

# Synology Setup Guide

Setup Guide for Synology NAS

- [Synology Initial Setup Guide \(DSM Version 7\)](#)
  - [Synology NAS Setup & Configuration: Initial Steps](#)
  - [Shared Folder Setup](#)
  - [Data Protection and Monitoring Setup](#)
  - [Setting up Updates](#)
- [Synology Security Guide & Best Practices](#)
  - [User Security & Access Control](#)
  - [Remote Access Setup](#)
  - [Synology Firewall Setup](#)

# Synology Initial Setup Guide (DSM Version 7)

Guide for setting up Synology NAS system and Services

# Synology NAS Setup & Configuration: Initial Steps

These setup goes over a Synology NAS whether purchased new or factory reset. Ensure that your NAS is plugged in and has internet access before proceeding.

This Guide covers 7.0 Version install, and it assumes that NAS is plugged in, has drives and is truned on.

## Find Synology NAS & Install DSM

1. Navigate to the website <http://find.synology.com> and wait for your device to be found. DHCP will automatically give your DiskStation an IP address. Select **Connect**
2. **Accept** the End User License Agreement and proceed
3. Select **Install**
4. DSM 7 requests that you download the latest version of DSM using Synology's Download Center. Select the model NAS that you have, then in the OS Version section, select 7.0 Series. You can then Download the current DSM 7 Operating System

OS Version

[Operating System](#) [Desktop Utilities](#) [Packages](#) [Documents](#) [Android Apps](#) [EOL products](#)

---

Operating System

<b>DSM 7.0</b>	DSM is the operating system of DS1019+.	<a href="#">Download</a>	<a href="#">MD5</a>	<a href="#">Release Note</a> <a href="#">All Downloads</a>
----------------	---	--------------------------	---------------------	---

5. You will be informed that all data on your drives will be deleted. If you agree, select the checkbox next to **I understand that all data on these drives will be deleted**, then **Continue**
6. DSM will install and reboot when finished. After a few minutes have passed, open a new tab and navigate to your synology IP address or <http://find.synology.com>
7. Give your DiskStation
  1. Server Name (Device Name)

2. Username and Password
8. The next step will ask you to create a Synology account. You can do this at a later time if you'd prefer
9. The next step will ask you to enable Synology Active Insight and configuration backups. Select whichever you'd prefer, then proceed

## Set up a Synology NAS Storage Pool/Volume

DSM 7 has made storage pool creation incredibly easy and straightforward. You will be prompted immediately to set up a Storage Pool and Volume, but if you're not, open the Storage Manager and select Storage, then Create a Storage Pool.

1. You will be brought to a wizard that will guide you through the setup process. Select **Start**
2. Give your storage pool a description if you'd like, select the RAID type you will be using and select **Next** to proceed
3. Select the **Hard Drives** (generally all of them) that you'd like in this Storage Pool and select **Next**. NOTE: You can always add drives later and expand your storage pool/volume
4. You will be prompted that all data on the drives will be erased. Select **Continue**
5. The next option will ask if you'd like to perform drive checks. If you'd like to test the drives, you can select **Perform drive check**. If you'd like to skip it, select **Skip** drive check
6. This next section will determine how much of the volume you'd like to allocate. Generally, most people will use all of it, so you can select **Max**. If you'd like to use something smaller, you can enter the value
7. Click **Apply** and your storage pool will be created

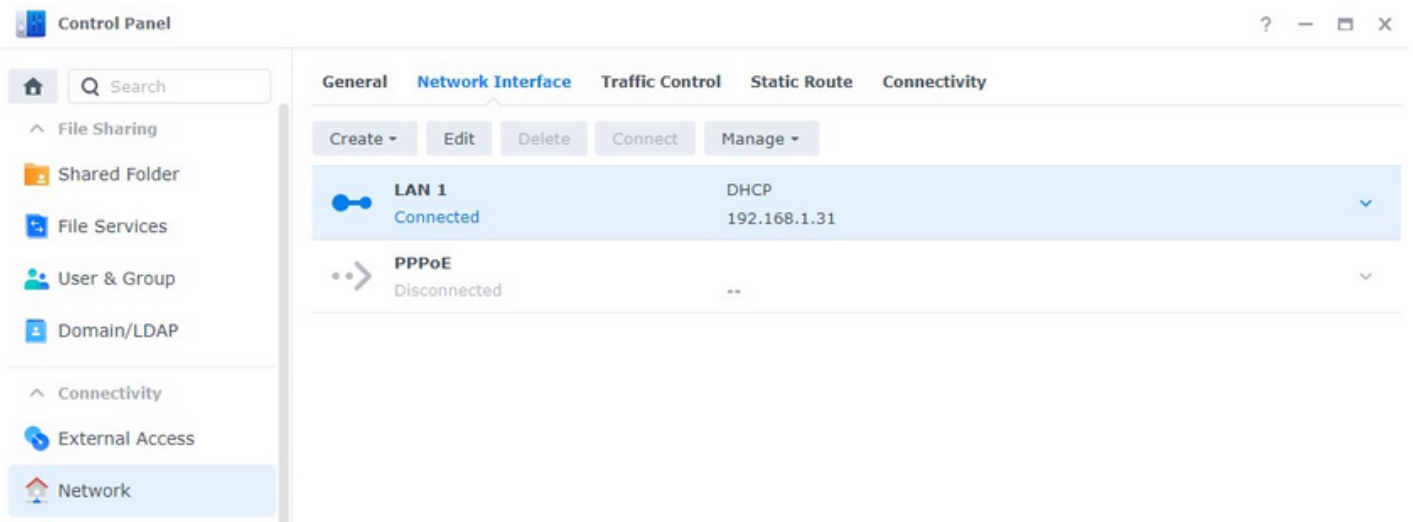
## Setup Static IP

To setup Synology NAS with static IP address so that it's always the same. It's best to make a DHCP reservation in your router's configuration.

1. Go to **Unifi > Client Devices**
2. Select Synology NAS and under setup **select** Static IP. This will automatically assign one, but you can change it if you want, just make sure you restart computer after

Its also a good idea to set a static IP address from DSM, although not needed if router DHCP is set correctly

1. Go to the **Control Panel** and select Network Interface. Select **Edit** on the LAN device

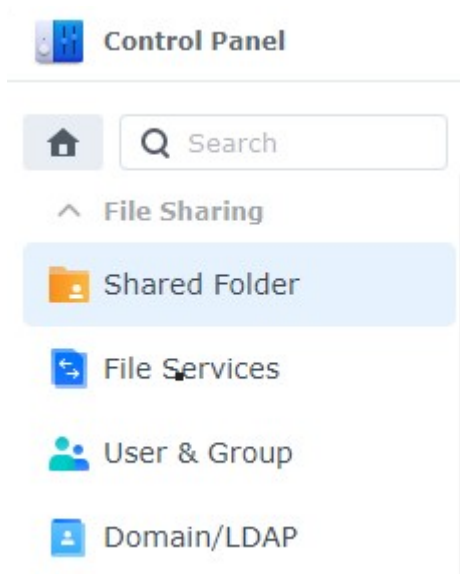


2. Select **Use manual configuration** and enter the **IP Address** you'd like to use
  1. The subnet mask, gateway, and DNS server can all stay as default (since they were pulled from DHCP). Select **OK**
  2. Your network settings will apply and your DSM session will refresh with your new IP address.

# Shared Folder Setup

File Share is one of the big features in Synology giving users power to create content and share between each other. Also, Shared Folders can be user or role based, and there is a good amount of security involved when setting up folders.

1. Open **Control Panel** and select **Shared Folder**.



2. Select **Create**. A new dialogue box will appear where you'll need to change a few settings:
  1. **Name: Name of the Shared Folder.**
  2. **Description: Description you'd like to use.**
  3. **Location: Volume you'd like to use.**
  4. The next three options are personal preference based on if you'd like the folders visible to others and if you'd like a recycle bin enabled (so files aren't deleted permanently).

### Set up basic information

Name \*:

Backups

Description:

Location:

Volume 1: Btrfs

- Hide this shared folder in "My Network Places"
- Hide sub-folders and files from users without permissions [i](#)
- Enable Recycle Bin
  - Restrict access to administrators only

Note: [How to set up a Recycle Bin emptying schedule](#)

\* This field is required.

3. Click **Next**
4. The next screen will ask if you'd like to [encrypt the shared folder](#). If you would, select the checkbox and enter an encryption key.

**A few things to note with encrypted files:** Encrypted files work by mounting/unmounting them with the encryption key (password) in DSM. When you mount the folder, it functions the same way as other shared folders do. It simply gives you the option to unmount the shared folder when you're done adding files.

When the drive is unmounted, **no one can access the files** until you mount the folder again. **If you lose the encryption key, your files will be lost forever.** Keep it somewhere safe!

4. Enable data checksum (if applicable) and file compression/folder quota if you'd like. Select **Next**.
5. Select **Next** and **Confirm Settings** if everything looks as desired

## Configure advanced settings

Enable data checksum for advanced data integrity [i](#)

File self-healing and data scrubbing are available to ensure data integrity.

Enable file compression [i](#)

Enable shared folder quota

0 GB ▾

**Note:** To ensure service quality, we recommend not enabling data checksum when the shared folder will be used for the following services:

- Hosting databases or virtual machines
- Storing video recordings of Surveillance Station

- After the folder is created, you will be brought to the folder's permissions. Change the permissions to match what you'd like. Your folder is now created!
- Change local users to Groups to so it's group based rather than user based, for better control.

## Configure user permissions

Local users ▾

Q Search

Name	Preview	Group Per...	No Access	Read/Write	Read Only	Custom
admin	Read/Write	Read/Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
frank	Read/Write	Read/Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
guest	No Access	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

# Data Protection and Monitoring Setup

Now that a storage pool, volume, and shared folder are created, we need to change a few settings to protect and monitor our data.

## Set up a Data Scrubbing Schedule on a Synology NAS

Data scrubbing inspects your volumes and modifies detected inconsistencies. In simple terms, this protects your NAS against bit-rot. There isn't a specific schedule that's mandatory, but it's a good idea to run it at a minimum, bi-annually.

1. Open **Storage Manager**, select **Storage Pool**, then **Schedule Data Scrubbing**. Then select **Set Schedule**



The screenshot shows the Synology Storage Manager interface. At the top, there are navigation tabs: 'Create', 'Schedule Data Scrubbing', 'Hot Spare', 'SSD Cache Advisor', and 'Global Settings'. Below the tabs, there are two main sections. The first section is for 'Storage Pool 1 - SHR', which is 21.8 TB and has a 'Healthy' status indicated by a green checkmark. The second section is for 'Volume 1 - SP1-SHR', which is 15.8 TB / 20.9 TB (75% full) and also has a 'Healthy' status indicated by a green checkmark.

1. Select **Enable Data Scrubbing schedule**, then select the **Storage Pool**, select a **Frequency** and **Save**

Performing data scrubbing periodically ensures data consistency and lowers the risk of data loss in the event of a drive failure.

Enable data scrubbing schedule

Data scrubbing can only run on one storage pool at a time. Please select and prioritize the storage pools that you want to perform data scrubbing.

<input checked="" type="checkbox"/>	Name	Status
<input checked="" type="checkbox"/>	Storage Pool 1	Scheduled on 08/08/2021

Frequency

Repeat every three months

Run data scrubbing only during specific periods

Running data scrubbing may take some time and occupy computing resources. You can set data scrubbing to run only during specific periods and thereby prevent this process from affecting the system performance when other important services or tasks are in progress.

Set Time Grid

Next run time: **08/08/2021 12:00 am**

Cancel

Save

## Set up Snapshots on a Synology

The easiest way to think of snapshots is that they “freeze” your files in time and allow you to recover those files later if necessary.

Every time a snapshot is created, a “restore” point is created, which allows you to recover files/folders from a point in time. The best part about this is that the snapshots themselves take up very little space and give you tons of flexibility!

1. Open the **Package Center**, search for **Snapshot** and install the **Snapshot Replication** package.

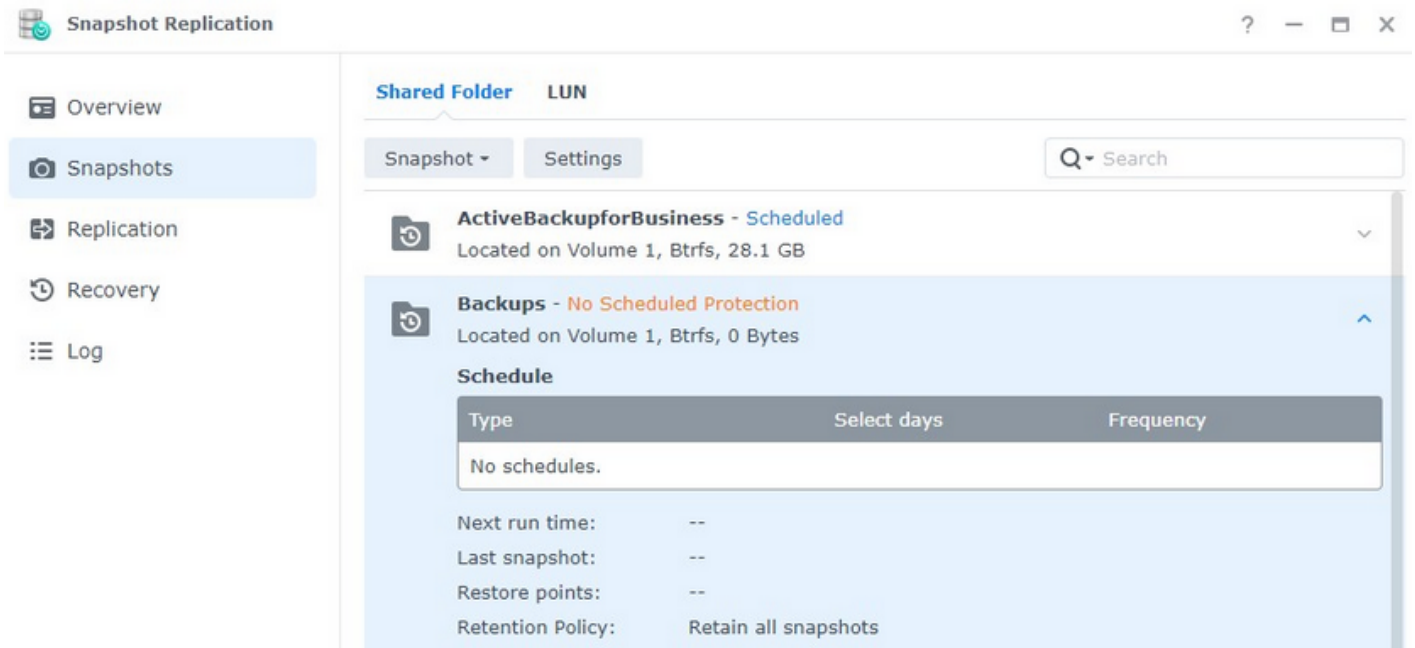


**Snapshot  
Replication**

06/01/2021

Open

- When the install finishes, launch the **Snapshot Replication** application. Select **Snapshots** and select **settings** on the folder you'd like to schedule protection for.



- Enable the snapshot schedule.** At this point, there are two final settings you'll need to check:

- **Retention:** Select how many snapshots you'd like to retain. Depending on the file type (and size), you'll most likely have different retention policies for different folders.
- **Snapshot Visibility:** If you would like snapshots to be visible, select the checkbox under the **Advanced** section.

## Settings

**Schedule**   **Retention**   **Advanced**

Enable snapshot schedule

Select days:

First run time:  :

Frequency:

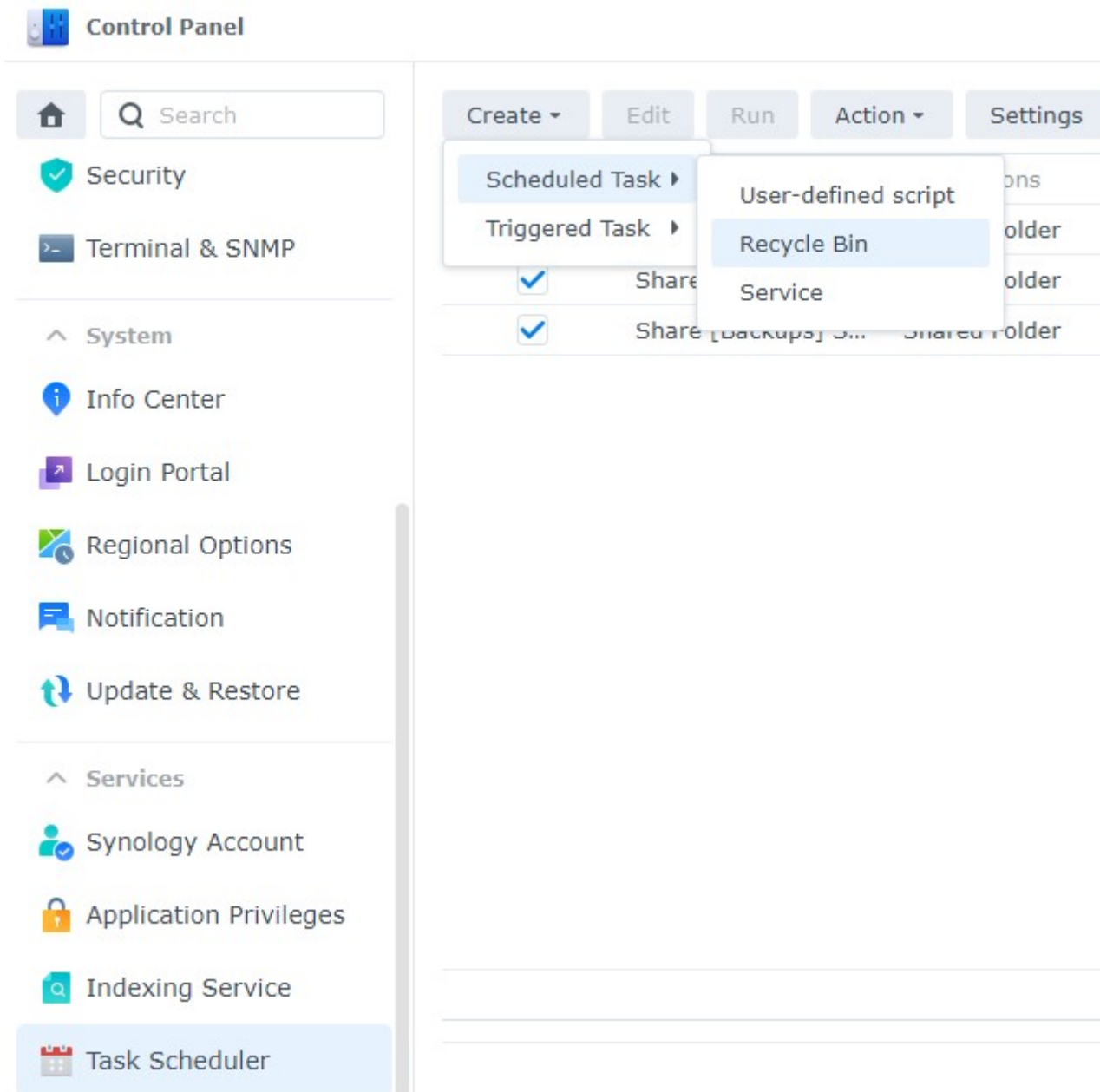
Last run time:

- After the snapshots have been configured, your system will start to create snapshots regularly. When the retention policy hits its maximum, old snapshots will be deleted.

# Set up a Recycle Bin Task on a Synology NAS

By default, the recycle bin will retain files until you empty it. However, there's an easy way to set up a schedule so that your NAS automatically deletes these old files after a certain period of time.

1. Open the **Control Panel** and select **Task Scheduler**
2. Select **Create**, then **Scheduled Task**, then **Recycle Bin**



- General: Enter a Task Name.

## Create task

**General** Schedule Task Settings

### General Settings

Task:

User:

Enabled

- **Schedule:** Specify when you'd like the task to run.

## Create task

General **Schedule** Task Settings

### Date

Run on the following days

Run on the following date

### Time

First run time:  :

Frequency:

Last run time:

- **TaskSettings:** Specify if you'd like all recycle bins to empty or only specific ones.
  - **Retention Policy:** This is an important step! I retain all deleted files for 14 days, but this is completely personal preference. This setting specifies when files are deleted. There are also advanced settings you can check.

## Create task

General Schedule **Task Settings**

### Empty Recycle Bin

- Empty all Recycle Bins
- Empty the Recycle Bin of the below shared folder

### Retention Policy

- Delete all files
- Number of days to retain deleted files:
- Limit Recycle Bin size (MB):

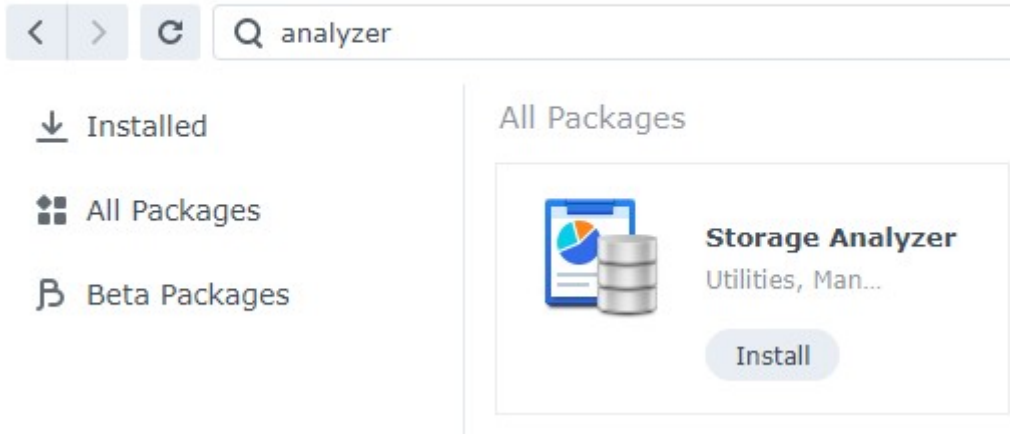
Advanced Settings

This is very important because when you're using a NAS, you generally have data rotating like snapshots and backup files.

## Set up the Storage Analyzer on a Synology NAS

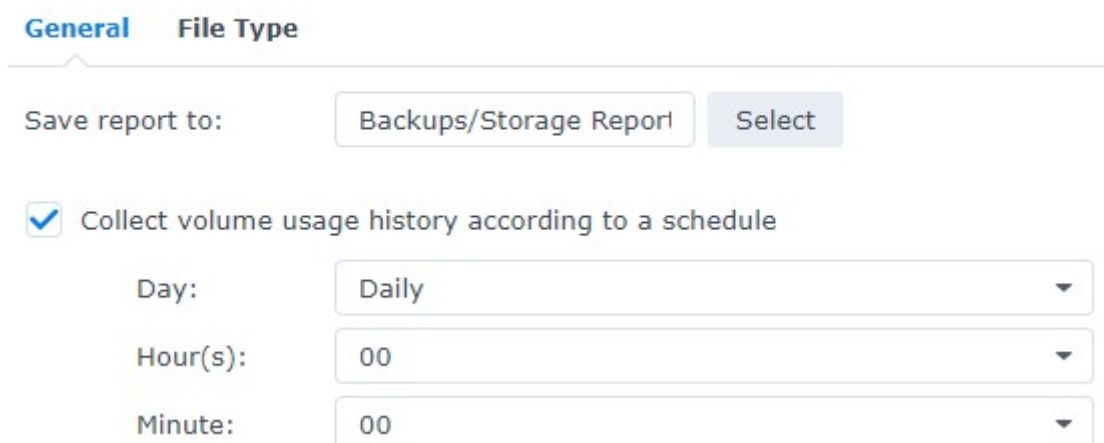
The storage analyzer allows you to see what files/folders are taking up space on your NAS and if any duplicates exist. It's a powerful tool that periodically comes in handy.

1. Open the **Package Center**, search for Analyzer, and install the **Storage Analyzer** package.

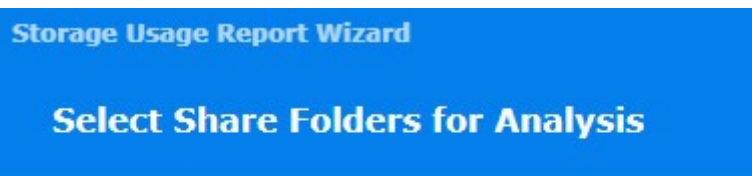


- When it's done installing, open the package. You will be asked to specify a location to save your reports. Select **Yes**. Specify a location to save your reports and the frequency you'd like reports generated.

### Settings



- A wizard will then start to assist you in the creation of the scheduled task. Give your report a name, set a schedule, and then specify the total number of reports you'd like to keep.
- Keep all Report Types selected (unless you don't want specific ones generated) and click
- Determine if you'd like to analyze all current and future shared folders, then select



- Analyze all the existing and future shared folders
- Only analyze specific shared folders

6. Select the settings you'd like to use to find duplicate files.

**Storage Usage Report Wizard**

## Advanced Settings

---

### Potential Duplicate Files

Find duplicate files when generating reports i

Ignore file names

Ignore modified time

Max number of duplicate files:  i

---

### File List

List files owned by these users by file group:

7. Select **Generate reports now**, then **Done**, and the process is officially set up!

## Summary

Item	Value
Enable Schedule	Yes
Generate reports accordin...	Sunday Monday Tuesday Wednesday Thursday F...
Generate reports now	No
Report Task	Storage Analyzer
Email	
Report Rotation	100
Report Type	Quota Usage,Files by Owner,Volume Usage,Shar...
Select shared folders	Include all shared folders
Find confirmed duplicate fi...	Yes
Ignore modified time	Yes

Generate reports now

Back

Done

This might not seem important on the surface, but understanding how your storage is being used is integral!

# Setting up Updates

Installing Synology's newest updates should be at the top of your list. Not only do you get new features, but more importantly, you get the newest security enhancements.

1. Open **Control Panel** and select **Update & Restore**
2. Select **Update Settings** and **Automatically install** the **new update**. Pick a date and time (preferably during the middle of the night) that updates will install

The screenshot shows the Synology Control Panel interface. On the left is a navigation sidebar with categories: Home, Security, Terminal & SNMP, System, Info Center, Login Portal, Regional Options, Notification, Update & Restore (highlighted), Services, Synology Account, and Application Privileges. The main content area is titled 'Control Panel' and has three tabs: 'DSM Update' (selected), 'Configuration Backup', and 'System Reset'. Under the 'DSM Update' tab, there is a text block stating 'Synology releases DSM updates from time to time. Install the updated version to improve system stability.' Below this, the system status is shown: 'Model name: VirtualDSM', 'Current DSM version: DSM 7.0-41222 (Release notes)', and 'Status: Your DSM version is up-to-date.' Two buttons are present: 'Manual DSM Update' and 'Update Settings'. The 'Update Settings' modal is open, showing the option 'Automatically install the new update' selected. The 'Check schedule' is set to 'Saturday' at '03:00'.

Control Panel

Home Search

Security

Terminal & SNMP

System

Info Center

Login Portal

Regional Options

Notification

Update & Restore

Services

Synology Account

Application Privileges

DSM Update Configuration Backup System Reset

Synology releases DSM updates from time to time. Install the updated version to improve system stability.

Model name: VirtualDSM

Current DSM version: DSM 7.0-41222 ([Release notes](#))

Status: Your DSM version is up-to-date.

Manual DSM Update Update Settings

Update Settings

Select how to proceed when there is new DSM update available

Notify me and let me decide whether to install the new update

Automatically install the new update

Check schedule: Saturday

03 : 00

# Synology Security Guide & Best Practices

Steps for securing Synology NAS system

# User Security & Access Control

The majority of NAS security needs to be done preventatively to easily recover from potential issues that might arise in the future.

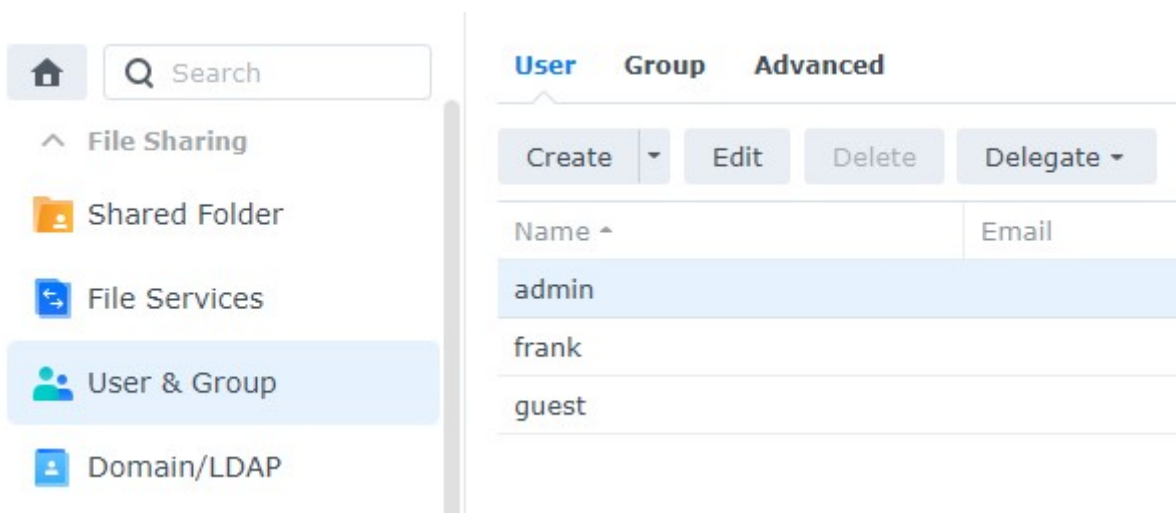
It's important to note that cybersecurity is always evolving and staying up to date with best practices is important. These are things I normally change, but depending on your needs, you can potentially secure your NAS even further.

Making sure that every user on NAS system is properly created, assigned, and given least amount of privilege, can help with reducing any type of cyberattack.

## Disable Admin Account

First we must create a new user and ensure that they have admin permissions before disabling the admin user. Disabling Guest account is good practice as well, but it's personal preference, if group based access is properly managed.

1. Select **Control Panel**, then select **User & Group** and **Edit** the admin user



1. Select **Disable this account**, then select **Save**. This will ensure that the admin account is disabled

**Info** User Groups Permissions Quota Speed Limit

Name \*:

Description:

Email:

Password: Last changed: 09/15/2020

[Change Password](#)

Disallow the user to change account password

Password is always valid if the password expiration is enabled

Disable this account

Immediately

After:

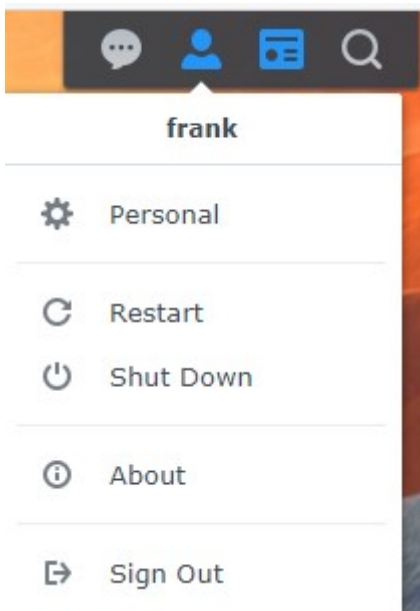
\* This field is required.

[Cancel](#)

[Save](#)

## Enable Two Factor Authentication

1. Select the **Person** icon in the top right and select **Personal**



2. Select **Enable 2-step Authentication**. The email service will need to be enabled for this

## Sign-in Method

Use a verification code (OTP) as the second sign-in step to strengthen your account security.

### 2-Factor Authentication

Add an extra layer of security by implementing a second authentication step.



3. Select **2-step Authentication**, then **Verification code (OTP)**.
4. Select **Next** to protect your DSM account with **2-factor Authentication**

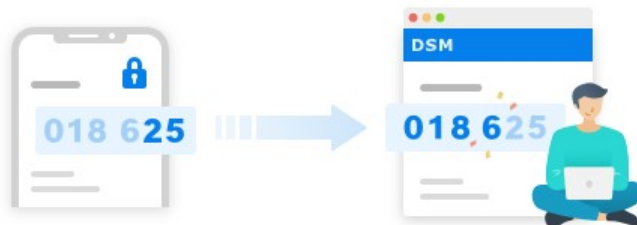
#### Set up 2-factor authentication



### Protect your DSM account with 2-factor authentication

2-factor authentication requires you to enter your password along with a verification code (OTP) when signing in to VirtualDSM. You can receive an OTP code even if your mobile device is offline.

**Note:** Enabling 2-factor authentication applies to Synology package logins. [Learn more](#)



Back

Next

The next section will suggest that you install Synology's Secure SignIn. **This is not required.** This is simply Synology's TOTP application – you are free to use whatever TOTP application you'd like.

5. Scan the **QR code**, enter the **code**, then select **Next**.
6. Set up the **Email service provider**, then select **Next**
7. Two-factor authentication is now set up

If you'd like to force all users to set up two-factor authentication

1. Go to **Control Panel**
2. Under **Security** select **Account** and under 2-Factor Authentication select All users or Specific users or groups. It's good idea to have any users that can remotely access NAS to have MFA setup, both TOTP and Push Notification with **Synology Secure SignIn**

The screenshot shows the Windows Control Panel interface. On the left is a navigation pane with categories like File Sharing, User & Group, and Security. The main area is titled 'Account' and shows 'Secure SignIn Service' with a status of 'Connection failed'. Below that, the '2-Factor Authentication' section is expanded, showing a checkbox for 'Enforce 2-factor authentication for the following users' with radio button options for 'Administrator group users', 'All users', and 'Specific users or groups'. A 'Settings' button is visible below these options. A note at the bottom of the section says 'Note: You can set up 2-factor authentication for your account in [Personal](#).' The 'Account Protection' section is partially visible at the bottom.

## Enable Auto Block

Auto block will automatically block IP addresses that have failed a certain number of logins during a certain period of time.

1. Open **Control Panel** and select **Security**
2. Select **Account**. Ensure **Enable auto block** is selected. Set the **Login Attempts** and **Within parameters** to be what you'd like, then apply. This will ensure that IP addresses are automatically blocked after a certain number of failed login attempts

The screenshot shows the Windows Control Panel interface. On the left, the 'Security' category is selected. The main content area is titled 'Protection' and contains the 'Auto Block' settings. The 'Enable auto block' checkbox is checked. Below it, there are input fields for 'Login attempts' (set to 5) and 'Within (minutes)' (set to 10). The 'Enable block expiration' checkbox is unchecked. Below that, there is an input field for 'Unblock after (days)' (set to 0).

Control Panel

Security Account Firewall Protection Certificate Advanced

Auto Block

Enable this option to block IP addresses with too many failed login attempts. For support, see DSM Help.

Enable auto block

An IP address will be blocked if it reaches the number of failed login attempts with

Login attempts:

Within (minutes):

Enable block expiration


When block expiration is enabled, blocked IP addresses will be unblocked after the

Unblock after (days):

## Disable SSH

There are multiple reasons why you might want to use SSH, but if you're not **actively** using it, you should disable it. Even if you enable two-factor authentication above, SSH does **not** use it. For this reason, if your network is compromised, an attacker can try and brute force your password through SSH.

1. Open **Control Panel**, then select **Terminal & SNMP**.
2. Ensure that **Enable SSH** service is not checked off.

- 
- File Sharing
  - Shared Folder
  - File Services
  - User & Group
  - Domain/LDAP
- Connectivity
  - External Access
  - Network
  - Security
  - Terminal & SNMP**

**Terminal**   **SNMP**

Use Terminal service to login and manage your system. SSH/Tel administrators group. Please refer to [Terminal](#) for more details.

Enable Telnet service

Enable SSH service

Port:

[Advanced Settings](#)

**Note:** It is recommended to set a strong password for the login

# Remote Access Setup

# Synology Firewall Setup