EINRICHTUNG NAS

Letzte Änderung: **05.02.2024**

Diese Anleitung beschreibt die Einrichtung der NAS (Datenablage) für die Musterlösung Grundschule SH.

Änderung vom 05.02.2024

- Einige Screenshots wurden ausgetauscht.

Änderung vom 29.11.2023

- Die Screenshots im Kapitel Datensicherung einrichten wurden angepasst. Die Sicherheitsrotation soll abweichend zur bisherigen Einrichtungsanleitung aktiviert werden.

Änderung vom 04.10.2023:

- Das maximale SMB-Protokoll für die Dateidienste wird auf „SMB3“ eingestellt (siehe Kapitel Ordner anlegen).
- Die Screenshots zur Einrichtung von Quickconnect in Ausnahmefällen wurden entfernt (siehe Kapitel Cloudzugriff einrichten).

Änderung vom 10.07.2023:

- Der Ordner und das Benutzerkonto „DKS“ wird in „Wartung“ umbenannt (siehe Kapitel Benutzerkonten anlegen und Kapitel Ordner anlegen).

Ältere Änderungen sind hier zu finden: Kapitel Änderungshistorie.

1 Hinweise

Innerhalb der Musterlösung Grundschule SH wird für die Nutzung einer Datenablage und weiterer zentraler Funktionen (VPN-Server, Cloudzugriff) ein Synology-NAS eingesetzt. Das passende Disk- beziehungsweise Rackstationmodell von Synology hängt vom angedachten Nutzungsszenario ab.

Grundsätzlich sollte eine Synology-Diskstation mit mindestens **2 Festplatten** zum Einsatz kommen, die im **Raid 1** betrieben werden (beziehungsweise Synology Hybrid Raid mit Ausfalltoleranz), so dass sichergestellt ist, dass auch beim Ausfall einer Festplatte, dass System weiterläuft. Die Größe der Laufwerke sollte mindestens **2 TB** betragen, hängt jedoch von der angedachten Nutzung ab. Über eine extern angeschlossene Festplatte sollte ein **Backup** realisiert werden.

Aktuell wird innerhalb der Musterlösung Grundschule SH das **Synology-Modell DS 723+** (Windows-Endgeräte) bzw. **DS 224+** (iPads) verwendet.

2 Grundlegende Einrichtung

Zunächst die Synology-Diskstation beziehungsweise -Rackstation über beide Anschlüsse „LAN 1“ und „LAN 2“ mit dem Switch der Musterlösung (Adminnetz) verbinden und wie in der mitgelieferten Anleitung beschrieben die aktuelle Version (7.2 bzw. neuer) des Diskstation-Managers (DSM) installieren.

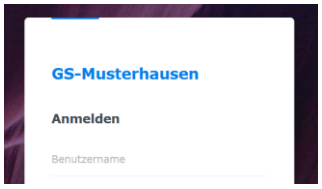
Für den vorhandenen Admin-Nutzer ein Übergangs-Kennwort erstellen.

Hinweis: Der Benutzer wird später durch einen anderen Admin-User ersetzt.

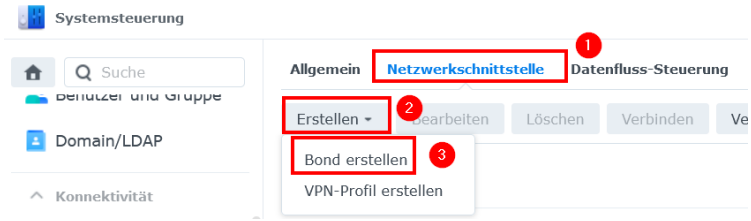
3 Netzwerkkonfiguration vornehmen

In der Systemsteuerung „Netzwerk“ (1) öffnen und unter „Allgemein“ (2) – falls noch nicht geschehen – als Servernamen den Schulnamen (zum Beispiel „GS-Musterhausen“) eingeben (3). Es sind maximal 15 Zeichen erlaubt, Leerzeichen darf der Name nicht enthalten:

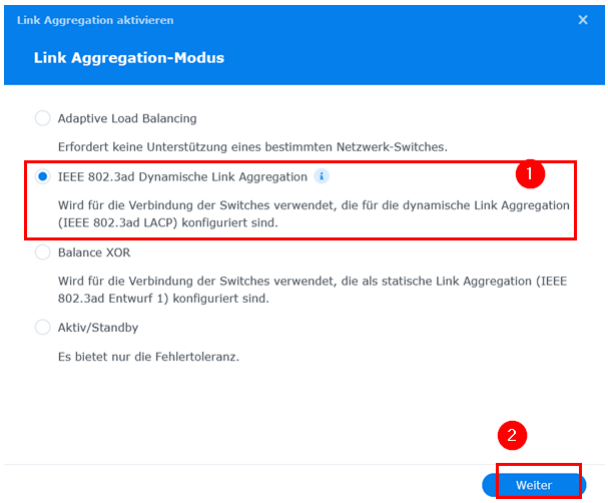
Hinweis: Der vergebene Servername erscheint über dem Login-Bereich der Diskstation. Dass hier der Name der Schule auftaucht, ist insbesondere für den Außenzugriff wichtig:



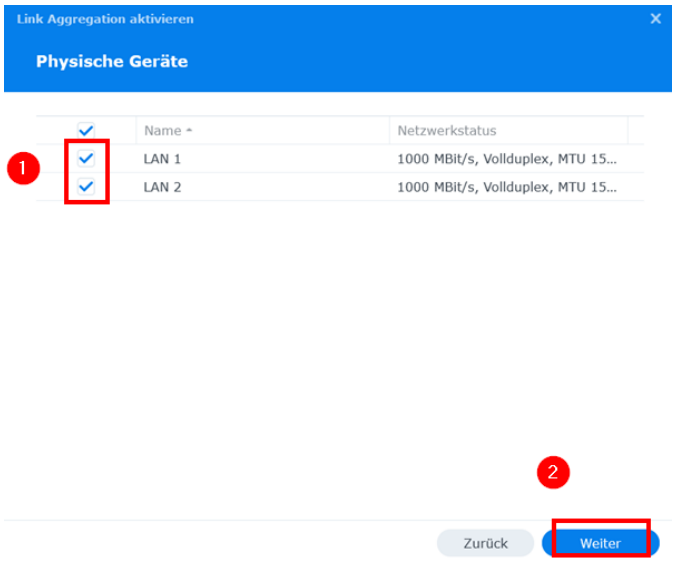
Die beiden angeschlossenen LAN-Ports sollen aggregiert werden. Dazu im Reiter „Netzwerkschnittstelle“ (1) den Menüpunkt „Erstellen“ (2) und „Bond erstellen“ (3) wählen:



Im Einrichtungsassistenten zur Link-Aggregation „Dynamische Link Aggregation“ (Balance-TCP) wählen (1) und mit „Weiter“ bestätigen (2):

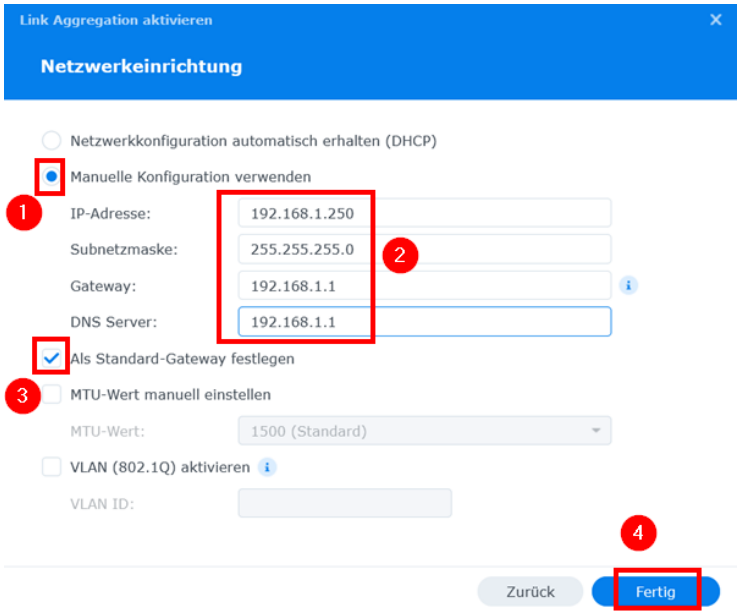


Die beiden Ports „LAN 1“ und „LAN 2“ auswählen (1) und mit „Weiter“ bestätigen (2):

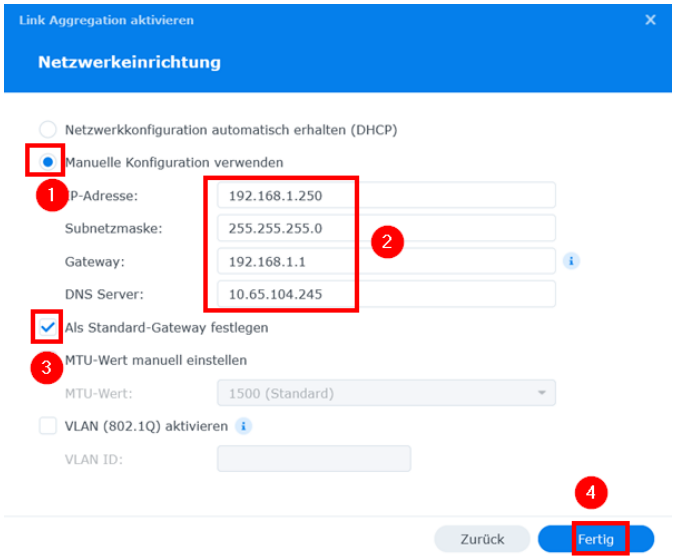


Im Anschluss die manuelle Schnittstellen-Konfiguration einstellen (1) und je nach genutzter Internetanbindung nachfolgende Einstellungen vornehmen:

- Wenn der pädagogische Breitbandanschluss des Landes **nicht** genutzt wird: Die IP-Adresse der Datenablage auf 192.168.1.250, das Standard-Gateway auf 192.168.1.1 sowie den DNS Server auf 192.168.1.1 (alternativ auch 9.9.9.9) festlegen (2), Häkchen für „Als Standard-Gateway festlegen“ setzen (3) und mit „Fertig“ bestätigen (4):

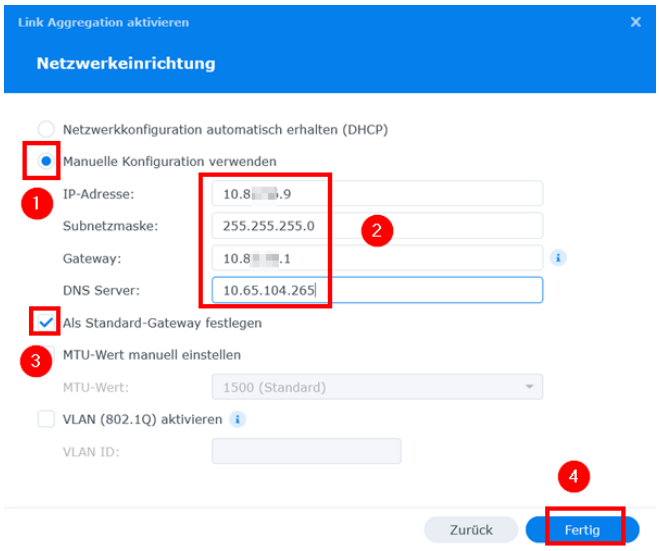


- Wenn der pädagogische Breitbandanschluss des Landes genutzt wird: Die IP-Adresse der Datenablage auf 192.168.1.250, das Standard-Gateway auf 192.168.1.1 sowie den DNS Server auf 10.65.104.245 (Dataport-DNS) festlegen (2), Häkchen für „Als Standard-Gateway festlegen“ setzen (3) und mit „Fertig“ bestätigen (4):

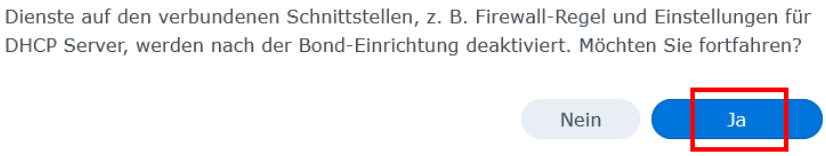


- Wenn die Dataport-Lösung dSchulLAN/dSchulWLAN genutzt wird: Es müssen hier die von Dataport zugewiesenen IP-Adressräume genutzt werden. Die Datenablage erhält dabei eine vorgegebene IP-Adresse aus dem Servernetz (2). **Wichtig**: Der letzte Teil der IP-Adresse (Hostanteil) muss eine „9“ sein, da diese Adresse auf die öffentliche IP-Adresse der Schule weitergeleitet wird (wird u. a. für VPN benötigt):
    - IP-Adresse: 10.84/85/86/87.y.**9***
    - Standard-Gateway: 10.84/85/86/87.y.**1***
    - DNS-Server: 10.65.104.245 (Dataport-DNS)

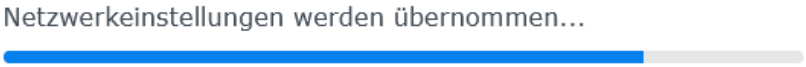
  ***Hinweis:** Jeder Schulstandort erhält individuelle IP-Adressräume für die unterschiedlichen Netze. Der genaue IP-Adressbereich kann der vom IQSH an die Schule versandten E-Mail zur Freischaltung des pädagogischen Anschlusses entnommen werden.
  Häkchen für „Als Standard-Gateway festlegen“ setzen (3) und mit „Fertig“ bestätigen (4):



Die nachfolgende Abfrage mit „Ja“ beantworten:

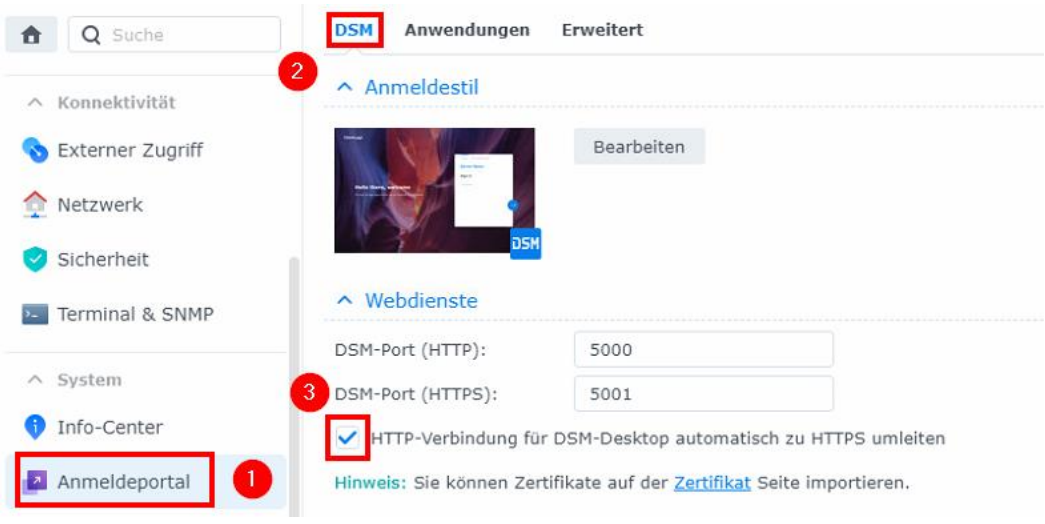


Übernahme der Netzwerkeinstellungen abwarten:



Wichtig: Am UniFi-Switch, an dem die beiden LAN-Anschlüsse angebunden sind, muss nun die Port-Aggregation eingeschaltet werden (siehe Anleitung „Musterlösung Grundschule SH_Einrichtung Netzwerk und WLAN.pdf“). Ohne Port-Aggregation am Switch ist die Datenablage ggf. nicht mehr erreichbar. In diesem Fall hilft nur der NAS-Reset der Stufe 1. Dabei werden lediglich die Netzwerkeinstellungen des Gerätes und das Admin-Passswort zurückgesetzt. Die Schritte werden hier erklärt: https://kb.synology.com/de-de/DSM/tutorial/How_to_reset_my_Synology_NAS_7#t1. Im Anschluss muss ein neues Admin-Passwort gesetzt werden und die Netzwerkeinstellungen wie oben beschrieben erneut vorgenommen werden.

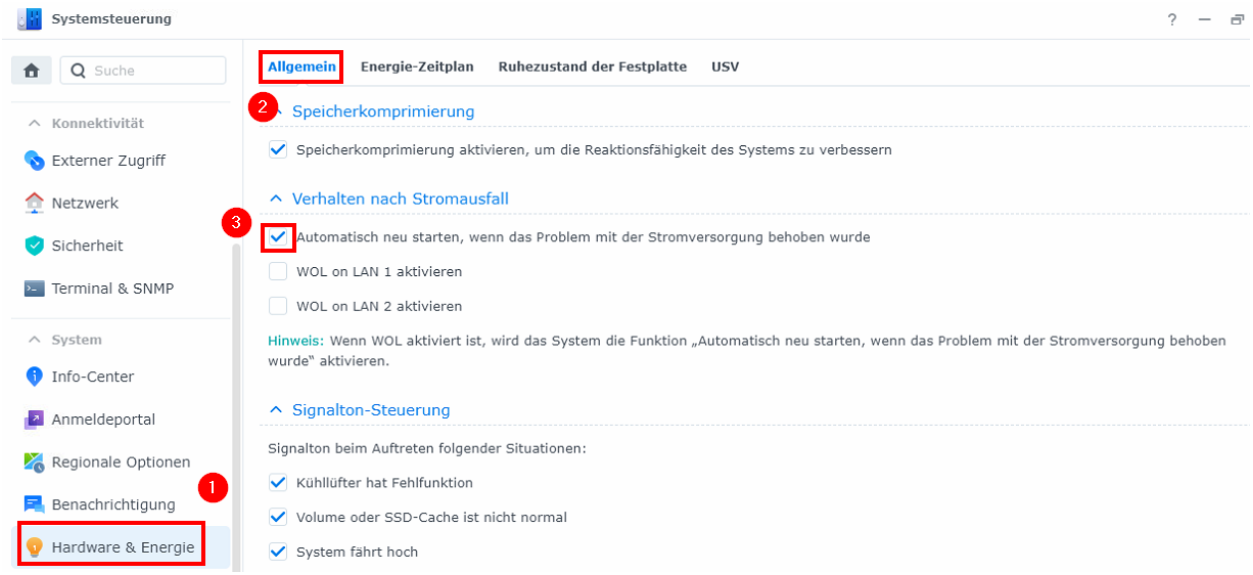
In der System-Steuerung den Punkt „Anmeldeportal“ (1) öffnen und im Reiter „DSM“ (2) die Umleitung der Webschnittstelle auf HTTPS aktivieren (3):



Mit „Speichern“ bestätigen.

4 Energieeinstellungen

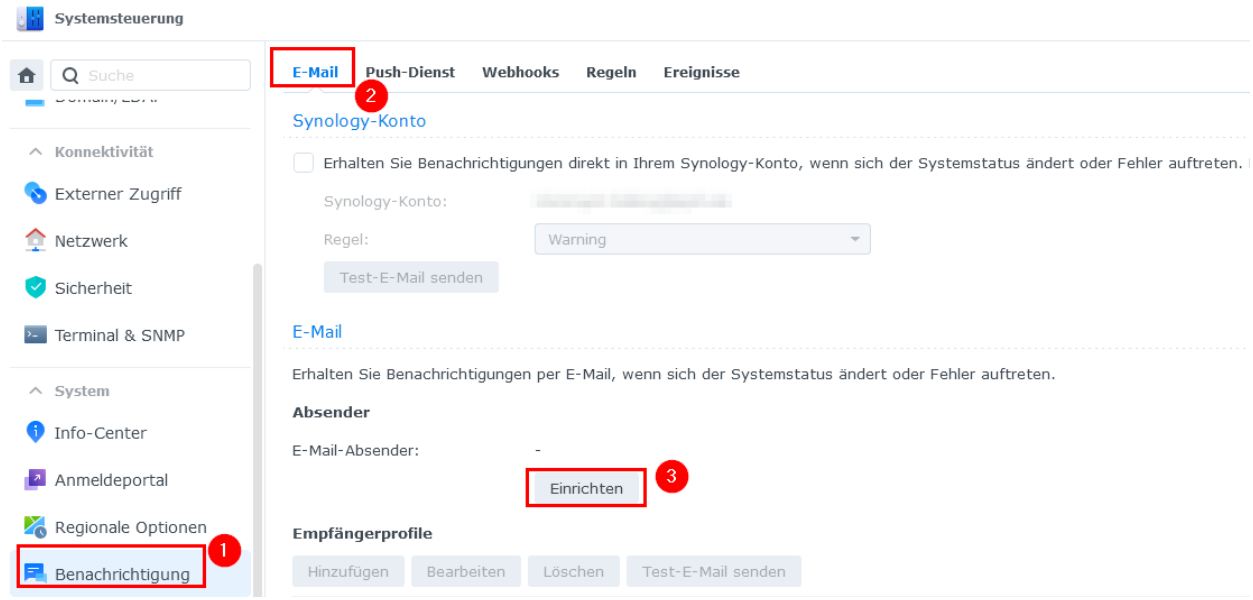
Damit die Datenablage nach einem Stromausfall automatisch wieder hochfährt, soll in der Systemsteuerung unter „Hardware & Energie“ (1) und im Reiter „Allgemein“ (2) die Einstellung „Automatisch neu starten, wenn das Problem mit der Stromversorgung behoben wurde“ (3) aktiviert werden:



Mit „Übernehmen“ bestätigen.

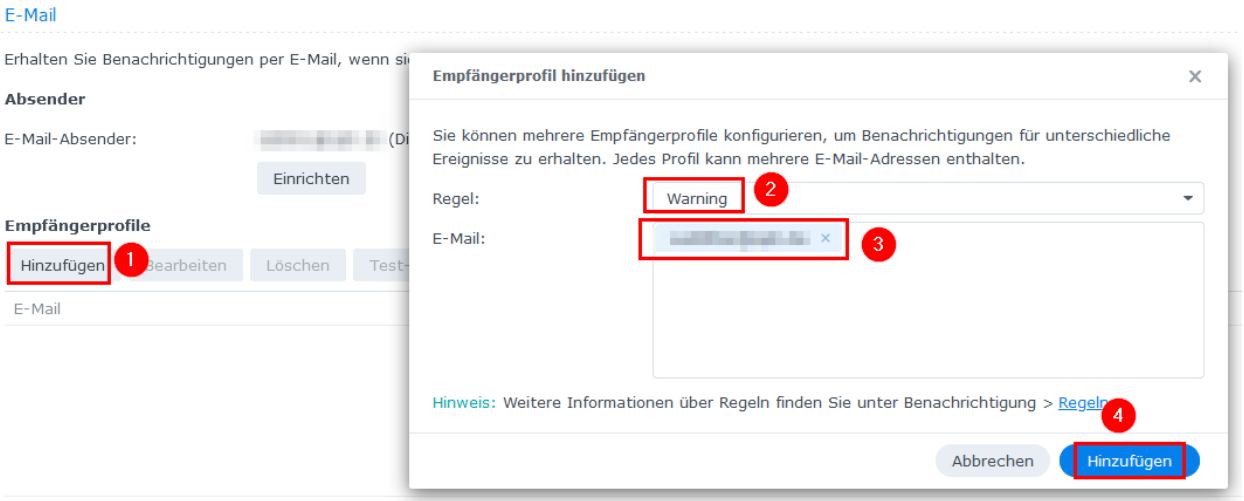
5 Benachrichtungsdienst aktivieren

In der Systemsteuerung unter „Benachrichtigung“ (1) und „E-Mail“ (2), die E-Mail-Benachrichtigung einrichten (3):

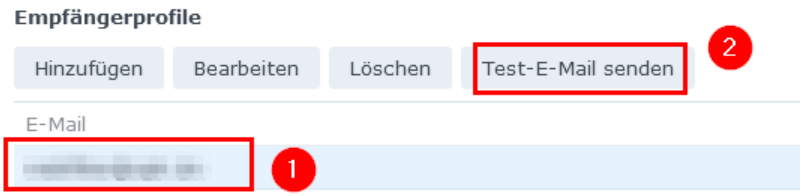


Den Serviceanbieter auf „Benutzerdefinierte SMTP-Server“ einstellen (1), SMTP-Server (2) plus Anmeldedaten (3) hinterlegen, als Absendername zur späteren Identifizierung den Namen der Schule ergänzen (4) und den Absender eintragen (6). Im Anschluss mit „Speichern“ bestätigen (6):

Empfängerprofil hinzufügen (1), Regel z. B. auf „Warning“ stellen (2), E-Mail-Adresse(n) für den oder die Empfänger - die Adresse kann auch identisch mit dem Absender sein - eintragen (3) und mit „Hinzufügen“ bestätigen (4):



Im Anschluss den Empfänger auswählen (1) und eine Test-E-Mail versenden (2):



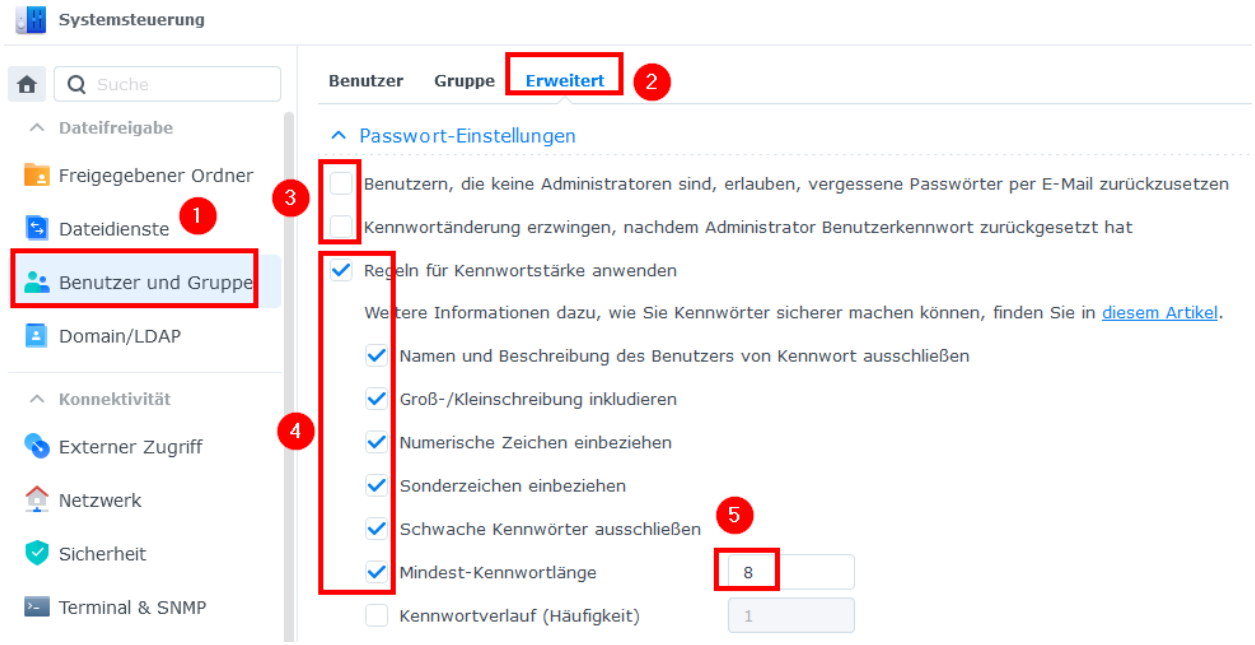
Hinweis: In welchen Fällen eine Nachricht verschickt wird, wird durch das oben gewählte vorkonfigurierte Profil (z. B. „Warning“) geregelt. Bei Bedarf kann im Reiter „Regeln“ (1) auch ein eigenes Profil hinzugefügt werden (2):

6 Benutzerkonten

- Auf der Datenablage sollen folgende Benutzer angelegt werden:
- Benutzer „**Lehrer**“ für den schulinternen Zugriff auf den Ordner „Lehrer“
- Benutzer „**Kollegium**“ für den browserbasierten Zugriff von zu Hause auf die Ordner „Daten“, „Lehrer“ und „Oeffentlich“
- **Admin-Benutzer** für den Administrationszugriff auf die Datenablage
- Zusätzlich bei der Nutzung von Windows-Geräten:
    - Benutzer „**Wartung**“ für den Zugriff der Softwareverteilung auf den Ordner „Wartung“

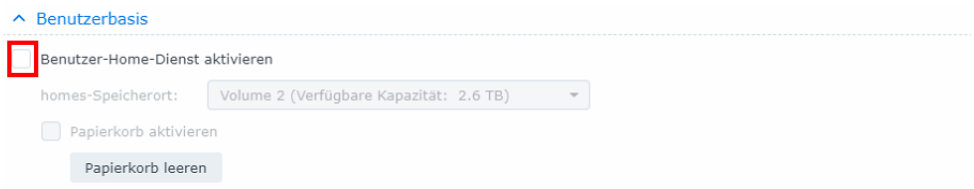
6.1 Erweiterte Einstellungen vornehmen

In der Systemsteuerung den Menüpunkt „Benutzer und Gruppe“ (1) wählen und im Reiter „Erweitert“ (2) die Passwortrichtlinien und die Regeln für die Kennwortstärke folgendermaßen einstellen (3-5):



Alle Änderungen mit „Übernehmen“ bestätigen.

Der Benutzer-Home-Dienst (ebenfalls unter den erweiterten Einstellungen) bleibt deaktiviert:

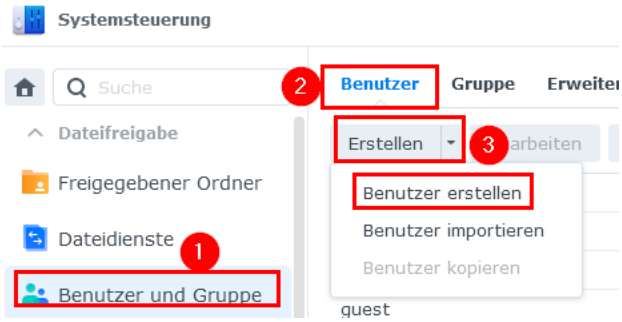


Hinweis: Um den administrativen Aufwand so gering wie möglich zu halten, sollen die Lehrkräfte später den Account „Kollegium“ gemeinsam benutzen. Wenn jedoch von der Schule für jede Lehrkraft ein eigener Account gewünscht wird, sollten dafür folgende Einstellungen vorgenommen werden:

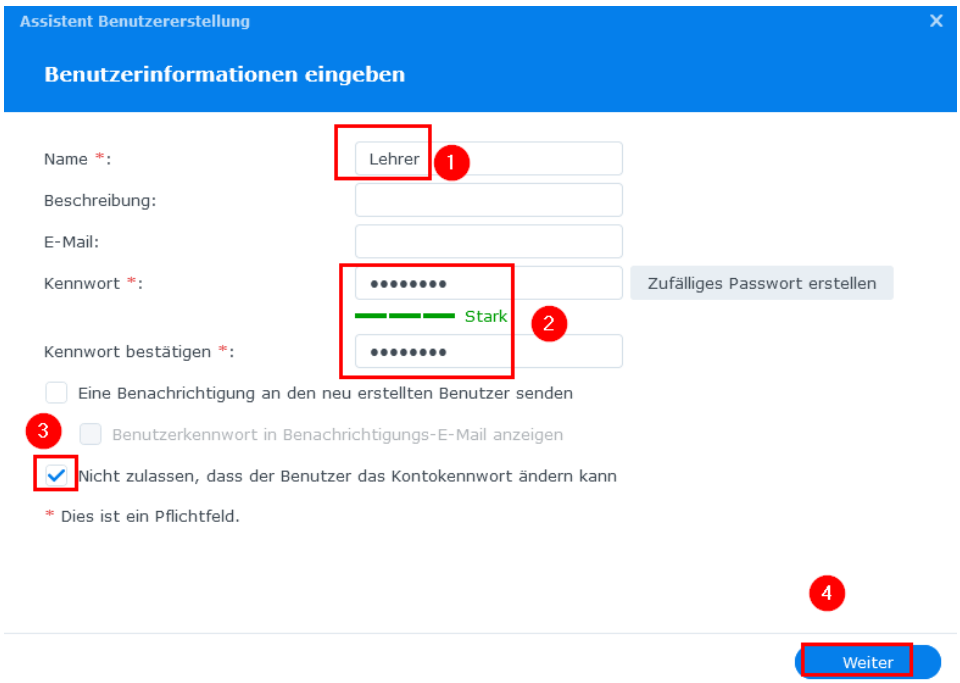
- Den oberen Punkt „Benutzern, die keine Administratoren sind, erlauben, vergessene Passwörter per E-Mail zurückzusetzen“ wieder aktivieren.
- Damit Passwörter selbst per E-Mail zurückgesetzt werden können, muss der Mailserver aktiviert werden (siehe Kapitel Benachrichtungsdienst aktivieren).
- Zusätzlich sollte der Benutzer-Home-Dienst aktiviert werden, damit jeder Benutzer im eigenen passwortgeschützten Bereich ein Dokument anlegen kann. Dazu in der Systemsteuerung „Benutzer“ – „Erweitert“ wählen und den Home-Dienst aktivieren.

6.2 Benutzerkonten anlegen

Den Benutzer „**Lehrer**“ einrichten. Dazu im Menü „Benutzer und Gruppe“ (1) wählen, im Reiter „Benutzer“ (2) den Button „Erstellen“ und „Benutzer erstellen“ (3) wählen:



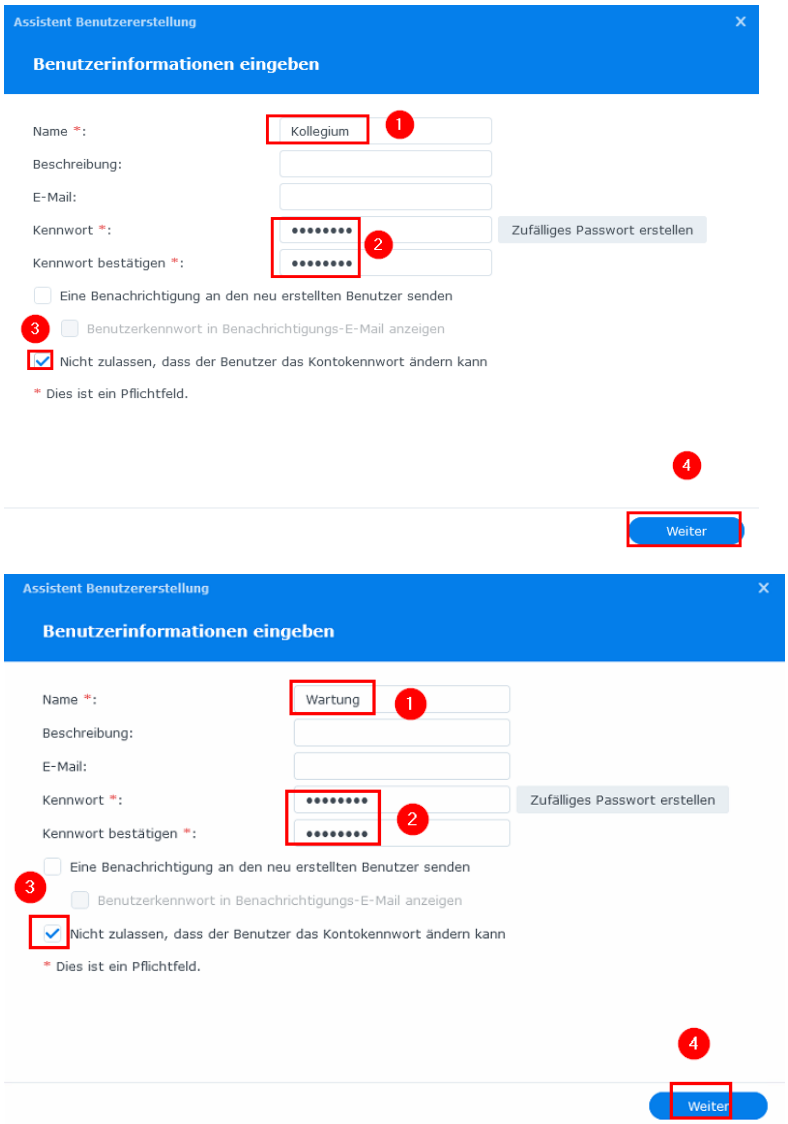
Als Benutzernamen „Lehrer“ eingeben (1), ein starkes Kennwort vergeben (2), die Möglichkeit zur Passwortänderung deaktivieren (3) und mit „Weiter“ bestätigen (4):



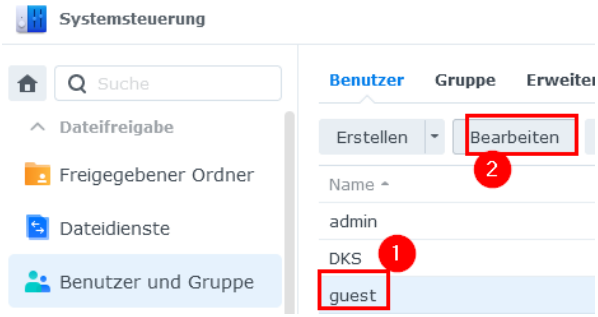
Hinweis: Das Passwort muss den oben eingerichteten Vorgaben entsprechen und soll in der IT-Dokumentation der Schule notiert werden.

Die dann folgenden Einstellungen können jeweils mit „Weiter“ bestätigt und im abschließenden Fenster mit „Fertig“ gespeichert werden.

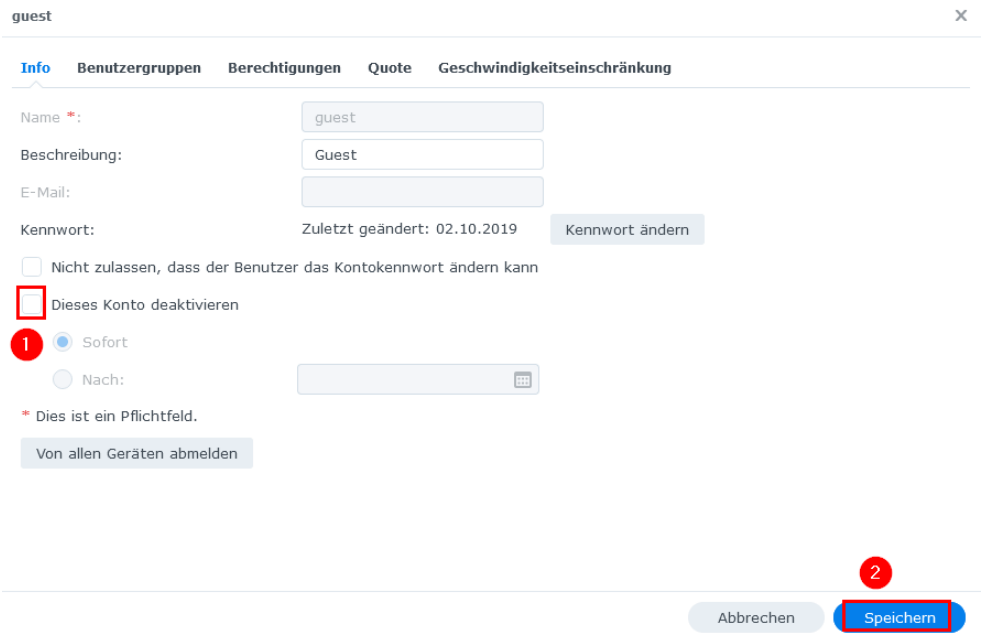
Dieselben Schritte für den Benutzer „**Kollegium**“ sowie zusätzlich bei der Nutzung von Windows-Endgeräten für den Benutzer „**Wartung**“ wiederholen (1-4). Auch hier jeweils die Möglichkeit zur Passwortänderung deaktivieren (3):



Damit auch Benutzer ohne Kennung Lese- und Schreibzugriff auf den Tauschordner „Daten“ beziehungsweise „Programme“ erhalten, muss der Gast-Account noch aktiviert werden. Dazu den Benutzer „**guest**“ wählen (1) und die Einstellungen mit „Bearbeiten“ öffnen (2):

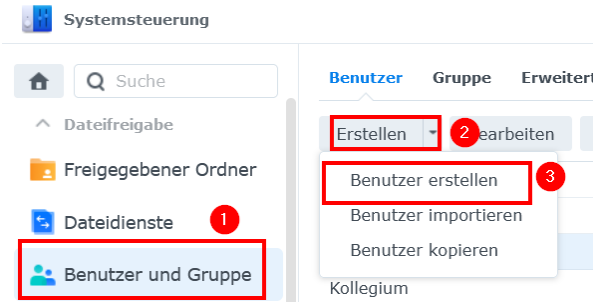


Häkchen für „Dieses Konto deaktivieren“ entfernen (1) und mit „Speichern“ bestätigen (2):

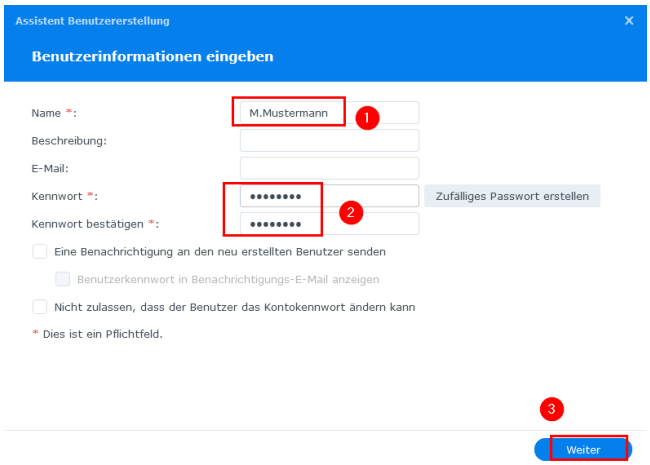


Wichtig: Für das Konto „guest“ soll kein Passwort festgelegt werden. Falls versehentlich doch ein Passwort vergeben wurde, lässt sich ein leeres Passwort erneut nur setzen, indem dafür kurzzeitig die Option „Regeln für Kennwortstärke anwenden“ deaktiviert wird (siehe Kapitel Erweiterte Einstellungen vornehmen).

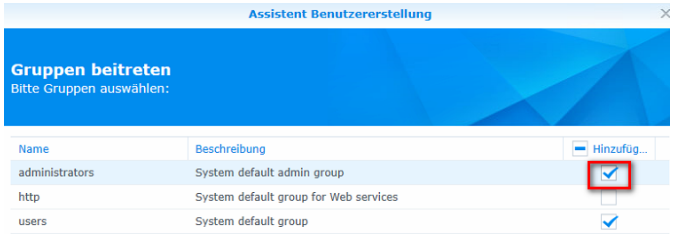
Um die Sicherheit zu erhöhen, soll der vorhandene Benutzer „Admin“ durch einen Admin-User mit anderem Namen ersetzt werden. Dazu unter „Benutzer und Gruppe“ (1), „Erstellen“ (2) und „Benutzer erstellen“ (3) einen neuen Benutzer anlegen:



Für den neuen **Admin-Benutzer** einen individuellen Namen (1) und ein sicheres Passwort (2) vergeben und mit „Weiter“ bestätigen (3):



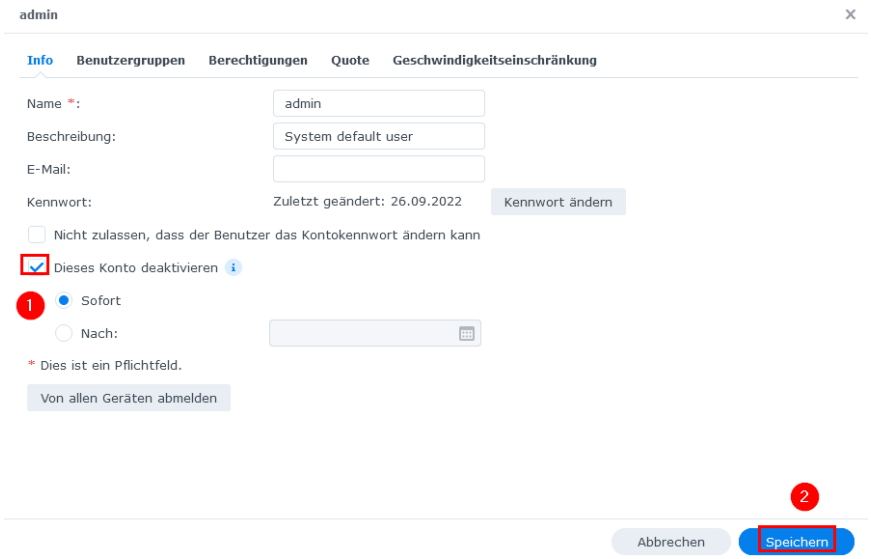
Den neuen Benutzer zusätzlich der Gruppe „administrators“ hinzufügen und mit „Weiter“ bestätigen:



Berechtigungen für Ordner und Anwendungen vergeben und mit „Übernehmen“ den Benutzer anlegen.

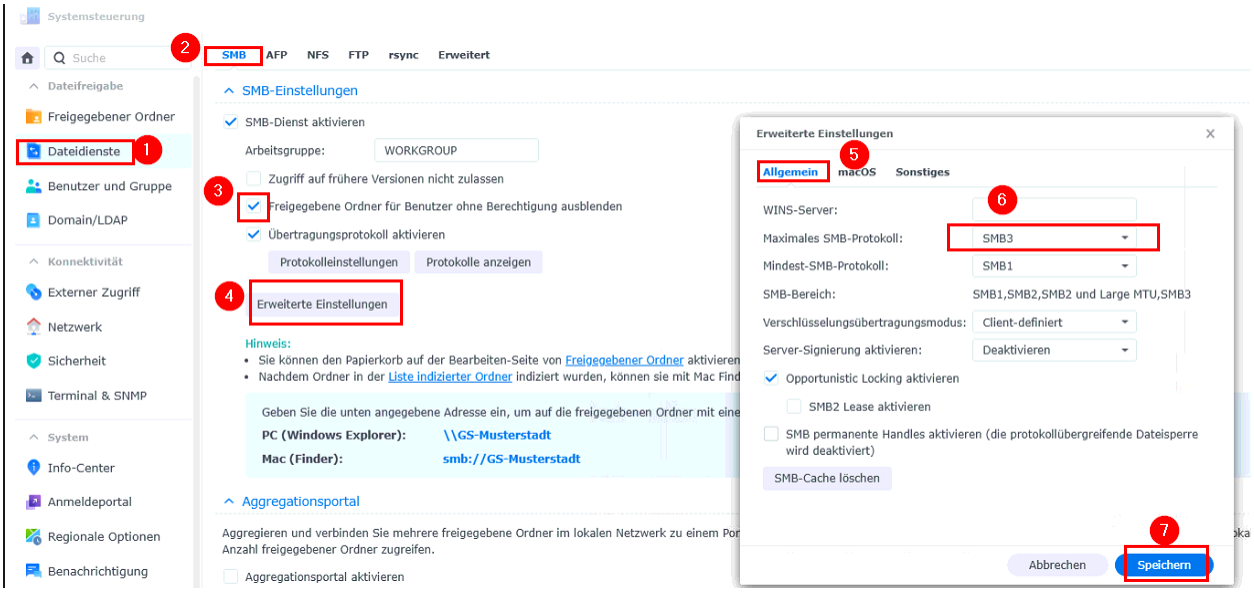
Hinweis: Bei Bedarf können weitere Admin-Konten eingerichtet werden.

Im Anschluss mit dem neuen Admin-User einloggen und den alten Benutzer „Admin“ über Systemsteuerung – „Benutzer und Gruppe“ – „Bearbeiten“ deaktivieren (1+2):



7 Ordner anlegen

Zunächst in der Systemsteuerung unter „Dateidienste“ (1) und dem Reiter „SMB“ (2) die Option „Freigegebene Ordner für Benutzer ohne Berechtigung ausblenden“ aktivieren (3) und mit „Übernehmen“ bestätigen. Im Anschluss „Erweiterte Einstellungen“ (4) wählen, im Reiter „Allgemein“ (5) das maximale SMB-Protokoll auf „SMB3“ (6) und mit „Speichern“ (7) bestätigen:



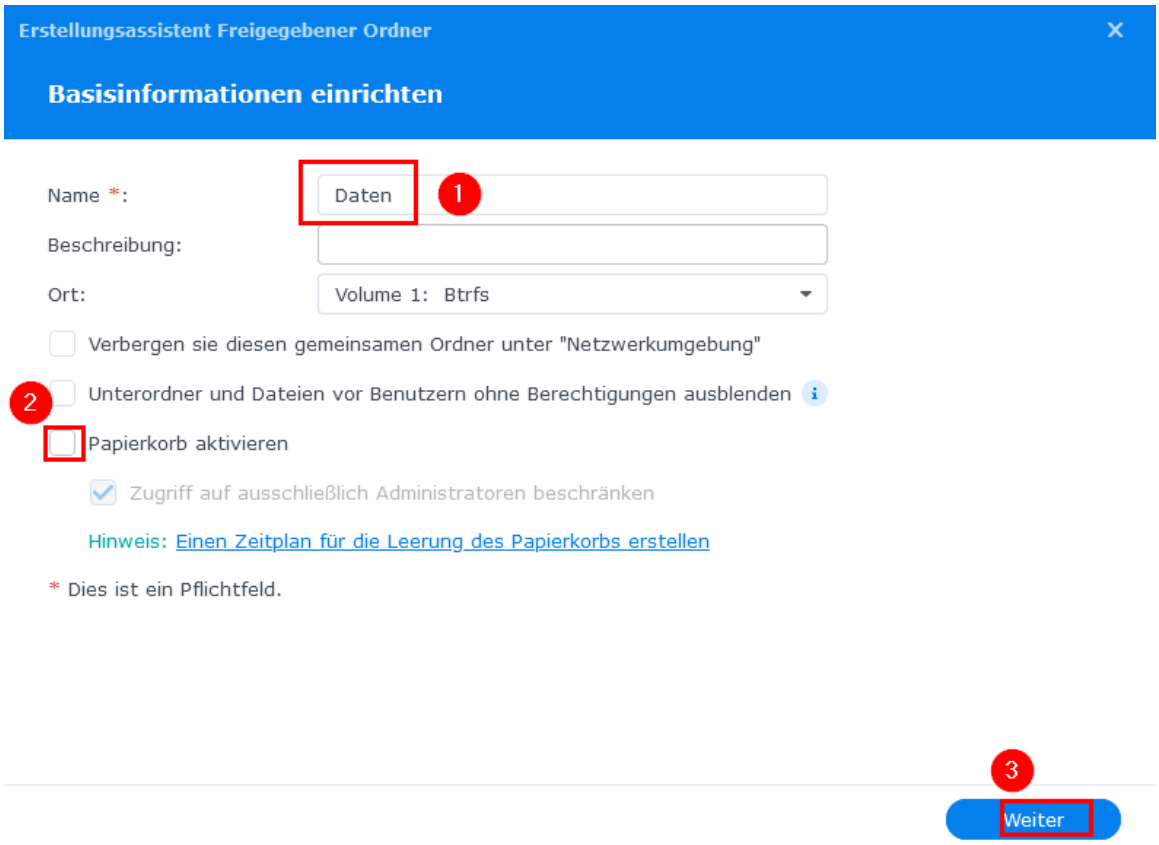
Im Anschluss den Hinweis zum Neustart des SMB-Dienstes bestätigen.

Danach sollen folgende Ordner angelegt werden:

- Ordner „**Daten**“ zum Austausch von Dokumenten und anderen Dateien
- Ordner „**Programme**“ für die Ablage von Programmdaten wie zum Beispiel der Lernwerkstatt
- Ordner „**Lehrer**“ zum Austausch und Ablegen von Dateien für Lehrkräfte
- Ordner „**Oeffentlich**“ zum öffentlichen Bereitstellen von Materialien durch Lehrkräfte
- Zusätzlich bei der Nutzung von Windows-Geräten:
    - Ordner „**Wartung**“ für die Softwareverteilung

In einem ersten Schritt den Ordner „**Daten**“ anlegen. Dazu in der Systemsteuerung „Freigegebener Ordner“ (1) und dort „Erstellen“ (2) sowie „Freigegebenen Ordner erstellen“ (3) wählen:

Als Namen „Daten“ eingeben (1), den Papierkorb deaktivieren (2) und mit „Weiter“ bestätigen (3):

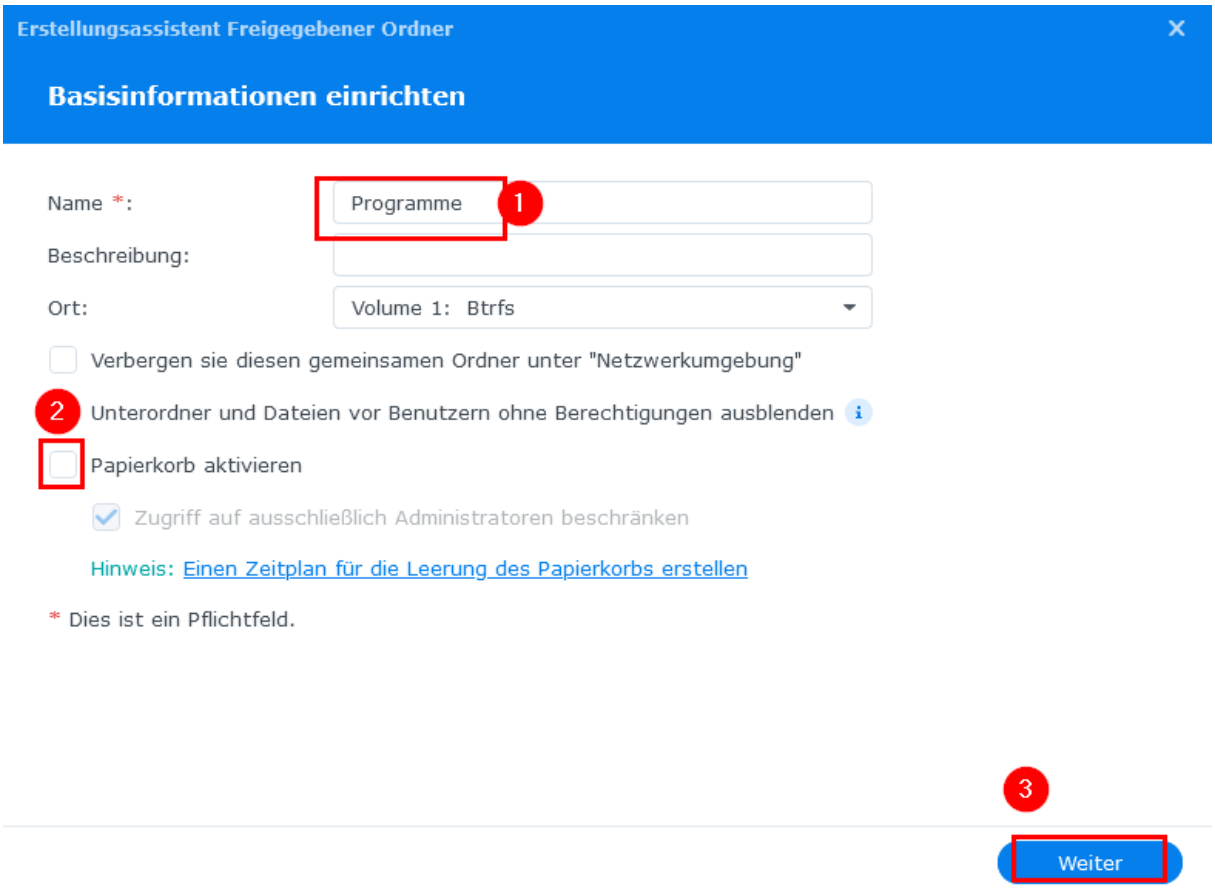


Im Anschluss 4x mit „Weiter“ bestätigen.

Im letzten Fenster zu den Benutzerberechtigungen allen Benutzern außer dem deaktivieren Admin-User Lese- und Schreibrechte gewähren und mit „Übernehmen“ bestätigen:

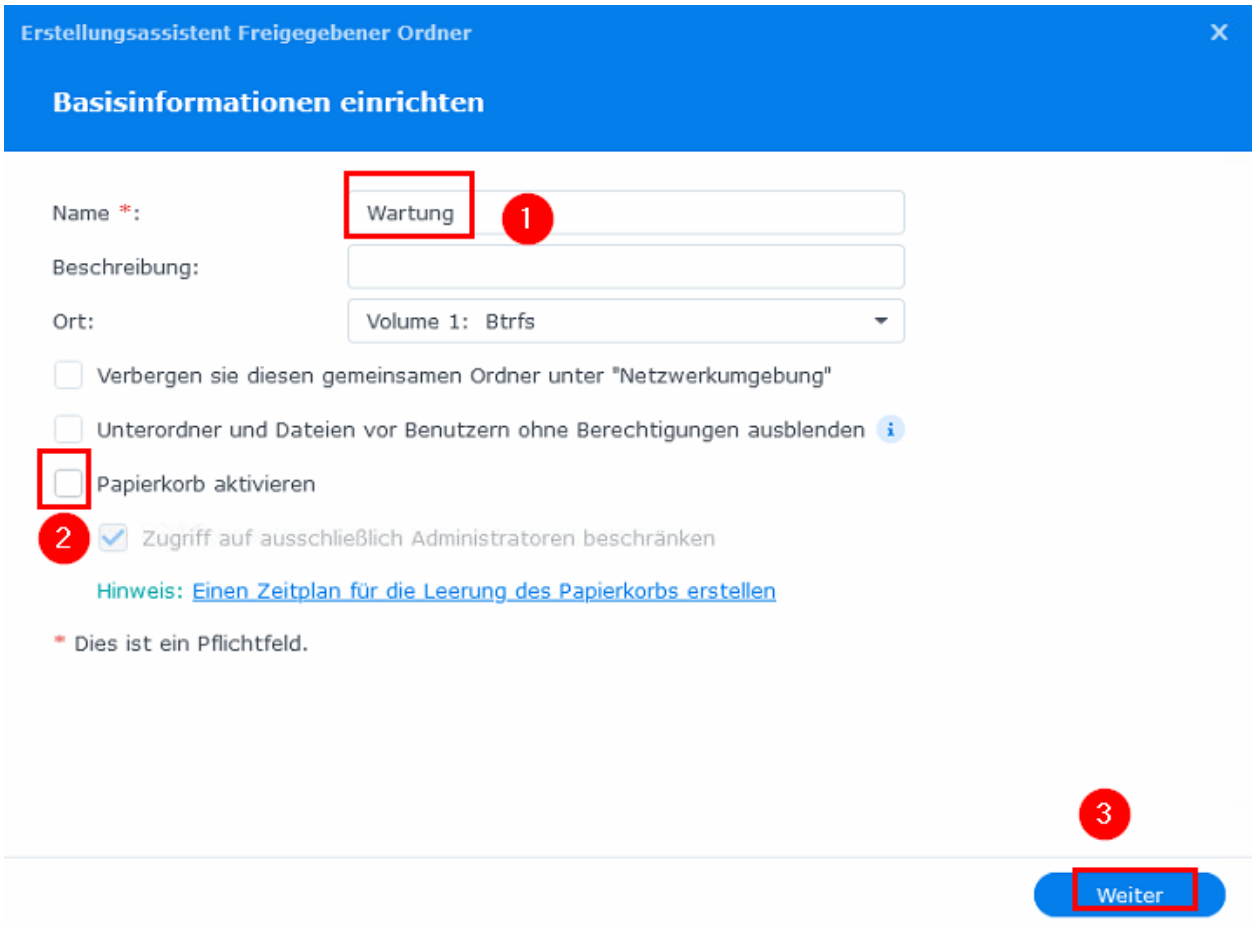
Hinweis: Indem der Benutzer „guest“ Lese- und Schreibberechtigung bekommt, ist ein Zugriff ohne Benutzeranmeldung möglich ist.

Den Ordner „**Programme**“ wie oben beschrieben mit deaktviertem Papierkorb anlegen (1-3):

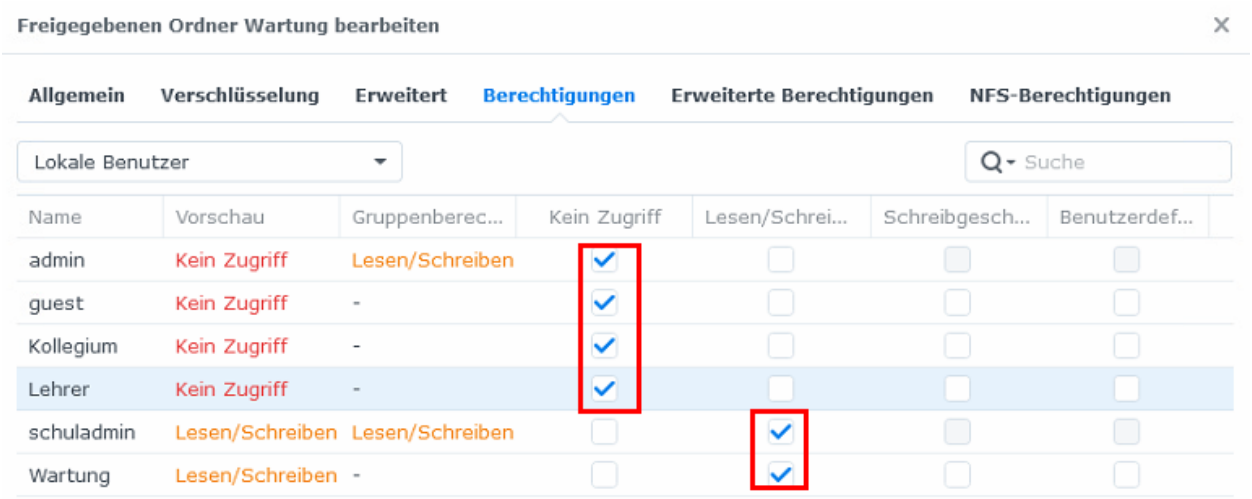


Zugriff auf den Ordner „Programme“ nur für die Benutzer „Wartung“, “guest“ und „Lehrer“ sowie aktive Admin-Konten erlauben:

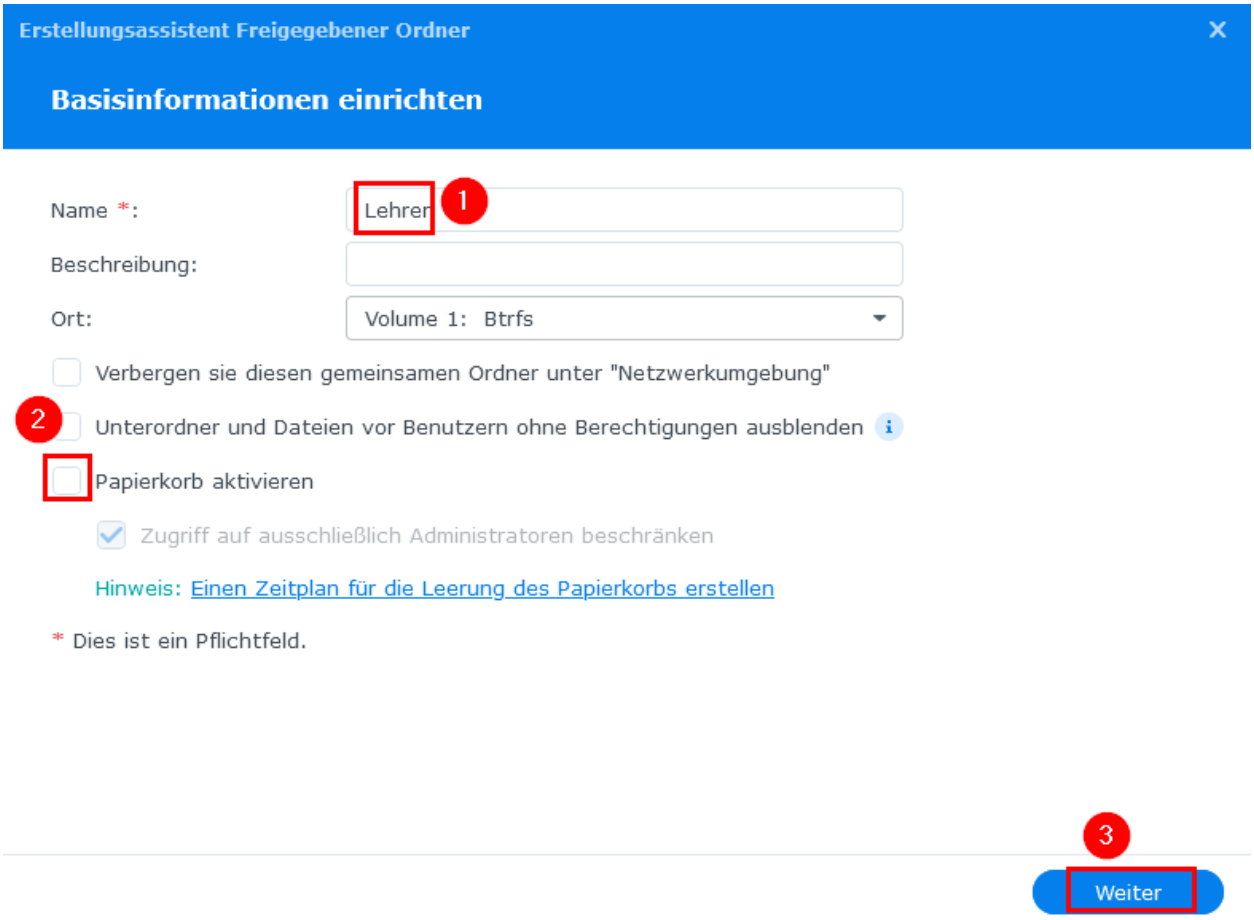
Den Ordner „**Wartung**“ wie oben beschrieben anlegen und den Papierkorb deaktivieren (1-3):



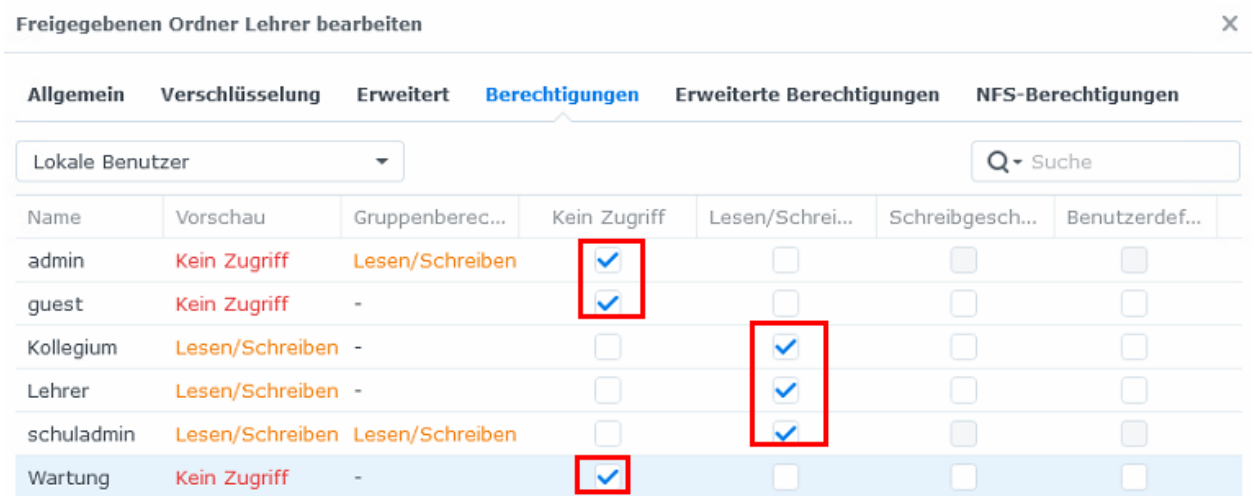
Zugriff auf den Ordner „Wartung“ nur für den Benutzer „Wartung“ sowie aktive Admin-Konten erlauben:



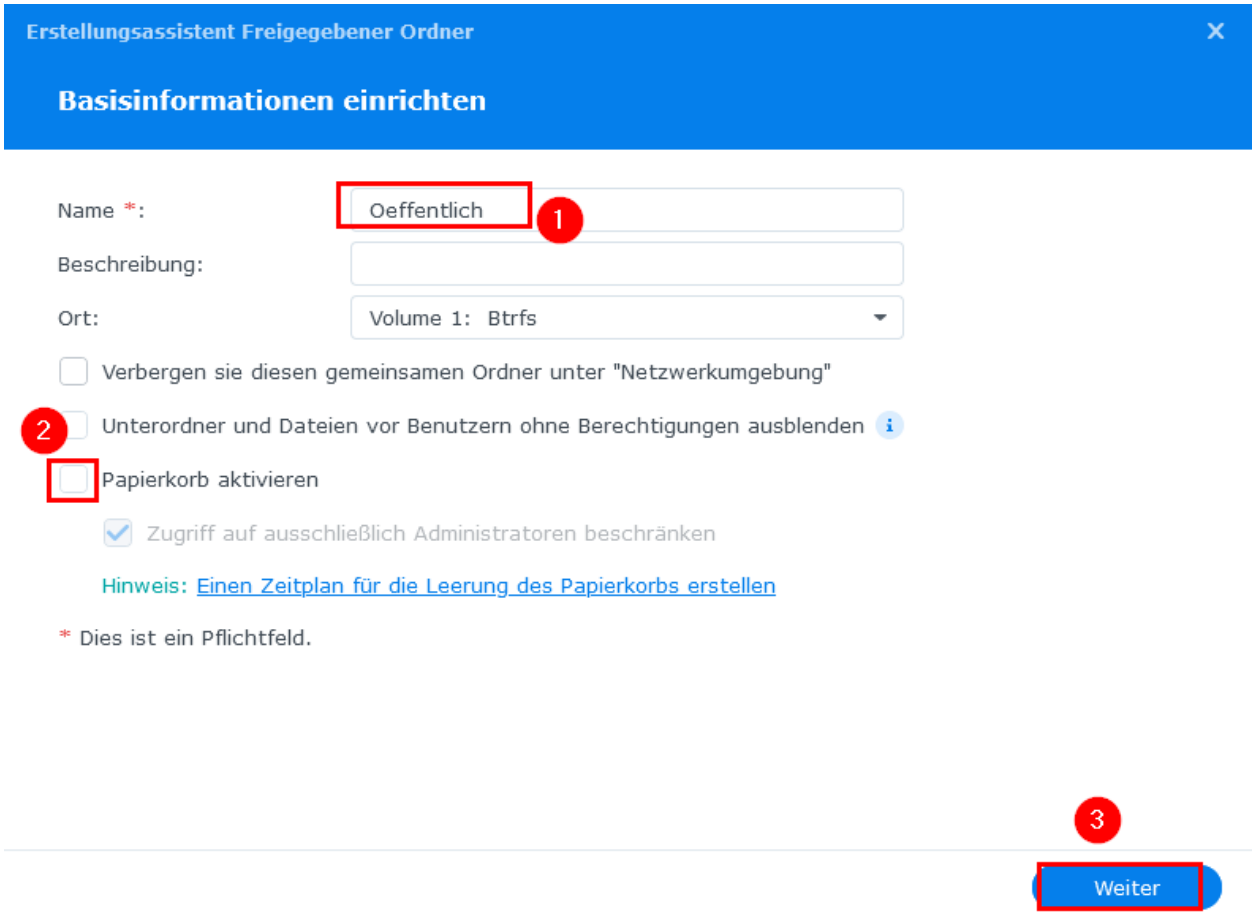
Den Ordner „**Lehrer**“ wie oben beschrieben mit deaktiviertem Papierkorb anlegen (1-3):



Zugriff auf den Ordner „Lehrer“ nur für die Benutzer „Kollegium“ und „Lehrer“ sowie aktive Admin-Konten erlauben:



Den Ordner „**Oeffentlich**“ wie oben beschrieben anlegen und den Papierkorb deaktivieren (1-3):

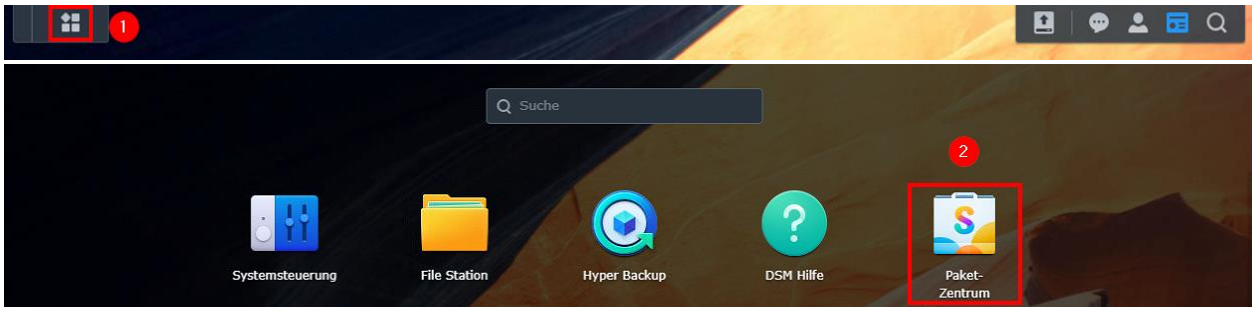


Zugriff auf den Ordner „Oeffentlich“ nur für die Benutzer „Lehrer“ und „Kollegium“ sowie aktive Admin-Konten erlauben:

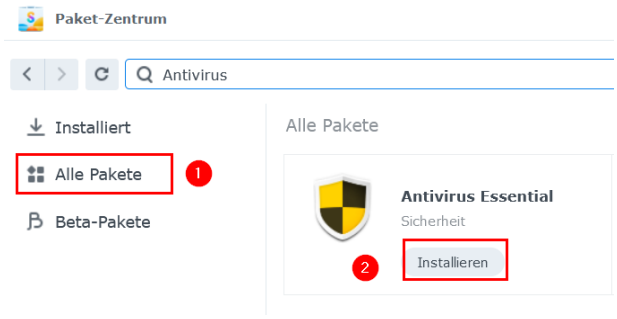
8 Virenscan einrichten

Um eine Ausbreitung von Viren zu verhindern, sollen die Daten auf dem NAS regelmäßig auf Viren gescannt werden.

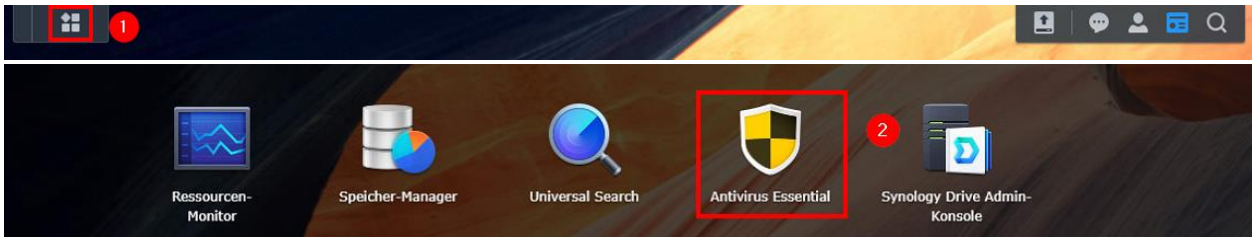
Dazu muss über das Paketzentrum das Paket „Antivirus Essential“ installiert werden. Dazu über das Hauptmenü (1) das Paketzentrum (2) öffnen:



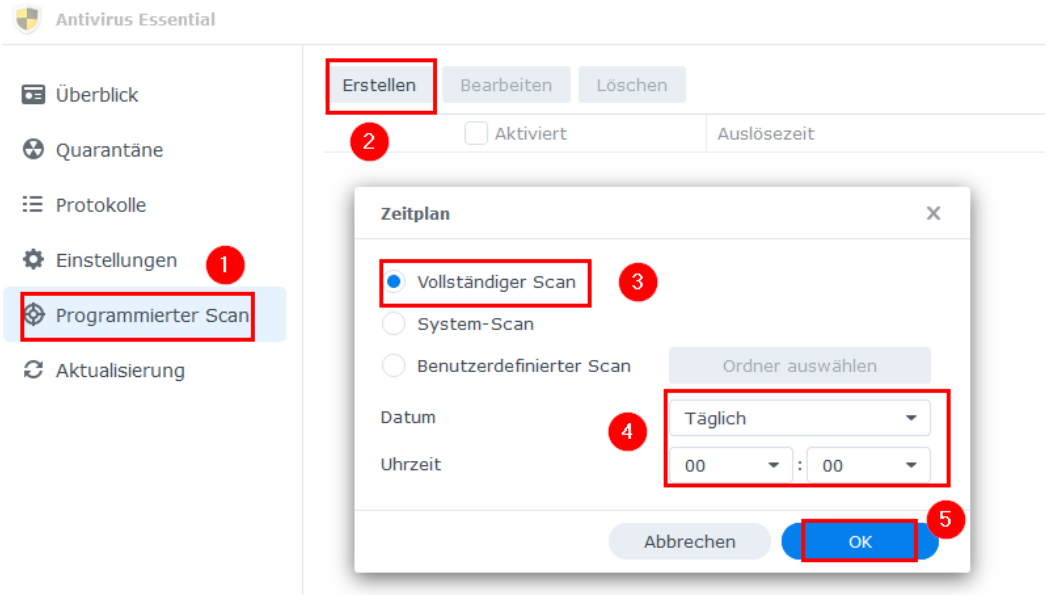
Unter „Alle Pakete“ (1) das Paket „Antivirus Essential“ (2) installieren:



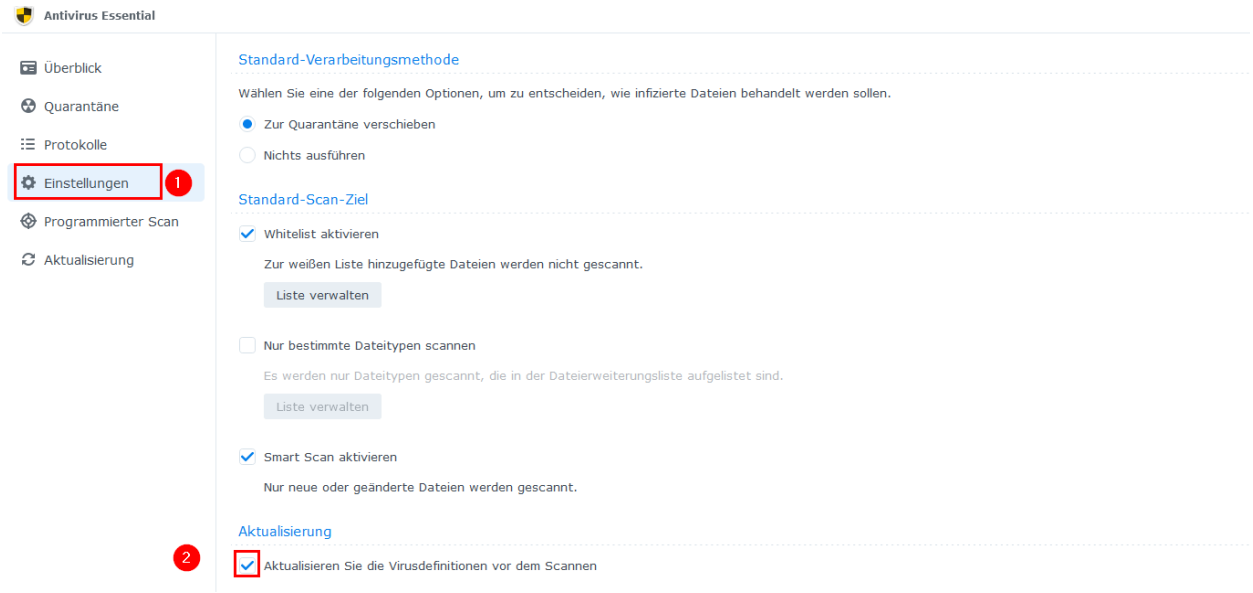
Nach der Installation über das Hauptmenü (1) „Antivirus Essential“ (2) öffnen:



Unter „Programmierter Scan“ (1) und „Erstellen“ (2) einen neuen Scan-Auftrag (3+4) anlegen und mit „OK“ bestätigen (5):



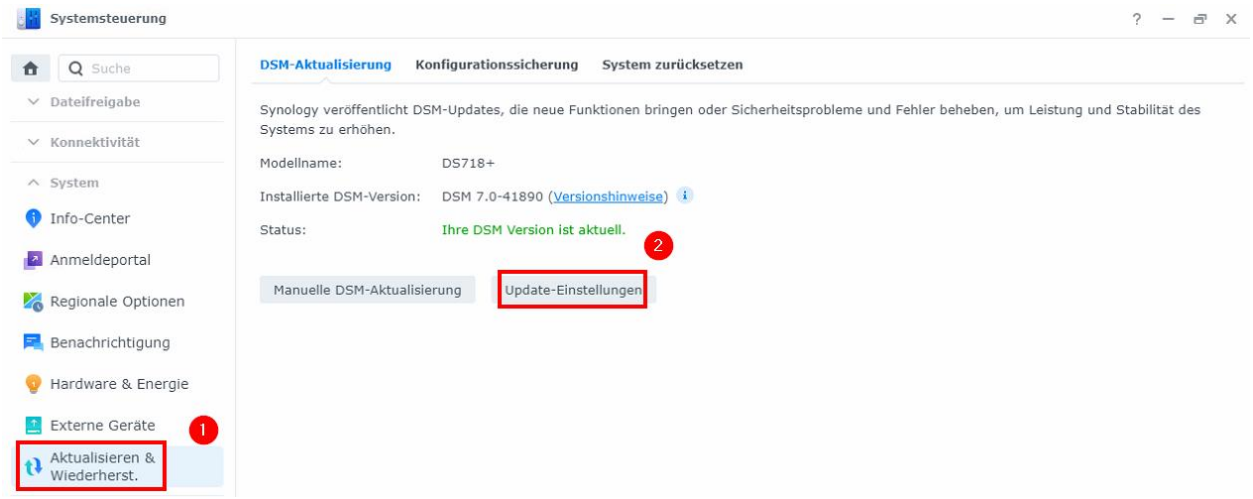
Unter „Einstellungen“ (1) überprüfen, ob die automatische Aktualisierung der Virendefinitionen vor dem Scannen aktiviert ist (2):



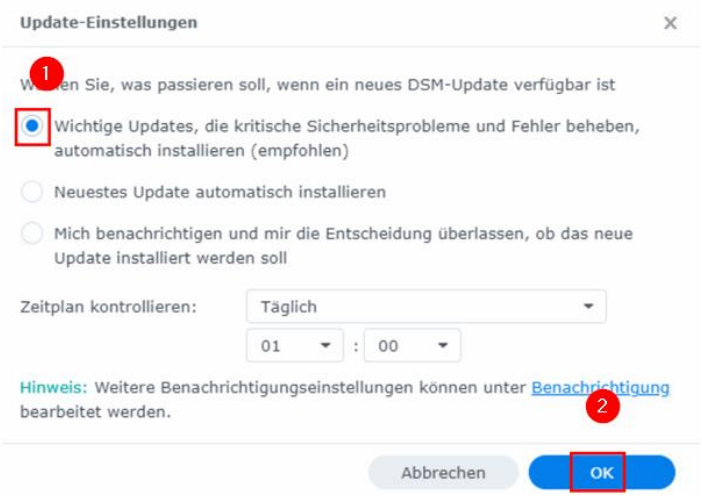
Bei Änderungen mit „Übernehmen“ bestätigen.

9 Automatische Updates

Wichtige Updates sollen automatisiert eingespielt werden. Dazu in der Systemsteuerung „Aktualisieren und Wiederherstellen“ (1) wählen und dort die Update-Einstellungen (2) öffnen:



Dort das Häkchen für „Wichtige Updates, die kritische Sicherheitsprobleme und Fehler beheben, automatisch installieren“ (1) setzen, die vorgegebenen Zeitplaneinstellungen beibehalten und mit „OK“ (2) bestätigen:

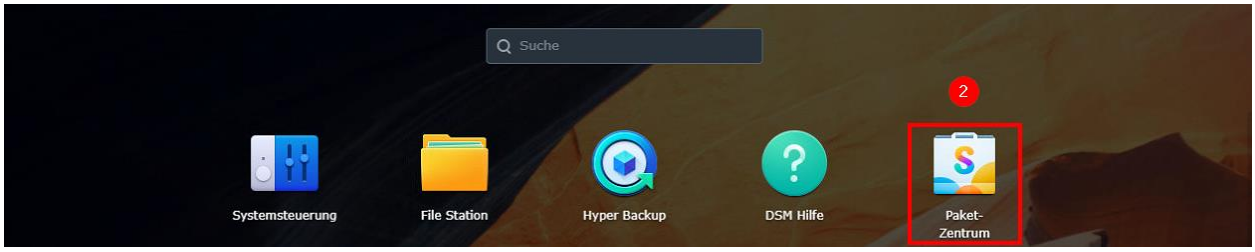


10 Datensicherung einrichten

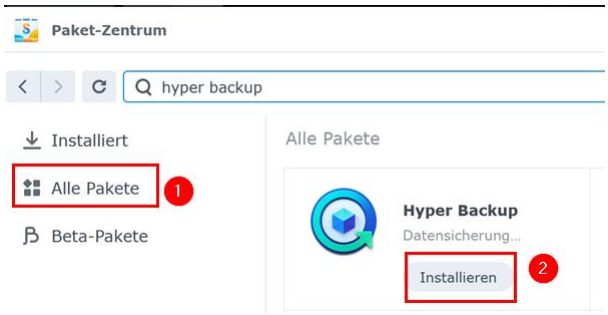
Die Nutzung eines Raid 1 (beziehungsweise SHR mit Ausfalltoleranz) bietet zwar einen Schutz vor Datenverlusten, wenn eine Festplatte defekt ist. Wenn jedoch 2 Festplatten betroffen sind oder Daten gelöscht worden sind, ist die Lösung nicht ausreichend. Daher wird empfohlen, zusätzlich noch eine Sicherung der auf dem NAS gespeicherten Daten auf einem externen Laufwerk vorzunehmen, so dass notfalls eine Datenwiederherstellung vorgenommen werden kann.

Beispieleinrichtung einer Datensicherung:

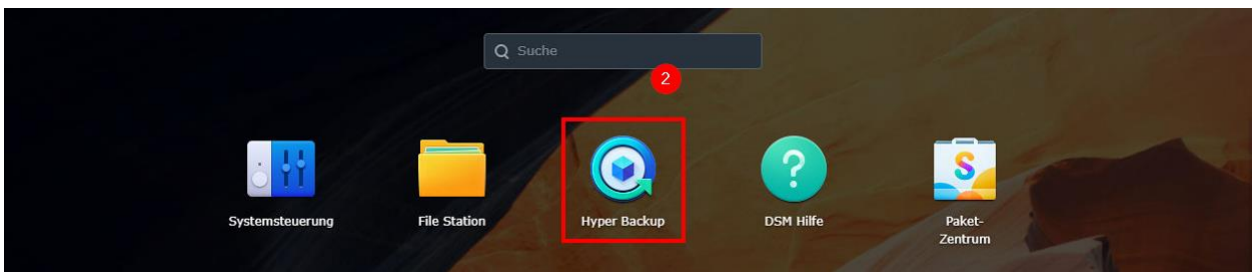
Zunächst im Paket-Zentrum die App „Hyper Backup“ installieren. Dazu über das Hauptmenü (1) das Paketzentrum (2) öffnen:



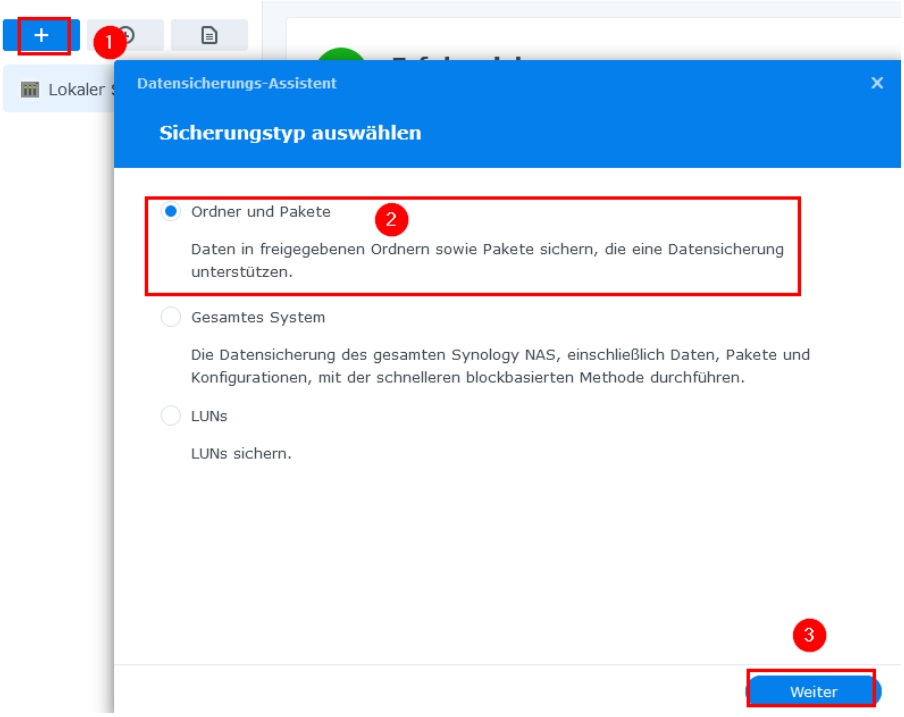
Unter „Alle Pakete“ (1) das Paket „Hyper Backup“ (2) installieren:



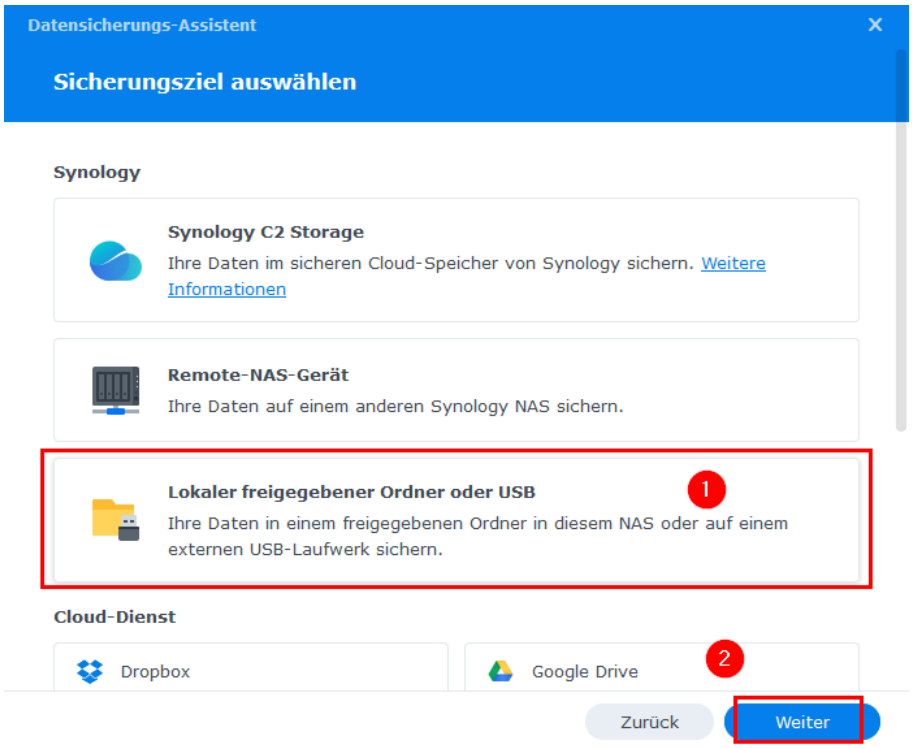
Nach der Installation über das Hauptmenü (1) die App „Hyper Backup“ (2) öffnen:



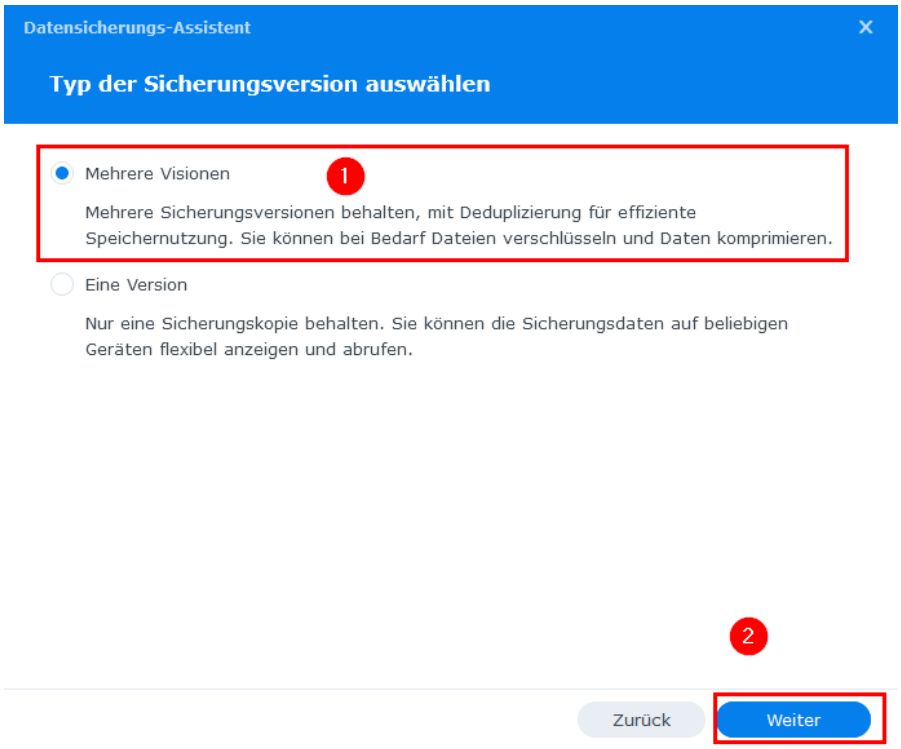
Das Plus-Symbol (1) wählen, als Sicherungstyp „Ordner und Pakete“ (2) einstellen und mit „Weiter“ (3) bestätigen:



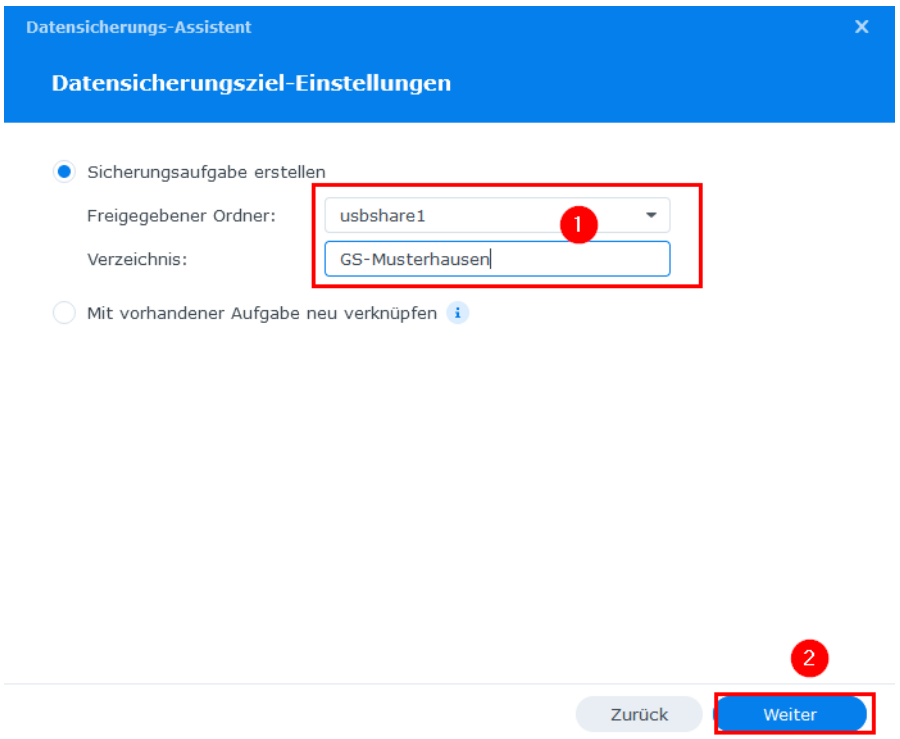
„Lokaler freigegebener Ordner oder USB“ (1) wählen und mit „Weiter“ (2) bestätigen:



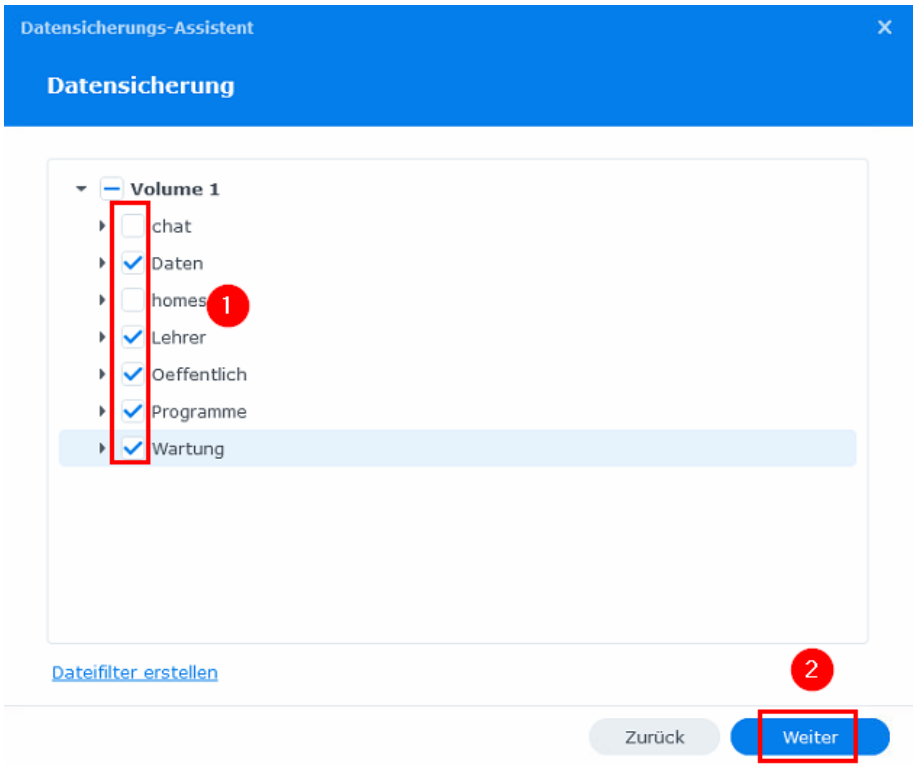
„Mehrere Versionen“ (1) wählen und mit „Weiter“ (2) bestätigen:



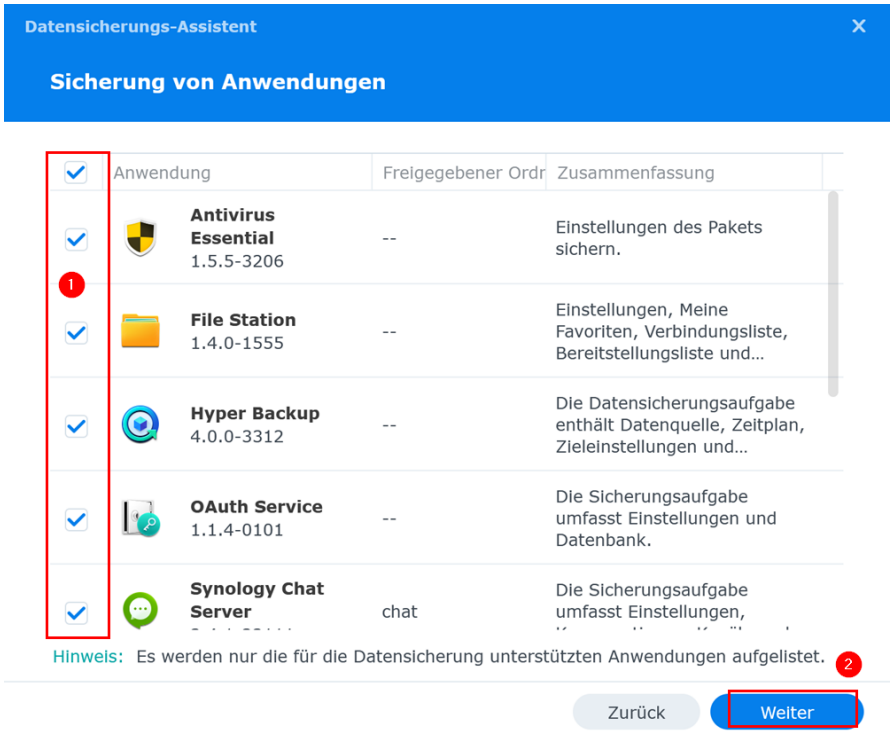
Für den freigegebenen Ordner „usbshare1“ auswählen sowie einen Verzeichnisnamen vergeben (1) und mit „Weiter“ (2) bestätigen:



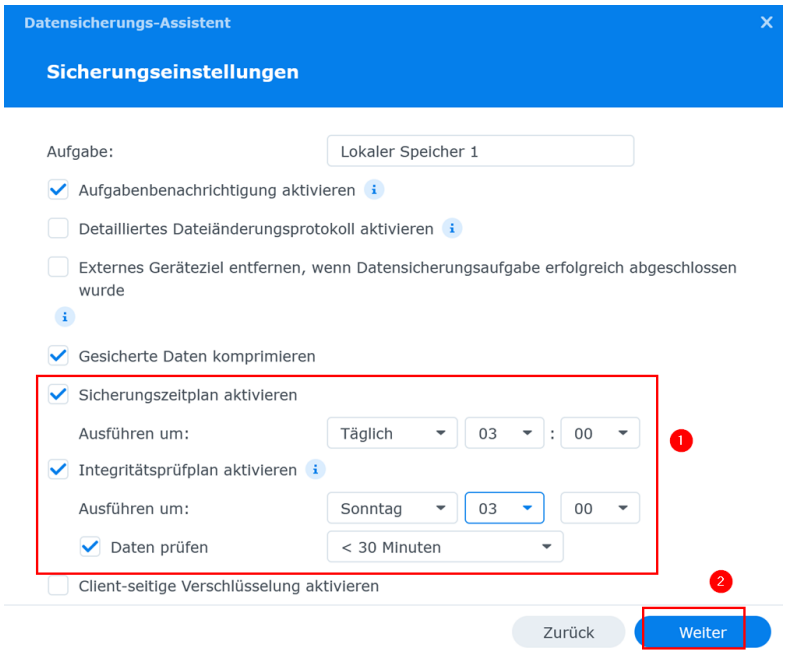
Die Verzeichnisse „Daten“, „Lehrer“, „Oeffentlich“, „Programme“ und „Wartung“ ins Backup einbeziehen (1) und mit „Weiter“ (2) bestätigen:



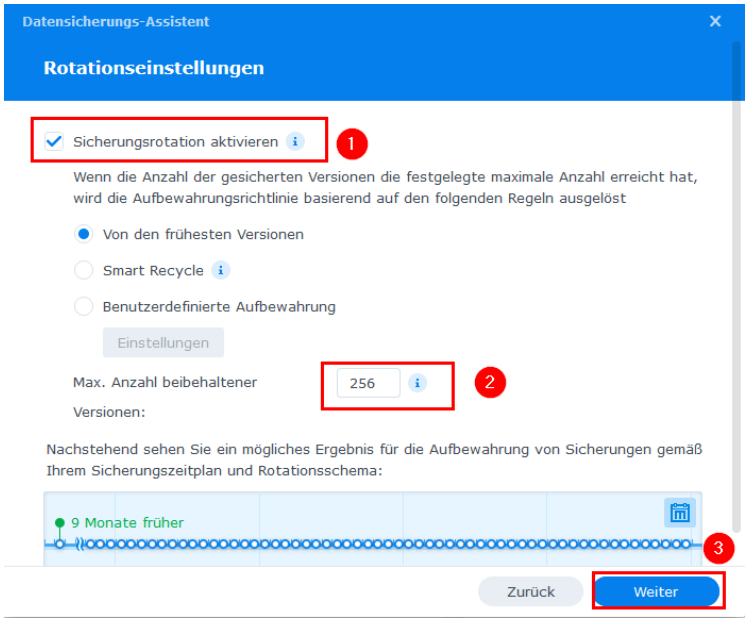
Alle installierten Anwendungen mitsichern (1) und mit „Weiter“ (2) bestätigen:



Einen Sicherungszeitplan einstellen sowie die Integritätsprüfung aktivieren (1) und mit „Weiter“ (2) bestätigen:

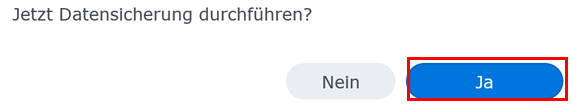


Die voreingestellten Werte zu den Rotationseinstellungen (1+2: aktive Sicherheitsrotation ab 256 Versionen) ohne Änderung mit „Weiter“ (2) bestätigen:



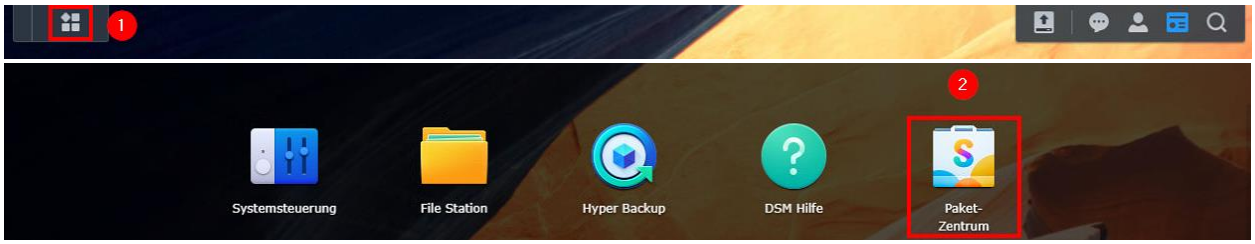
Im Anschluss die Zusammenfassung mit „Fertig“ bestätigen.

Am Ende testweise die erste Datensicherung durchführen:

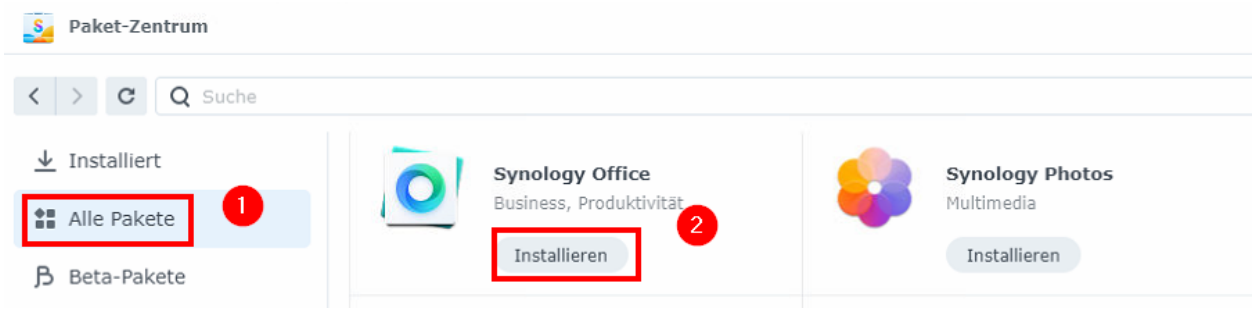


11 Office-Paket installieren

Für die Nutzung der kollaborativen Office-Anwendung soll über das Paketzentrum das Paket „Synology Office“ installiert werden. Dazu über das Hauptmenü (1) das Paketzentrum (2) öffnen:



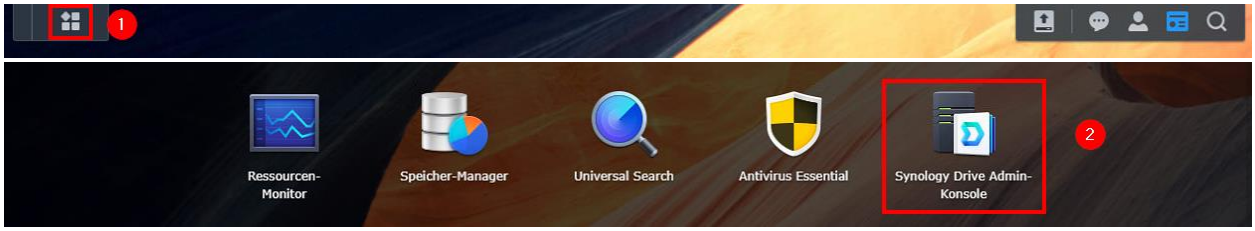
Dort unter „Alle Pakete“ (1) das Paket „Synology Office“ installieren (2):



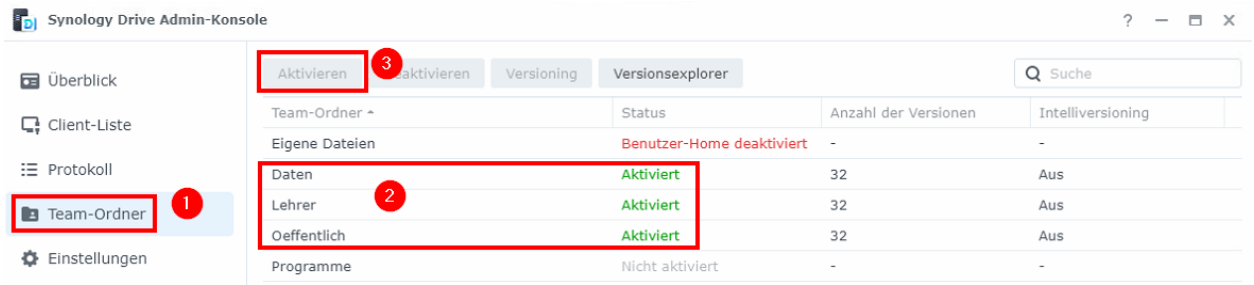
Hinweis: Bei der Installation wird automatisch auch das Paket „Synology Drive“ mitinstalliert.

Damit Office-Dokumente angelegt werden können, soll der Ordner „Daten“ dafür freigeschaltet werden:

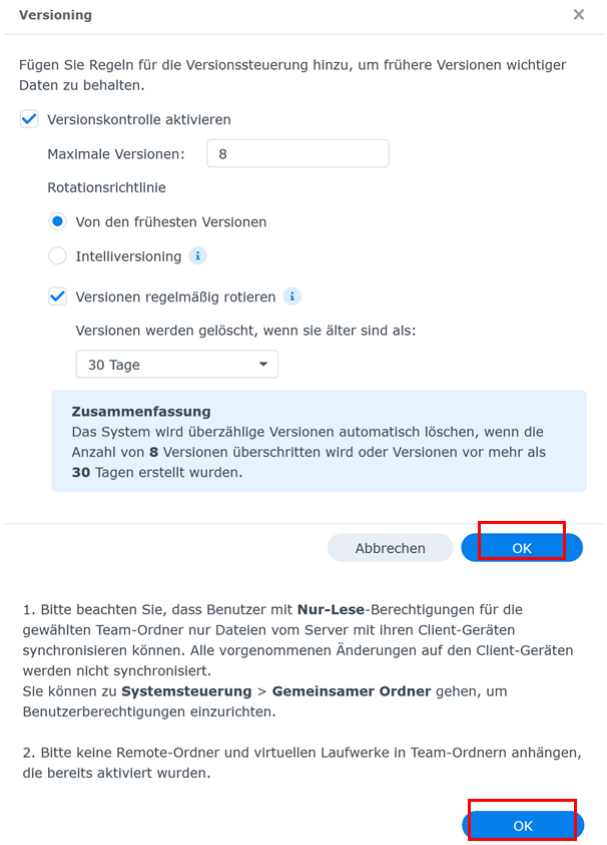
In die Paketübersicht wechseln und dort „Synology Drive Admin-Konsole“ öffnen:



Dort im Menü „Team-Ordner“ (1) wählen und für die Ordner „Daten“, „Lehrer“ und „Oeffentlich“ (2) den Menüpunkt „Aktivieren“ (3) wählen:



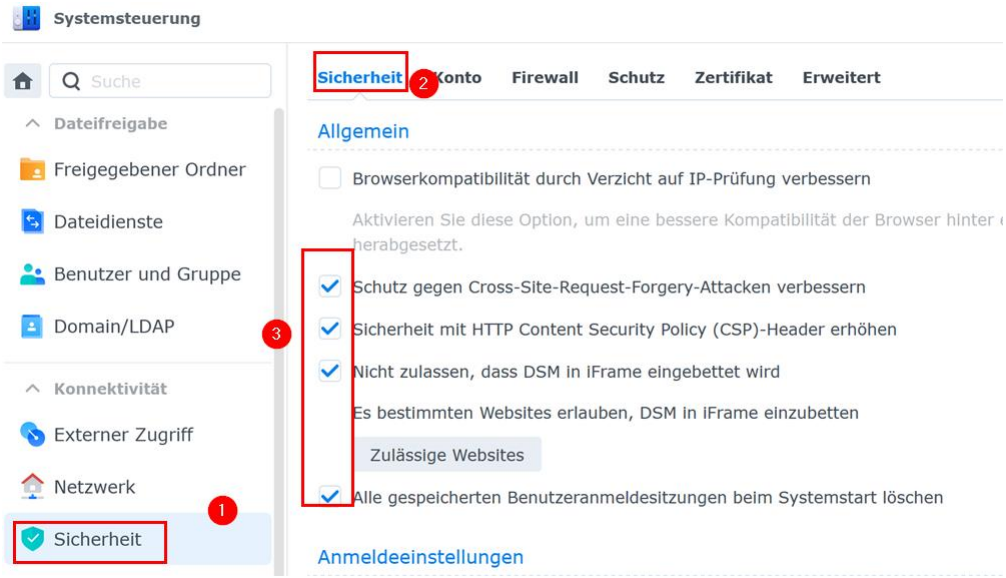
Jeweils die vorgeschlagene Konfiguration für Versionierung und die anschließenden Hinweise mit „OK“ bestätigen:



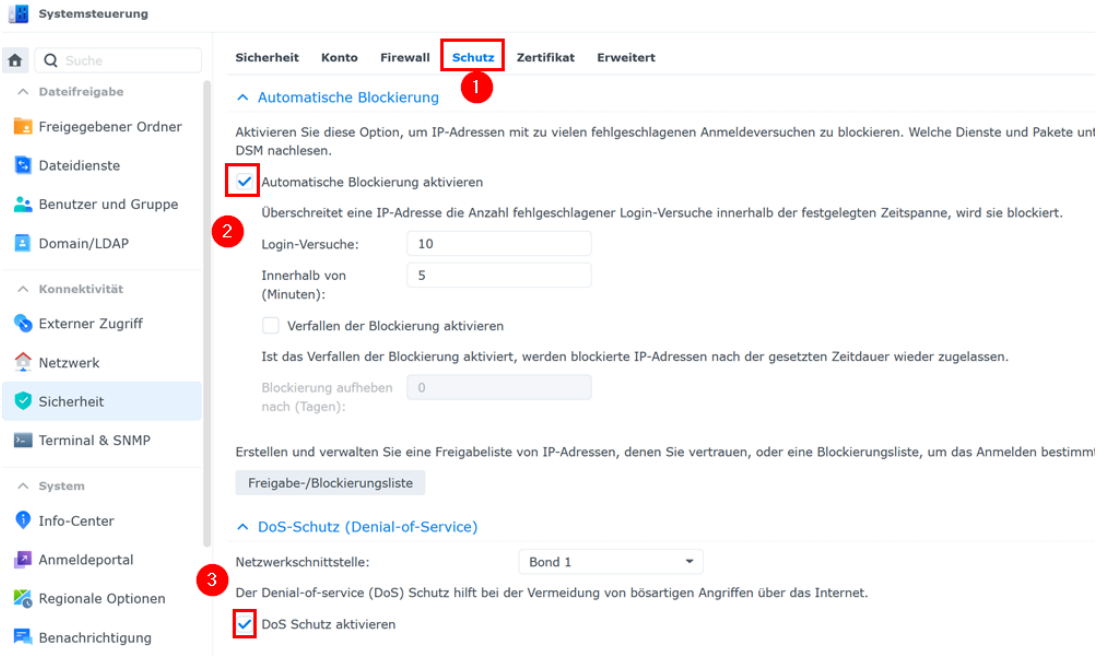
12 Sicherheitseinstellungen

Hinweis: Da die Synology-NAS von außen erreichbar sein soll, sollen die Sicherheitseinstellungen angepasst werden. Dazu gehört auch, dass der vorhandenen Admin-User durch einen alternativen User mit Adminrechten ersetzt wird (siehe Kapitel Benutzerkonten).

In der Systemsteuerung den Punkt „Sicherheit“ (1) öffnen und für den Reiter „Sicherheit“ (2) folgende Einstellungen (3) vornehmen:



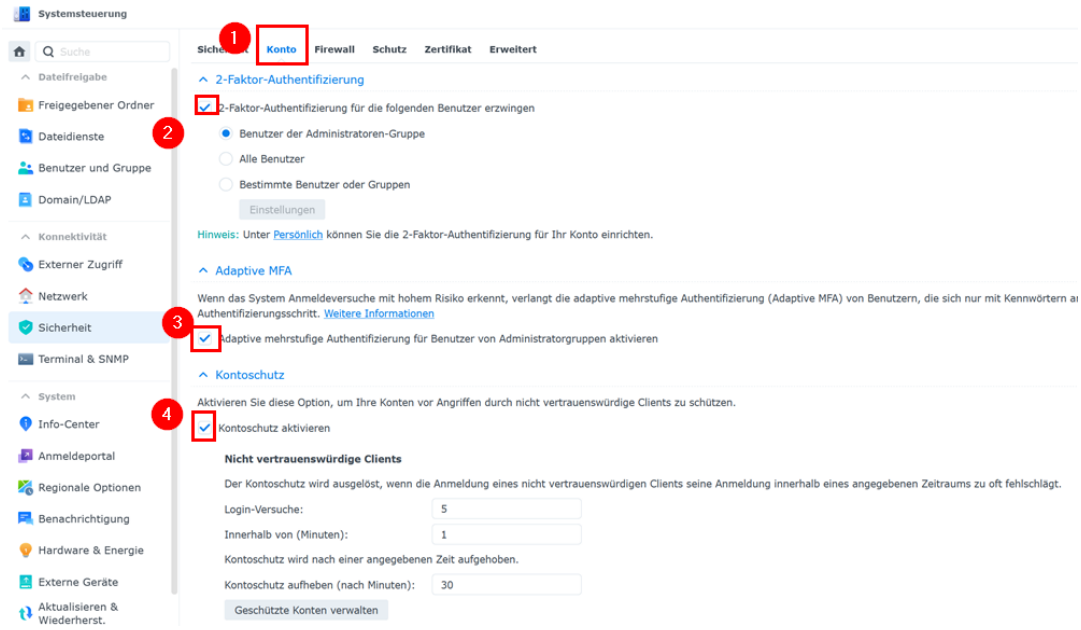
Im Reiter „Schutz“ (1) die automatische Blockierung (2) und den DoS-Schutz (3) aktivieren:



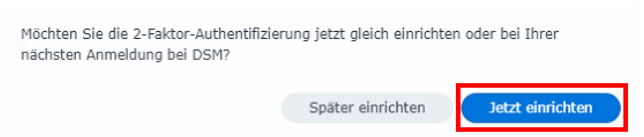
Alle Sicherheitseinstellungen mit „Übernehmen“ bestätigen.

12.1 Kontoschutz aktivieren und Zwei-Faktor-Authentisierung einrichten

Im Reiter „Konto“ (1) die Haken für „2-Faktor-Authentifizierung erzwingen“ für Benutzer der Administratoren-Gruppe (2), für „Adaptive mehrstufige Authentifizierung für Benutzer der Administratorengruppen aktivieren“ (3) und für „Kontoschutz aktivieren“ (3) setzen:

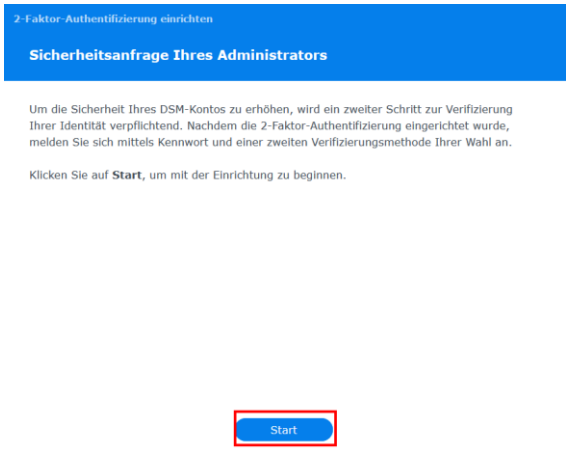


Im Anschluss mit der Einrichtung der Zwei-Faktor-Authentisierung für das aktuell eingeloggte Admin-Konto beginnen und „Jetzt einrichten“ wählen:

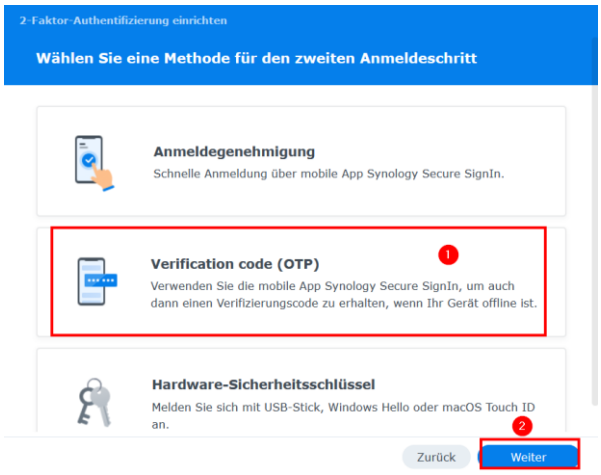


Hinweis: Es wird zur Einrichtung ein Gerät (z. B. ein Smartphone) mit einer beliebigen Authenticator-App benötigt.

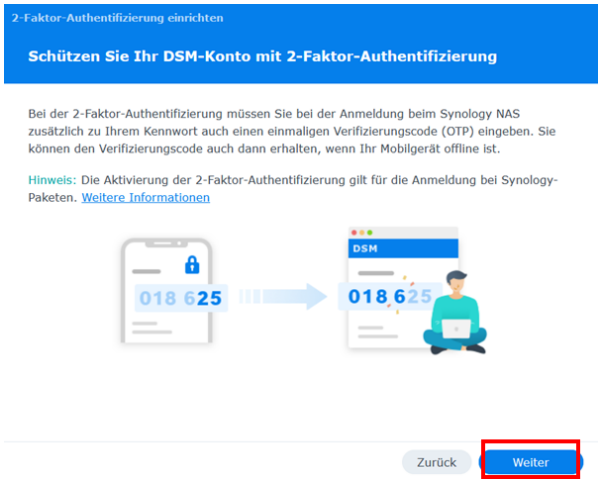
Mit „Start“ die Einrichtung beginnen:



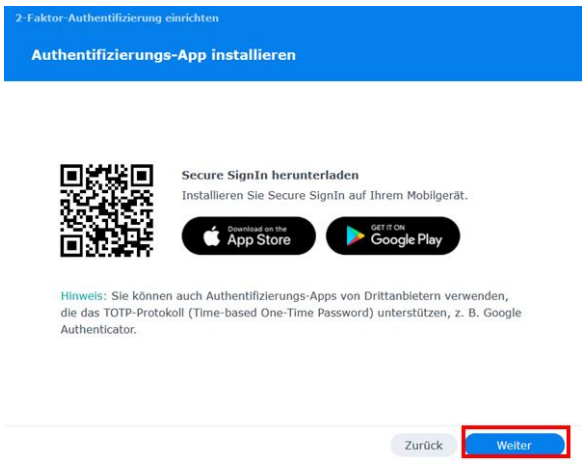
„Verification code (OTP)“ (1) mit „Weiter“ bestätigen (2):



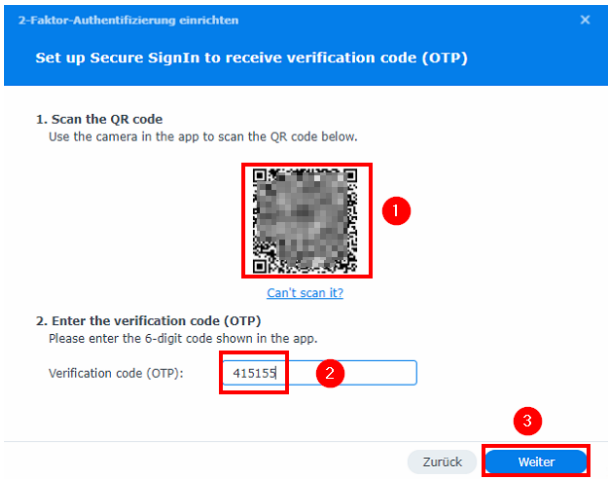
Mit „Weiter“ bestätigen:



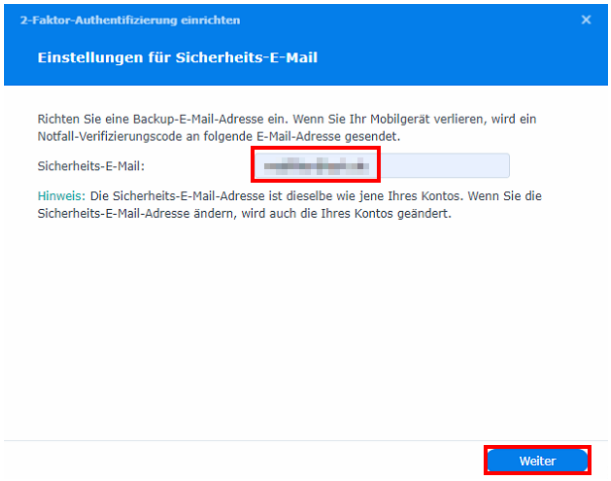
Wenn noch nicht vorhanden eine Authentifizierungs-App auf dem Smartphone installieren und mit „Weiter“ bestätigen:



Mit Hilfe der Authenticator-App den QR-Code (1) einscannen, den dort erstellten sechsstelligen Code eingeben (2) und mit „Weiter“ (3) bestätigen:



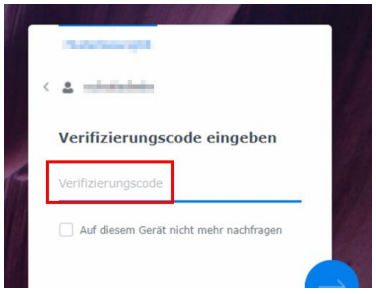
E-Mail-Adresse des Administratorkontos hinterlegen:



Hinweis: Hier dieselbe E-Mailadresse verwenden, die dem Admin-Konto im Kapitel Benachrichtungsdienst aktivieren zugewiesen wurde.

Mit „Fertig“ bestätigen.

Meldet sich der Admin-Benutzer nun neu an der Diskstation an, erscheint zusätzlich zur Passwortabfrage auch noch die Abfrage des Verifizierungscodes, der über die oben registrierte Authenticator-App aufgerufen werden kann:



Hinweis: Falls noch weitere Admin-Benutzer eingerichtet wurden, wird die Einrichtung der Zweifaktor-Authentisierung genau wie oben beschrieben beim nächsten Login ins entsprechende Admin-Konto vorgenommen.

12.2 Firewall aktivieren und konfigurieren

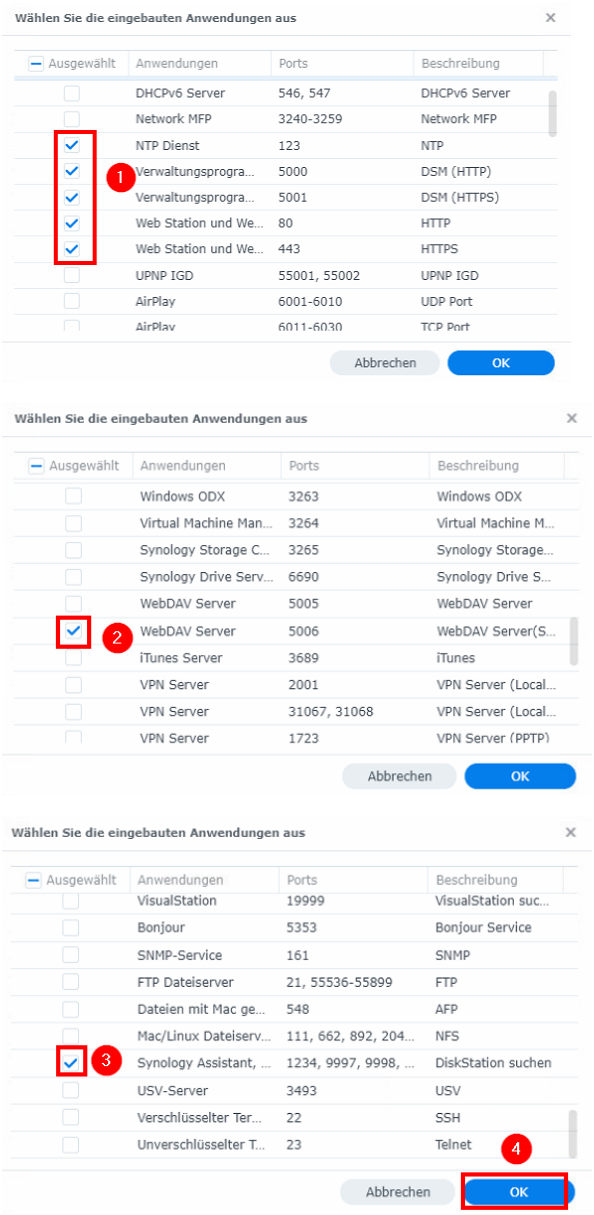
Zurück in die Systemsteuerung zum Menüpunkt „Sicherheit“ wechseln.

Im Reiter „Firewall“ (1) den Haken für „Firewall aktivieren“ (2) setzen und „Regeln bearbeiten“ (3) wählen:

Im Anschluss über „Erstellen“ eine neue Regel anlegen:

Ports auf „Aus einer Liste integrierter Anwendungen auswählen“ (1) umstellen und „Auswählen“ (2) anklicken:

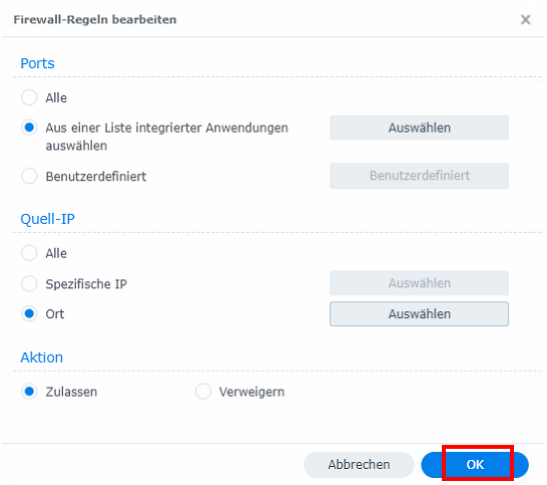
Haken für die Ports 123 (NTP-Dienst), 5000 + 5001 (Verwaltungsprogrammoberfläche), 80 + 443 (Webstation und Webmail), 5006 (WebDAV-Server), 1234 + 9997 + 9998 + 9999 (Synology Assistant, Netzwerksicherheit) setzen (1-3) und mit „OK“ bestätigen (4):



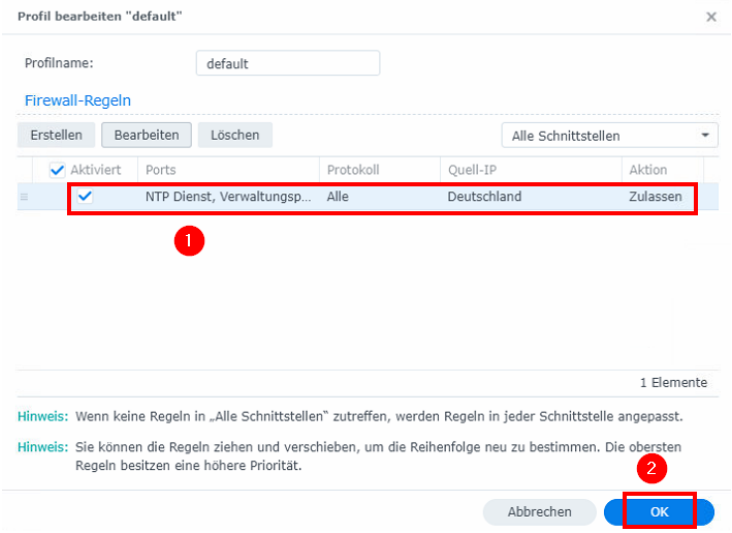
Im Anschluss die Quell-IP auf „Ort“ (1) umstellen und „Auswählen“ (2) anklicken:

„Deutschland“ suchen (1), anhaken (2) und mit „OK“ (3) bestätigen:

Am Ende die Firewallregel mit „OK“ anlegen:



Die neue Regel erscheint nun in der Übersicht (1) und muss mit „OK“ (2) bestätigt werden:



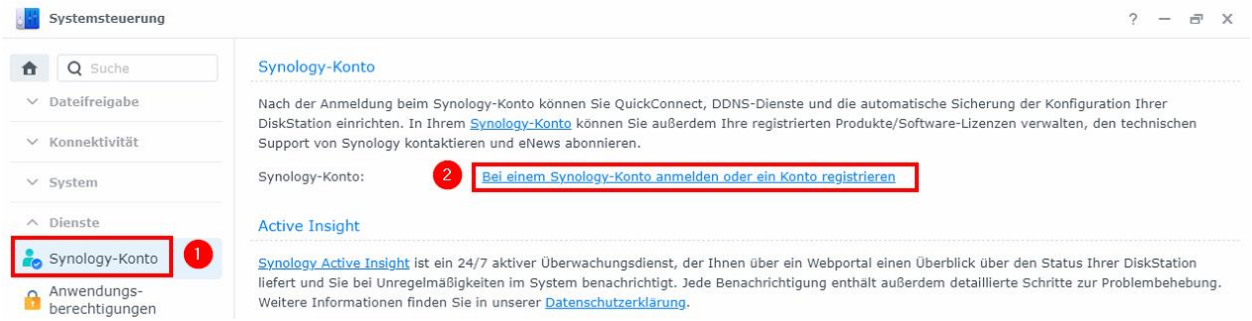
Hinweis: Die Firewall sperrt alle Zugrifft außerhalb der oben genannten Ports und von außerhalb Deutschlands.

13 Cloudzugriff einrichten

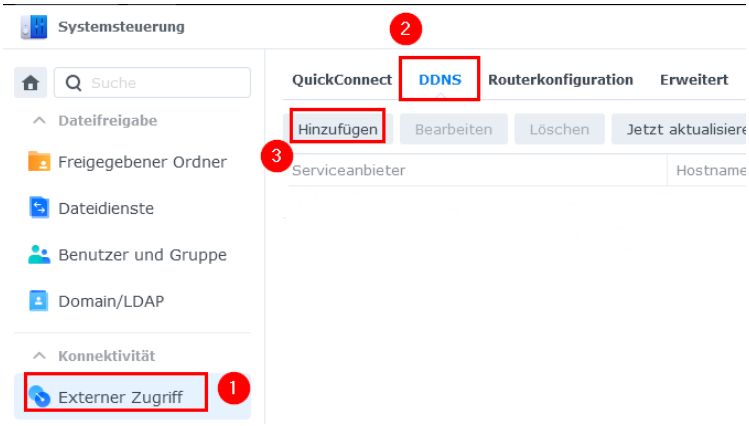
Damit Lehrkräfte auch von zu Hause auf die Datenablage zugreifen können, soll standardmäßig der Cloudzugriff ermöglicht werden.

Zunächst unter https://account.synology.com einen Synology-Account für die Schule anlegen. Dazu soll eine offizielle E-Mail-Adresse der Schule beziehungsweise des Schulträgers verwendet werden, da der unten festgelegte Hostname der Schule an den Account gebunden ist.

In der Systemsteuerung den Menüpunkt „Synology-Konto“ (1) sowie „Bei einem Synology-Konto anmelden“ (2) wählen und mit den neuen Zugangsdaten anmelden:

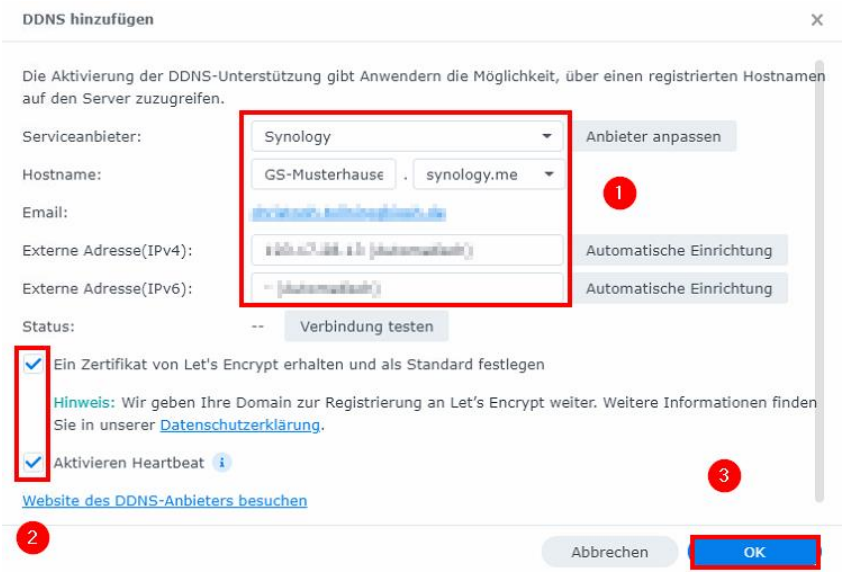


In der Systemsteuerung unter „Externer Zugriff“ (1) den Reiter „DDNS“ (2) und anschließend „Hinzufügen“ (3) wählen:



Hinweis: Der DynDNS-Dienst soll auch dann genutzt werden, wenn die Schule (zum Beispiel über den Breitbandanschluss des Landes) bereits eine öffentliche IP-Adresse hat. Zum einen ist der Aufruf der Diskstation über einen Domainnamen (GS-Musterhausen.synology.me) einfacher. Zum anderen wird über den DynDNS-Dienst auch gleich ein Zertifikat bereitgestellt, sodass beim Aufruf der Seite keine Sicherheitsabfrage kommt.

Die DDNS-Unterstützung aktivieren, als Serviceanbieter „Synology“ wählen und einen passenden Hostnamen für die Schule vergeben (1). Dieser soll aus dem Namen bzw. Kürzel der Schule und dem Domainnamen „synology.me“ bestehen (zum Beispiel GS-Musterhausen.synology.me). Im Anschluss Haken für Let’s Encrypt-Zertifikat und Heartbeat setzen (2) und mit „OK“ (3) bestätigen:

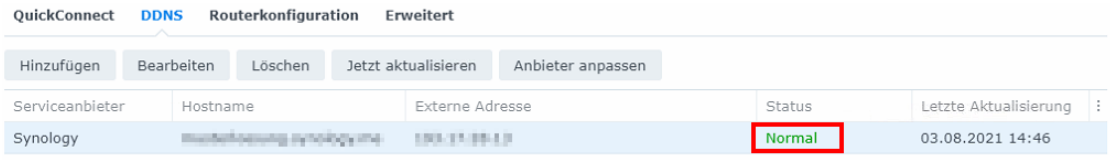


Hinweis: Da der Hostname möglicherweise bereits vergeben wurde, sollte die Verbindung über den Button „Verbindung testen“ geprüft werden.

Im Anschluss das vorgeschlagene Zertifikat von Let`s Encrypt als Standardzertifikat festlegen:

Hinweis: Ohne Zertifikat würde der Aufruf der Webseite später mit einer Sicherheitsabfrage starten. Das Zertifikat muss alle drei Monate verlängert werden. Diese Aufgabe übernimmt die Diskstation automatisiert.

Der eingerichtete Dienst sollte dann mit dem Status „Normal“ aufgelistet werden:



Damit man beim Aufrufen des Hostnamens auch auf die Synology-Diskstation weitergeleitet wird, muss – falls noch nicht geschehen - noch eine Weiterleitung im Router des Unterrichtsnetzes vorgenommen werden:

- Variante 1: Wird ein Draytek-Router beziehungsweise UniFi-Security-Gateway (USG) verwendet, muss dort der Port 443 auf den von der Diskstation verwendeten HTTPS-Port (im Normalfall Port „5001“ – siehe „Netzwerk“ – „DSM-Einstellungen“) auf die IP-Adresse

der Datenablage (192.168.1.250) weitergeleitet werden. Wenn dies noch nicht eingerichtet wurde, findet man die notwendigen Schritte in den zugehörigen Anleitungen:
    - Draytek: „Musterlösung Grundschule SH_Einrichtung Netzwerk und WLAN.pdf“,
    - USG: „Musterlösung Grundschule SH_Einrichtung Netzwerk und WLAN_Landes-Breitbandnetz.pdf“ (im Archiv des SchulCommSy-Raumes).
- Variante 2: Wird die Dataport-Lösung dSchulWLAN genutzt, ist keine zusätzliche Einstellung notwendig. Zugriffe auf die öffentliche IP der Schule werden in diesem Fall durch den Dataport-Router direkt auf die Diskstation weitergeleitet.

Zum Abschluss den Aufruf der Diskstation über den oben angelegten Hostnamen testen. **Wichtig**: Der Aufruf der Seite innerhalb des Unterrichtsnetzes ist nur möglich, wenn ein interner DNS im Router eingerichtet bzw. bei Dataport beantragt wurde (siehe nächstes Kapitel).

Hinweis: In **Ausnahmefällen** - wenn sich zum Beispiel eine Portweiterleitung nicht realisieren lässt - muss die Einrichtung des DDNS-Dienstes übersprungen und stattdessen „QuickConnect“ eingerichtet werden:

- In der Systemsteuerung „Externer Zugriff“ wählen, den Reiter „QuickConnect“ aufrufen, dort einen Haken für „QuickConnect aktivieren“ setzen und eine passende Quickconnect-ID angeben. Diese soll aus dem Namen bzw. Kürzel der Schule bestehen (zum Beispiel „GS-Musterhausen“).
- Mit „Übernehmen“ bestätigen.
- Im Anschluss Firewall-Benachrichtigung mit „OK“ bestätigen.
- Nach erfolgreicher Registrierung wird die Webadresse zum Aufrufen der Diskstation angezeigt.

13.1 Internen DNS-Eintrag einrichten/beantragen

Hinweis: Um auch innerhalb des Unterrichtsnetzes auf die öffentliche Webadresse der Datenablage zugreifen zu können, muss ein interner DNS-Eintrag für das pädagogische Breitbandnetz eingerichtet/beantragt werden.

Wenn der pädagogische **Landes-Breitbandanschluss genutzt** wird:

Einrichtung eines internen DNS-Eintrags bei Dataport beantragen. Dazu über das IQSH-Helpdesk-Formular (https://www.secure-lernnetz.de/helpdesk) im Bereich „Breitband“ – „Unterrichtsnetz“ – „Störung im Betrieb“ ein Ticket mit Angabe der Schule (Name und Adresse), der Webadresse der schulischen Datenablage (https://xyz.synology.me) sowie der WAN-Adresse des Draytek-Routers (IP-Adresse: 10.84/85/86/87.x.9) angeben:

Beispieltext:

Liebes Helpdesk-Team,

hiermit beantrage ich das Anlegen eines internen DNS-Eintrages für den pädagogischen Breitbandanschluss des Landes für folgende Schule:

[Schulname]

[Schuladresse]

Der interne DNS soll dabei für die Domain [https://xyz.synology.me] auf die interne Adresse [10.84/85/86/87.x.9] angelegt werden.

Mit freundlichen Grüßen

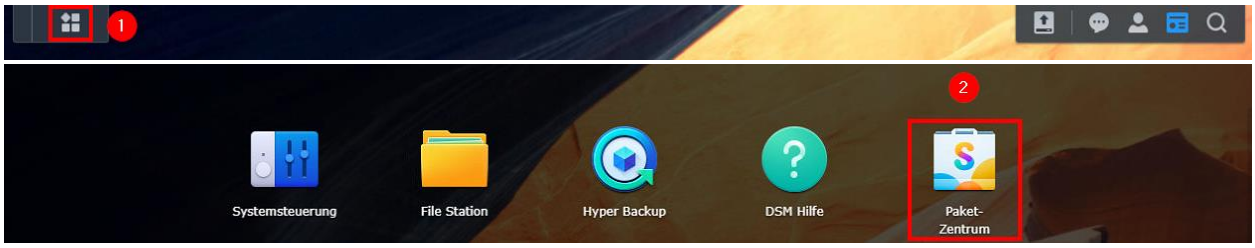
Wenn der pädagogische **Landes-Breitbandanschluss nicht genutzt** wird:

Der DNS-Eintrag kann direkt im Draytek-Router eingetragen werden. Die dafür notwendigen Schritte sind in der Anleitung „Musterlösung Grundschule SH_Einrichtung Netzwerk und WLAN (ohne Landes-Breitbandanschluss).pdf“ im Kapitel „Internen DNS anlegen“ zu finden.

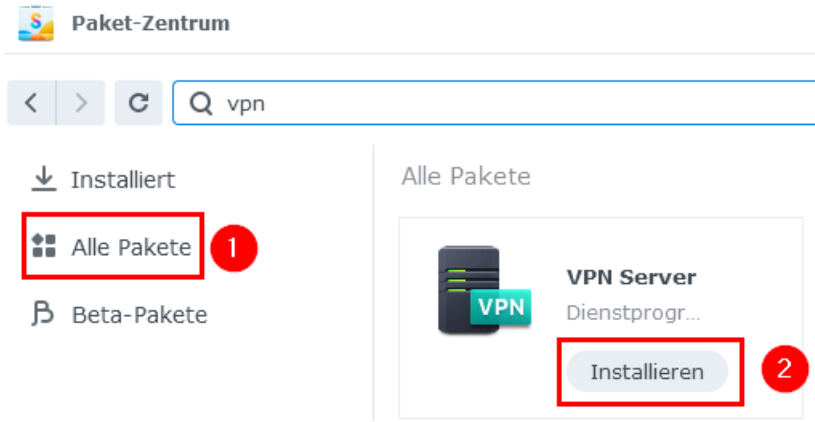
14 VPN einrichten (nur bei Nutzung von dSchulWLAN)

Wenn die **Dataport-Lösung dSchulWLAN** eingerichtet wurde, soll die Datenablage auch die Funktion des VPN-Servers übernehmen.

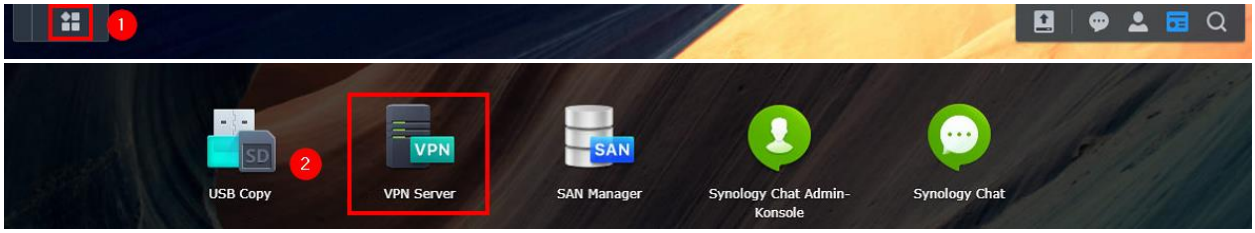
Dafür zunächst über das Paket-Zentrum das Paket „VPN Server“ installieren. Dazu über das Hauptmenü (1) das Paketzentrum (2) öffnen:



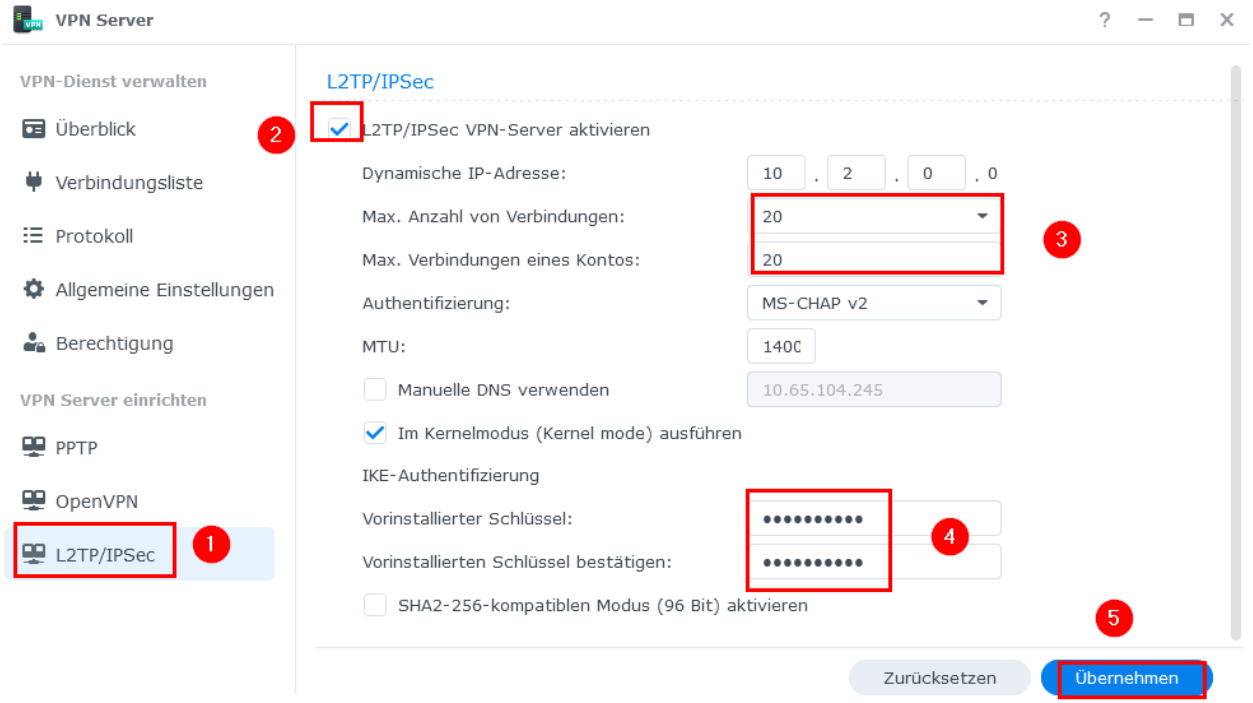
Unter „Alle Pakete“ (1) das Paket „VPN Server“ (2) installieren:



Im Anschluss über das Hauptmenü (1) die Einstellungen des Paketes „VPN Server“ (2) öffnen:



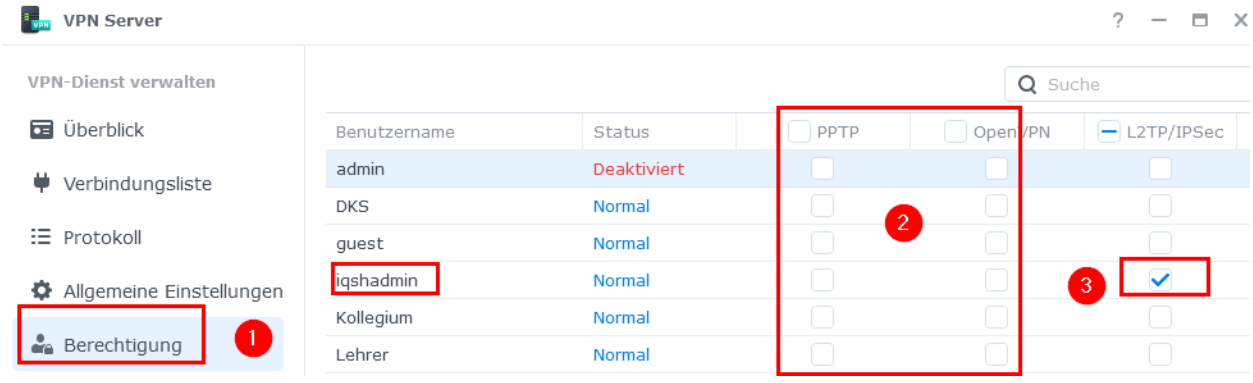
Im Menüpunkt „L2TP/IPSec“ (1) den VPN-Server aktivieren (2), die Anzahl der max. Verbindungen sowie der Verbindungen mit demselben Konto hochsetzen (3), einen vorinstallierten Schlüssel vergeben (4) und mit „Übernehmen“ (5) bestätigen:



Hinweis: Die gesamte Kommunikation wird über den Pre-shared Key verschlüsselt. Dafür sollte daher ein sicheres Passwort gewählt werden. Seiten wie https://www.uni-muenster.de/IT-Sicherheit/passwortgenerator.html berechnen einen Code, der entsprechend sicher ist. Der Schlüssel muss sowohl dem Server als auch jedem Client, der eine VPN-Verbindung aufbauen will, mitgeteilt werden.

Den vorinstallierten Schlüssel in der IT-Dokumentation der Schule vermerken.

Im Anschluss unter „Berechtigung“ (1) die Dienste „PPTP“ und „OpenVPN“ für alle Benutzer deaktivieren (2) und nur für den/die Adminbenutzer den Dienst „L2TP/IPSec“ aktivieren (3):



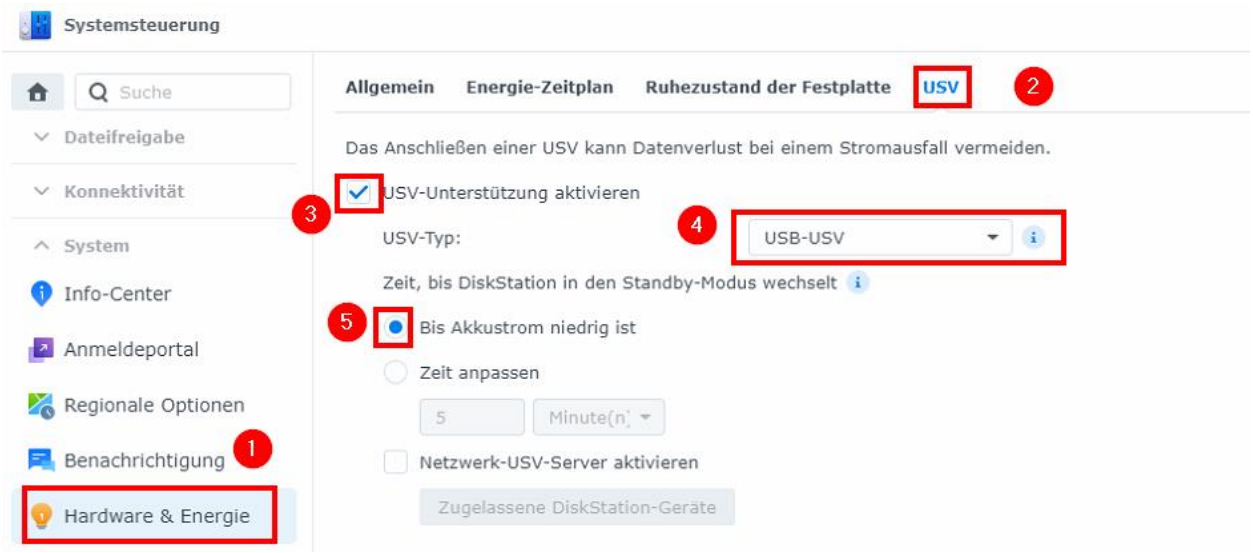
Hinweis: Sofern auch ein VPN-Zugriff von den dienstlichen Lehrkräfte-Endgeräten ins Unterrichtsnetz ermöglicht werden soll, ein neues gemeinsames Konto für das Kollegium bzw. Einzel-Accounts für Lehrkräfte anlegen und diese(s) für „L2TP/IPSec“ berechtigen. Die Schritte zur VPN-Einrichtung auf dem LK-Endgerät werden in der Anleitung „Musterlösung Grundschule SH_VPN-Verbindung herstellen.pdf“ beschrieben.

15 USV Einrichten

Hinweis: Es wird empfohlen die Synology-NAS an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen, damit im Falle eines Stromausfalles das Gerät geregelt in den sicheren Modus runterfahren kann.

USV per USB-Kabel mit der Synology-Diskstation verbinden.

In der Systemsteuerung den Menüpunkt „Hardware & Energie“ (1) und dort den Reiter „USV“ (2) wählen. Die USV-Unterstützung aktivieren (3), als USV-Typ „USB-USV“ (4) wählen und den Standbymodus aktivieren sobald „Akkustrom niedrig ist“ (5):



Änderungen mit „Übernehmen“ bestätigen.

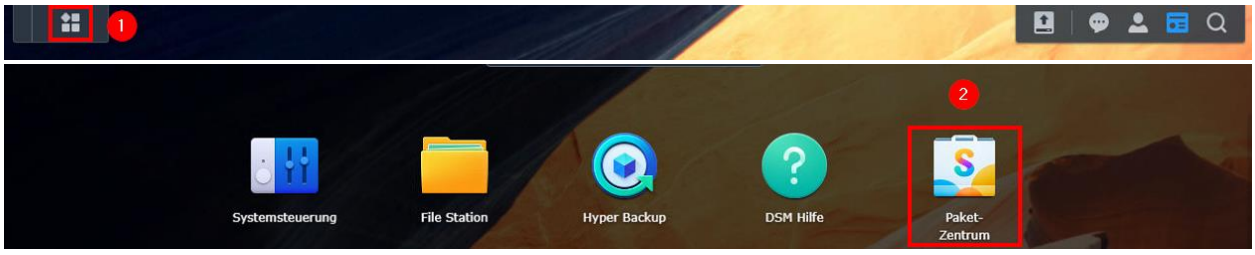
Hinweis: Je nach verwendetem USV-Modell müssen ggf. leicht geänderte Einstellungen vorgenommen werden.

16 WebDAV einrichten

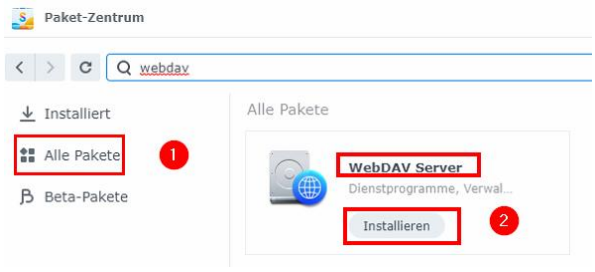
Hinweis: Um einen externen Zugriff auf Netzwerk-Ordner der Datenablage zur ermöglichen, soll WebDAV aktiviert werden. Um dieses Protokoll nutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Für das Unterrichtsnetz muss eine öffentliche IP-Adresse (z. B. über den Breitbandanschluss des Landes) existieren bzw. ein DynDNS-Dienst eingerichtet worden sein (siehe Anleitung „Musterlösung Grundschule SH_Einrichtung Netzwerk und WLAN.pdf“). **Wichtig**: Die Erreichbarkeit der Datenablage über eine Quickconnect-Adresse reicht nicht aus.
- Für den WebDAV-Port 5006 muss eine Weiterleitung im Router eingerichtet worden sein (siehe Anleitung „Musterlösung Grundschule SH_Einrichtung Netzwerk und WLAN.pdf“).
- Bei Nutzung des Landes-Breitbandanschlusses: damit WebDAV auch innerhalb des Unterrichtsnetzes funktioniert, muss die Domain-Adresse der Datenablage im internen DNS eingetragen werden (siehe Kapitel Internen DNS-Eintrag einrichten/beantragen).

Sind die Voraussetzungen erfüllt, muss auf der Datenablage das Paket „WebDAV Server“ installiert werden. Dazu über das Hauptmenü (1) das Paketzentrum (2) öffnen:

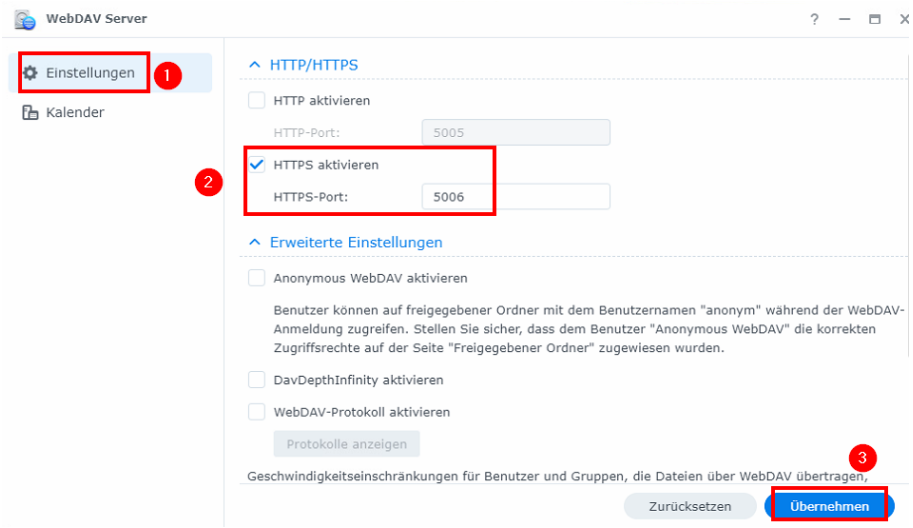


Dort unter „Alle Pakete“ (1) das Paket „WebDAV Server“ suchen und installieren (2):



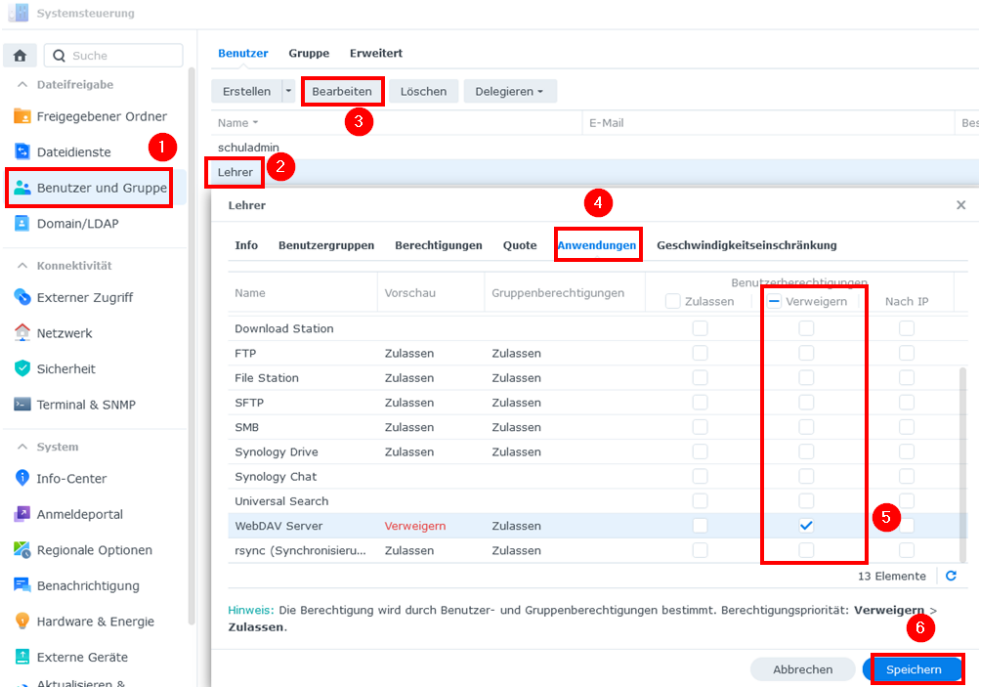
Nach der Installation das Paket öffnen:

Unter „Einstellungen“ (1) dann ein Haken für „HTTPS aktivieren“ (2) setzen und mit „Übernehmen“ (3) bestätigen:



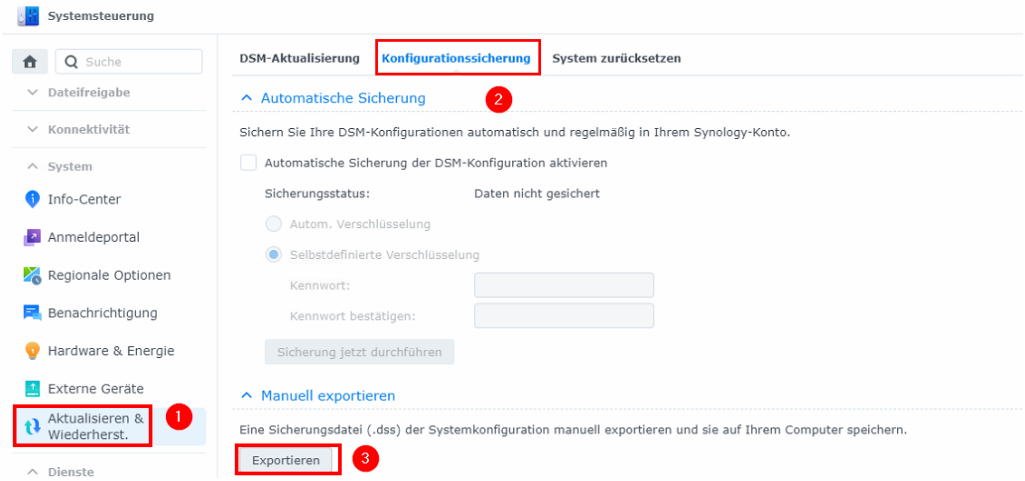
Hinweis: Per Voreinstellung haben alle bisher angelegten Benutzer nun eine Zugriffsmöglichkeit per WebDAV. Da der Benutzer „Lehrer“ auch noch auf den Ordner „Programme“ zugreifen kann, soll dieser Benutzer nicht für den WebDAV-Zugriff verwendet werden. Dem Benutzer soll die WebDAV-Berechtigung entzogen werden.

In der Systemsteuerung auf den Menüpunkt „Benutzer und Gruppe“ (1) klicken, den Benutzer „Lehrer“ auswählen, mit „Bearbeiten“ (3) die Eigenschaften öffnen, dort im Reiter „Anwendungen“ (4) das Häkchen für „WebDAV Server“ unter „Verweigern“ (5) setzen und mit „Speichern“ (6) bestätigen:



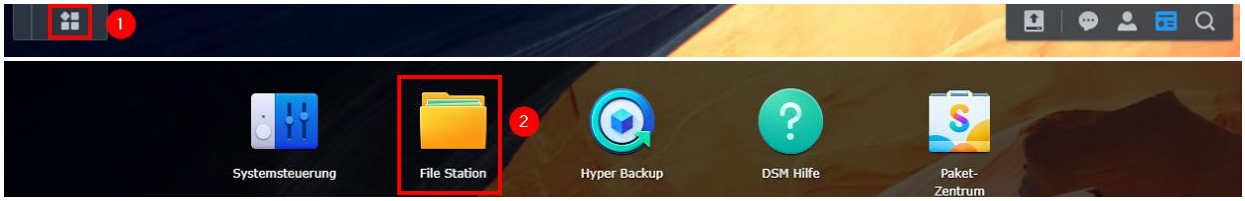
17 Konfiguration sichern

Die oben durchgeführten Einstellungen für die Datenablage sollen abschließend in einer Konfigurationsdatei abgespeichert werden. Dazu in der Systemsteuerung „Aktualisieren und Wiederherstellen“ (1) wählen und im Reiter „Konfigurationssicherung“ (2) den Menüpunkt „Exportieren“ (3) anklicken:

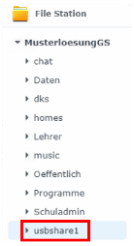


Anschließenden Hinweis mit „OK“ bestätigen und die DSS-Datei herunterladen.

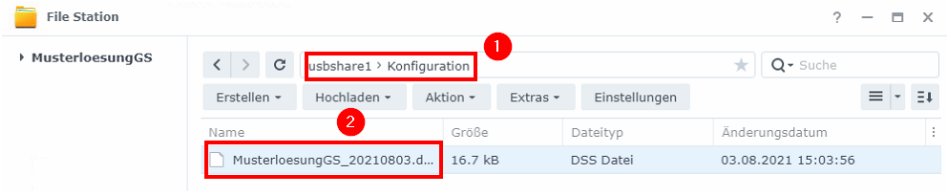
Im Anschluss über das Hauptmenü (1) die Synology-Anwendung „File Station“ (2) öffnen:



Dort die USB-Festplatte auswählen:



Auf der USB-Festplatte den Ordner „Konfiguration“ (1) anlegen und in diesen Ordner die Konfigurationsdatei (2) hochladen:



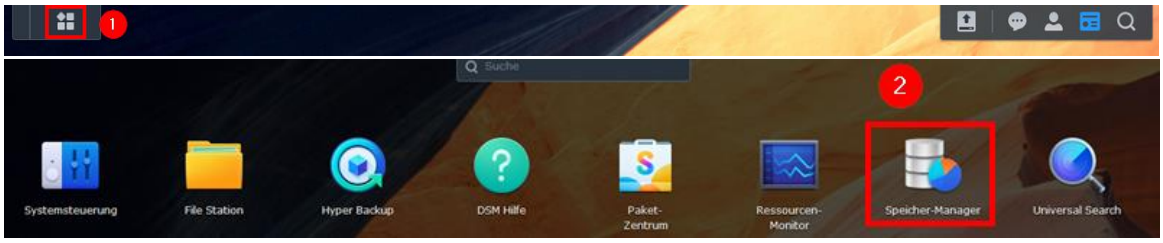
18 SSD Cache einbinden (optional)

Hinweis: Bei Bedarf kann das Synology-Diskstation-Modell 723+ zusätzlich zu den eingebauten Festplatten um zwei Caching-SSDs (M.2 NVMe-Speichermodule) erweitert werden. Der SSD-Cache verbessert dabei die Zugriffsleistung auf Dateien, indem häufig genutzte kleine Dateien auf den SSDs zwischengespeichert werden. Dies ist insbesondere hilfreich, um zum Beispiel die Nutzung von Netzwerkprogrammen wie der Lernwerkstatt oder den gleichzeitigen Zugriff vieler Endgeräte auf die Datenablage zu verbessern. Passende SSDs für das angegebene Modell findet man auf der Synology-Kompatibilitätsliste unter https://www.synology.com/de-de/compatibility.

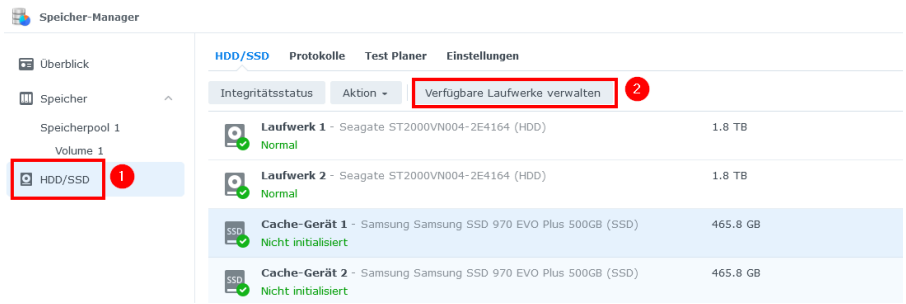
Folgende Schritte sind notwendig, um den SSD Cache zu nutzen:

Zunächst die Synology Diskstation herunterfahren und die beiden Speichermodule auf der Unterseite des Gerätes in die leeren Steckplätze einbauen (siehe Handbuch für Synology NAS 723+).

Im Anschluss über das Hauptmenü (1) den Speicher-Manager (2) aufrufen:



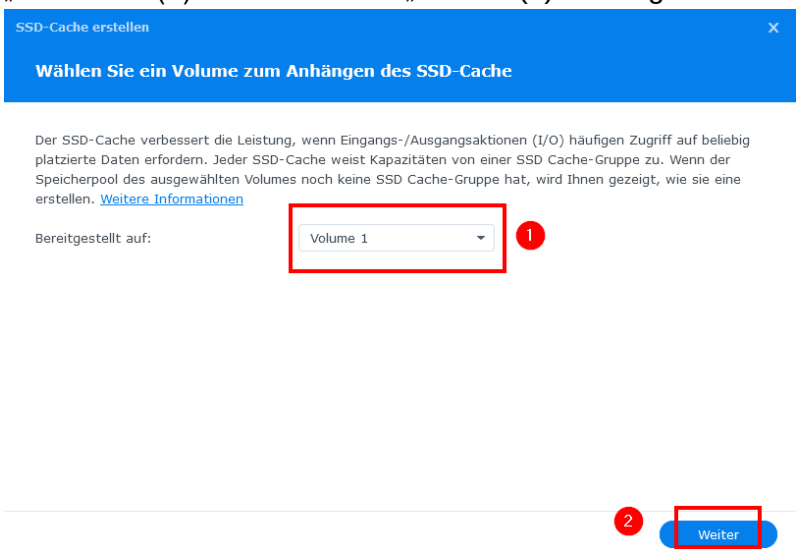
Dort unter dem Menüpunkt „HDD/SSD“ (1) die Option „Verfügbare Laufwerke verwalten“ (2) auswählen:



„SSD-Cache“ erstellen auswählen:

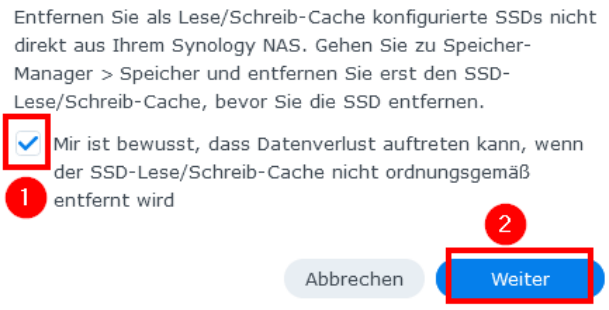
Im Einrichtungs-Assistenten nachfolgenden Optionen wählen.

- „Volume 1“ (1) wählen und mit „Weiter“ (2) bestätigen:

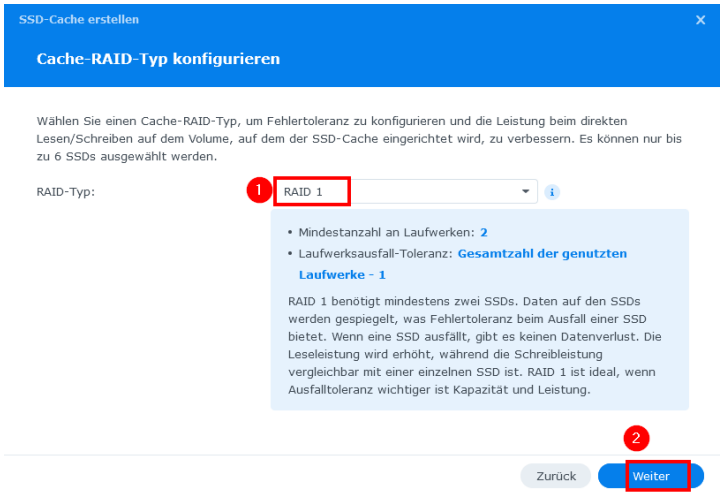


- Den Lese/Schreib-Cache aktivieren (1) und mit „Weiter“ (2) bestätigen:

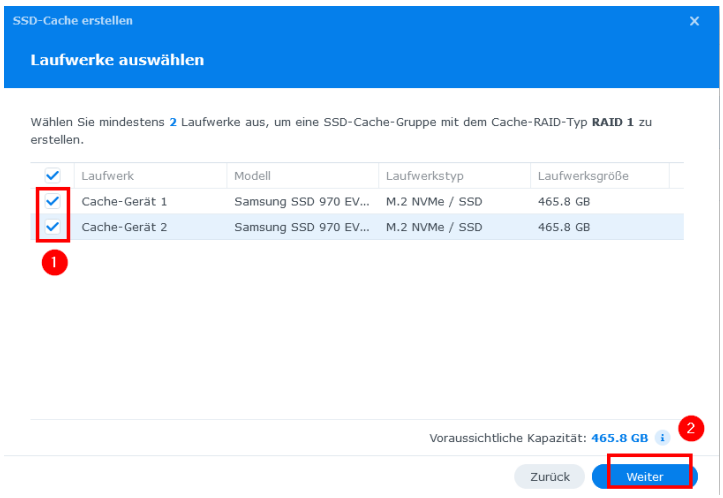
- Folgenden Hinweis akzeptieren (1) und mit „Weiter“ (2) bestätigen:



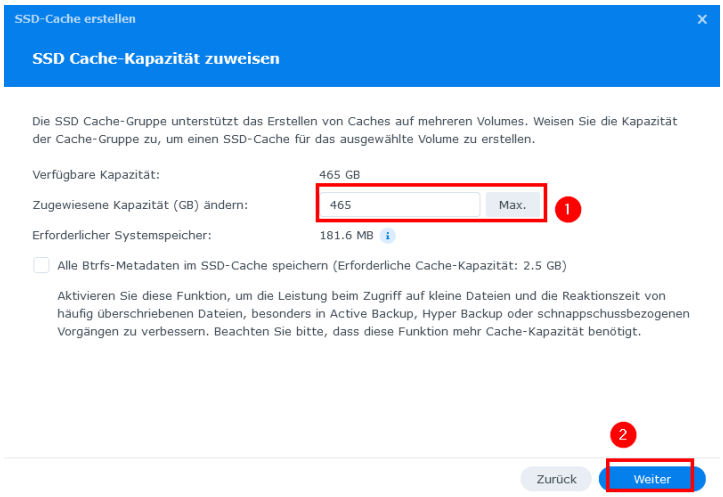
- „RAID 1“ wählen (1) und mit „Weiter“ (2) bestätigen:



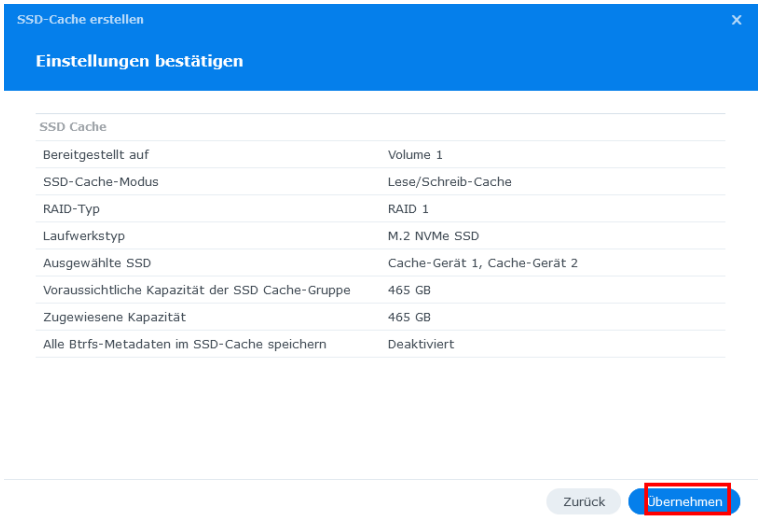
- Beide neuen SSD-Laufwerke auswählen (1) und mit „Weiter“ (2) bestätigen:



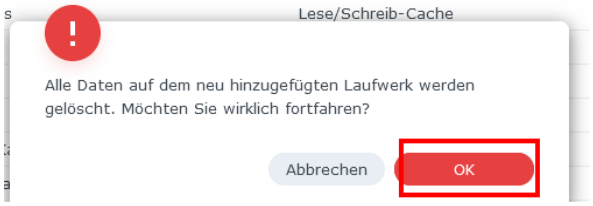
- Die maximal mögliche Speichergröße (1) angeben und mit „Weiter“ (2) bestätigen:



- Einstellungen mit „Übernehmen“ bestätigen:

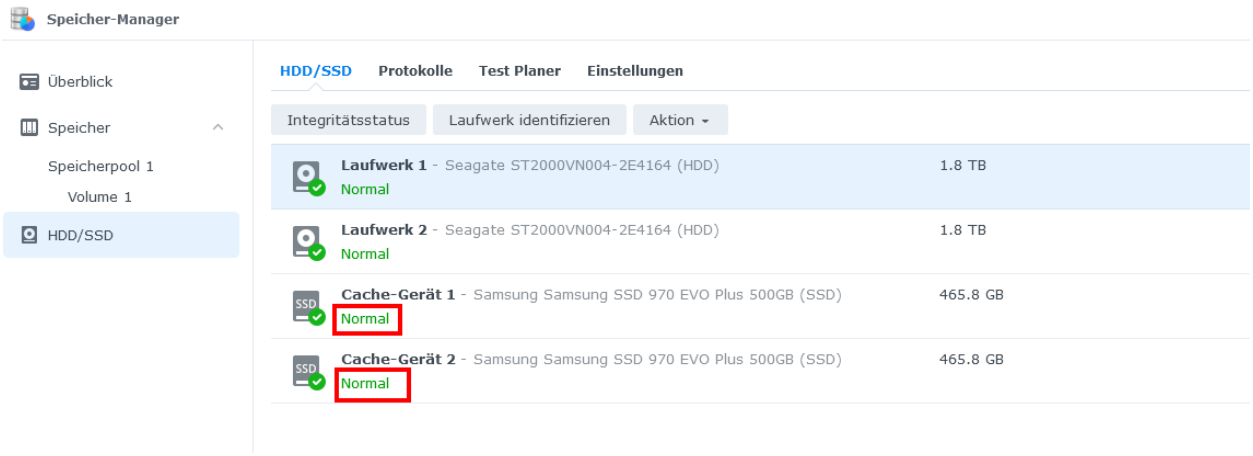


- Löschen von Daten auf den neuen Laufwerken mit „OK“ bestätigen:



Im Anschluss wird der SSD-Cache eingebunden.

Nach kurzer Zeit ist der Einbindungsprozess abgeschlossen. Die SSD-Laufwerke erhalten dann die Statusmeldung „Normal“:



Änderungshistorie

Änderung vom 05.02.2024

- Einige Screenshots wurden ausgetauscht.

Änderung vom 29.11.2023:

- Die Screenshots im Kapitel Datensicherung einrichten wurden angepasst. Die Sicherheitsrotation soll abweichend zur bisherigen Einrichtungsanleitung aktiviert werden.

Änderung vom 04.10.2023:

- Das maximale SMB-Protokoll für die Dateidienste wird auf „SMB3“ eingestellt (siehe Kapitel Ordner anlegen).
- Die Screenshots zur Einrichtung von Quickconnect in Ausnahmefällen wurden entfernt (siehe Kapitel Cloudzugriff einrichten).

Änderung vom 10.07.2023:

- Der Ordner und das Benutzerkonto „DKS“ wird in „Wartung“ umbenannt (siehe Kapitel Benutzerkonten anlegen und Kapitel Ordner anlegen).

Änderung vom 30.06.2023:

- Aufgrund der Anpassung an die aktuelle DSM-Version 7.2 wurden zahlreiche Screenshots ausgetauscht und vereinheitlicht.
- Die Kapitel „DDNS-Dienst einrichten“ und „Quickconnect einrichten“ wurden im übergeordneten Kapitel „Cloudzugriff einrichten“ zusammengeführt.

Änderung vom 26.06.2023:

- Das Kapitel „Internen DNS beantragen“ aus der Netzwerk-Anleitung wurde in diese Anleitung eingefügt (siehe Internen DNS-Eintrag einrichten/beantragen).

Änderung vom 15.05.2023:

- Es wurden nur kleinere Änderungen durchgeführt: z. B. das Anpassen einiger Screenshots an die aktuelle DSM-Betriebssystem-Version.

Änderung vom 22.09.2022:

- Die Screenshots zum Kapitel „SSD Cache einbinden“ wurden angepasst (siehe Kapitel SSD Cache einbinden).

Änderung vom 22.09.2022:

- Die Datenablage soll mit beiden LAN-Anschlüssen am Switch angebunden werden und die zugehörigen Ports aggregiert werden, um u. a. eine höhere Bandbreite beim Zugriff

mehrerer Geräte auf die Datenablage zu ermöglichen (siehe Kapitel Netzwerkkonfiguration vornehmen).

Änderung vom 01.07.2022:

- Die Netzwerkkonfiguration (DNS-Server) bei Nutzung des Breitbandanschlusses des Landes wurde korrigiert (siehe Kapitel Netzwerkkonfiguration vornehmen).

Änderungen vom 29.04.2022:

- Die Option „Freigegebene Ordner für Benutzer ohne Berechtigung ausblenden“ wird aktiviert (siehe Kapitel Ordner anlegen).

Änderungen vom 05.04.2022:

- Der QuickConnect-Dienst wird nur noch in Ausnahmefällen aktiviert (siehe Kapitel QuickConnect einrichten).

Änderung vom 22.03.2022:

- Um den Zugriff auf Dateien der Datenablage – insbesondere im Zusammenhang mit Netzwerkprogrammen – zu verbessern, können bei Bedarf zusätzlich Caching-SSDs in das Synology-Diskstation-Modell 720+ eingebaut und eingebunden werden (siehe Kapitel SSD Cache einbinden).

Änderung vom 25.02.2022:

- Der Benutzer „Kollegiumwebdav“ muss nicht mehr zusätzlich eingerichtet werden. Sowohl für den WebDAV-Zugriff als auch für den browserbasierten Zugriff sollen der Benutzer „Kollegium“ bzw. alternativ persönliche Benutzerkonten für Lehrkräfte genutzt werden.

Änderungen vom 21.12.2021:

- Die Zwei-Faktor-Authentisierung für Benutzer der Administratorengruppe wird aktiviert (siehe Kapitel Kontoschutz aktivieren und Zwei-Faktor-Authentisierung einrichten). Für jeden Administrator bzw. jede Administratorin sollte daher ein eigenes Benutzerkonto angelegt werden (siehe Kapitel Benutzerkonten anlegen).
- Die Firewall-Einstellungen wurden angepasst (siehe Kapitel Firewall aktivieren und konfigurieren).

Änderungen vom 19.11.2021:

- Um einen externen Zugriff auf Netzwerk-Ordner der Datenablage zur ermöglichen, wird ein weiterer Nutzer „Kollegiumwebdav“ angelegt (Kapitel 5), der nur auf die Ordner „Daten“ und „Lehrer“ zugreifen kann (Kapitel 6). Zudem wird das Paket „WebDAV Server“ installiert und eingerichtet sowie der WebDAV-Zugriff für die Benutzer „Kollegium“ und „Lehrer“ gesperrt (Kapitel 16).
- Ältere Änderungen sind in der Änderungshistorie am Ende der Anleitung zu finden.

Änderungen vom 03.08.2021:

- Als DSM-Version wird die Version 7.0 und neuer verwendet.
- In der neuen DSM-Version kann der Pushdienst nicht mehr für eine E-Mail-Adresse eingerichtet werden. Stattdessen soll die E-Mail-Benachrichtigung aktiviert werden (siehe Kapitel Benachrichtungsdienst aktivieren).