Quick Guide

PowerPanel® Business Local

Shutdown NAS

Dokumentversion: 1.2 Stand: Mai 2025
erstellt von: Athanasia Balkoura

CyberPower Software & Integration Support – Germany

1.1. Zielgruppe

IT-Administratoren, Systembetreuer, Netzwerktechniker und Endkunden, die NAS-Systeme (z. B. Synology, QNAP) in Kombination mit einer CyberPower-USV einsetzen und einen automatisierten Shutdown bei Stromausfall einrichten möchten.

1.2. Kurzbeschreibung

Dieser Anwendungshinweis beschreibt die Konfiguration der Power PowerPanel® Business Local Software, um ein NAS im Ereignisfall automatisch über SSH-Befehle herunterzufahren. Unterstützt werden Windows-, Linux- und macOS-basierte Systeme.

Die Anleitung umfasst:

- *Vorbereitung der Systemumgebung*
- *Aktivierung des SSH-Zugriffs*
- *Konfiguration externer Shutdown-Skripte*
- *Tipps für die Absicherung und Netzwerkstabilität*

Inhaltsverzeichnis

1. Ziel

Dieser Anwendungshinweis beschreibt das automatisierte Herunterfahren von Computer und NAS bei Stromversorgungsunterbrechungen mithilfe der PowerPanel® Business Local Software und des SSH-Dienstes. Ziel ist es, Datenverlust und Systemabstürze zu vermeiden. Die erforderlichen Konfigurationsschritte für Windows, Linux und macOS sind in den folgenden Kapiteln aufgeführt.

Hinweis: Wenn die USV ausschließlich das NAS mit Strom versorgt und keine Kommunikation über USB oder Netzwerk mit dem Computer besteht, ist dieser Anwendungshinweis nicht anwendbar. In diesem Fall wird empfohlen, das NAS direkt über eine USB-Verbindung mit der USV zu koppeln. Weitere Informationen zur Energieverwaltung sind dem Benutzerhandbuch des jeweiligen NAS-Systems zu entnehmen.

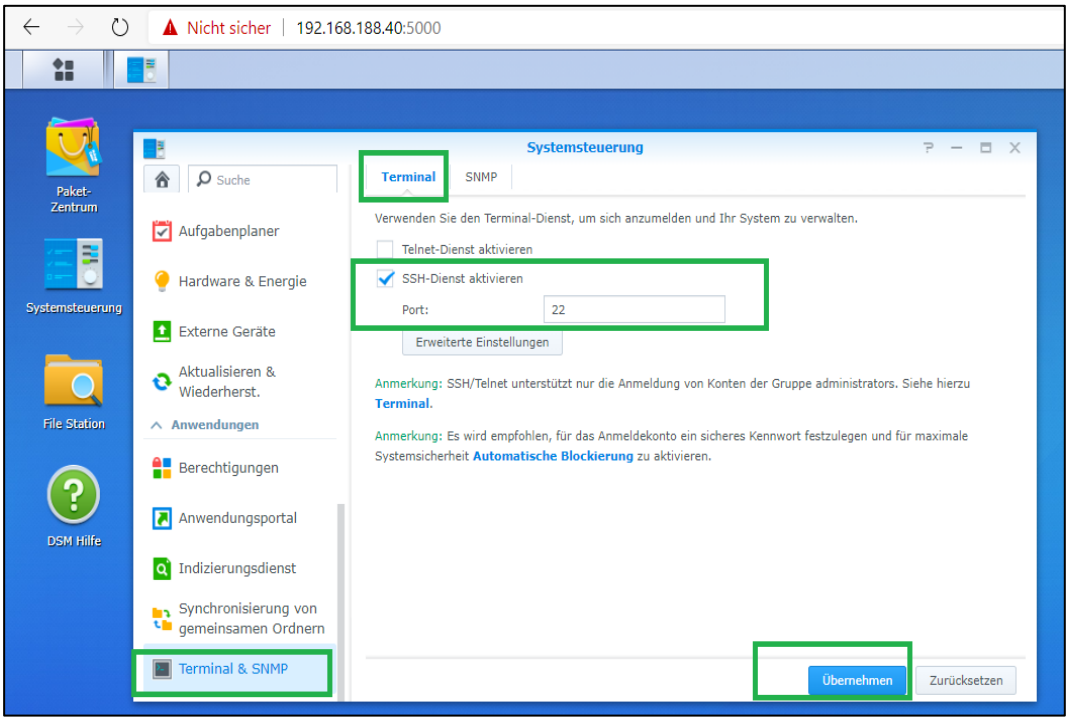
2. Vorbereitung

2.1. SSH-Dienst aktivieren

Um das NAS per Fernzugriff über SSH steuern zu können, muss der SSH-Dienst aktiviert werden.

QNAP NAS

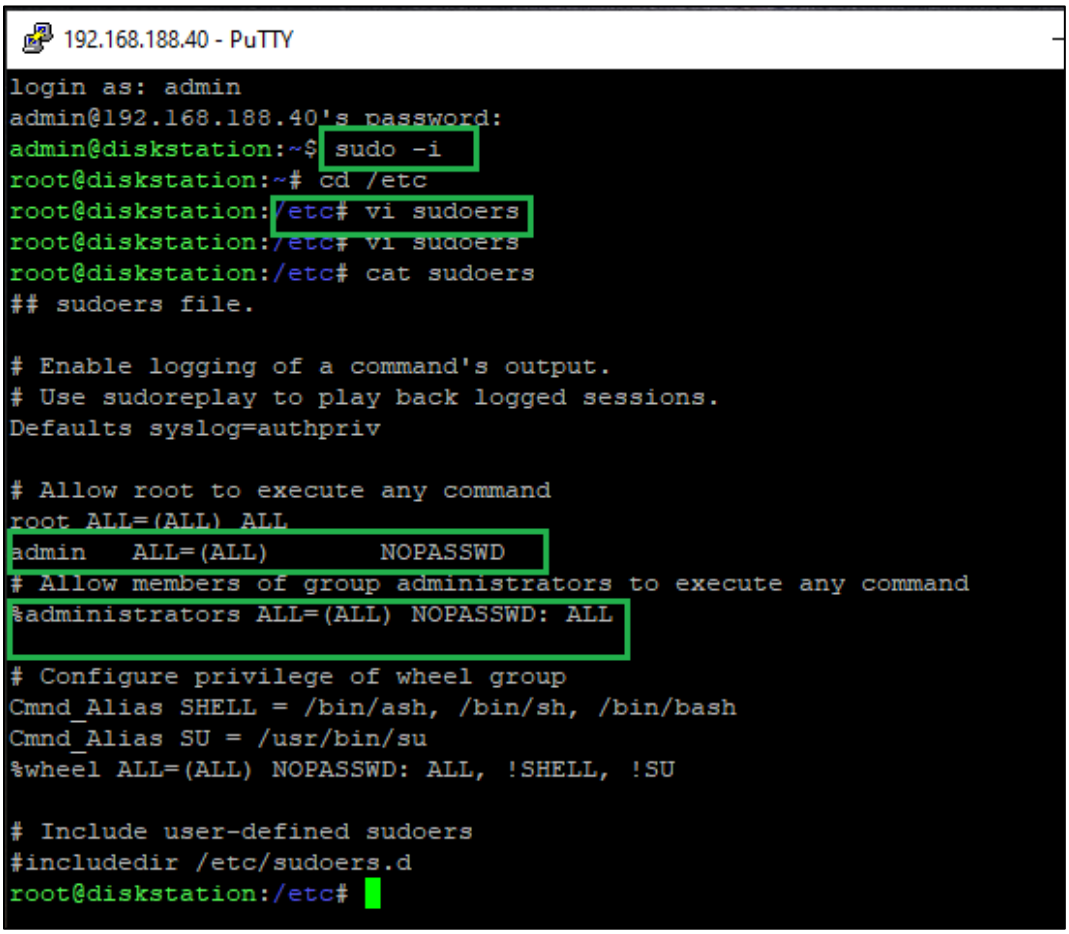
Melden Sie sich am QTS-Webinterface als Administrator an. Navigieren Sie zu
Systemsteuerung > Netzwerk- und Dateidienste > Telnet/SSH
und aktivieren Sie die Option **„SSH-Verbindung zulassen“**.



Synology NAS

Melden Sie sich am DSM-Webinterface als Administrator an. Öffnen Sie
Systemsteuerung > Erweiterter Modus > Anwendungen > Terminal & SNMP
und aktivieren Sie dort **„SSH-Dienst aktivieren“**.

Hinweis: Synology erlaubt SSH/Telnet-Zugriff nur für Konten der Administratorgruppe. Stellen Sie sicher, dass die Datei /etc/sudoers entsprechend angepasst wurde.



2.2. PowerPanel® Software installieren

Stellen Sie sicher, dass die passende Version der PowerPanel® Business Local/Remote Software auf dem System installiert ist. Die aktuelle Software sowie weiterführende Informationen sind verfügbar unter: https://www.cyberpower.com/de/de/download

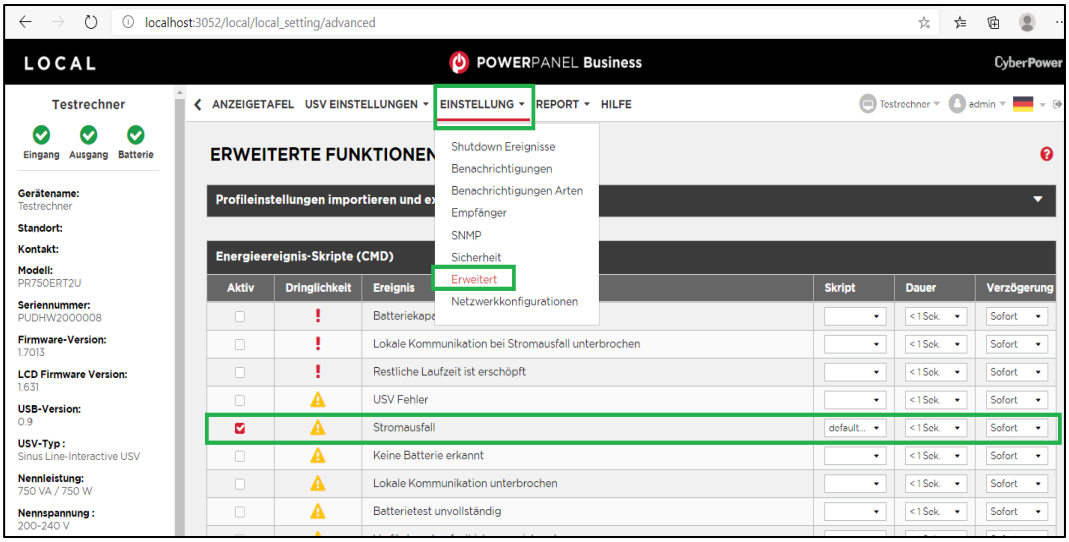
- **Windows**: PowerPanel® Business Local/Remote für Windows
- **Linux**: PowerPanel® Business Local/Remote für Linux
- **macOS**: PowerPanel® Business Local/Remote für Mac

2.3. Verbindung zwischen NAS, USV und Computer herstellen

1. Das NAS und der Computer müssen über die batteriegepufferten Steckdosen der USV mit Strom versorgt werden.
2. Verbinden Sie die USV per USB- oder seriellem Kabel mit dem Computer, damit die PowerPanel® Software die USV überwachen kann.
3. Die Netzwerkverbindung zwischen dem Computer und dem NAS muss stabil und vollständig erreichbar sein.

3. Konfiguration der Einstellungen in PowerPanel® Business Local

Um das NAS im Ereignisfall herunterzufahren, muss in PowerPanel® Business Local ein entsprechender externer Befehl hinterlegt und das richtige Ereignis aktiviert werden.



1. Öffnen Sie die PowerPanel-Weboberfläche auf dem lokalen System durch Eingabe von http://127.0.0.1:3052/ oder http://localhost:3052/local in den Webbrowser.
2. Melden Sie sich an und wechseln Sie zu **„Einstellung“** > **„Erweitert“**.
3. Aktivieren Sie im Abschnitt **„Ereignisse“** das Ereignis **„Stromausfall“**.
4. Wählen Sie im Feld **„Externer Befehl“** die Datei **default.cmd** (unter Windows) oder **default.sh** (unter Linux/macOS) aus.
5. Optional: Passen Sie die Verzögerungszeit für das Herunterfahren des NAS in Abhängigkeit von dessen Reaktionszeit an.

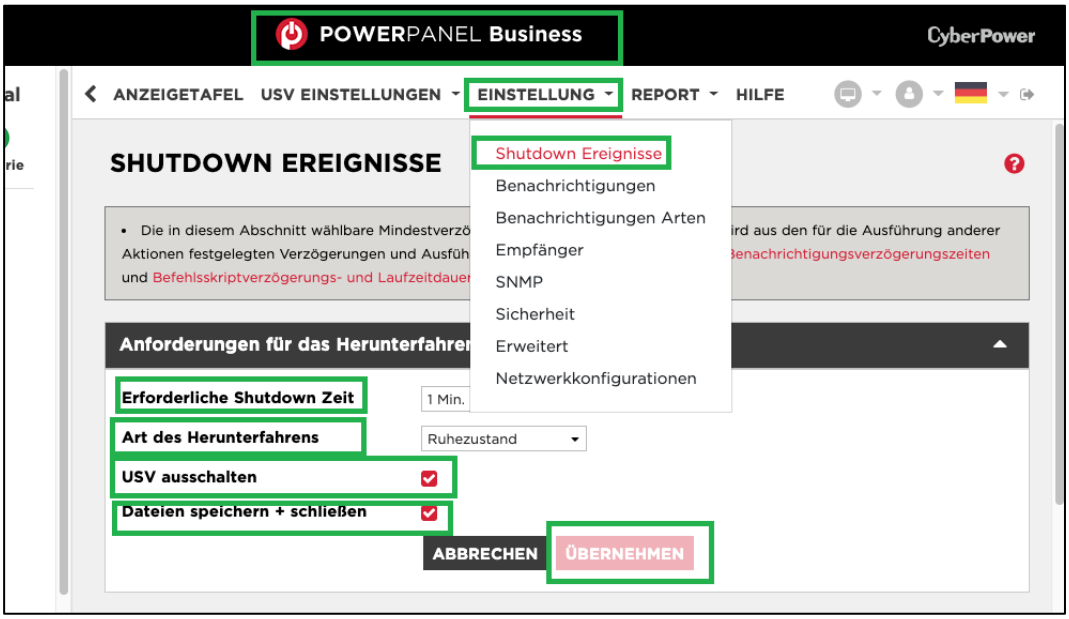
- **Hinweis: Die externe Befehlsdatei wird ausgeführt, bevor das lokale System heruntergefahren wird. Dadurch bleibt ausreichend Zeit für die kontrollierte Abschaltung des NAS.**

4. USV-Abschaltverzögerung konfigurieren

Damit das NAS und der angeschlossene Computer genügend Zeit zum ordnungsgemäßen Herunterfahren haben, muss die USV so konfiguriert werden, dass sie die Ausgangsspannung verzögert abschaltet.

1. Öffnen Sie die PowerPanel-Weboberfläche über http://localhost:3052/remote.
2. Navigieren Sie nach dem Login zu **„Einstellung“** > **„Shutdown-Ereignisse“**.
3. Aktivieren Sie die Option **„Computer herunterfahren“**.
4. Aktivieren Sie zusätzlich die Optionen **„Dateien speichern und schließen“** sowie **„USV ausschalten“**, sofern gewünscht.
5. Wählen Sie unter **„Erforderliche Shutdown-Zeit“** eine ausreichend große Verzögerung aus, damit das NAS vollständig heruntergefahren werden kann, bevor die USV den Strom abschaltet.

TIPP: Falls das NAS mehrere Minuten benötigt, um Dienste zu beenden, sollte die Verzögerungszeit entsprechend angepasst werden (z. B. auf 5 Minuten).



5. Konfiguration in Windows

5.1. SSH-Tool für das Herunterfahren vorbereiten

Für den SSH-Zugriff auf das NAS wird das Tool plink.exe empfohlen, ein Kommandozeilen-SSH-Client aus dem PuTTY-Projekt. Dieses wird verwendet, um den Herunterfahrbefehl an das NAS zu senden.

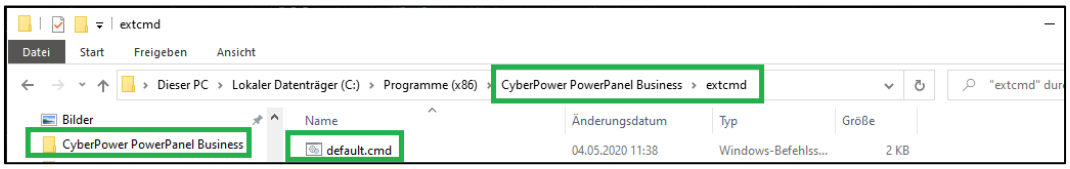
Download-Link:
https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Speichern Sie plink.exe in einem Pfad, auf den der PowerPanel-Befehl Zugriff hat. Beispiel: C:\Tools\plink.exe

- **Hinweis: Der Pfad zu plink.exe muss exakt im Befehl angegeben werden.**

5.2. Externen Befehl in PowerPanel Business Local bearbeiten

1. Navigieren Sie zum Installationsverzeichnis der Software, z. B.: C:\Program Files (x86)\CyberPower PowerPanel Business\extcmd\



2. Öffnen Sie die Datei default.cmd mit Administratorrechten in einem Texteditor.
3. Fügen Sie unter dem Abschnitt: doEventOccurCommand folgenden Befehl ein, angepasst an Ihr NAS-System:

Beispiel für Synology NAS:

```
echo y | "C:\Tools\plink.exe" -ssh -pw AdminPasswort AdminBenutzer@IP-Adresse "sudo /sbin/shutdown -P now"
```

Beispiel für QNAP NAS:

```
echo y | "C:\Tools\plink.exe" -ssh -pw AdminPasswort admin@IP-Adresse "poweroff -d 10"
```

Variablen:

- AdminBenutzer: Benutzername mit Admin-Rechten auf dem NAS
- AdminPasswort: Passwort des Benutzerkontos
- IP-Adresse: Aktuelle IP-Adresse des NAS
- -d 10: (optional) Verzögerung in Sekunden vor dem Herunterfahren

4. Speichern Sie die Datei. Die Änderung bewirkt, dass beim Auftreten eines Ereignisses wie Stromausfall der Shutdown-Befehl an das NAS gesendet wird.

Beispielaufbau default.cmd bei Synology NAS:

```
@echo off

if "%EVENT_STAGE%"=="OCCUR" goto doEventOccurCommand

if "%EVENT_STAGE%"=="FINISH" goto doEventFinishCommand

goto end



: doEventOccurCommand

echo y | "C:\Tools\plink.exe" -ssh -pw AdminPasswort admin@192.168.1.100 "sudo /sbin/shutdown -P
now"

goto end



: doEventFinishCommand

rem Optionale Befehle für das Ende eines Ereignisses

goto end



:end

exit
```

6. Konfiguration in Linux

6.1. SSH-Schlüssel für NAS-Verbindung erstellen

Um die NAS-Geräte über die automatische SSH-Anmeldung fernsteuern zu können, müssen Sie den SSH-Client mit einem SSH-Schlüssel einrichten, damit die PowerPanel-Software das Shell-Skript mit einem kurzen Abschaltbefehl auf dem entfernten NAS ausführen kann.

Dieser SSH-Schlüssel wird auf dem Root-Account für den PowerPanel-Dämon generiert, um ein Shell-Skript auszuführen. Generieren Sie mit den folgenden Schritten ein Paar privater und öffentlicher Schlüssel zur Fernanmeldung des SSH-Servers des NAS:

```
cyberpower@debianlive:~$ su root
Password:
root@debianlive:/home/cyberpower#
```

1. Melden Sie sich als **root**-Benutzer an oder verwenden Sie sudo:

2. Generieren Sie ein neues RSA-Schlüsselpaar (ohne Passphrase):

```
ssh-keygen -t rsa
```

3. Drücken Sie bei allen Abfragen einfach die Eingabetaste, um die Standardwerte zu übernehmen.

```
root@debianlive:/home/cyberpower# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
```

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

4. Nachdem Sie die Passphrase bestätigt haben, wird das Schlüsselpaar generiert.

```
Your identification has been saved in /root/.ssh/id_rsa2.
Your public key has been saved in /root/.ssh/id_rsa2.pub.
The key fingerprint is:
SHA256:pMMzcrldMlrFVFEvVvAFj3N2mskP/vUHGqQG0XWv9Fw root@debianlive
The key's randomart image is:
+---[RSA 2048]----+
|         ..o+o=oo|
|        .o.  . B.|
|        ..o   * E|
|     . +..  .+ %o|
|    . O S..o  B o|
|     o O +o ...o |
|      o ..   o..o|
|            .  .+|
|                +|
+----[SHA256]-----+
```

5. Kopieren Sie den öffentlichen Schlüssel auf das NAS:

```
ssh-copy-id -i /root/.ssh/id_rsa.pub AdminBenutzer@IP-Adresse
```

- AdminBenutzer: Admin-Konto des NAS
- IP-Adresse: IP-Adresse des NAS

6. Bei der ersten Verbindung bestätigen Sie mit yes und geben das NAS-Passwort ein.

```
root@debianlive:/home/cyberpower# ssh-copy-id -i /root/.ssh/id_rsa.pub admin@192
.168.188.39
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa
.pub"
The authenticity of host '192.168.188.39 (192.168.188.39)' can't be established.
RSA key fingerprint is SHA256:lY0ENKLeUJLQCvVA2cpB9cZDEloeF2kXyje0iap7R2c.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
admin@192.168.188.39's password:
```

6.2. Externen Befehl in PowerPanel bearbeiten

1. Öffnen Sie die Datei default.sh im PowerPanel-Verzeichnis, z. B.:

```
vim /opt/PowerPanel/extcmd/default.sh
```

2. Fügen Sie unter der entsprechenden Bedingung folgenden Befehl ein:

```
/usr/bin/ssh AdminBenutzer@IP-Adresse /sbin/poweroff
```

Ersetzen Sie AdminBenutzer und IP-Adresse durch die realen Werte des NAS.

3. Stellen Sie sicher, dass default.sh ausführbar ist:

```
chmod +x /opt/PowerPanel/extcmd/default.sh
```

4. Die Ausführung erfolgt automatisch, wenn ein konfiguriertes Energieereignis auftritt.

- **Hinweis: Die Kommunikation erfolgt passwortlos durch den SSH-Schlüssel. Falls die Verbindung**

```
#!/bin/sh


# You can write your own commands by any *.sh
# *.sh file supports Unix/Linux shell command

# Available environment variable
# $EVENT_STAGE when an event occurred, there are two stage for invoking commands.
# When an event occurred, it enters OCCUR stage and invoking related commands.
# When an event finished, it enters FINISH stage and invoking related commands.
# $EVENT represents the event identification, $EVENT_CONDITION represents the condition identification.
#  To understand the value definition of both environment variable, please check online help or user's manual.
# $MODULE_NO represents a UPS module number to help identify which module the event occur on. (Agent only)

# Please save the script here
# centos:  usr/local/PPB/extcmd/host-stop-shutdown.sh
#Ubuntu : /opt/PPB/extcmd


if [ "$EVENT_STAGE" = "OCCUR" ]; then

/usr/bin/ssh AdminAccount@IpAddress /sbin/poweroff
        echo
fi

if [ "$EVENT_STAGE" = "FINISH" ]; then
        echo
fi
```

fehlschlägt, prüfen Sie Firewall, Benutzerrechte und Pfade zum ssh-Befehl.

7. Konfiguration in MacOS

7.1. SSH-Schlüssel erstellen

Für den automatisierten SSH-Zugriff auf das NAS ist ein passwortloses Login erforderlich. Dazu wird ein SSH-Schlüsselpaar erzeugt und auf dem NAS hinterlegt.

1. Öffnen Sie das Terminal unter
   Programme > Dienstprogramme > Terminal.

2. Generieren Sie ein neues RSA-Schlüsselpaar:

ssh-keygen -t rsa

Bestätigen Sie alle Eingaben mit der Eingabetaste, um die Standardwerte (ohne Passphrase) zu verwenden.

```
user@Users-Mac-mini ~ % sudo ssh-keygen -t rsa
Password:
Generating public/private rsa key pair.
Enter file in which to save the key (/var/root/.ssh/id_rsa):
Created directory '/var/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /var/root/.ssh/id_rsa.
Your public key has been saved in /var/root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:gzxu8Gpug5Hwj86GdbPV88DEuNRcFy54pf9rg5YfQ2c root@Users-Mac-mini.local
The key's randomart image is:
+---[RSA 3072]----+
|             o.  |
|          ..+.   |
|        =..+..   |
|.     .o.=. o    |
| o ...+=S   . . E|
|  = o+o.=.   o o |
| o * ++  +   o+  |
|..+ *o    . + o+ |
| oo+o.     . oo. |
+----[SHA256]-----+
```

3. Kopieren Sie den öffentlichen Schlüssel auf das NAS:

scp ~/.ssh/id_rsa.pub AdminBenutzer@IP-Adresse:~/.ssh/mac_keys

```
user@Users-Mac-mini ~ % scp ~/.ssh/id_rsa.pub admin@192.168.188.39:~/.ssh/mac_keys

The authenticity of host '192.168.188.39 (192.168.188.39)' can't be established.
RSA key fingerprint is SHA256:lY0ENKLeUJLQCvVA2cpB9cZDEloeF2kXyje0iap7R2c.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.188.39' (RSA) to the list of known hosts.
admin@192.168.188.39's password:
```

4. Melden Sie sich per SSH am NAS an:

```
ssh AdminBenutzer@IP-Adresse
```

5. Hängen Sie den öffentlichen Schlüssel an authorized_keys an:

```
cat ~/mac_keys >> ~/.ssh/authorized_keys
```

6. Ändern Sie die Zugriffsberechtigung des öffentlichen Schlüssels.

```
chmod 600 ~/.ssh/authorized_keys
```

7. Beenden Sie die SSH-Sitzung mit:

```
exit
```

Hinweis: Falls Root-Rechte erforderlich sind, verwenden Sie den Befehl sudo, statt einen Root-Login dauerhaft zu aktivieren.

7.2. Externen Befehl bearbeiten

1. Öffnen Sie die Datei default.sh im PowerPanel-Verzeichnis:

```
vim /Applications/PowerPanel/extcmd/default.sh
```

2. Fügen Sie folgenden Befehl ein, je nach NAS-Typ:

Für Synology:

```
/usr/bin/ssh AdminBenutzer@IP-Adresse "sudo /sbin/poweroff"
```

Für QNAP:

```
/usr/bin/ssh AdminBenutzer@IP-Adresse "/sbin/poweroff"
```

Ersetzen Sie AdminBenutzer und IP-Adresse durch die tatsächlichen Zugangsdaten des NAS.

3. Speichern Sie die Datei und machen Sie sie ausführbar:

```
chmod +x /Applications/PowerPanel/extcmd/default.sh
```

7.3. Energieoptionen konfigurieren (optional)

Falls macOS direkt an der USV angeschlossen ist, können zusätzliche Optionen über die Systemeinstellungen gesetzt werden:

1. Öffnen Sie Systemeinstellungen > Energie sparen.
2. Wechseln Sie zur Registerkarte **„USV “**.

3. Klicken Sie auf „Optionen für das Ausschalten… “.
4. Legen Sie z. B. fest:
   „Computer ausschalten nach Nutzung der USV-Batterie für: [Zeitdauer] “.
5. Schließen Sie die Konfiguration mit **„Fertig“** ab.

Beispiel von default.sh bei Synology NAS:

```
#!/bin/sh


# You can write your own commands by any *.sh
# *.sh file supports Unix/Linux shell command

# Available environment variable
# $EVENT_STAGE when an event occurred, there are two stage for invoking commands.
# When an event occurred, it enters OCCUR stage and invoking related commands.
# When an event finished, it enters FINISH stage and invoking related commands.
# $EVENT represents the event identification, $EVENT_CONDITION represents the condition identification.
#  To understand the value definition of both environment variable, please check online help or user's manual.
# $MODULE_NO represents a UPS module number to help identify which module the event occur on. (Agent only)

# Please save the script here
# centos:  usr/local/PPB/extcmd/host-stop-shutdown.sh
#Ubuntu : /opt/PPB/extcmd


if [ "$EVENT_STAGE" = "OCCUR" ]; then

/usr/bin/ssh AdminAccount@IpAddress /sbin/poweroff
        echo
fi

if [ "$EVENT_STAGE" = "FINISH" ]; then
        echo
fi
```

8. Vorschlag

Für das automatisierte Herunterfahren eines NAS ist ein Benutzerkonto mit Administratorrechten erforderlich. Bei Synology-Systemen entspricht das Root-Passwort standardmäßig dem Administratorpasswort, sofern nicht geändert.

Da NAS-Systeme häufig dynamische IP-Adressen über DHCP erhalten, kann es bei wechselnden Adressen zu Verbindungsproblemen kommen. Um eine stabile Kommunikation sicherzustellen, wird die Verwendung eines **statischen IP-Adressbereichs** oder eines **Dynamic DNS (DDNS)-Dienstes** empfohlen. Informationen zur DDNS-Konfiguration finden Sie im Benutzerhandbuch des jeweiligen NAS-Herstellers.

Die PowerPanel® Business Lokal Software wurde erfolgreich mit NAS-Systemen von **Synology** und **QNAP** getestet. Eine vollständige Übersicht kompatibler Systeme steht auf der CyberPower-Website zur Verfügung.

CyberPower

CyberPower | USV Systeme, PDU, Überspannungsschutz | Professionelle Stromversorgung Lösungen

CyberPower Systems GmbH

Edisonstr. 16,

85716 Unterschleissheim

Germany

T: +49-89-1 222 166 -0 F: +49-89-1 222 166 -29

E-mail: service@cyberpower.de

Web: www.cyberpower.de

CyberPower Wiki: Home | CyberPower Wiki (cyberpowersystems.de)

Dokumentversion: 1.2 Stand: Mai 2025
erstellt von: Athanasia Balkoura

CyberPower Software & Integration Support – Germany