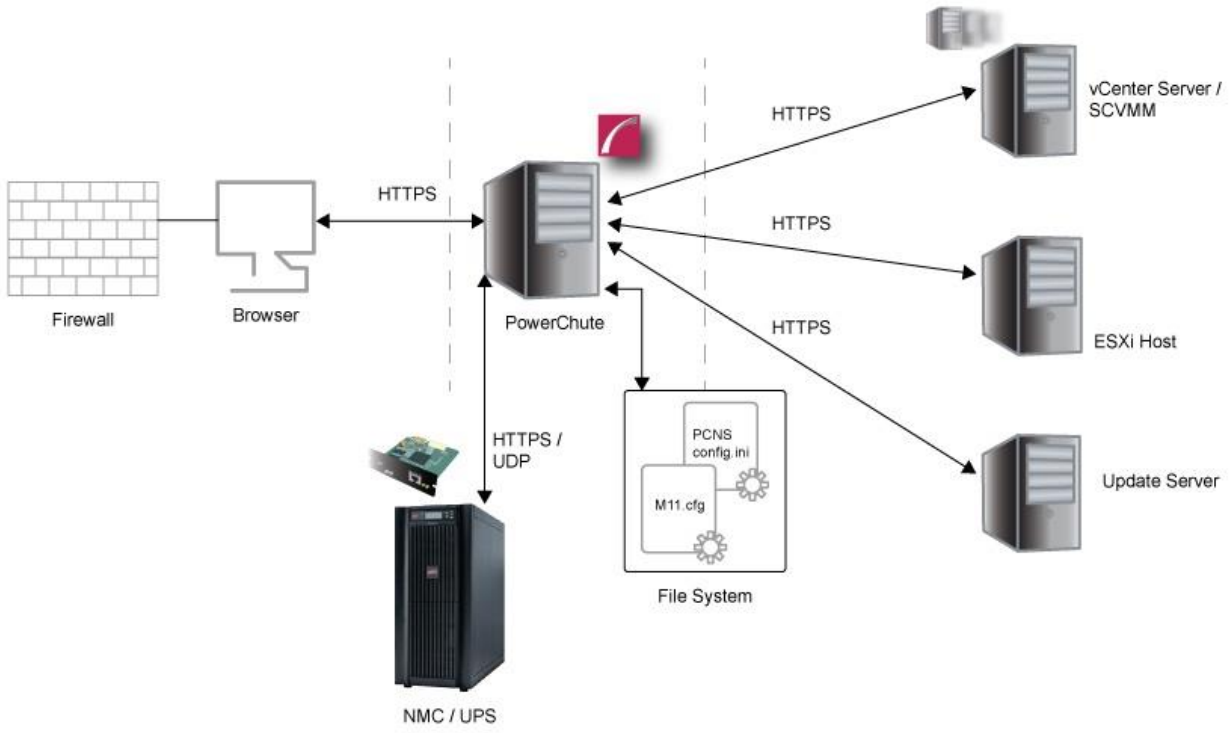
PowerChute also communicates with external VMware components using a secure HTTPS connection.

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 A for detailed instructions).

PowerChute communicates with the Network Management Card using HTTP/HTTPS for registration and control tasks. It receives status updates from the UPS/NMC via UDP packets sent to port 3052. For more information on how to harden security for PowerChute and the NMC please refer to Appendix B.

PowerChute stores configuration information on the local file system using the pcnsconfig.ini file and user credentials using the m11.cfg file.

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 3rd Party Root Certification Authority.



Java Runtime Environment (JRE)

JRE Utilization

PowerChute Network Shutdown installs a custom JRE to operate. PowerChute is shipped with an up-to-date private JRE as each new PowerChute version is released.

PowerChute Network Shutdown uses the following java modules:

java.base	java.compiler
java.desktop	java.naming
java.scripting	java.instrument
java.sql java.xml	java.logging
jdk.crypto.cryptokijdk.zipfs	java.rmijava.management

Use the Java Update feature to update the JRE used by PowerChute, as JRE software updates and security fixes are regularly released. See the PowerChute Network Shutdown User Guide available on the APC website for more information.

For more information on JRE versions included with and supported by PowerChute Network Shutdown, please refer to the 'Operating System, Processor, JRE and Browser Compatibility Chart' available from the APC website at: http://www.apc.com/whitepaper/?um=200

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 and are encrypted using AES-128 bit encryption. User credentials can be restored via the pcnsconfig.ini file.

Vulnerability Reporting & Management

How to report a Vulnerability

Cyber security incidents and potential vulnerabilities can be reported to Schneider Electric using the following link:

https://www.schneider-electric.com/en/work/support/cybersecurity/report-an-incident.jsp

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.

Appendix A – 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 PCNS 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 public JRE or `C:\Program Files\APC\PowerChute\jre_x64|jre_x32` if private JRE was selected during the installation)

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 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 return.
5. Use the same password that was specified in step 3 in section “Changing the password for the Java Keystore”.
6. Verified 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. Enter the required values when prompted – the first 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.
3. Use the .CSR file to create a new certificate 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 the file created in step 1.

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

Replacing the Default PowerChute SSL Certificate - continued

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 PCNS service.
3. Open a command prompt and change directory to `C:\Program Files\APC\PowerChute\group1 folder`
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.
7. Start the PCNS service.
8. PowerChute should be using the new signed certificate and there should not be an SSL Cert security warning displayed by the browser when the PowerChute Web Interface is launched.

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 using the command “service PowerChute stop”.
2. Open `/opt/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 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 displayed without error. (`<path_to_jre>` is the location of the public JRE or `/opt/APC/PowerChute/group1/jre_x64|jre_x32` if private JRE was selected during the installation)

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 directory to `/opt/APC/PowerChute/group1`
4. Type “`<path_to_jre>/bin/keytool -genkey -alias securekey -keyalg RSA -keystore keystore - keysize 2048`” and press return.
5. Use the same password that was specified in step 3 in section “Changing the password for the Java Keystore”.
6. Verified that the file keystore now exists in the group1 folder.

Replacing the Default PowerChute SSL Certificate - continued

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.csr`" and press Enter.
2. Enter the required values when prompted – the first 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.
3. Use the .CSR file to create a new certificate 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 PCNS service.
3. Open a command prompt and change directory to `/opt/APC/PowerChute/group1` folder.
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.
7. Start the PCNS service.
8. PowerChute should be using the new signed certificate and there should not be an SSL Cert security warning displayed by the browser when the PowerChute Web Interface is launched.

> ⚠ **Note**
>
> If using Microsoft Active Directory Certificate Services and you see error
>
> "keytool error: java.lang.Exception: Incomplete certificate chain in reply"
>
> please see the following post:
>
> What do I do when keytool.exe can't establish a certificate chain from my certs?

Appendix B – Security Hardening for PowerChute and Network Management Card

Recommended configuration changes to increase security for PowerChute communication with the Network Management Card.

Network Management Card

1. Change the default Authentication Phrase via Configuration->Shutdown->PowerChute Shutdown Parameters.
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.** Please refer to these manuals for more information.
4. Replace the default self-signed SSL certificate with the new one via Configuration->Network->Web->SSL Certificate.
5. Please see the Security Guides for the Network Management Cards for more information on how to secure them – available here.

PowerChute Network Shutdown

1. 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.
2. During the Setup Wizard, on the Network Management Card connection page, change the protocol to HTTPS and port to 443. Disable the option “Accept Untrusted SSL Certs”.
3. Replace the default self-signed SSL certificate for the PowerChute UI using the instructions in Appendix A.
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. 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.
6. 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.
7. Prevent Remote Access to the Web UI if this is not required using a firewall rule for TCP ports 3052 ad 6547. To prevent Denial of Service attacks such as the SSL THC DOS 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.
8. 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 available on the APC Website for more information.
9. If using SNMP with PowerChute, it is recommended to only use SNMP v3 and to choose SHA-2 and AES-128 or higher for Authentication and Privacy. 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.
10. The PowerChute Network Shutdown virtual appliance enables SSH services by default. If you do not require remote SSH access to the virtual appliance, it is recommended you disable this service. To disable SSH services, issue the following commands as the root user:

```
systemctl stop sshd

systemctl disable sshd
```

    Where access is required, it is recommended that you follow this guide to harden the SSH service.