# Security Handbook

## PowerChute™ Serial Shutdown

**TME11287-001**

**Publication Date: March, 2023**

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

# Overview

## Content and Purpose of this Guide

This guide documents the security features in PowerChute™ Serial 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.

PowerChute uses a self-signed SSL Certificate by default that has a 2048-bit RSA public key and uses the SHA-512 Signature Hash Algorithm. See **Appendix** for details on how to replace SSL certificates for Windows.

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.

### Authentication & Password Requirements

During PowerChute installation, you must enter a username and password which will be used to log on to the PowerChute UI. The username must be between 6 and 128 characters in length, and the password requires:

- Minimum 8 and maximum 128 characters in length
- One upper and lower case letter
- One number or special character (#?!@$%^*-)
- The username also cannot be part of the password.
- The username and password can only contain US-ASCII characters. It is not supported to include whitespace.

No password or passphrase is stored in PowerChute in plain text. The username and password 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 pcssconfig.ini file. For information on how to reset your credentials, see the **PowerChute Serial Shutdown User Guide** on the APC website.

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

It is not recommended to delete the pcssconfig.ini, pcssconfig_backup.ini, m11.cfg, or m11.bk files from the installation directory. Deleting these files will result in the PowerChute service not starting, and PowerChute must be uninstalled and re-installed.

It is recommended to delete the silentInstall.ini file after successful installation. It contains the PowerChute Serial Shutdown credentials in plain text. The installer does not modify the INI file during installation.

### Watchdog Features

#### Account Lock-Out

PowerChute will automatically “lock out” for 2 minutes after three unsuccessful login attempts (incorrect username and/or password) to prevent brute force password cracking.

### Automatic Logout

By default, the PowerChute session times out after 15 minutes of inactivity and users will be automatically logged out of the PowerChute UI.

### Multiple Logins

Only one user can be logged in to the PowerChute UI at a time. Multiple logins are not supported, and login attempts while the user is already logged in will be unsuccessful.

Logins, logouts, and unsuccessful login attempts to the PowerChute UI are configurable events in the **Event Configuration** screen. For more information, see the **User Guide**.

## 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.

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

## 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.

## Physical Access

It is strongly recommended that PowerChute is deployed in a secure location, where the PowerChute server and connected UPS are protected by physical restraints that prevent unauthorized access, and where access is restricted to those who maintain the equipment.

## Third Party Licenses

Third party licenses used in PowerChute Serial Shutdown are available to view in the THIRDPARTYLICENSEREADME.txt file in the Agent directory. If the default location was chosen during installation, this text file can be found at:

- `C:\Program Files\APC\PowerChute Serial Shutdown\agent` for Windows systems

# PowerChute Serial Shutdown - Communication/Access Model

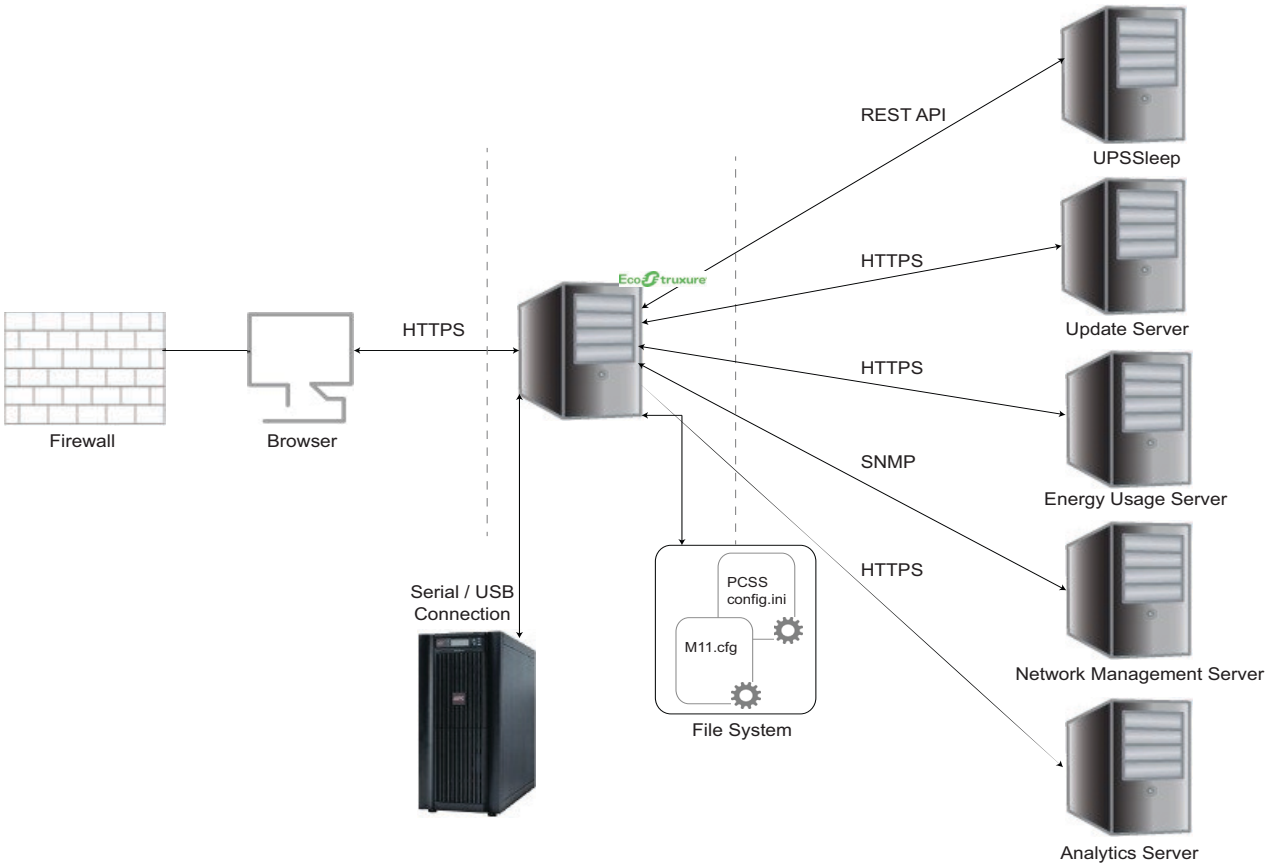
The diagram below represents the access points to PowerChute Serial Shutdown and its communication paths with external components such as the UPSSleep utility. PowerChute is primarily accessed via a secure HTTPS connection using a supported web browser (for the latest browser details, see **https://www.apc.com/wp/?um=100**).

PowerChute uses a self-signed SSL Certificate by default that has a 2048-bit RSA public key and uses the SHA-512 Signature Hash Algorithm. The default self-signed cert can be replaced (see **Appendix** for detailed instructions).

PowerChute stores configuration information on the local file system using the pcssconfig.ini file and user credentials using the m11.cfg file. Administrator access is required on all operating systems to access these files.

It is not recommended to delete the pcssconfig.ini, pcssconfig_backup.ini, m11.cfg, or m11.bk files from the installation directory. Deleting these files will result in the PowerChute service not starting, and PowerChute must be uninstalled and re-installed.

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.



# Java Runtime Environment (JRE)

## JRE Utilization

PowerChute Serial Shutdown installs a custom JRE to operate. PowerChute is shipped with the latest version of **Adoptium OpenJDK** Java at the time of release.

PowerChute uses the following Java modules:

| | |
|---|---|
| java.base | java.compiler |
| java.datatransfer | java.desktop |
| java.instrument | java.logging |
| java.management | java.naming |
| java.prefs | java.security.jgss |
| java.security.sasl | java.sql |
| java.transaction.xa | java.xml |
| jdk.crypto.cryptoki | jdk.crypto.ec |
| jdk.localedata | jdk.unsupported |
| jdk.xml.dom | |

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 Serial Shutdown User Guide** on the APC website for more information.

For more information on JRE versions included with and supported by PowerChute Serial Shutdown, refer to the **Operating System, Processor, JRE and Browser Compatibility Chart**.

# Secure Backup Recommendations

## INI File

Some configuration settings, such as scheduled shutdowns, SNMP settings, and language settings, applied via the User Interface are stored on the local file system using the pcssconfig.ini file. A backup of this file (pcssconfig_backup.ini) is also stored.

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 pcssconfig.ini file. Administrator access is required on Windows operating systems to access these files.

It is not recommended to delete the pcssconfig.ini, pcssconfig_backup.ini, m11.cfg, or m11.bk files from the installation directory. Deleting these files will result in the PowerChute service not starting, and PowerChute must be uninstalled and re-installed.

# 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 Notifications and Patches

Schneider Electric regularly posts **security notifications** with information on vulnerabilities and available patches. Subscribe to our **newsletter** to receive security notifications.

## Product Center Page

The **Product Center page** is accessible via the PowerChute menu in the web user interface 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 in the **Quick Status** and **About** screens and the **Event Log**. Software updates must be applied manually.

**NOTE:** The Updates Notification feature will only work if the Enable PowerChute Updates checkbox in the **Preferences** screen is selected.

## Software Integrity

All PowerChute Serial Shutdown web downloads include a list of MD5 and SHA-256 hash values that can be validated for authenticity using the **MD5/SHA-1/SHA-256 Hash Signature Reference Guide** on the APC website. In addition, the Windows installer is digitally signed.

For Windows, in addition to the installer, the following files are digitally signed:

| | |
|---|---|
| agent\pbeagent.exe | agent\bin\SysLogger.exe |
| agent\lib\win*.dll | agent\systemlogger\EventMessage.dll |
| agent\comp*.jar | agent\lib\application.jar |
| agent\lib\m11.jar | agent\lib\pcss_ds.jar |
| agent\lib\util.jar | agent\Resources*.jar |

.EXE and .DLL file signatures can be verified by navigating to the file in Windows File Explorer. Right-click on the file, and click **Properties**. The **Digital Signatures** tab includes the signature details.

.JAR file signatures can be verified using the jarsigner tool. This jarsigner tool is not part of the stripped OpenJDK version installed with PowerChute. If you do not have a full JDK installed on your system, you can download one that contains the jarsigner tool from **https://adoptium.net/**. For more information, consult the **jarsigner tool documentation**.

# Security Hardening and Removal Guidelines

This section includes recommended configuration changes to increase security for PowerChute.

## Security Hardening Guidelines

1. Change the credentials for the PowerChute-keystore via the pcssconfig.ini file. See **Changing the Password for the Java Keystore**.
2. Replace the default self-signed SSL certificate for the PowerChute UI using the instructions in **Appendix**.
3. Change the default password for the CACERTS keystore located below using the command: `keytool.exe -storepasswd -new <new password> -keystore cacerts -storepass changeit`
   - **Windows:** C:\Program Files\APC\PowerChute Serial Shutdown\jre\lib\security\cacerts
4. Ensure that the file permissions set for the jre folder and its contents allow read/write access only for trusted users and LocalSystem account on Windows.
5. Prevent Remote Access to the Web UI if this is not required using a firewall rule for TCP port 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.
6. Use the Java Update feature in PowerChute to update the JRE regularly as software updates and security fixes are released. See the **PowerChute Serial Shutdown User Guide** on the APC website for more information.
7. 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.
8. It is recommended that command files 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.

## Secure Removal Guidelines

For information on how to uninstall PowerChute Serial 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 **FA159894**.

# Appendix: Replacing the Default PowerChute SSL Certificate

PowerChute stores the Web Interface SSL certs in a Java keystore file located in the agent directory:

- **Windows:** `C:\Program Files\APC\PowerChute Serial Shutdown\agent\keystore`

This appendix outlines how to replace the default PowerChute SSL certificate in the Java keystore.

## Changing the Password for the Java Keystore

To change the password for the keystore:

1. Stop the PowerChute service via the services console – PowerChute Serial Shutdown – or using the command `net stop APCPBEAgent`
2. Open `C:\Program Files\APC\PowerChute Serial Shutdown\agent\pcssconfig.ini`
3. In the section `[Credentials]`, and add the line `KS_Access_Data = keystore_password`. (`keystore_password` can be replaced with a password of your choice. It must be at least 6 characters). Save the INI file.

   **NOTE:** The `KS_Access_Data` value must match the keystore password provided in step 4 of **Create a new Keystore for the trusted SSL cert**.
4. Start the PowerChute service via the services console – PowerChute Serial Shutdown – or using the command `net start APCPBEAgent`
5. Verify that the keystore password has been changed:
   a. Open a command prompt window and change directory to `C:\Program Files\APC\PowerChute Serial Shutdown\agent`
   b. Type "`<path_to_jre>\bin\keytool.exe -list -v -keystore keystore`" (`<path_to_jre>` is `C:\Program Files\APC\PowerChute Serial Shutdown\jre` to use the JRE that ships with PowerChute Serial Shutdown, or any public JRE can be used).
   c. Enter the password you specified in step 3 when prompted.
   d. Verify the keystore contents are displays without error.

## Create a new Keystore for the trusted SSL cert

1. Stop the PowerChute service via the services console – PowerChute Serial Shutdown – or using the command `net stop APCPBEAgent`
2. Delete the existing keystore file – `C:\Program Files\APC\PowerChute Serial Shutdown\agent\keystore`
3. Open a command prompt and change the directory to `C:\Program Files\APC\PowerChute Serial Shutdown\agent`
4. Type "`..\jre\bin\keytool -genkey -alias securekey -keyalg RSA -keystore keystore -keysize 2048`" and press Enter to create a new keystore and private key. Use the same password that was specified in step 3 in section **Changing the Password for the Java Keystore**.

   **NOTE:** The "first and last name" specified must match the hostname or FQDN (Fully Qualified Domain Name) of the server where PowerChute is installed. For example: localhost.
5. Type "`..\jre\bin\keytool -list -v -keystore keystore -storepass <password_provided>`" to verify that the keystore now exists in the agent folder.

   **NOTE:** The keytool generates a self-signed certificate using the private key. This can be updated with a signed certificate signing request (CSR) if required. See **Create a certificate signing request (CSR) and a new SSL cert signed by a Trusted CA**.
6. Start the PowerChute service via the services console – PowerChute Serial Shutdown – or using the command `net start APCPBEAgent`

## Create a certificate signing request (CSR) and a new SSL cert signed by a Trusted CA

1. Type "`..\jre\bin\keytool.exe -certreq -alias securekey -keystore keystore -file newpowerchute.scr`" and press Enter to create a CSR from the private key and self-signed cert in the keystore. You will be prompted to enter the keystore's password specified in step 4 of **Create a new Keystore for the trusted SSL cert**.
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.

## Create your own certificate authority (CA) and sign the CSR

For more information, see Knowledge Base article **FA410362** on the APC website.

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

1. Copy `ca.crt` and `newpowerchute.crt` to `C:\Program Files\APC\PowerChute Serial Shutdown\agent`.
2. Stop the PowerChute service via the services console – PowerChute Serial Shutdown – or using the command `net stop APCPBEAgent`.
3. Open a command prompt and change the directory to `C:\Program Files\APC\PowerChute Serial Shutdown\agent`
4. Import the root CA cert using the command: `..\jre\bin\keytool.exe -import -trustcacerts -alias root -file rootca.crt -keystore PowerChute-keystore`

   You will be prompted to enter the keystore's password specified in step 4 of **Create a new Keystore for the trusted SSL cert**, and asked to confirm that you trust the cert.
5. Import the Web Server SSL cert using the command: `..\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). For more information, see Knowledge Base article **FA410362** on the APC website.
7. Start the PowerChute service via the services console – PowerChute Serial Shutdown – or using the command `net start APCPBEAgent`
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?**

# 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.



**TME11287-001** **03/2023**