

Synology

Alles Themen rund um die Synology

- [Ordner Berechtigungen](#)
- [Externe Festplatte sicher löschen](#)
- [Neuinstallation](#)
- [Self-Service-Password Installation](#)
- [LDAP Installation](#)

Ordner Berechtigungen

Ordner vor dem Löschen schützen

Folgende Ordner- und Dateistruktur ist vorhanden:

```
Demoordner
Demoordner/Datei1.pdf
Demoordner/Datei2.pdf
Demoordner/FooOrdner/
Demoordner/FooOrdner/Datei3.pdf
Demoordner/FooOrdner/Datei4.pdf
```

`Demoordner` ist eine Freigabe und `FooOrdner` ist der zu schützende Ordner. Sämtliche Dateien sollen gelöscht werden können.

Demoordner

Im freigegebenen/übergeordnetem Ordner `Demoordner` muss die Berechtigung `Unterordner und Dateien löschen` dem Benutzer/Gruppe entzogen werden.

Berechtigungs-Editor

Benutzer oder Gruppe:

Übernehmen von:

Typ:

Anwenden auf:

Berechtigung

- Ordner durchqueren/Dateien ausführen
- Ordner auflisten/Daten lesen
- Attribute lesen
- Erweiterte Attribute lesen
- Leseberechtigungen

▼ Schreiben

- Dateien erstellen/Daten schreiben
- Ordner erstellen/Daten anhängen
- Attribute schreiben
- Erweiterte Attribute schreiben
- Unterordner und Dateien löschen
- Löschen

Berechtigung

Benutzerdefiniert

Lesen & Schreib...

Lesen & Schreib...

Lesen & Schreib...

OK

Schließen

OK

Schließen

Die Berechtigung **Löschen** bedeutet "Dateien löschen".

FooOrdner

Beim zu schützenden Ordner **FooOrdner** müssen die **Berechtigungen ausschließlich** gemacht werden.

Eigenschaften

Allgemein

Berechtigung

Erstellen

Löschen

Bearbeiten

Erweiterte Optionen ▾

Benutzer oder Gruppe



foo



G-Demo@ldap.familie-jonas.bayern



administrators

Zulassen

Lesen & Schreib...



administrators@ldap.familie-jonas.bayern

Zulassen

Lesen & Schreib...

Übernommene Berechtigungen ausschließen

Übernommene Berechtigungen ausdrücklich machen

Berechtigungsprüfung

Auf diesen Ordner, die Unterordner und Dateien anwenden.

OK

Schließen

Der eingeschlossenen Berechtigung das **Löschen** entziehen

Eigenschaften

Allgemein **Berechtigung**

Erstellen Löschen Bearbeiten Erweiterte Optionen ▾

Benutzer oder Gruppe	Typ	Berechtigung
	Verweigern	Benutzerdefiniert
	Zulassen	Benutzerdefiniert
	Zulassen	Lesen & Schreib...
	Zulassen	Lesen & Schreib...
	Zulassen	Lesen & Schreib...

Berechtigungs-Editor

Benutzer oder Gruppe:

Übernehmen von:

Typ:

Anwenden auf:

Berechtigung

- Ordner durchqueren/Dateien ausführen
- Ordner auflisten/Daten lesen
- Attribute lesen
- Erweiterte Attribute lesen
- Leseberechtigungen
- ▾ **Schreiben**
 - Dateien erstellen/Daten schreiben
 - Ordner erstellen/Daten anhängen
 - Attribute schreiben
 - Erweiterte Attribute schreiben
 - Unterordner und Dateien löschen
 - Löschen

OK Schließen

Die Berechtigung **Löschen** bedeutet "Diesen Ordner löschen".

Externe Festplatte sicher löschen

Festplatte sicher löschen NAS

You:

Ich habe Festplatten die ich sicher löschen möchte. Ich hatte mal eine Software die alle Sektoren mehrfach mit 0 und 1 nacheinander beschreibt.

Da das ganze aber sehr lange dauert, würde ich es gerne von meiner Synology erledigen lassen. Ich habe ein externen Festplattengehäuse mit USB Anschluss.

ChatGPT:

Wenn du deine Festplatten sicher löschen möchtest, indem du sie mehrfach mit Daten (z. B. abwechselnd 0en und 1en) überschreibst, kannst du das auch direkt über deine **Synology NAS** erledigen - vorausgesetzt, sie erkennt das externe USB-Gehäuse korrekt. Hier sind deine Optionen:

? Variante 1: Per SSH mit `dd` oder `shred` (wenn verfügbar)

1. **SSH aktivieren** (Systemsteuerung > Terminal & SNMP > SSH-Dienst aktivieren).
2. **Mit SSH verbinden** (z. B. per `ssh admin@ip-der-nas`).
3. **Festplatte identifizieren:**

```
dmesg | grep sd
lsblk
fdisk -l
```

Achte auf Geräte wie `/dev/sdq` (für die USB-Platte).

4. **Festplatte überschreiben mit `dd` (1-mal mit Nullen):**

```
dd if=/dev/zero of=/dev/sdq bs=1M status=progress
```

5. **Optional: Überschreiben mit zufälligen Daten:**

```
dd if=/dev/urandom of=/dev/sdq bs=1M status=progress
```

6. Optional: `shred` (wenn verfügbar, für mehrfaches Überschreiben):

```
shred -v -n 3 -z /dev/sdq
```

`-n 3` = dreimaliges Überschreiben, `-z` = letzter Durchgang mit Nullen.

“**Achtung:** Stelle sicher, dass du wirklich das richtige Gerät erwischst! Falsches Gerät = Datenverlust!

? Variante 2: DSM-Oberfläche (eingeschränkt)

DSM selbst bietet **keine vollständige Löschfunktion** für externe Laufwerke. Interne Volumes kannst du ggf. mit „Sicher löschen“ (Secure Erase) formatieren, aber **nicht über USB angeschlossene Laufwerke**.

?? Wichtige Hinweise

- Der `dd`-Befehl ist zwar einfach, aber **zeitintensiv**, vor allem bei großen Laufwerken.
- Die Nutzung von `shred` ist effektiver, aber ggf. **nicht standardmäßig auf DSM vorhanden** (du müsstest `shred` per `ipkg` oder `Entware` installieren).
- Ein einfacher `dd` mit `/dev/zero` oder `/dev/urandom` reicht oft aus, insbesondere bei SSDs und nicht-geheimen Daten.

Möchtest du wissen, wie du `shred` oder ähnliche Tools auf der Synology nachinstallierst?

You:

ja wie installiere ich es

ChatGPT:

Um `shred` oder andere Linux-Tools wie `coreutils` auf deiner **Synology NAS** zu installieren, kannst du den Paketmanager **Entware** verwenden. Das geht so:

? Schritt-für-Schritt: `shred` auf Synology über Entware installieren

1. SSH-Zugang aktivieren

- Öffne DSM:
`Systemsteuerung > Terminal & SNMP > SSH-Dienst aktivieren`
- Dann per SSH verbinden:

```
ssh admin@<IP-deiner-NAS>
```

2. Entware installieren

Entware ist ein Paketmanager ähnlich wie `apt` oder `brew`. Die Installation hängt von deinem NAS-Modell und deiner DSM-Version ab.

Möglichkeit A: Manuell (empfohlen)

1. **Starte Synology Package Center.**
2. Aktiviere unter *Einstellungen > Paketquellen* „Installation von Paketen aus beliebigen Quellen“.
3. Gehe zur Webseite: <https://github.com/Entware/Entware/wiki/Install-on-Synology-NAS>
4. Dort findest du ein passendes Skript, z. B.:

```
wget -O - http://bin.entware.net/aarch64-k3.10/installer/generic.sh | sh
```

(Der genaue Befehl hängt von deiner Architektur ab — `uname -a` hilft.)

3. Pfad konfigurieren (falls nötig)

Nach der Installation musst du `/opt/bin` in den Pfad aufnehmen:

```
echo 'export PATH=$PATH:/opt/bin' >> ~/.profile  
source ~/.profile
```

4. `shred` installieren

```
opkg update  
opkg install coreutils-shred
```

“Jetzt kannst du `shred` verwenden:

```
shred -v -n 3 -z /dev/sdq
```

? Wie findest du deine CPU-Architektur?

Führe aus:

```
uname -m
```

Ergebnis:

- `x86_64` → PC-Architektur
 - `armv7l` oder `aarch64` → ARM, je nach Modell
-

Soll ich dir helfen, den richtigen `Entware`-Installer für dein NAS-Modell zu finden, wenn du mir das Modell oder die Architektur nennst?

You:

```
ipkg install coreutils-shred Unknown package 'coreutils-shred'. Collected errors:
```

- `opkg_install_cmd`: Cannot install package coreutils-shred.

ChatGPT:

Danke für den Hinweis! Der Fehler deutet darauf hin, dass du `ipkg` statt `opkg` verwendest – das ist typisch für ältere Systeme oder das veraltete **Optware**. Aktuell und empfohlen ist **Entware**, das `opkg` nutzt.

? So geht's korrekt mit **Entware**:

? Schritt 1: Alte `ipkg`-/Optware-Installation entfernen (falls vorhanden)

Falls du wirklich noch `ipkg` nutzt, solltest du das durch Entware ersetzen, da `ipkg` veraltet ist und viele Pakete nicht mehr verfügbar sind.

? Neuinstallation von Entware (aktuell & gepflegt)

1. CPU-Architektur prüfen:

```
uname -m
```

Beispiel-Ausgaben:

- `x86_64` → 64-Bit Intel/AMD
- `armv7l` oder `aarch64` → ARM-basiert (z. B. DS218, DS220 etc.)

2. Passendes Install-Skript finden: Öffne diese Seite:

<https://github.com/Entware/Entware/wiki/Install-on-Synology-NAS>

3. Installer ausführen (je nach Architektur):

Beispiel (für `aarch64` / ARM64):

```
wget -O - - http://bin.entware.net/aarch64-k3.10/installer/generic.sh | sh
```

4. `opkg` einrichten und `shred` installieren:

```
echo 'export PATH=$PATH:/opt/bin:/opt/sbin' >> ~/.profile
source ~/.profile
opkg update
opkg install coreutils-shred
```

5. Verwendung:

```
shred -v -n 3 -z /dev/sdq
```

Wenn du magst, kannst du mir das Ergebnis von `uname -m` und dein NAS-Modell sagen – dann gebe ich dir exakt den passenden Install-Befehl für dein Gerät.

You:

gibt es shred auch als synology package mit oberfläche?

ChatGPT:

Leider **gibt es `shred` oder ein vergleichbares Tool mit grafischer Oberfläche nicht als offizielles Synology-Paket** im DSM-Paketzentrum. Synology bietet keine GUI-basierte Lösung zum **sicheren Überschreiben externer Laufwerke** an – insbesondere nicht für via USB angeschlossene Festplatten.

? Alternativen mit (teilweiser) Oberfläche:

1. Secure Erase – nur für interne SSDs (über DSM)

- DSM unterstützt Secure Erase **nur für bestimmte interne SSDs, nicht** für USB-Platten.

- Zu finden unter:

Speicher-Manager > HDD/SSD > Aktion > SSD sicher löschen

(nur sichtbar, wenn SSD unterstützt wird)

2. Drittanbieter-Tools auf PC verwenden (GUI)

Wenn du Wert auf eine Oberfläche legst, wäre es einfacher, die Platte direkt an einen PC (Windows/Linux/macOS) anzuschließen und dort eines der folgenden Tools zu verwenden:

Tool	Plattform	Funktion	Oberfläche
DBAN	Bootbar	Mehrfaches Überschreiben	Nein (textbasiert)
Eraser	Windows	Einzelnes oder mehrfaches Löschen	☐
Hard Disk Sentinel	Windows/Linux	S.M.A.R.T. + Löschen	☐
Parted Magic	Bootbar (Linux)	Secure Erase, <code>shred</code> , <code>dd</code> , GUI	☐
macOS Festplattendienstprogramm	macOS	Mehrfaches Löschen	☐

3. Docker-Container auf Synology mit Web-GUI?

- Du könntest theoretisch ein Linux-basiertes Tool wie `shred` in einem Docker-Container installieren, aber auch hier hättest du keine intuitive GUI, außer du setzt manuell eine Weboberfläche auf.

? Fazit

- **DSM selbst bietet keine GUI-Lösung für sicheres Löschen externer Laufwerke.**
- Die einfachste Lösung mit GUI ist, die Festplatte an einen Windows- oder Linux-PC anzuschließen und dort ein passendes Tool zu nutzen.

Möchtest du z. B. ein **bootfähiges Tool wie DBAN oder Parted Magic** verwenden und brauchst eine Anleitung dazu?

You:

```
root@Tresor001:~# shred -v -n 3 -z /dev/sdq
shred: /dev/sdq: pass 1/4 (random)...
shred: /dev/sdq: pass 1/4 (random)...722MiB/3.7TiB 0%
shred: /dev/sdq: pass 1/4 (random)...1.4GiB/3.7TiB 0%
shred: /dev/sdq: pass 1/4 (random)...2.2GiB/3.7TiB 0%
shred: /dev/sdq: pass 1/4 (random)...3.0GiB/3.7TiB 0%
shred: /dev/sdq: pass 1/4 (random)...3.8GiB/3.7TiB 0%
shred: /dev/sdq: pass 1/4 (random)...4.6GiB/3.7TiB 0%
shred: /dev/sdq: pass 1/4 (random)...5.4GiB/3.7TiB 0%
shred: /dev/sdq: pass 1/4 (random)...6.2GiB/3.7TiB 0%
```

(random)...7.0GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...7.8GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...8.5GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...9.3GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...10GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...11GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...12GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...13GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...14GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...15GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...16GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...17GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...18GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...19GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...20GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...21GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...22GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...23GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...24GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...25GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...26GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...27GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...28GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...29GiB/3.7TiB 0% shred: /dev/sdq: pass 1/4 (random)...30GiB/3.7TiB 0%

Kann ich das mit screen in den Hintergrund auslagern?

ChatGPT:

Ja, absolut – du **kannst** `shred` **mit** `screen` **in den Hintergrund auslagern**, damit die Löschung weiterläuft, auch wenn du die SSH-Verbindung trennst. Das ist auf der Synology sehr sinnvoll bei langen Vorgängen wie dem sicheren Löschen großer Festplatten (wie deine 3.7 TiB).

? So nutzt du `screen` auf deiner Synology:

1. `screen` installieren (falls noch nicht vorhanden):

```
opkg install screen
```

2. Neuen Screen starten:

```
screen -S shred-session
```

Du befindest dich jetzt in einer neuen virtuellen Konsole.

3. Befehl ausführen:

```
shred -v -n 3 -z /dev/sdq
```

4. Screen trennen (ohne den Prozess zu stoppen):

Drücke:

```
Ctrl + A, dann D
```

→ Das trennt die Sitzung, `shred` läuft im Hintergrund weiter.

5. Später wieder verbinden:

Zeige alle laufenden Screens:

```
screen -ls
```

Wieder verbinden:

```
screen -r shred-session
```

?Tipp: Log-Datei schreiben (optional)

Falls du den Fortschritt auch später nachvollziehen willst:

```
shred -v -n 3 -z /dev/sdq | tee /volume1/shred-log.txt
```

Möchtest du stattdessen `tmux` verwenden oder soll ich dir ein einfaches Script für das Löschen mit automatischem Logging schreiben?

You:

was ist tmux?

ChatGPT:

`tmux` ist ein moderner Terminal-Multiplexer – ähnlich wie `screen`, aber leistungsfähiger und flexibler. Er erlaubt dir, mehrere Shell-Sitzungen **in einem einzigen Terminalfenster** zu verwalten, zu teilen und dauerhaft laufen zu lassen, selbst wenn du die SSH-Verbindung trennst.

? Vergleich: `tmux` vs. `screen`

Feature	<code>screen</code>	<code>tmux</code>
Aktiv entwickelt	<input type="checkbox"/> (veraltet)	<input type="checkbox"/>
Fenster teilen (horizontal/vertikal)	<input type="checkbox"/> (rudimentär)	<input type="checkbox"/>
Mehrere Panes gleichzeitig anzeigen	<input type="checkbox"/>	<input type="checkbox"/>

Feature	screen	tmux
Anpassbares Layout	☐	☐
Scrollen mit Maus / Copy-Paste	☐	☐
Konfigurierbarkeit	Einfach	Hoch

? Beispiel: `shred` in `tmux` ausführen

1. Installieren (falls nötig):

```
opkg install tmux
```

2. Neue Session starten:

```
tmux new -s shred
```

3. Deinen Löschbefehl ausführen:

```
shred -v -n 3 -z /dev/sdq
```

4. Session trennen (ohne Abbruch): Drücke:

```
Ctrl + B, dann D
```

5. Wieder verbinden:

```
tmux attach -t shred
```

6. Offene Sessions anzeigen:

```
tmux ls
```

? Fazit

Wenn du nur gelegentlich eine einzelne Aufgabe wie `shred` laufen lässt, ist `screen` **völlig ausreichend**. Wenn du aber mehr willst (z. B. mehrere Prozesse gleichzeitig, visuelles Layout, Komfort), lohnt sich `tmux`.

Möchtest du `tmux` gleich ausprobieren oder eine kleine Cheat-Sheet-Hilfe dafür bekommen?

Neuinstallation

Ports (80/443) freigeben

Ausgelöste Aufgabe erstellen die beim Hochfahren ausgeführt wird:

Aufgabe erstellen

Allgemein Aufgabeneinstellungen

Allgemeine Einstellungen

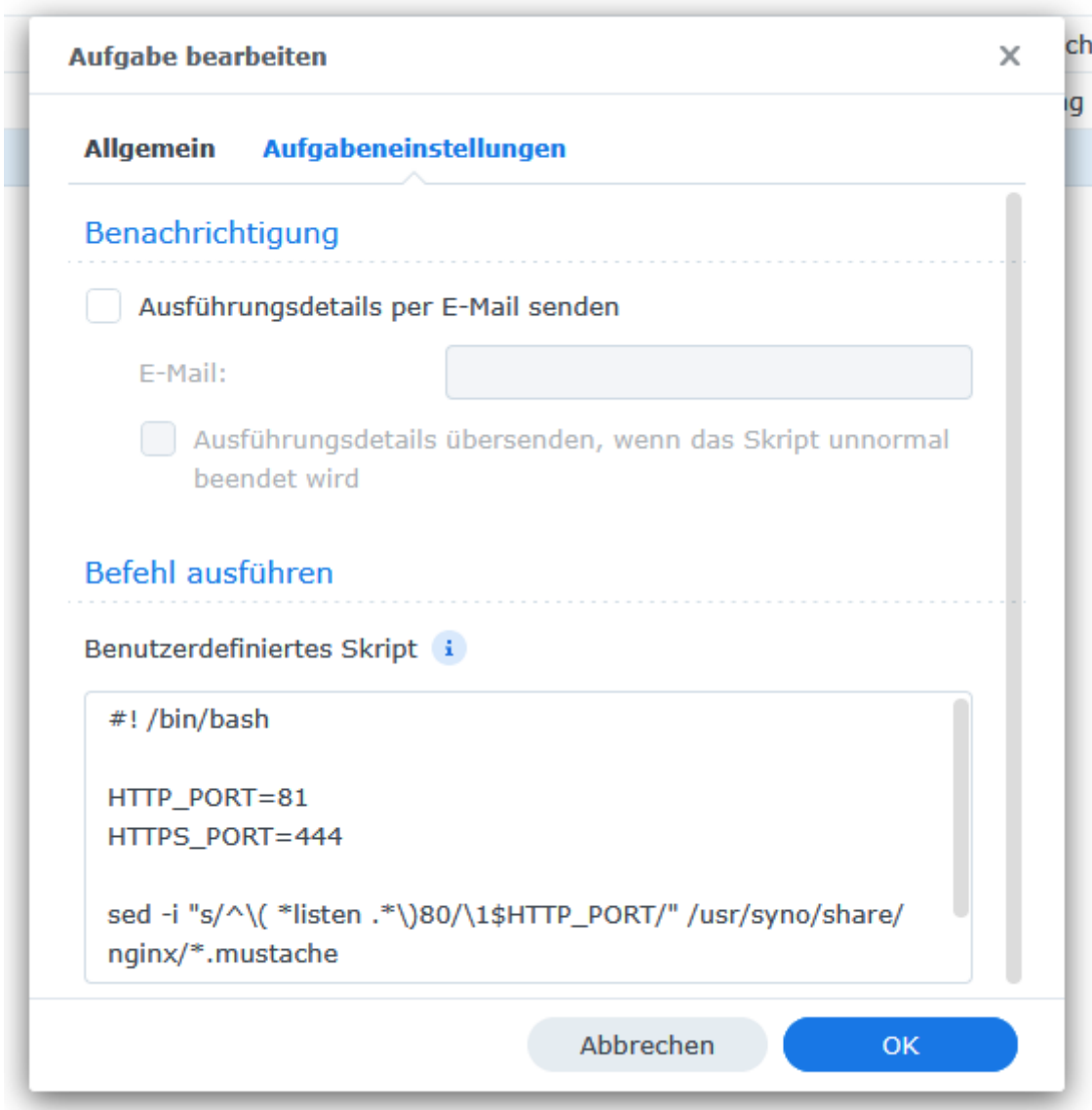
Aufgabe:

Benutzer:

Ereignis:

Vor-Aufgabe:

Aktiviert



```
#!/bin/bash

HTTP_PORT=81
HTTPS_PORT=444

sed -i "s/^\( *listen .*\)80/\1$HTTP_PORT/" /usr/syno/share/nginx/*.mustache
sed -i "s/^\( *listen .*\)443/\1$HTTPS_PORT/" /usr/syno/share/nginx/*.mustache
```

Service neu starten damit die Ports freigegeben werden

```
sudo synosystemctl restart nginx
```

Quelle: <https://www.simplehomelab.com/free-ports-80-and-443-on-synology/>

Die Synology 1x komplett neu starten, da nicht alle Ports gelöst wurden

Portainer installieren

Neues Netzwerk anlegen

```
docker network create --label com.docker.compose.network=default traefik
```

```
version: '2'
services:
  portainer:
    image: portainer/portainer-ce
    container_name: portainer
    labels:
      - com.centurylinklabs.watchtower.enable=true
      - traefik.enable=true
      - traefik.http.routers.portainer.rule=Host(`portainer.lindtal-server.schulen-
freudenberg.de`)
      - traefik.http.routers.portainer.entrypoints=web
      - traefik.http.routers.portainer.middlewares=portainer-redirect-websecure
      - traefik.http.routers.portainer.entrypoints=websecure
      - traefik.http.routers.portainer.tls.certresolver=allinkl
      - traefik.http.middlewares.portainer-redirect-websecure.redirectscheme.scheme=https
      - traefik.http.services.portainer.loadbalancer.server.port=9000
      - traefik.docker.network=traefik
    environment:
      - TZ=Europe/Berlin
    volumes:
      - /volume1/docker/portainer/data:/data
      - /var/run/docker.sock:/var/run/docker.sock:ro
    ports:
      - 8000:8000
      - 9000:9000
    restart: unless-stopped
    #network_mode: bridge
    networks:
      - traefik
networks:
  traefik:
```

```
external: true
```

Traefik installieren

docker-compose.yml

```
services:
  traefik:
    image: traefik:v3.4
    container_name: traefik
    environment:
      - IONOS_API_KEY=123.456
    volumes:
      - /volume1/docker/traefik/letsencrypt:/letsencrypt
      - /volume1/docker/traefik/config:/etc/traefik
      - /var/run/docker.sock:/var/run/docker.sock
    ports:
      - 80:80
      - 443:443
      - 32789:8080
    restart: unless-stopped
    healthcheck:
      test: ["CMD", "traefik", "healthcheck"]
      interval: 30s
      timeout: 5s
      retries: 3
    networks:
      - traefik
  whoami:
    image: "traefik/whoami"
    container_name: "simple-service"
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.whoami.rule=Host(`whoami.localhost`)"
      - "traefik.http.routers.whoami.entrypoints=web"
    networks:
      - traefik
networks:
  traefik:
```

```
external: true
```

`traefik.yml` und `rules.yml` anlegen

Self-Service-Password Installation

Neuen Benutzer Anlegen

Eine neuen Benutzer `service.ssp` anlegen und diese der `admin` und `Directory Operators` Gruppe hinzufügen.

Verbindungstest

Bei Verbindungsproblemen kann man mittels `ldapsearch` versuchen sich zum Server zu verbinden:

ldapsearch & nano installieren

```
apt-get update \  
&& apt-get install -y --no-install-recommends ldap-utils nano \  
&& rm -rf /var/lib/apt/lists/*
```

ldapsearch mit ssl

```
ldapsearch -x -H 'ldaps://ldap.schulen-freudenberg.de' -D 'CN=service.login,OU=IT  
admins,OU=Services,DC=ldap,DC=schulen-freudenberg,DC=de' -W -b 'DC=ldap,DC=schulen-  
freudenberg,DC=de' -LLL -d -1
```

ldapsaerch ohne ssl

```
ldapsearch -x -H 'ldap://ldap.schulen-freudenberg.de' -D 'CN=service.login,OU=IT  
admins,OU=Services,DC=ldap,DC=schulen-freudenberg,DC=de' -W -b 'DC=ldap,DC=schulen-  
freudenberg,DC=de' -LLL -d -1
```

LDAP Installation

? Zertifikat mit ACME automatisch installieren & verwalten (Docker, Synology, All-Inkl)

☐ Offizielles Projekt:

☐ [acme.sh - GitHub](#)

? Docker Container

```
version: "2.1"
services:
  acme.sh:
    image: neilpang/acme.sh
    container_name: tool-acme.sh
    environment:
      - PUID=1026          # Benutzer-ID (z. B. acme user)
      - PGID=100         # Gruppen-ID
      - TZ=Europe/Berlin
      - UMASK_SET=002
    network_mode: host
    volumes:
      - /volume3/docker/acme/config:/acme.sh # persistente Konfiguration
      - /volume3/docker/acme/key:/key       # optionale Schlüsselablage
    command: daemon
    restart: unless-stopped
```

? DSM-Zugangsdaten setzen (für Deployment auf Synology)

☐ Anleitung: [Synology NAS Guide \(acme.sh\)](#)

Im Container:

```
export SYNO_USERNAME=adminUser
export SYNO_PASSWORD=adminPassword
export SYNO_SCHEME=https
export SYNO_HOSTNAME=dsm.familie-jonas.bayern
export SYNO_PORT=5001
export SYNO_CREATE=1
```

? Benachrichtigung per Pushover aktivieren

☐ [Pushover Notify-Hook Doku](#)

1. Zugangsdaten exportieren:

```
export PUSHOVER_TOKEN=your_token
export PUSHOVER_USER=your_user_key
```

2. Notify-Hook aktivieren:

```
acme.sh --set-notify --notify-hook pushover --notify-level 3
```

`--notify-level` Bedeutungen:

Level	Beschreibung
0	Deaktiviert
1	Nur bei Fehlern
2	Bei erfolgreicher Erneuerung oder Fehler
3	Immer (auch wenn Zertifikat übersprungen wurde)

☐ **Hinweis:** Nach erfolgreichem Test mit `--notify-level 3` ggf. auf `--notify-level 2` reduzieren.

? DNS API (All-Inkl)

☐ Doku: [dns_kas](#)

```
export KAS_Login=<ACCOUNTID>
export KAS_Authdata=<PLAINTEXTPASSWORD>
export KAS_Authtype=plain
```

? Zertifikat manuell testen

Zertifikat erstellen:

```
acme.sh --issue -d ldap.familie-jonas.bayern --dns dns_kas --keylength 2048 --server letsencrypt
```

Hinweis:

Ohne `--keylength` erstellt `acme.sh` standardmäßig ein **ECC-Zertifikat**.

Die Angabe `--keylength 2048` erzwingt ein **RSA-Zertifikat**, das besser kompatibel ist – z. B. mit Synology DSM.

Zertifikat deployen:

```
acme.sh --deploy -d ldap.familie-jonas.bayern --deploy-hook synology_dsm
```

?? Automatische Erneuerung (Cronjob im Container)

Interner Cronjob aktivieren:

```
acme.sh --install-cronjob
```

→ Dieser läuft alle 24h automatisch im Container (sofern `command: daemon` im Docker aktiv ist)

Manuell testen:

```
acme.sh --cron
```

Beispielausgabe:

```
[Wed Aug 6 09:59:57 CEST 2025] ===Starting cron===  
[Wed Aug 6 09:59:57 CEST 2025] Already up to date!  
[Wed Aug 6 09:59:57 CEST 2025] Automatically upgraded to: 3.1.2  
[Wed Aug 6 09:59:57 CEST 2025] Renewing: 'ldap.familie-jonas.bayern'  
[Wed Aug 6 09:59:57 CEST 2025] Skipping. Next renewal time is: 2025-10-04T07:27:23Z  
[Wed Aug 6 09:59:57 CEST 2025] Add '--force' to force renewal.  
[Wed Aug 6 09:59:57 CEST 2025] Skipped ldap.familie-jonas.bayern  
[Wed Aug 6 09:59:57 CEST 2025] Sending via: pushover
```

```
[Wed Aug 6 09:59:59 CEST 2025] PUSHOVER send success.
```

```
[Wed Aug 6 09:59:59 CEST 2025] pushover Success
```

```
[Wed Aug 6 09:59:59 CEST 2025] ===End cron===
```

? Optional: Alles als Shell-Skript zusammenführen

```
#!/bin/bash

# Konfiguration setzen
export SYN0_USERNAME=adminUser
export SYN0_PASSWORD=adminPassword
export SYN0_SCHEME=https
export SYN0_HOSTNAME=dsm.familie-jonas.bayern
export SYN0_PORT=5001
export SYN0_CREATE=1

export KAS_Login=<ACCOUNTID>
export KAS_Authdata=<PLAINTEXTPASSWORD>
export KAS_Authtype=plain

export PUSHOVER_TOKEN=your_token
export PUSHOVER_USER=your_user_key

# Zertifikat ausstellen + deployen
acme.sh --issue -d ldap.familie-jonas.bayern --dns dns_kas --keylength 2048 --server
letsencrypt --force
acme.sh --deploy -d ldap.familie-jonas.bayern --deploy-hook synology_dsm
```

Dieses Skript kann auch über den DSM-Aufgabenplaner regelmäßig (oder auch einmalig zum Anlegen der Konfiguration) ausgeführt werden – alternativ zur Docker-internen Automatik.