

PowerChute Network Advanced

User Guide

JPU06873

08/2026

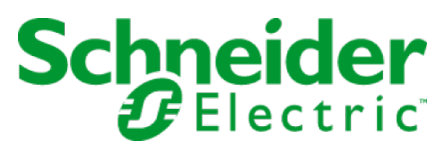


Table of Contents

Legal Information.....	4
Introduction.....	5
Installation	
Prerequisites Checklist.....	7
Prerequisites by Environment	10
Preliminary Steps for Installation.....	11
Installing on Windows.....	12
Log in to PowerChute Network Advanced.....	12
Uninstalling on Windows	14
Home	15
Virtual Environment	
Nutanix AHV	17
Nutanix Shutdown Sequence	19
Nutanix Startup Sequence	21
Custom Platform.....	22
Triggers	27
UPS Configuration	
Create UPS Configuration.....	28
Update UPS Configuration	30
Delete UPS Configuration	30
License	
License Prerequisites	32
Activate License	32
Increase License Quantity.....	33
Decrease License Quantity	33
Return License	33
Deployment	
Check Deployment Status.....	34
Import Deployment	35
Delete from UPS	35
Logs.....	36
Testing	37
Security Information and Recommendations	
Java Runtime Environment (JRE).....	39
Digital Signature Verification	39

PowerChute Network Advanced

User Credentials..... 40

Vulnerability Reporting and Management 40

Security Hardening Guidelines..... 42

Secure Removal..... 43

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric and its subsidiaries referred to in this document are the property of Schneider Electric or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

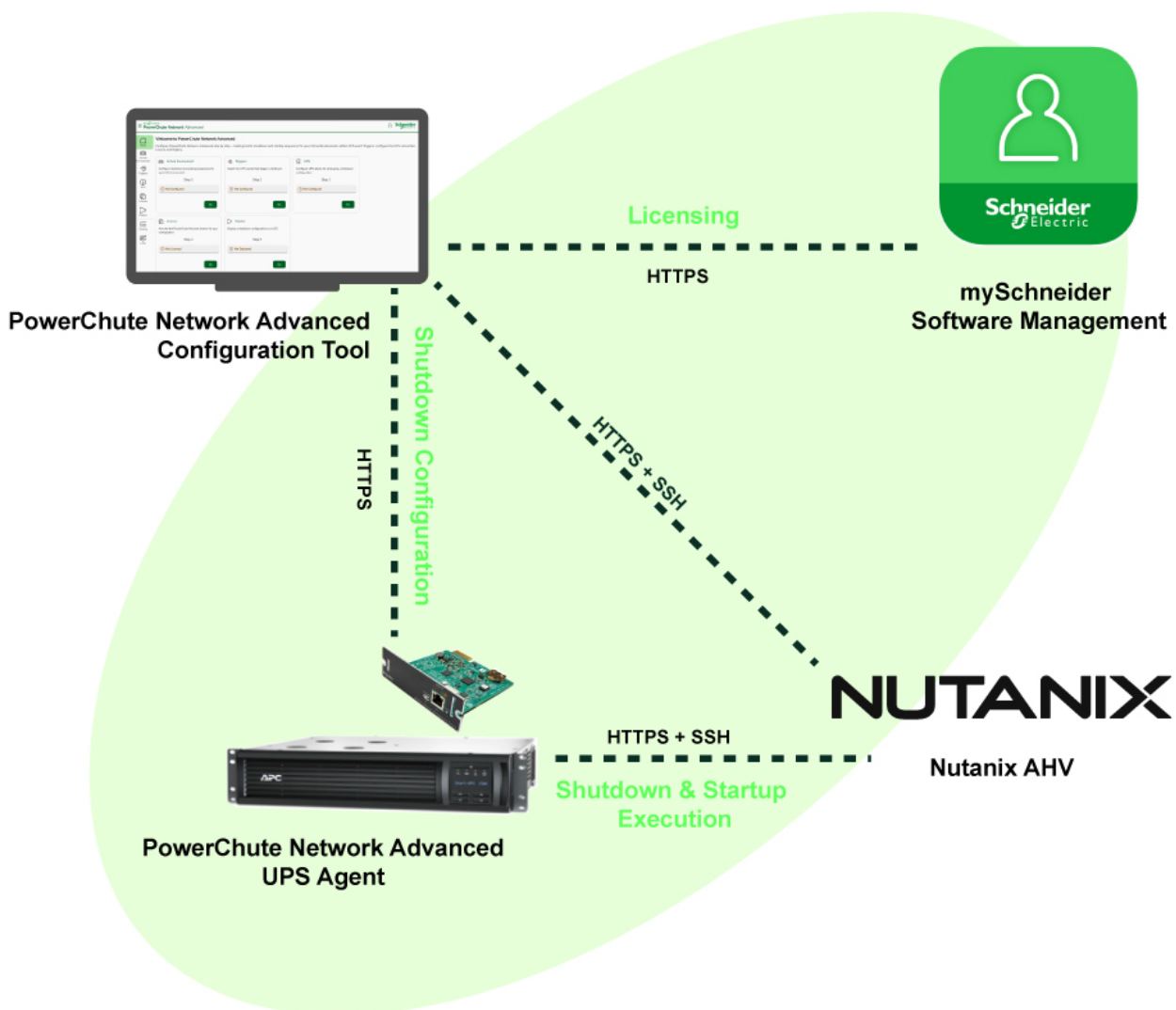
Introduction

PowerChute™ Network Advanced provides graceful network-based shutdown of Hyperconverged Infrastructure (HCI), virtual servers, and network devices.

The **PowerChute Network Advanced Configuration Tool** can be installed on a Microsoft Windows® device. The Configuration Tool is used to create and deploy a configuration (containing virtual environment details, shutdown/startup instructions, SSL certificates, SSH fingerprints) to the PowerChute Network Advanced **UPS Agent** on the Network Management Card (NMC). This equips the UPS Agent with a configured response to a UPS critical event.

In the case of a UPS critical event, the PowerChute Network Advanced UPS Agent on the Network Management Card (NMC) performs a graceful, unattended system shutdown of HCI clusters before the UPS battery is exhausted, without interaction with the Configuration Tool.

The diagram below represents the access points to PowerChute Network Advanced and its communication paths with external components such as Nutanix AHV®. The PowerChute Configuration Tool is accessed via a secure HTTPS connection using a supported web browser.



Installation

The following sections describe the prerequisites and steps to install the PowerChute Network Advanced Configuration Tool.

In this chapter:

- [Prerequisites](#)
- [Prerequisites by Environment](#)
- [Preliminary Steps for Installation](#)
- [Installing on Windows](#)
- [Uninstalling on Windows](#)

Prerequisites Checklist

Before you install PowerChute Network Advanced, check that you have the following prerequisite requirements in place.

Software Requirements

- A supported operating system and browser as listed on the [Operating System and Compatibility Chart](#).
- Administrator privileges are required to run the PowerChute installer.

Subscription License

Check that you have purchased the correct number of PowerChute subscription licenses for your virtual infrastructure. If you do not have a valid subscription license, you can purchase one using the part numbers below:

Part Number	License Description
SWPCNS1Y-DIGI	PowerChute Network Subscription, 1-year.
SWPCNS3Y-DIGI	PowerChute Network Subscription, 3-year.
SWPCNS5Y-DIGI	PowerChute Network Subscription, 5-year.
SWPCNS6Y-DIGI	PowerChute Network Subscription, 6-year.
SWPCNS7Y-DIGI	PowerChute Network Subscription, 7-year. Note: This part number is available for purchase with Schneider Electric IT Partners in Japan only.

Note:

- Subscription License part numbers for both PowerChute Network Advanced and PowerChute Network Shutdown are the same.
- A PowerChute Network Advanced subscription Activation ID can be used in the Secure NMC System Tool to download and deploy required firmware updates. See [Preliminary Steps for Installation > Updating the NMC firmware with the Secure NMC System Tool](#)

PowerChute Configuration Tool

The Configuration Tool user interface (UI) is accessible via a secured web browser via HTTPS and supports TLS v1.2 or 1.3 which provides authentication and encrypted communication for sensitive communications. HTTP is not supported.

- PowerChute uses a self-signed SSL Certificate by default that has a 4096-bit RSA public key, and uses the SHA-256 Signature Hash Algorithm.
See Knowledge Base article [FAQ000283328](#) for details on how to replace the default self-signed certificate for the PowerChute Configuration Tool.

Network Management Card Connection

A UPS Network Management Card (NMC) provides an interface between your Schneider Electric UPS and your network. To establish communications between PowerChute and the NMC, HTTPS must be enabled on the NMC. See [Preliminary Steps for Installation > Updating the NMC firmware with the Secure NMC System Tool](#)

You must know the IP address of the NMC. The NMC must have PowerChute Network Advanced compatible firmware installed:

NMC Platform	Embedded or Pre-Installed	Firmware Version
NMC3	Embedded in Smart-UPS or installed AP9640 / AP9641 / AP9643	View the Operating System and Compatibility Chart for more information on applicable firmware versions.

- PowerChute Network Advanced access enabled on NMC. In the NMC web interface, go to **Configuration > Shutdown** to review the access setting. It is enabled by default.
- The NMC uses a self-signed SSL certificate by default when HTTPS is enabled. Refer to the [NMC 3 Security Handbook](#) for details on how to create a new SSL certificate.
- The communication mechanism between the NMC and PowerChute provides security measures:
 - User credentials are never sent in plain text.
 - PowerChute will only process communication from a trusted and authenticated Network Management Card

Firewall

PowerChute needs to be able to connect to the NMC Web Access port. The default is port 443.

Note: 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.

Network Time Protocol (NTP)



Both the Network Management Card and the computer on which the Configuration Tool is installed are required to be synchronized with NTP for successful communication. **A time discrepancy of greater than ten minutes will prevent successful UPS communication and configuration deployment, even if the UPS Configuration has a Connected status.**

Recommendations:

- Follow the steps documented at [NMC User Guide > General menu > Date/Time screen](#) to configure NTP on the NMC.
- On the PowerChute Configuration Tool installation machine, check the Windows **Date & Time** configuration to synchronize the clock.

Prerequisites by Environment

Nutanix AHV Prerequisites

External User Credentials

To authenticate the connection to Nutanix Prism Central, an IP address/Hostname, Port, Cluster Name and administrator username and password are required.

To authenticate the connection to Nutanix Prism Element, the Cluster administrator username and password are required.

Note: To connect PowerChute to the Prism Element and Prism Central VMs, the “nutanix” user account credentials for each must be used. You cannot use the “admin” user account credentials as this account does not have the necessary permissions for shutdown tasks.

Preliminary Steps for Installation

Perform these steps **before** installing and using the PowerChute Network Advanced Configuration Tool.

Updating the NMC firmware with the Secure NMC System Tool

Before installing PowerChute Network Advanced, update the Network Management Card (NMC) to the latest PowerChute-compatible firmware using the Secure NMC System Tool:

1. Install the Network Management Card (NMC) in your UPS and configure it with an IP address.
For installation instructions, see the [Network Management Card Installation Guide](#) and [Prerequisites](#).
2. During [UPS Configuration](#), PowerChute will check that the NMC has a compatible firmware version installed. If the firmware requires an update, you are prompted to download and install the Secure NMC System Tool: <https://www.se.com/ww/en/product/SFNMC3SNST/>
 - For more information, see the [Secure NMC System Tool User Guide](#).
 - To view the PowerChute Network Advanced compatible firmware for your NMC device, see the [Operating System and Compatibility Chart](#)
 - A PowerChute Network Advanced subscription Activation ID can be used in the Secure NMC System Tool to download and deploy required firmware updates.

Installing on Windows

1. Download the PowerChute installation executable file, **PCNASetup.exe**, from the [Schneider Electric website](#).

Note: You must have administrator rights to run the installer.

2. **Verify the digital signature** of the installer file. See [Digital Signature Verification](#).
3. To install on Windows, double-click on the file and extract it.
4. At the welcome dialog, click **Next** to continue.
5. At the License Agreement dialog, review the license terms, and click **I Agree** to continue.
6. PowerChute Network Advanced is installed at the following location:

C:\Program Files\Schneider Electric\PowerChute Network Advanced

7. Click **Finish** to close the installer.

Log in to PowerChute Network Advanced

1. Upon installation, a PowerChute Network Advanced shortcut is added to the Desktop and Start menu. Click it to open a browser and visit **https://localhost/**

As PowerChute uses a self-signed certificate by default, you are notified that the connection is not private. Click **Proceed to localhost**, or the equivalent option in your chosen browser.

2. At first login, a file named bootstrap-credentials.txt is created by PowerChute in the installation directory at the following location:

C:\Program Files\Schneider Electric\PowerChute Network Advanced\config\

Open the file to get the initial password for first login.

3. On the PowerChute login page, enter a chosen username and the password provided in step 2 above .
4. You are immediately prompted to create a secure password that meets the following requirements:
The password requires **a minimum 8 and maximum 128 characters** in length.

Note: Full administrative access to PowerChute is provided only when you create a new password.

Changing your password

To change your password:

1. Click the user icon



2. Select **Change Password**

3. Enter your current password and your new chosen password.

Note: The password requires **a minimum 8 and maximum 128 characters** in length.

4. Click the **Change Password** button to save your changes.

See also: [Security Recommendations > Reset your Password](#)

Uninstalling on Windows

Note: Before you uninstall PowerChute Network Advanced, it is required to first return your license. See [Licensing > Return License](#)

If you do not return your license before uninstalling, it is necessary to contact [Customer Support](#) to retrieve the license.

There are two ways to uninstall PowerChute Network Advanced:

- On Windows, go to **Settings > Apps > Installed Apps > PowerChute Network Advanced**. In the More Options menu, click **Uninstall**.
- Alternatively, you can run the **Uninstall.exe** file included in the PowerChute installation directory:

C:\Program Files\Schneider Electric\PowerChute Network Advanced\Uninstall.exe

Home

The Home view provides a dashboard overview of your PowerChute Network Advanced configuration, and provides a step-by-step approach to completing your configuration for deployment to the PowerChute UPS Agent:

1. [Virtual Environment](#)
2. [Triggers](#)
3. [UPS Configuration](#)
4. [License](#)
5. [Deployment](#)

The screenshot shows the 'PowerChute Network Advanced' dashboard. At the top, there's a header with the 'EcoStruxure' logo and the product name. On the right is the 'Schneider Electric' logo. A left sidebar contains navigation icons for Home, Virtual Environment, Triggers, UPS, License, Deploy, Testing, and Logs. The main area is titled 'Welcome to PowerChute Network Advanced' and contains a brief description. Below this, there are five configuration steps, each in a card:

- Virtual Environment (Step 1):** Configure shutdown and startup sequences for your HCI environment. Status: **Not Configured**. Button: **Go**.
- Triggers (Step 2):** Select the UPS events that trigger a shutdown. Status: **Not Configured**. Button: **Go**.
- UPS (Step 3):** Configure UPS details for deploying a shutdown configuration. Status: **Not Configured**. Button: **Go**.
- License (Step 4):** Activate the PowerChute Network license for your configuration. Status: **Not Licensed**. Button: **Go**.
- Deploy (Step 5):** Deploy a shutdown configuration to a UPS. Status: **Not Deployed**. Button: **Go**.

Each section has a status indicator to give insight into outstanding actions, your connection status, and/or your configuration status. Click **Go** to visit any step at any time.

Virtual Environment

The first step in configuring PowerChute Network Advanced is to specify the details of your Virtual Environment.

First select your Virtual Platform type:

- [Nutanix AHV](#)
- [Custom Platform](#)

Nutanix AHV

Configure the connection details of your Nutanix Acropolis Hypervisor® (AHV) virtual environment to allow the PowerChute Network Advanced UPS Agent to execute graceful, unattended shutdown and startup of the HCI cluster.

Prism Central Details

Enter the details to connect to Nutanix Prism Central:

- The **IP address or hostname** of Nutanix Prism Central
- The TCP **Port** for administrative access to Prism Central. The default is 9440.
- The administrative **Username** and **Password** to access Prism Central.
- The Prism Element **Cluster Name** to be supported by PowerChute. **Note:** This is case-sensitive.

Click **Save**.

Note: Once configured, if you change the Prism Central IP address, you will also need to update the Prism Element Cluster Credentials and Nutanix User details for the new virtual environment.

Prism Central Nutanix User

Enter the **password** of the built-in Prism Central Nutanix user administrative account and click **Save**.

Prism Element Credentials

Enter the **Username** and **Password** of the Prism Element cluster administrative account.

Click **Save**.

Prism Element Nutanix User

Enter the **password** of the built-in Prism Element Nutanix user administrative account and click **Save**.

It is recommended to check the **Shutdown** and **Startup** sequence durations to verify they are sufficient for your environment.

See next:

- [Nutanix Shutdown Sequence](#)
- [Nutanix Startup Sequence](#)

Click **Submit** to complete your Virtual Environment connection.

Upon submit:

- You are prompted to review the SSL certificates for Prism Central and Prism Element cluster and accept them.
- You are prompted to carefully review and select all of the Prism Central and Prism Element CVM SSH keys that PowerChute will add to the trust store.

The PowerChute Configuration Tool then connects to the environment, validates the credentials provided, and gathers the cluster and CVM SSH keys to be added to the PowerChute trust store. **This process may take a few minutes.** Once completed, all Prism Central Details are available for your reference at **Prism Central Details > Configure**.

Nutanix Connection Troubleshooting

During PowerChute - Virtual Environment connection you may encounter messages in the user interface to indicate the connection has been unsuccessful.

Unable to authenticate when requesting <Environment Details>. Check your credentials.

If the Configuration Tool cannot successfully connect to Nutanix Prism Central/Element with the credentials provided:

- Check that the credentials provided are correct.
- Check if the Nutanix account is locked:
 - Log into Nutanix Prism Central/Element with the credentials.
 - If locked, Nutanix will indicate "Account locked due to too many failed attempts".
 - Wait the lockout duration (typically 15 minutes) and try again, or request that an administrator unlocks the account manually.

Nutanix Shutdown Sequence

Once you have [connected to the Nutanix cluster](#), you can specify durations for each of the steps in the shutdown sequence for your virtual environment, allowing sufficient time for each step to provide graceful shutdown of the Nutanix cluster when a critical UPS event such as **On Battery** occurs. Each duration is specified in minutes.

Note: If any of the steps in the shutdown sequence are completed before the duration specified, PowerChute proceeds to the next step in the sequence.

If you select **Enable UPS Shutdown**, the UPS will be turned off when the shutdown sequence is completed.

A total of the estimated time in minutes required for the shutdown sequence to complete is shown.

Shut down User VMs

The duration in minutes to allow all the User VMs to gracefully shutdown. Nutanix Files and the associated VMs are not included in this duration, see Shut down Nutanix Files below.

Power off User VMs

The time allocated for any User VMs that did not gracefully shut down to be powered off, so that the cluster service may be successfully stopped later in the shutdown sequence.

Shut down Nutanix Files

The time allowed to shut down the Nutanix Files and the associated VMs.

Note: It is recommended to allow sufficient time for all your File Server (FS) VMs to gracefully shut down. If the FS VMs are not shut down, this may prevent the Cluster and Controller VMs from shutting down.

Abort Protection Domain (PD) Replications

A protection domain is a collection of VMs that are backed up or replicated on a schedule to recover data. PowerChute will use the duration specified to abort any active protection domain replications before moving to the next step in the sequence.

Stop Prism Central

The time allowed to stop the Prism Central cluster service. *

Shut down Prism Central VMs

The time allowed to shut down and power off the associated Prism Central Virtual Machines. *

Stop Cluster

The time allowed to stop Prism Element cluster services running on the Controller VMs.

Shut down Hosts

The time allowed to shut down and power off the AHV Hosts.

Shut down CVMs

The time allowed to shut down the Prism Element Controller VMs

***Note:** This duration is used only when the Prism Central Service is hosted on the Prism Element cluster being supported by PowerChute. If PowerChute detects that the Prism Central Service is not hosted on the Prism Element cluster, it skips this step in the sequence.

Nutanix Startup Sequence

A startup sequence is disabled by default. Select **Enable Startup Sequence** to run a startup sequence when power is restored to the UPS following a shutdown. You can specify the durations for each of the steps in the startup sequence. Allow sufficient time for each step to provide graceful startup of the Nutanix cluster when the critical UPS event that caused the shutdown has been resolved. Each duration is specified in minutes.

Note: If any of the steps in the startup sequence are completed before the duration specified, PowerChute proceeds to the next step in the sequence.

A total of the estimated time in minutes required for the startup sequence to complete is shown.

Wait for CVMs

The duration that PowerChute will wait for the Prism Element Controller VMs to power on after all the AHV hosts are started.

Start Cluster

The duration that PowerChute will wait for Prism Element cluster services to start.

Start Prism Central VM

The duration that PowerChute will wait for the Prism Central VM to power on and start up.*

Start Prism Central Cluster Service

The duration that PowerChute will wait for the Prism Central Cluster service to start.*

Start Nutanix Files

The duration that PowerChute will wait for the Nutanix Files and the associated VMs to power on and start up.

Start User VMs

The duration that PowerChute will wait for the User VMs to power on and start up.

Note: Protection Domain (PD) Replications will resume automatically once cluster services are operational.

***Note:** This duration is used only when the Prism Central Service is hosted on the Prism Element cluster being supported by PowerChute. If PowerChute detects that the Prism Central Service is not hosted on the Prism Element cluster, it skips this step in the sequence.

Custom Platform

PowerChute Network Advanced allows you to define custom SSH-based startup and shutdown behavior for your environment. For example, you can use custom SSH commands to perform graceful shutdown of Next-Generation Firewalls (NGFW), Network-attached Storage (NAS) devices or Storage Area Networks (SAN).

A PowerChute Network Advanced subscription license is not required for a custom platform.

On the **Virtual Environment** page, select **Custom** from the list of Virtual Platforms.



Note: If you have previously defined a **Nutanix AHV** virtual environment and you select **Custom** from Virtual Platform list, the Nutanix AHV virtual environment details and sequences are discarded.

Supported Remote Hosts

SSH connections to remote hosts with minimal shell features (including the NMC) are not supported by the PowerChute Network Advanced UPS Agent. Only remote hosts with commands `echo` and `stty` available are supported. These commands are required to successfully initialize the SSH session. If they are not available, error messages are written to the PowerChute UPS Agent Log:

```
SSH Client:      | ERROR    | Not found (echo __READY__****__READY__)
SSH Client:      | ERROR    | - SSH expect string not received
```

See also: [Logs](#)

Environment

On the Virtual Environment tab, enter the connection details of the remote host:

1. **IP or Hostname:** The IP address or hostname of the remote host on which you want to execute custom SSH commands.
2. **Username** and **Password:** Enter the username and password to connect to the remote host.
3. Click **Submit** to complete your Virtual Environment connection.

Upon submit, you are prompted to carefully review and select all of the SSH keys that PowerChute will add to the trust store.

The PowerChute Configuration Tool then connects to the environment, validates the credentials provided, and gathers the SSH keys to be added to the PowerChute trust store. **This process may take a few minutes.**

Shutdown Sequence

Once you have connected to the virtual environment, you can define a shutdown sequence to be executed through a sequence of commands, using command types **Send**, **Wait for** and **Sleep**. See [Commands](#).

If you select **Enable UPS Shutdown** and click submit, the UPS will be turned off when the shutdown sequence is completed.

1. Click on the edit icon  to add a command to the custom SSH shutdown sequence.
2. Define a **Custom SSH Name** to identify the set of commands to be executed.
3. Click the **+Add** button to add a command. A sequence can contain up to 50 commands. See [Commands](#).
4. Click **Save** to add the commands to the shutdown sequence. A total of the estimated time in minutes required for the shutdown sequence to complete is shown.



You can delete commands in a sequence by clicking on the delete icon:

Startup Sequence

A startup sequence is disabled by default. Select **Enable Startup Sequence** and click submit to create a custom SSH startup sequence for your virtual environment when power is restored to the UPS following a shutdown.

1. Click on the edit icon  to add a command to the custom SSH startup sequence.
2. Define a **Custom SSH Name** to identify the set of commands to be executed.
3. Click the **Add** button to add a command, as described in [Commands](#) . A sequence can contain up to 50 commands.
4. Click **Save** to add the commands to the startup sequence. A total of the estimated time in minutes required for the shutdown sequence to complete is shown.

Commands

When a shutdown or startup sequence is triggered, commands are executed sequentially.

There are three command types available:

- [Send](#)
- [Sleep](#)
- [Wait for](#)

Send

Purpose: Sends an input command to the remote host.

Description:

Use the **Send** command to send an input command to be executed on the remote system, or to send a response to a preceding command prompt (e.g. confirm YES/NO).

Examples:

- **Send:** execute shutdown
- **Send:** YES

Use of Sudo in a Command Sequence

Commands requiring sudo privileges typically display a prompt requiring the user to enter their password before the command is executed.

Important:

- Do not use the Send command to send a sudo command.
- Do not use the Send command to send the password.
- Do not use the Wait for command to match a password prompt

These actions would result in the password being stored unencrypted, and it would be visible in plain text in the PowerChute UPS Agent logs when the startup or shutdown sequence runs.

Recommendation:

To allow the user [defined in the Virtual Environment tab](#) to run **specific commands** without being prompted for a password, you can add a NOPASSWD rule to the /etc/sudoers file, e.g.:

```
poweruser ALL=(ALL:ALL) NOPASSWD: /usr/sbin/shutdown
poweruser ALL=(ALL:ALL) NOPASSWD: /usr/bin/virsh
```

Sleep

Purpose: Pauses command execution for a specified duration.

Description:

A duration in seconds that the PowerChute UPS Agent will wait before proceeding to the next step in the command.

Example:

- **Duration:** 60 Seconds

Wait for

Purpose: Waits for an output string within a timeout window.

Description:

The **Wait for** command can be used to verify the output of a preceding command before the next command is processed. It includes a configurable timeout duration, to specify the time in seconds that the PowerChute UPS Agent will wait for the expected output string.

Example:

- **Wait for:** Do you want to continue? (y/n)
- **Duration:** 20 Seconds

Timeouts and Precision in Output Strings

If the timeout duration expires before the expected output string is received from the remote host:

- The **Wait for** command is considered unsuccessful and **the sequence is terminated**.
- Any subsequent actions in the sequence are **not executed, and the SSH session is disconnected**.



To create a successful sequence, verify first that the value configured for each **Wait for** command matches the actual output returned by the preceding command.

Example:

Custom SSH Name:

Commands - Define commands to be executed on the remote host +

Type	Send	
Command	hostname	
Type	Wait for	
Duration	10 seconds	
Text Output	testpccc	
Type	Send	
Command	whoami	
Type	Wait for	
Duration	10 seconds	
Text Output	testpc	
Type	Sleep	
Duration	60 seconds	

Save

In the above example, the hostname of remote host **testpc** is queried. As the expected **Wait for** response does not match the correct output (due to misspelling of testpccc), the sequence is terminated, the SSH session is disconnected, and the subsequent whoami and sleep commands are not executed.

Pattern Matching in the Wait for Command

The text specified in the wait-for command will be matched **anywhere** in the output of the preceding commands.

For example, if the command produces multi-line output like the following:

```
$ myCommand
  output line 1
  output line 2
  output line 3
```

If line 3 is specified as the expected output of the **Wait for** command, it will succeed and the next command in the sequence will be executed.

Controlling Matches

The following characters can be used in the expected text output in the wait-for command. These can be used to:

1. Control where the wait-for command matches output from preceding commands, and
2. Match sequences of characters in the output.

Character	Matches
.	Any single character
^	Start of input (anchor)
\$	End of input (anchor)
*	Zero or more of previous character

Pattern Match Examples

Sample usage of the matching control characters is shown in the following examples:

Pattern	Matches	Doesn't Match
`login:`	"login:"	"Login:"
`a.c`	"abc", "adc", "a1c"	"ac", "aabc"
`^hello`	"hello world"	"say hello"
`world\$`	"hello world"	"world hello"
`o*k`	"k", "ok", "ook"	"oak"
`^ok\$`	"ok"	"ok!", "okay"
`start.*end`	"start1234end"	"end1234start"

Triggers

Create a trigger configuration to define the UPS events that prompt a graceful shutdown of the target environment.

Trigger Name

Enter a name for the trigger configuration. Maximum 127 characters permitted.

Configurable Triggers

Time On Battery

Specify the number of minutes the UPS is On Battery when PowerChute triggers a shutdown sequence.

The duration must be between 1 and 2880 minutes.

Runtime Remaining

When the UPS is running on battery power, specify the minutes of runtime remaining when PowerChute triggers a shutdown sequence.

The runtime remaining must be between 1 and 2880 minutes.

Non-Configurable Triggers

These non-configurable triggers are enabled by default and cannot be disabled.

Low Battery

Trigger a shutdown sequence when the UPS is running on battery power and the runtime remaining falls below the Low Battery duration configured on the Network Management Card.

UPS Turn Off

Trigger a shutdown sequence when a graceful shutdown command is issued to the UPS using the NMC user interface or the LCD display.

UPS Configuration

The PowerChute Network Advanced UPS Agent runs on the Network Management Card (NMC) in your UPS. In the PowerChute Configuration Tool, you must create a **UPS Configuration** to specify the connection details for the NMC before you can deploy a shutdown configuration to the NMC.

Create UPS Configuration

Connection Details

To create a UPS Configuration, the following fields are required:

Field Name	Description
UPS Configuration Name	A meaningful name for the UPS configuration. Maximum 127 characters.
IP Address	The IPv4 address or hostname of the NMC
Username	The username of an NMC administrator account.
Password	The password of the NMC administrator account.
Port	The HTTPS port number of the NMC. The default is 443. To configure the HTTPS port number of the NMC, see the NMC User Guide - Network on Configuration menu .
MAC address	The MAC address of the NMC. Note: This field is automatically populated upon successful connection.
Serial number	The serial number of the NMC. In the NMC user interface, see About > Network to find the serial number. Note: Once a connection has been successfully created and a license is activated for this UPS Configuration, this field becomes read-only.

Click **Connect** to save the UPS Configuration. The Configuration Tool will try to connect to the NMC.

Certificate Validation

The NMC uses a self-signed SSL certificate by default when HTTPS is enabled. During connection, the Configuration Tool checks if the SSL certificate of the NMC is trusted. If it is not, the Configuration Tool

displays the untrusted certificate details for you to review and accept. Once accepted, the Configuration Tool stores the certificate in its trust store, and the connection proceeds.

UPS Connection

When the Configuration Tool tries to connect to the NMC using the connection details, there are two possible results:

1. **Not connected** - PowerChute has not successfully connected to the NMC. See [Connection Troubleshooting](#) to identify and resolve the connection issue. Click **Connect** to try a new connection attempt.
2. **Connected** - PowerChute can communicate with the agent running on the NMC using the connection details.

Connection Troubleshooting

During PowerChute - NMC connection you may encounter messages in the user interface to indicate that connection has been unsuccessful.

Cannot connect to the device. Check the details and try again

If the Configuration Tool cannot successfully connect to the NMC:

- Check that the IP address and port details are correct.
- Download the [Logs](#) to check for network connection error details.

If the issue persists, contact [Customer Support](#).

Invalid Credentials

The username or password of the administrator account you have entered is incorrect. Check the details and try again.

Administrator Account Required

The NMC account you have provided does not have administrative permissions. Enter the username and password of an NMC account with **User Type: Administrator**.

Firmware Update Required

The firmware installed on the NMC does not support PowerChute Network Advanced. Update the NMC firmware using the Secure NMC System tool. **See:** [Updating the NMC firmware with the Secure NMC System Tool](#).

PowerChute Secure Authentication

Once a successful connection to the NMC is established, the Configuration Tool will authenticate with the NMC. The Configuration Tool uses bearer token authentication over HTTPS to provide secure authentication with the NMC.

Note: The authentication token between the Configuration tool and the NMC is **valid for 180 days**. Expiration of this authentication token does not impact the function of the PowerChute Network Advanced UPS Agent on the NMC, and the shutdown configuration will continue to help protect the configured target environment.

- Once expired, you will see a UPS Configuration status of **Not Connected** on the UPS Configuration page.
- Click **Connect** to re-connect the Configuration Tool to the NMC.

Update UPS Configuration

On the UPS Configuration page, click the edit icon  to update the UPS configuration when:

- The UPS Connection has status **Not Connected**:
 - The NMC SSL certificate may have expired. Click **Connect** to review and accept a new SSL certificate.
 - The NMC authentication token may have expired after 180 days. Click **Connect** to refresh the connection.
- NMC Connection details of username, password or port have been updated on the NMC, or the IP address of the NMC has changed on the network.

Note: If you change the IP address/hostname of the NMC to the address/hostname of a different NMC, the license status is set to **Not Licensed** and you will be required to update the license details and **Deploy** to the new NMC specified.

See also: [Switch to a Different NMC and HCI Cluster](#)

Delete UPS Configuration

Note: If you have not yet deployed a configuration to the UPS, and you want to **permanently** delete the UPS Configuration, **it is recommended to first return any associated license before deleting it**.

If you do not, and you uninstall the PowerChute Network Advanced Configuration Tool, you will no longer be able to return the license and will have to contact [Customer Support](#).

See [License > Return License](#).

If you have already deployed the configuration to the UPS, see [Deployment > Delete from UPS](#)

To delete a UPS configuration, on the **UPS Configuration** page, click the delete icon . You will be prompted to confirm before deletion.

Note: Refer to the application logs for deletion errors. See [Logs](#).

Switch to a Different NMC and HCI Cluster

After [deployment](#), if you want to use the Configuration Tool with a different NMC and HCI Cluster, it is recommended to first [Delete the existing UPS Configuration](#) **without returning the license**, and then add one for the new NMC. This allows you to:

- Create a new UPS Configuration for the new NMC. Check that you have entered the correct serial number for the new NMC.
- Enter the required connection details and credentials for the new HCI cluster. See [Virtual Environment](#)
- Update the relevant [Triggers](#).
- Activate a [License](#) for the new configuration.
- Deploy the configuration to the PowerChute UPS Agent running on the new NMC. See [Deployment](#)

This approach lets you manage multiple UPS configurations from a single Configuration Tool installation.

To switch back to a previously licensed NMC and Cluster configuration, update the UPS Configuration details and reconnect to the original NMC, import the deployment and configure the Virtual Environment. The original license remains associated with that configuration.

License

PowerChute Network Advanced is a licensed product. A subscription license is required for each node. A **node** is defined as a host that is supported by PowerChute and part of a Virtualization/HCI cluster and provides compute resources. A PowerChute Network License can be purchased through your Schneider Electric IT Partner.

A free trial of PowerChute Network Advanced is available. Visit the [PowerChute Network Help Center](#) on the [Schneider Electric Community](#) to find out more.

License Prerequisites

Before you license your PowerChute Network Advanced deployment, you need to:

1. Define your [Virtual Environment](#) to indicate the number of nodes to be licensed.
2. Define your [Triggers](#) - the UPS events that prompt a graceful shutdown of the virtual environment.
3. Define your [UPS Configuration](#) to specify the NMC on which the PowerChute agent will be deployed. The MAC Address of the NMC is the Device ID for the PowerChute license, and the serial number of the NMC is the Device Name for the PowerChute license.

Only one license Activation ID can be used per PowerChute Network Advanced deployment. The quantity included per Activation ID should cover all nodes supported by the PowerChute deployment.

Activate License

To license your PowerChute Network Advanced Deployment:

1. Purchase a license through your Schneider Electric IT Partner for the number of nodes required for your environment.
2. Visit **License** in the PowerChute Network Advanced Configuration Tool.
3. Select **Activate Online**
4. Enter the license's **Activation ID**. This is in the format **ACT-XXXX-XXXX-XXXX-XXXX**
5. Enter your **Proxy IP Address and Port Number, Proxy Username and Proxy Password** if required.
6. Review the **Quantity** of nodes in your cluster supported by the PowerChute instance that is automatically populated. One license is required for each node supported by PowerChute.
7. Review the automatically populated Device ID (MAC address) and Device Name (Serial Number) for the PowerChute license to verify their values are correct.
8. Click the **Activate** button.

9. PowerChute will contact the Schneider Electric Cloud Licensing Server to validate the provided Activation ID. If the license is successfully validated, PowerChute will display the license details.

Increase License Quantity

If the quantity of nodes in the cluster supported by PowerChute increases, PowerChute sets the current license status to **Unlicensed**. To increase the License quantity for the additional nodes:

1. Enter the **Activation ID** of the current license.
2. Review the **Quantity** value of the **Activate License** form to check it represents the number of nodes that have been added.
3. Click **Activate** to increase the license quantity used.

If the **Activation ID** does not contain sufficient quantity to cover the increase in nodes, you can purchase additional quantity for your Activation ID at [mySchneider Software Management](#), or via your Schneider Electric IT Partner. Once sufficient quantity is purchased for the Activation ID, you can click **Activate** on the **License** page of the Configuration Tool to activate the license for the additional nodes.

Decrease License Quantity

If the number of nodes in the cluster supported by PowerChute decreases, you can **Return License** as described below. Once returned, you can use the same **Activation ID** to activate your license for the reduced number of nodes required.

Return License

You can return your PowerChute Network Advanced license to apply it to another PowerChute Network Advanced configuration, if the configuration has not yet been deployed. Returning a license will increase the available quantity associated with your Activation ID by the quantity that was returned.

You can view how many licenses you have remaining in mySchneider Software Management:

1. Log in to [mySchneider Software Management](#)
2. You can view the total quantity, available quantity, and expiration date of the licenses associated with your Activation ID.

To return a license, click the **Return License** button in the License screen of the PowerChute Network Advanced Configuration Tool interface.

Note: If the configuration has been deployed, the Return License button is disabled. To return the license of a deployed configuration, you must first delete the configuration from the UPS, which automatically returns the license. See [Delete UPS Configuration](#).

For more information on PowerChute Network Advanced licensing, visit the [PowerChute FAQ on Schneider Electric Community](#).

Deployment

The deployment page provides an overview of the configuration of your UPS Connection, Triggers, and Virtual Environment, and indicates if you are ready to deploy the shutdown/startup configuration to the PowerChute Network Advanced UPS Agent running on the Network Management Card.

Check Deployment Status

The **Deployment Details** section provides an overview of

- [UPS Connection](#)
- [Trigger](#)
- [Virtual Environment](#)

If the configuration is complete, the name of the UPS Connection, Trigger and Virtual Environment are shown.

If configuration is outstanding, **Not Configured** is shown.

Deployment cannot occur until all three are configured, and the license status is **Licensed**, or for custom platforms, **License Not Required**.

Once all of the deployment details are completed, click **Deploy** to deploy the configuration to the UPS:

- You are asked to confirm the deployment.
Note: If the UPS has an existing deployment, the existing deployment will be overwritten.
- The deployment progress is shown: **Connected > Started > Success**

If the deployment is not successful, see the below status messages and recommended actions.

Deployment Message	Recommended Actions
Unable to create the configuration bundle	Re-submit the Virtual Environment to validate the configuration.
License is not active	Check the License status on the License page.
Invalid or missing configuration	Re-submit the Virtual Environment to validate the configuration.
Configuration is in use (locked)	The configuration is in use on the Network Management Card. A shutdown or startup sequence or another deployment may be in progress. Check the Logs for more information.
Unable to connect to the agent. Check network connectivity.	Check the UPS Configuration and if it is not connected, see Connection Troubleshooting .

If the deployment issue persists, download the [Logs](#) and contact [Customer Support](#).

Import Deployment

You can import the configuration currently deployed on the UPS to make changes to it using the PowerChute Configuration Tool.

Use Import:

- To make changes to the configuration of a PowerChute Network Advanced Agent already deployed to an NMC.
- To reuse the configuration of an Agent on a different NMC.
- When you have installed the Configuration Tool on different computer and want to make changes to an existing deployment.

The UPS Configuration must be completed before a deployment can be imported, to provide the Configuration Tool with the connection details of the NMC from which to import the deployment.

Note: Importing a configuration overwrites the current configuration in the PowerChute Configuration Tool and cannot be undone.

1. On the deployment page, click **Import**.
2. A dialog indicates that the configuration currently in the Configuration Tool will be overwritten by the import. Click **Import** to proceed.
3. **Configuration Successfully Imported from UPS** indicates that the import was successful.

Note: Following import, it is necessary to resubmit the Virtual Environment Configuration to connect to the environment and to review and validate the SSH keys that PowerChute will add to the trust store.

Delete from UPS

Once deployed, you can delete the deployment from the UPS by clicking **Delete from UPS**.

This action:

- Removes the PowerChute Network Advanced Agent configuration from the NMC, as defined in the UPS Configuration.
- Disables PowerChute Network Advanced Agent service on the NMC.
- Returns your license automatically. The quantity associated with the license is increased in accordance with the returned license. Once returned, you can use the activation ID of the returned license to apply it to a new configuration.

Note: You cannot delete a deployment from the UPS when a shutdown/startup sequence is in progress.

Logs

Schneider Electric Customer Care may request an export of PowerChute technical log files to help identify and troubleshoot any issues. To export the files:

1. Go to the **Logs** page.
2. Click **Download** to export the logs as a .zip file.
3. Save the timestamped log archive in a secure location.
4. Extract the archive to view the logs.

The log archive contains the Network Management card logs, application logs, error logs, and PowerChute service logs.

Testing

When you have configured your Virtual Environment and associated shutdown and startup sequences, following deployment you can test the efficacy of the shutdown/startup sequences.

This action performs a shutdown or startup as configured in the shutdown sequence or startup sequence of the Virtual Environment configuration. Following the test, the PowerChute UPS Agent is reset to an idle state, where no shutdown or startup sequence is running, and the UPS Agent is ready to perform a subsequent shutdown/startup sequence in response to a **Trigger**.

Note: During a startup test, the reset of the UPS Agent to idle state will occur even if the startup sequence is disabled on the Virtual Environment Page.

To perform a Shutdown or Startup Test:

1. Go to **Testing**
2. On the **Shutdown** or **Startup** tab, click **Test**.
3. Wait a few moments for the **Test Result** to appear:
 - **Passed** - The test sequence has successfully initiated and is in progress. Monitor the Virtual Environment and review the UPS Agent [Logs](#) to check the results of the sequence.
 - **Test Unsuccessful** - The test sequence has not been successfully initiated and is not running. Review the Agent [Logs](#) to check the results of the sequence. Review the below table for details on the possible cause.

Message	Recommended Actions
No UPS connection configured for test shutdown/startup.	Go to UPS Configuration to check the UPS connection status.
No deployment found for test shutdown/startup. Please deploy a configuration before running the test.	Go to Deployment and check the deployment status.
Test shutdown/startup unsuccessful. The agent is disabled. Please enable the agent and try again.	The PowerChute Network Advanced UPS Agent has been disabled on the NMC. In the NMC web interface, go to Configuration > Shutdown and enable PowerChute Network Advanced access.

If the deployment issue persists, download the [Logs](#) and contact [Customer Support](#).

Important:

- If **Enable UPS Shutdown** is selected in the shutdown sequence, the UPS turns off at the end of the shutdown sequence. The UPS will remain off and must be turned on via the NMC user interface (**Control > UPS**).
 - If a startup sequence is configured in PowerChute, turning on the UPS will automatically initiate the configured startup sequence for the supported environment, and no startup test is required.
 - If no startup sequence is configured, running a Startup Test only returns the UPS Agent state from Shutdown to Idle, ready to perform future shutdown or startup sequences, but it does not initiate a startup of the supported environment. In this case, the startup of the supported environment must be performed manually.

Security Information and Recommendations

Java Runtime Environment (JRE)

PowerChute Network Advanced installs a custom Java 21 JRE to operate. PowerChute Network Advanced provides a list of the Java modules used at the following location:

```
C:\Program Files\Schneider Electric\PowerChute Network Advanced\jre\release
```

The application JARs (Java Archives) are digitally signed to confirm their authenticity and integrity. See [Digital Signature Verification](#).

Digital Signature Verification

This section describes how to verify the digital signatures of PowerChute Network Advanced components using Windows PowerShell.

Installation Files

The PowerChute installer (**PCNASetup.exe**), uninstaller (**Uninstall.exe**) and application service executable (**PCNA.exe**) files are digitally signed. To verify the digital signatures using Windows PowerShell, use the following command:

```
Get-AuthenticodeSignature "<filename file location>" | Format-List *
```

Check that the response indicates that the signature was verified and is signed by SCHNEIDER ELECTRIC USA, INC.

Note: If the digital signature is not verified, do not proceed and contact [Customer Support](#).

JAR Files

.JAR file signatures can be verified using the jarsigner tool. The jarsigner tool is not part of the JDK 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 [Adoptium OpenJDK](#). For more information, consult the [jarsigner tool documentation](#).

To verify the digital signature of the application JAR files (**pcna.jar**, **nutanix_plugin-x.x.x** and **custom_plugin-x.x.x**) using Windows PowerShell, use the following command:

```
- jarsigner -verify -verbose -certs .\<jar file name>
```

Check that the response indicates that the signature was verified and is signed by SCHNEIDER ELECTRIC USA, INC.

Note: If the digital signature is not verified, do not proceed and contact [Customer Support](#).

User Credentials

User credentials are never stored in plain text. Before being stored, passwords are converted to one-way cryptographic hashes using current industry best practices, with unique salts applied to each password. Stored credential data is also encrypted at rest to provide an additional layer of protection. As forgotten passwords cannot be recovered, they must be reset rather than retrieved.

Reset your password

Follow the steps below to reset a lost or forgotten password.

If you know your current password and want to change it, see [Changing your Password](#).

Note:

Resetting your password using the steps below will also remove all stored UPS Configuration and Virtual Environment credentials. Following reset, it will be necessary to:

- Re-enter the UPS Connection credentials and reconnect to the UPS.
- Re-enter the Virtual Environment credentials and resubmit them.

To reset the password to access the PowerChute Network Advanced Configuration Tool:

1. On the computer where the PowerChute Configuration Tool is installed, open the Windows Services management console (services.msc)
2. Stop the PowerChute Network Advanced service.
3. Create a blank text file called reset-credentials.trigger and save it at this location:

`C:\Program Files\Schneider Electric\PowerChute Network Advanced\Config\`

4. Start the PowerChute Network Advanced service.
5. Follow the steps outlined in [Installing on Windows > Log in to PowerChute Network Advanced](#)

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](#).

Update Notifications

If a security vulnerability is detected in PowerChute that requires a software update, a new release will be made available on the [Schneider Electric](#) website. Software updates must be applied manually. Periodically review the [Release Notes published on the Schneider Electric Community](#) to keep updated with the latest releases.

Security Notifications

Security Bulletins in relation to known vulnerabilities are published on the [Schneider Electric Cybersecurity support portal](#).

Software Bill Of Materials (SBOM)

A Software Bill of Materials (SBOM) is a comprehensive list of all software components used in a particular application or system. It provides details such as the names and versions of libraries, modules, frameworks and other software elements integrated into the final product. As libraries and components can change between PowerChute Network Advanced releases, an SBOM is a dynamic document that needs to be compiled upon request.

To request the SBOM for PowerChute Network Advanced, contact [Customer Support](#).

Security Hardening Guidelines

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

Network Management Card

1. HTTPS must be enabled via **Configuration > Network > Web > Access**. PowerChute Network Advanced does not support HTTP.
2. 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.
3. Replace the default self-signed SSL certificate with the new one in **Configuration > Network > Web > SSL Certificate**.
4. Ensure that NMC firmware updates are installed to apply the latest security updates and bug fixes.
5. Read the [NMC 3 Security Handbook](#) for more information on how to secure the Network Management Card.

PowerChute Network Advanced

1. Refer to Knowledge Base article [FAQ000283328](#) for details on how to replace the default self-signed certificate for the PowerChute Configuration Tool with your own certificate signed by a Certificate Authority (CA).
2. Prevent remote access to the PowerChute Configuration Tool using a firewall rule for the configured TCP port number (default is 443). See Knowledge Base article [FAQ000283331](#) for details on how to change the configured HTTPS port to an alternative port.
 - To prevent Denial of Service attacks such as the SSL/TLS resource exhaustion attack, this port should be blocked. It is not recommended to permit access to PowerChute on a public facing network interface.
3. The PowerChute Configuration Tool session timeout determines how long a user session remains active before the user is automatically logged out due to inactivity. The default is 15 minutes. See Knowledge Base article [FAQ000283330](#) for details on how to change the session timeout.

Secure Removal

To uninstall PowerChute Network Advanced, see [Uninstalling on Windows](#).

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 [FAQ000283329](#).

Schneider Electric

1884 Boulevard de la Défense

92000 Nanterre

France

Phone: +33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

© 2026 Schneider Electric. All Rights Reserved.

JPU06873

08/2026