Synology NAS User's Guide
for DSM 7.2

Table of Contents

Chapter 1: Introduction

Synology DiskStation Manager (DSM) is an intuitive web-based operating system for every Synology NAS, designed to help you manage your digital assets across all network locations. With DSM 7.2, your network-attached storage device can now do more than ever before, in addition to acting as a file-sharing center on your local area network.

DSM's main features and functionalities include:

- **File-sharing and syncing**: Instantly access, share, and sync your digital assets conveniently and securely across multiple devices whenever and wherever you want.

- **Backup and restoration**: Through our license-free backup solutions, back up and protect your digital assets on your computers, virtual machines, cloud services, and NAS to avoid service downtime that can jeopardize your personal or business goals.

- **Team collaboration**: In the privacy of your own cloud, create a motivated team culture while satisfying all collaboration needs with Synology Office, Calendar, and Chat.

- **Multimedia streaming**: Through an intuitive web-based interface, access and compile your multimedia content into a multimedia library that can be used by multimedia applications or packages at your convenience.

- **Video surveillance**: With our complete surveillance solution, you get intelligent monitoring and video management tools to safeguard your valuable assets in your business, home, and other environments.

- **Virtualization storage**: Streamlined provisioning and management of virtual machines allows you to access storage space over a storage network as if the space were on one local disk, with full certification for VMware® vSphere™, Microsoft® Hyper-V®, Citrix® XenServer™, and OpenStack virtualization environments.

Chapter 2: Quick Start Guide

This chapter provides an overview of the initial configurations of **Synology DiskStation Manager (DSM)**. To help you get started with your Synology NAS, perform the following instructions about drive setup, OS installation, storage initialization, and several built-in services of DSM management.

Install drives

As a data storage server, Synology NAS needs at least one 3.5" or 2.5" drive to ensure functionality. For detailed information on drive installation, refer to your model's Product Manual.

Back up drives before installation

If your drive comes from an old Synology NAS, follow the instructions in the HDD migration article to perform drive migration. The migration procedures mentioned in the article will help you keep most of your data. However, we strongly recommend that you back up data on the original Synology NAS, from which drives are moved, to avoid accidental data loss.

If your drive does not come from a Synology NAS that contains data, you need to back up data before the installation because the system will format the drives and erase all of the existing data during the installation.

About RAID types

After drive installation, you should set up a RAID array to add extra security and redundancy to your storage space. This section provides a brief introduction to RAID technology and the difference between each RAID type.

RAID (Redundant Array of Independent Disks) is a data storage technology that allows multiple independent drives to be combined into a RAID array for data redundancy and performance improvement. In a RAID array, the same data will be stored in different places across multiple drives to reduce the risk of data loss caused by a drive failure. Moreover, the RAID setup can boost the read-write performance because data will be striped across drives under certain RAID configurations.

Different RAID configurations provide different levels of redundancy and performance. The following is an overview of the RAID types supported by Synology NAS:

- **SHR**: Synology Hybrid RAID (SHR) is an automatic RAID management system designed by Synology. SHR provides fault tolerance when there are more than two drives. It is recommended for novice users because it will automatically deploy drives for the best interest of your storage space.

- **Basic**: Basic configuration is composed of only one independent drive, so it does not provide any fault tolerance or performance boost.

- **JBOD**: JBOD (Just a Bunch of Disks) configuration combines all drives into a single drive stack. Each JBOD drive is regarded as a separate and individual drive volume, so it allows easier control management of data storage. JBOD configuration does not provide any fault tolerance or performance boost.

- **RAID 0**: In contrast to JBOD, RAID 0 combines two or more drives and treats them as a single unit. In RAID 0, data are divided into blocks and split across multiple drives; therefore, the read-write speed increases with more drives added.

- **RAID 1**: RAID 1 requires at least two drives. In RAID 1, data are mirrored on all drives. Since the same data exist on all the drives in the array, the volume of the smallest member drive determines the total capacity of the array. This is the safest option to protect important data, but the write performance and capacity are relatively limited.

- **RAID 5**: RAID 5 requires at least three drives, and one of the drives is used for fault tolerance. RAID 5 stripes data blocks across multiple drives and distributes redundancy information, called parity, across all of the drives in the array. Upon failure of a single drive, the lost data can be reconstructed with the parity existing on the rest of the drives.

- **RAID 6**: RAID 6 requires at least four drives. RAID 6 features double distributed parity, so it has better data redundancy than RAID 5. However, because RAID 6 needs to write two parity blocks on all member drives, the write performance is slower than RAID 5.

- **RAID 10**: RAID 10 requires at least four drives. The drives have to be even because drives are combined into groups of two in which data is mirrored and striped. RAID 10 features the performance of RAID 0 and the data protection of RAID 1.

- **RAID F1**: RAID F1 requires at least three drives. Like RAID 5, RAID F1 implements data block striping and distributes parity data across all member drives. The only difference is that one of the drives will bear more parity information, so it will age faster, which prevents all the drives from coming to the end of their endurance at the same time. RAID F1 is recommended for an all-flash array.

> **Notes:**
> - RAID F1 and SHR are only available on specific models. Refer to the specifications of each model for detailed information.

Get started with DSM

This section guides you through how to perform the first-time installation of DSM via a web browser or Synology's mobile application.

Install DSM with Web Assistant

Your Synology NAS comes with a built-in tool, **Web Assistant**, which helps you download the latest version of DSM from the Internet and install it on your Synology NAS. To use Web Assistant, use the following steps:

1. Power on your Synology NAS.

2. Open a web browser on a computer within the same network where your Synology NAS is located, and go to "find.synology.com". The status of your NAS should be **Not installed**.

3. Select your Synology NAS and click **Connect** on Web Assistant.

4. Click **Install** to start the installation process and follow the on-screen instructions.
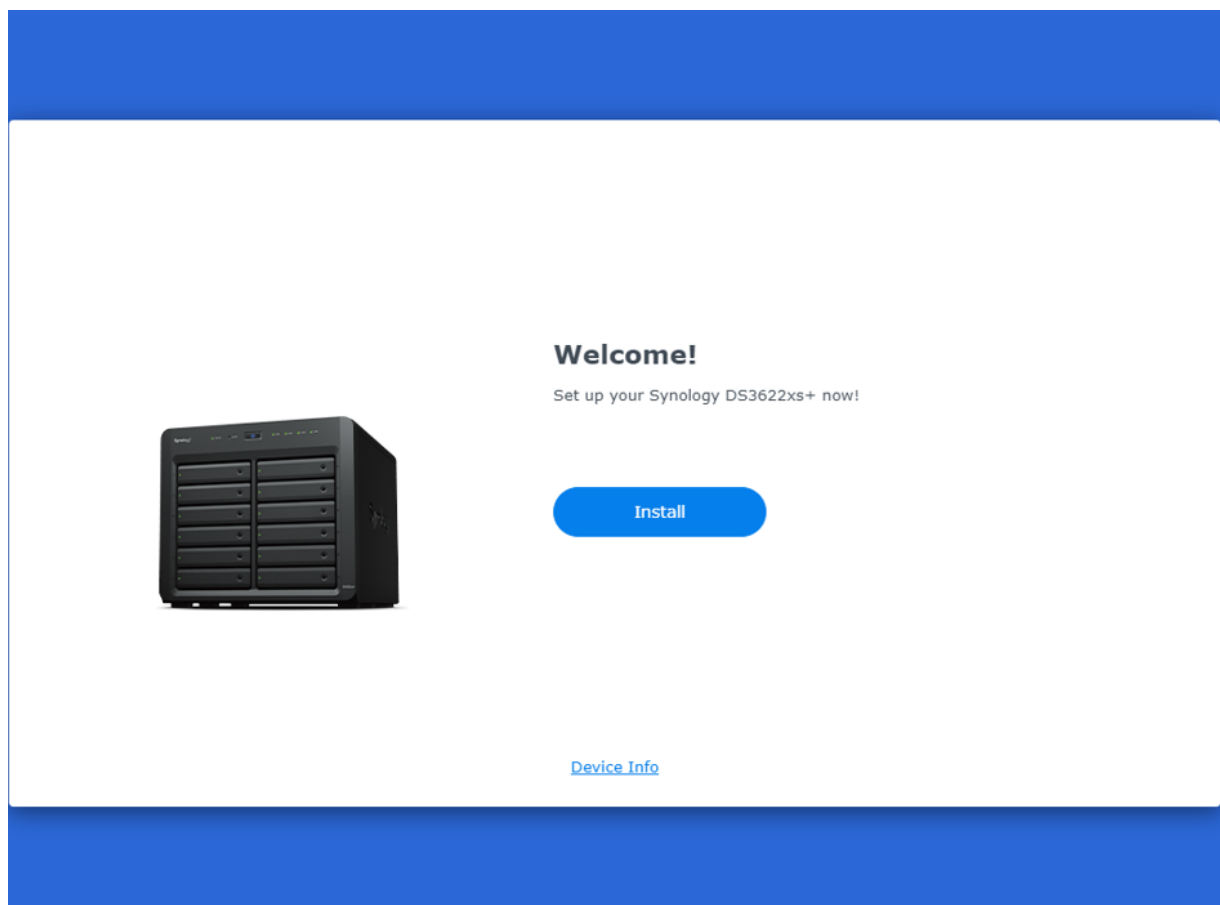
> **Notes:**
> - Both your Synology NAS and computer must be on the same local network.
> - We suggest using Chrome or Firefox as the browser for DSM installation.
> - For more information on the setup of Synology NAS and DSM, refer to your model's [Product Manual](#).

Install DSM with DS finder

You can also install **DS finder** (App Store/Google Play) on your mobile device to install DSM as demonstrated below:

1. Power on your Synology NAS.

2. Connect your mobile device to the local network where your Synology NAS is located, and launch DS finder.

3. Tap **SET UP NEW NAS** to start the setup process.

4. Follow the on-screen instructions to establish the connection between your mobile device and Synology NAS, and tap **SEARCH**. DS finder will search for your Synology NAS. The status of your NAS should be **Not installed**.

5. Select your Synology NAS and tap **INSTALL** to start the installation process and follow the on-screen instructions.

> **Notes:**
>
> - We use Android 10 for example in this chapter. The actual steps may vary across OS versions and devices.
>
> - Both your Synology NAS and mobile device must be on the same local network.
>
> - DS finder can only run on Android and iOS devices.
>
> - DS finder supports installing DSM on most Synology NAS models (except rack-mount models and desktop models of FS/XS series).

Sign up for a Synology Account

As the owner of a Synology NAS, you should have a **Synology Account** to access Synology online services and manage your customer information. Different from DSM user accounts (which can be used to sign in to DSM), a Synology Account allows you to manage your billing information, registered Synology products, requests for technical support, and Synology online services (e.g., QuickConnect, DDNS, and Synology C2). Learn more about the differences between Synology Accounts and DSM user accounts.

Sign up for a Synology Account and bind your Synology NAS during DSM installation or by following the steps below:

1. Go to the Synology Account registration page.

2. Enter your email address and click **Next**, or sign in using your Google account or your Apple ID. Then, follow the on-screen instructions to create a Synology Account.
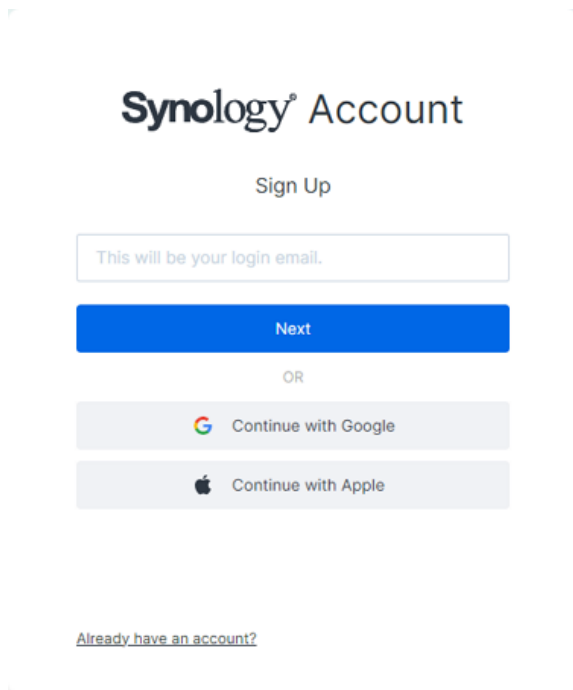
3. Go to the mailbox of the email you entered and click the email titled **Synology Account - sign up** (sent from "noreply@synologynotification.com") to get your verification code.

4. Enter the verification code and click **Next**.

5. Check the terms and privacy policy. Click **Submit**.

6. Go to **Control Panel** > **Synology Account**, and click **Sign in or sign up for a Synology Account**.
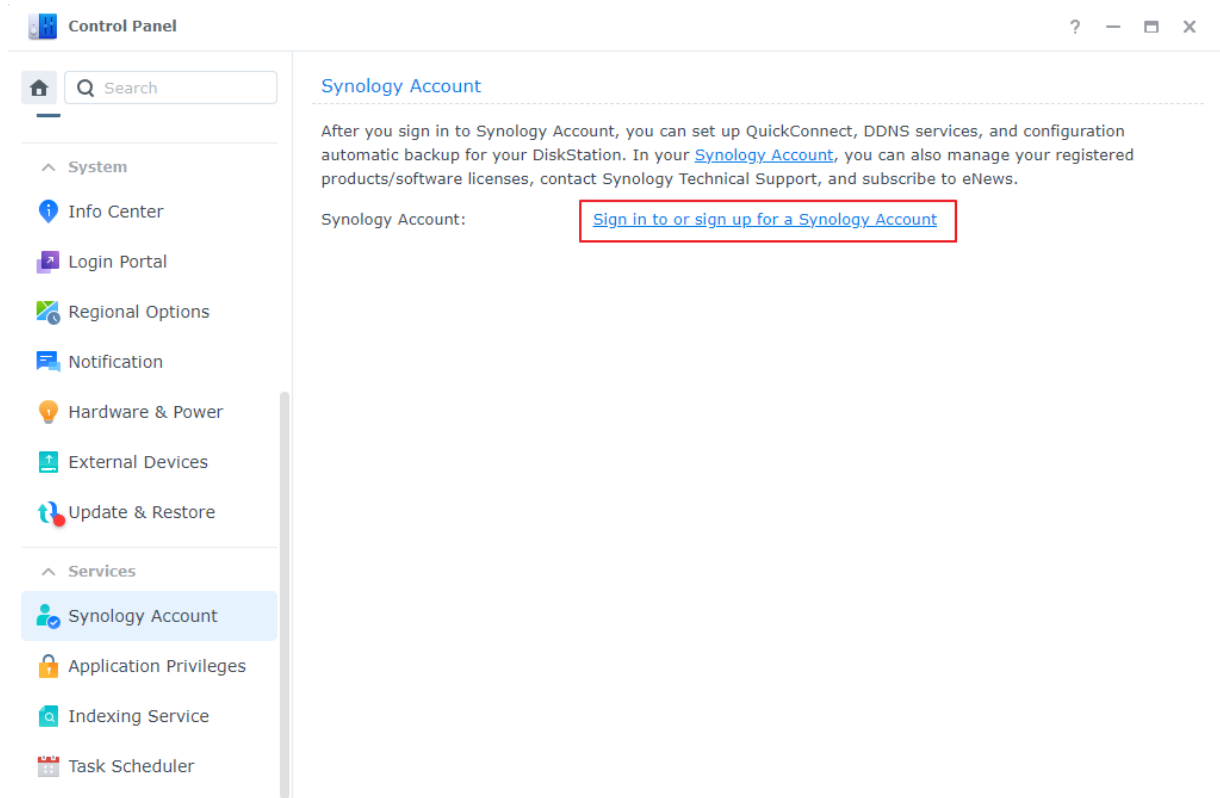
7. In the pop-up window, enter the credentials of your Synology Account and click **Sign In**.

8. Now, you have successfully registered for a Synology Account and bound your NAS to it.

Navigate your DSM desktop

After installing DSM on your Synology NAS, you can sign in to DSM using the DSM user account you have just added during the first-time installation. Follow the steps below to sign in via a web browser:

1. Make sure your computer and Synology NAS are connected to the same local network.

2. Open a browser on your computer and enter one of the following in the address bar:

   - **find.synology.com**: Enter this URL only if your computer and Synology NAS are connected to the same local area network.

   - **IP address of your NAS:5000**: If the IP address of your Synology NAS is "192.168.48.14", type "192.168.48.14:5000". The IP address depends on the settings made during the initial setup.

3. Enter your username and click the rightward arrow.

4. Enter your password and click the rightward arrow again to sign in.

DSM desktop

After signing in, you can see the DSM desktop, where your application and package windows are displayed. You can also create desktop shortcuts to frequently used applications.

Taskbar

The taskbar is located at the top of the screen and includes the following items:

1. **Show Desktop**: Minimize all launched application and package windows.

2. **Main Menu**: View and open applications and add-on packages. You can also click and drag icons to create desktop shortcuts.

3. **Open applications**: Displays currently launched applications and packages. You can right-click and pin the applications or packages to the taskbar for faster access in the future.

4. **External Devices**: Appears when an external device (e.g., a USB flash drive) is attached to your Synology NAS.

5. **Upload Queue**: Appears when you start uploading files to your Synology NAS. Click the icon to see more details, such as progress and upload speed.

6. **Storage Manager**: Appears when you start running Storage Manager tasks that may affect system performance. Click on this icon to see the status or progress of the tasks.

7. **Task Manager**: Appears when you start running Control Panel tasks that may affect system performance. Click on this icon to see more details about the tasks or manage the tasks.

8. **Notifications**: Displays notifications, such as errors, status updates, and package installation notifications.

9. **Options**: Shut down, restart, sign out of your Synology NAS, or modify personal account settings.

10. **Widgets**: Show or hide widgets. Widgets are located on the right side of DSM desktop by default, displaying various types of system information, such as storage, system health, etc.

11. **Search**: Quickly find specific applications, packages, or DSM Help articles.

Main menu

You can find a list of applications and packages installed on your Synology NAS here. To create a desktop shortcut, open **Main Menu**, and click and drag an application or package to the side.

Shutdown, restart, signing out, and personal settings

Click the **Options** menu (the person icon on the upper right) to shut down, restart, or sign out of your Synology NAS.

You can also select the **Personal** option from the drop-down menu to manage your account settings, such as the password, display language, sign-in methods, and display preferences.

The following list provides an overview of the tabs under this option:

- **Account**: Edit account settings.

- **Security**: Enable advanced sign-in methods and view recent login activities of your DSM account.

- **Display Preferences**: Edit date and time formats as well as the appearance of your desktop.

- **Email Delivery**: Add your email accounts at this tab. These email accounts are used in the following scenarios:

  - Delivering files stored in File Station as attachments.

  - Sending event invitation emails via Synology Calendar.

  - Sending notification emails when sharing files with others via Synology Drive.

- **Quota**: View your quota on all volumes set by the administrator's account, as well as the amount of capacity you have used on each volume. On models with Btrfs support, you can also view the quota and capacity usage of each shared folder.

- **Others**: Customize other personal account options.

Check regional options

In **Control Panel** > **Regional Options**, you can configure the following regional settings:

- **Time**: Set up system time settings of your DSM. You can check the current time, manually set the server's date and time, or have them set automatically using a network time server.

- **Language**: Set the language for display, notification, and code pages.

- **NTP Service**: Set your Synology NAS as a network time server to synchronize time with other devices over networks. Note that NTP service is required for Surveillance Station and high-availability clusters. If you have installed and launched Surveillance Station or Synology High Availability on your Synology NAS, the NTP service cannot be disabled.

Specify your QuickConnect ID

QuickConnect allows client applications to connect to your Synology NAS via the Internet without setting up port forwarding rules. It can work with Synology-developed packages, such as File Station, Synology Photos, Synology Drive, Surveillance Station, and mobile applications. You can either specify your QuickConnect ID during DSM installation, or activate the service by using the following steps:

1. Go to **Control Panel** > **External Access** > **QuickConnect**.

2. Tick the **Enable QuickConnect** checkbox.
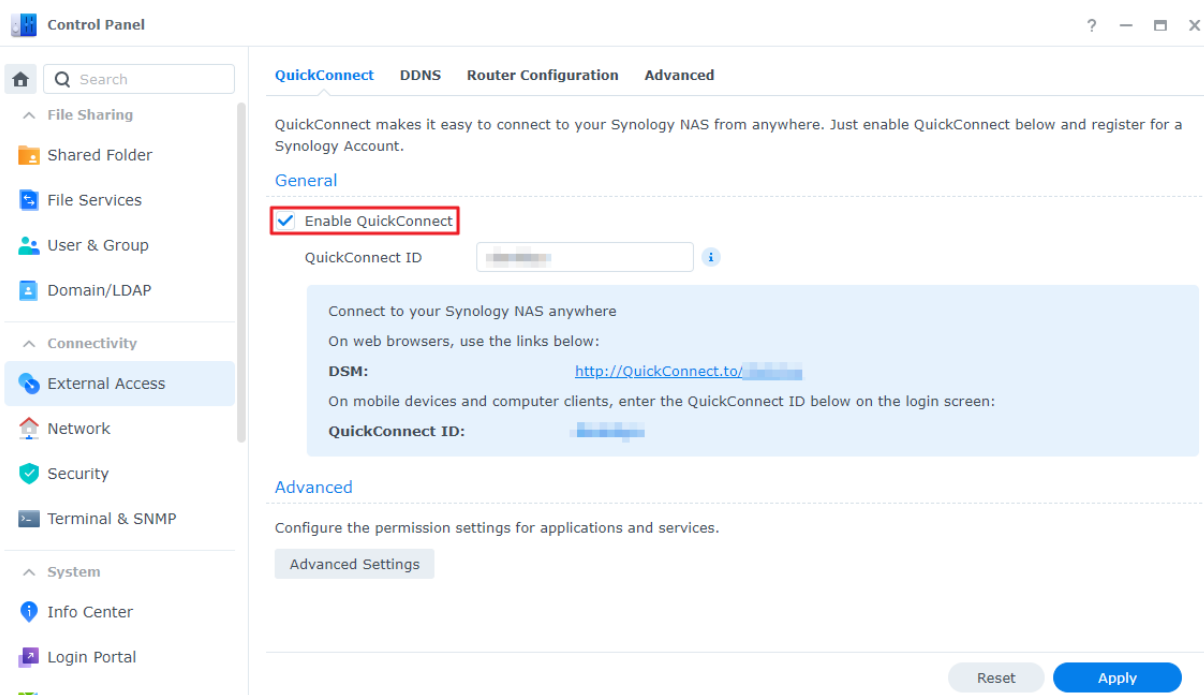
3. If you have not signed in to your Synology Account, a login window will pop up. Enter your existing Synology Account information or create a new account in the window.

4. Specify a new QuickConnect ID.

5. Click **Apply**.

Learn more about QuickConnect.

> **Notes:**
> - A customized QuickConnect ID can only include English letters, numbers, and dashes (-). It must start with a letter, and cannot end with a dash.

Configure storage space

This section guides you through the steps of storage pool creation using the built-in package, **Storage Manager**.

About storage pools and volumes

When launching Storage Manager for the first time, the **Storage Creation Wizard** will help you create and configure storage pools and volumes.

- A **storage pool** is a single storage unit consisting of multiple drives.

13

- A **volume** is a storage space created on a storage pool. You have to create at least one volume to store data on your Synology NAS.

Create storage pools and volumes

1. Launch **Storage Manager** from the DSM Main Menu. The **Storage Creation Wizard** will pop up to guide you through the steps below.

2. Choose a RAID type to protect your storage. Some RAID types are available on certain models according to the number of drive bays. To find out which RAID type is right for your storage pool, you can refer to the About RAID types section or the Choose a RAID Type article.

3. Deploy drives to make up the storage pool.

4. Allocate the volume capacity.

5. Select a file system. We recommend **Btrfs** for its data protection features. Learn more about the differences between file systems.

6. Confirm the settings. The system will automatically run the storage creation and optimization process in the background.

Create a shared folder and start sharing files

Through the setup of a shared folder, you can turn your Synology NAS into a convenient and secure file-sharing center. This section explains the role of shared folders on DSM and gives you instructions on file management using **File Station** and **DS file**.

About shared folders

A **shared folder** is a home directory where you can store and manage files and subfolders. You must have at least one shared folder to store files on your Synology NAS. Data stored in shared folders can be kept private or shared with specific users or groups based on custom permission settings.

Some packages or services require a dedicated shared folder to ensure functionality. This table shows the shared folders that are automatically created when certain applications, services, or packages are installed or enabled.

Set up and remove a shared folder

If you are a user belonging to the **administrators** group, including users delegated with administrative roles, you can create shared folders and grant users access permissions to the folders. You can also remove any shared folders as long as they were created by you.

- To set up a shared folder, go to **Control Panel** > **Shared Folder**. Click **Create** and follow **Shared Folder Creation Wizard** to configure shared folder settings. Learn more about shared

[folders](#).

- To remove a shared folder, go to **Control Panel** > **Shared Folder**. Select the shared folder and click **Delete**.

> **Notes:**
>
> - Removing a shared folder will also remove all of its data and snapshots. If you need the data, make sure to back them up first before the removal.

Manage files via File Station

File Station is a built-in file management tool in DSM. File Station provides a centralized interface where you can access and manage files and folders via web browsers and grant other users access to files based on the permissions you set. This section guides you through the file management process in File Station.

Customize File Station settings

Launch **File Station** and click **Settings**. You can perform the following actions here:

- Configure general settings.

- Mount shared folders, virtual drives, servers, and cloud services.

- Allow specific users to share file links or make a request for file access.

- Set speed limits for file transfers via File Station.

- Enable converting HTML files to plain text for security purposes.

Search for files or folders

File Station provides regular search and advanced search to meet different requirements:

- To perform a regular search, click the folder where the desired files or folders are located. Type a keyword in the **Search** field.

- To perform an advanced search, go to the folder where the desired files or folders are located. Click the **magnifying glass** icon next to the **Search** field to expand the advanced search

menu, where you can set multiple search conditions for a refined search result.
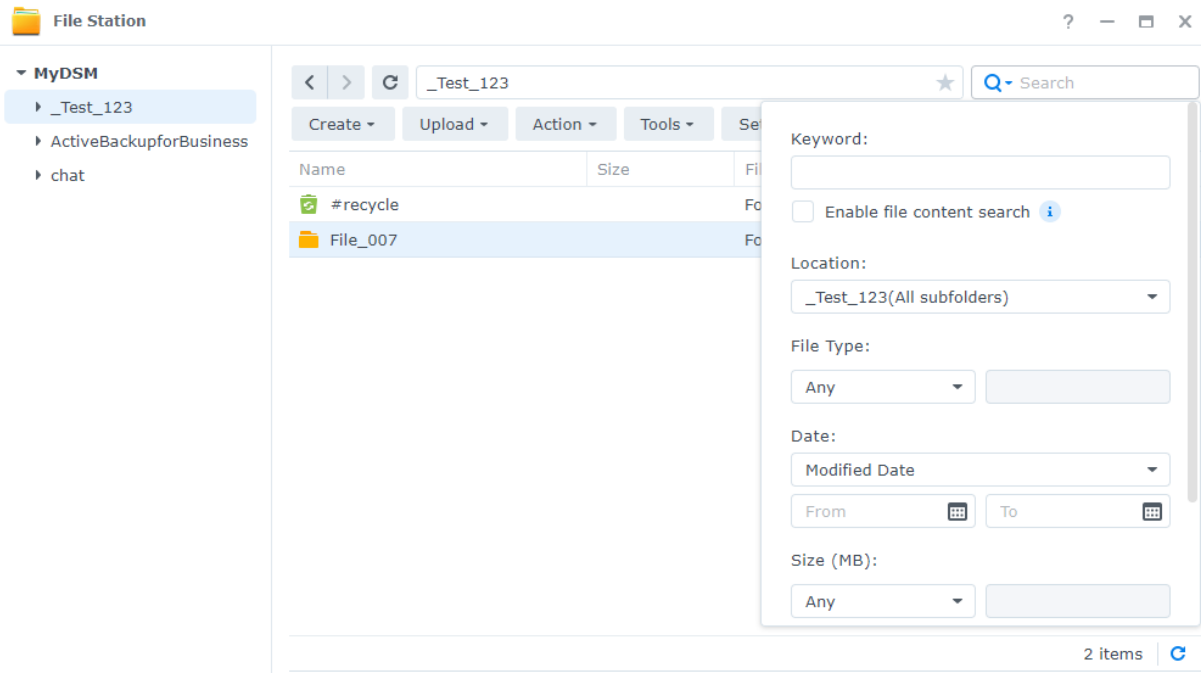
> **Notes:**
> - For faster search results, we recommend you to index shared folder contents.

Manage files and folders

Select a file or folder and click **Action**, or simply right-click it to perform the following actions:

- To send files as email attachments: Right-click a file and select **Send as email attachments**. You can directly send and share files as email attachments in File Station once you have set up email delivery settings in the **Personal** pop-up window.

- To view or rotate pictures: Double-click a picture to open it in a viewer window, where you can view and rotate it.

- To edit access permissions: Right-click a file or folder and select **Properties**. You can edit access permissions on the **Permission** tab.

- To generate file-sharing links: Right-click a file or folder and select **Share**. A shared link will be automatically generated. You can further specify validity periods or enable secure sharing.

Manage files via DS file

DS file is an app available on Android and iOS devices that allows you to access and manage files stored on your Synology NAS. With DS file, you can browse pictures, watch videos, and check work documents on-the-go. This section guides you through the process of installing and using DS file.

Install and sign in to DS file

1. Install **DS file** on your mobile device.

2. Enter the following information on the login page:

   - **Address** or **QuickConnect ID**: This can be either an internal or external IP address, DDNS hostname, or Synology QuickConnect ID. You have to enable QuickConnect in **Control Panel** first to sign in via QuickConnect ID. For detailed information, refer to the Specify your QuickConnect ID section.

   - **Account** and **Password**

   - **HTTPS**: Enable HTTPS connections if you want to make a secure HTTPS login. Note that playing multimedia content over HTTPS requires port forwarding configurations and a valid SSL/TLS certificate.

Manage files and folders

You can perform general file management by tapping the **More options** icon in the upper-right corner or the ⋮ icon next to a file or folder.

- To copy, delete, download, share, rename, compress, extract, or open an item: Press and hold down on an item and tap the **More options** icon to select an action to perform.

- To add a folder: In its parent folder, tap the **More options** icon, and choose **Add** > **Create Folder**.

- To upload an item: Go to the destination shared folder. Tap the **More options** icon > **Add** > **Upload**, and then select files to upload. You can go to the **Tasks** page to view the upload progress.

- To pin a file: You can pin files from your Synology NAS to your local mobile device. Tap the ⋮ icon next to a file and choose **Pin**. Once you pin a file, you can access it at **Offline Files** > **Pinned Files**.

- To sync a pinned file: You can make local pinned files stay synced with source files. Tap the ⋮ icon next to a file and choose **Sync** for instant sync. To sync all pinned files, refresh the **Pinned Files** page. All files will be synced upon your next login to DS file.

- To add a folder to **My Favorites**: Tap the ⋮ icon next to a folder and choose **Add to My Favorites**.

Install add-on packages

The **Package Center** offers a variety of Synology-designed and third-party packages that are compatible with your Synology NAS.

This section guides you through using the Package Center.

Install packages via the Package Center

1. Launch **Package Center**.

17

2. Go to the **All Packages** page to see available packages.

3. Find the package you wish to install and click **Install**. (For paid packages, click **Buy** to purchase with a credit card or click **Try** to use the trial version for evaluation.)

4. Once the package is successfully installed, it should appear in the **Main Menu**.

Install packages from the Download Center

1. Go to Synology's Download Center.

2. Select your product type and model.

3. Go to the **Packages** tab and download the desired package as an .spk file.

4. Launch **Package Center** in DSM.

5. Click the **Manual Install** button next to the search bar.

6. Click **Browse** to upload the .spk file.

7. Follow the wizard to install the new package.

In addition to package installation, you can also configure package-related settings, including auto-update, and package sources in the Package Center.

Learn more about the Package Center.

Create local users and groups

You can grant family members or business associates access to your Synology NAS by creating user accounts for them. For ease of administration, you can create groups to categorize users and manage them together.

This section guides you through creating users and groups in **Control Panel**. If you want to import a user list to create multiple user accounts in bulk, refer to the Import Users article.

Create a user

1. Go to **Control Panel** > **User & Group** > **User**.

2. Click **Create** to launch **User Creation Wizard**.

3. Enter the following information:

   - **Name**

   - **Description** (Optional)

   - **Email** (Optional): Enter the user's email address. System notifications, such as password reset messages, will be sent to the address specified here.

   - **Password**

   - **Confirm password**

4. On the same page, configure the following advanced settings that will be applied to the user:

5. **Send a notification mail to the newly created user**: You have to enable email notifications in **Control Panel** > **Notification** > **Email** to allow the system to send emails. If you have not yet set up notification settings, a confirmation dialog box will pop up and lead you to the setup page when you can tick this checkbox. For more information on notification settings, refer to the Manage notification settings section.

6. **Display user password in notification mail**

7. **Disallow the user to change account password**: This option appears only when you have enabled **Allow non-administrator users to reset forgotten passwords via email** in **Control Panel** > **User & Group** > **Advanced**.

8. **Password is always valid**: This option appears only when you have enabled **Password Expiration** in the **Advanced** tab. This option makes this user's password always valid and the rules of **Password Expiration** will not be applied to this user.

9. On the **Join groups** page, specify the groups to which the new user should belong. The default groups are **administrators**, **http**, and **users**. Refer to the Create a group section to customize groups.

10. On the **Assign shared folders permissions** page, choose which shared folders the user can access. When the user permissions conflict with group permissions, the privilege priority is as follows: **No access** > **Read/Write** > **Read only**. The **Preview** column displays the access privileges that will take effect.

11. On the **Assign user quota** page, you can specify the maximum amount of space the user can use for each volume/shared folder. Enter a value and select the size unit in the **User Quota** field.

12. On the **Assign application permissions** page, you can control which services the user can access. When the user permissions conflict with group permissions, the **Deny** permission always has priority over the **Allow** permission.

13. On the **Set user speed limit** page, you can enable a speed limit for different services (e.g., File Station, FTP, rsync, etc.) to restrict the amount of bandwidth consumed by the user when transferring files. For each service, you can select one of the following:

    ○ **Apply group settings**: If the user belongs to multiple groups, the group with a higher speed limit has priority over other ones.

    ○ **Set up speed cap**: Specify upload and download speed limits in the fields to the right.

    ○ **Advanced settings**: Two customized speed limits and the group limit can be applied to the user according to the schedule you set. You can modify the speed limit settings and set the schedule in the pop-up window.

14. On the **Confirm settings** page, check and confirm the settings summary.

15. Click **Done** to finish the setup.

Create a group

1. Go to **Control Panel** > **User & Group** > **Group**.

2. Click **Create** to launch **Group Creation Wizard**.

3. On the **Enter group information** page, enter a group name.

4. On the **Select members** page, add target users to the group.

5. On the **Assign shared folder permissions** page, specify group members' permissions to each shared folder.

6. On the **Assign group quota** page, you can enable a usage quota for each service to control how much storage can be used by each group member.

7. On the **Assign application permissions** page, you can control which services group members can access.

8. On the **Set group speed limit** page, you can enable a speed limit for different services (e.g., File Station, FTP, rsync, etc.) to restrict the amount of bandwidth consumed by each group member when transferring files. For each service, you can select one of the following:

   - **Set up speed cap**: Specify upload and download speed limits in the fields to the right.

   - **Advanced settings**: Two customized speed limits and group limit can be applied according to the schedule you set. You can modify the speed limit settings and set the schedule in the pop-up window.

9. On the **Confirm settings** page, check and confirm the settings summary.

10. Click **Done** to finish the setup.

Manage notification settings

You can have your Synology NAS automatically send notifications when specific events or errors occur. Available notification methods include emails, push service, and webhooks. This section provides a brief guide on notification setup at **Control Panel** > **Notification**.

1. Go to the **Email**, **Push Service**, or **Webhooks** tabs to set up the delivery channel for notification messages. For detailed instructions, refer to the respective articles:

   - **Email**: Receive notification messages at your Synology Account or a personal email address. For a personal email address, click **Set Up** to configure a sender email first.

   - **Push Service**: Receive notification messages on your mobile device or computer via a web browser.

   - **Webhooks**: Receive notification messages via Synology Chat, Microsoft Teams, LINE, SMS, or a custom webhook provider.

2. Go to the **Rules** tab to modify the rules that trigger the system to send notifications. The three default rules are: **All**, **Warning**, and **Critical**. Click **Add** to create a new rule. Once created, you can select it when you set up a delivery method. When setting up a notification method, the

default rules and any custom rules will appear in the selection list. You can choose from the list or create a new rule.
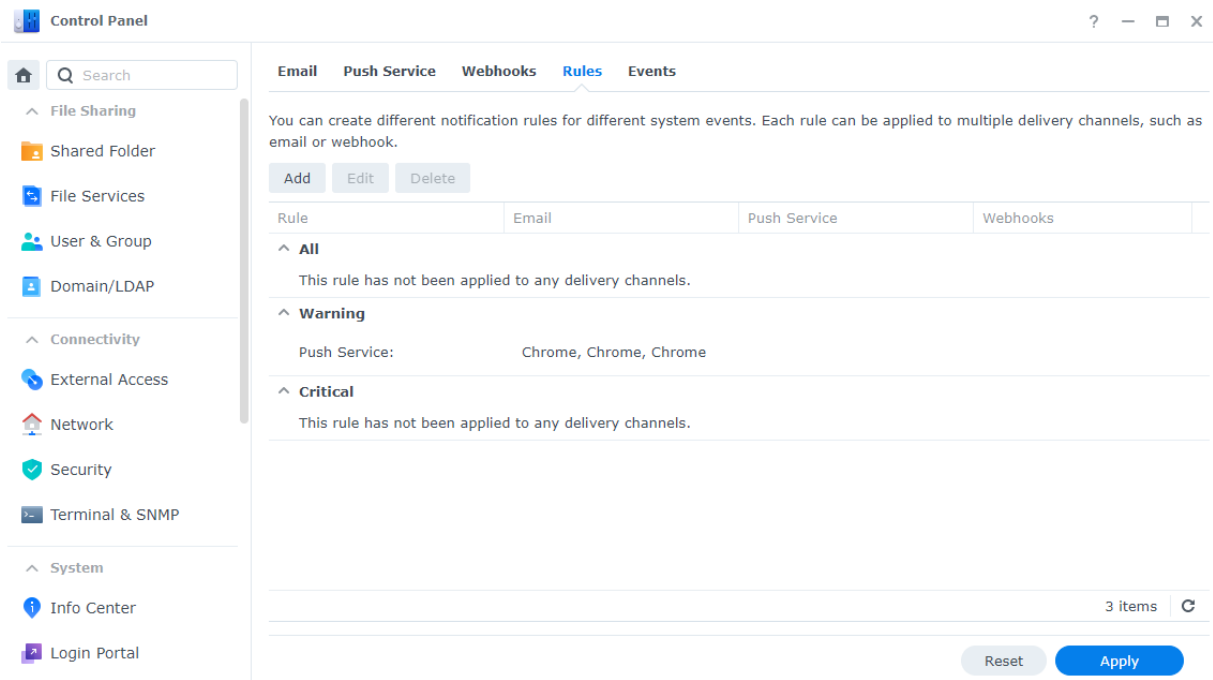
3. Go to the **Events** tab and configure the following settings:

   - **Message content**: Each event has its default notification message. You can also customize message content by selecting an event and then clicking **Edit Message**.

   - **Variables**: Variables are used in notification messages and are replaced with system information when the messages are sent. Certain variables can be modified. To do so, click **Edit Variables**.

> **Notes:**
>
> - You can go to **Regional Options** to change the notification language.

Fortify security

Once your Synology NAS is connected to the Internet, it is crucial to ensure system security. This section provides four methods to strengthen the security of your DSM.

Activate the firewall

1. Go to **Control Panel** > **Security** > **Firewall**.

2. Tick **Enable firewall** and click **Apply**. The default firewall profile will be applied to your DSM. Learn how to customize firewall profiles.
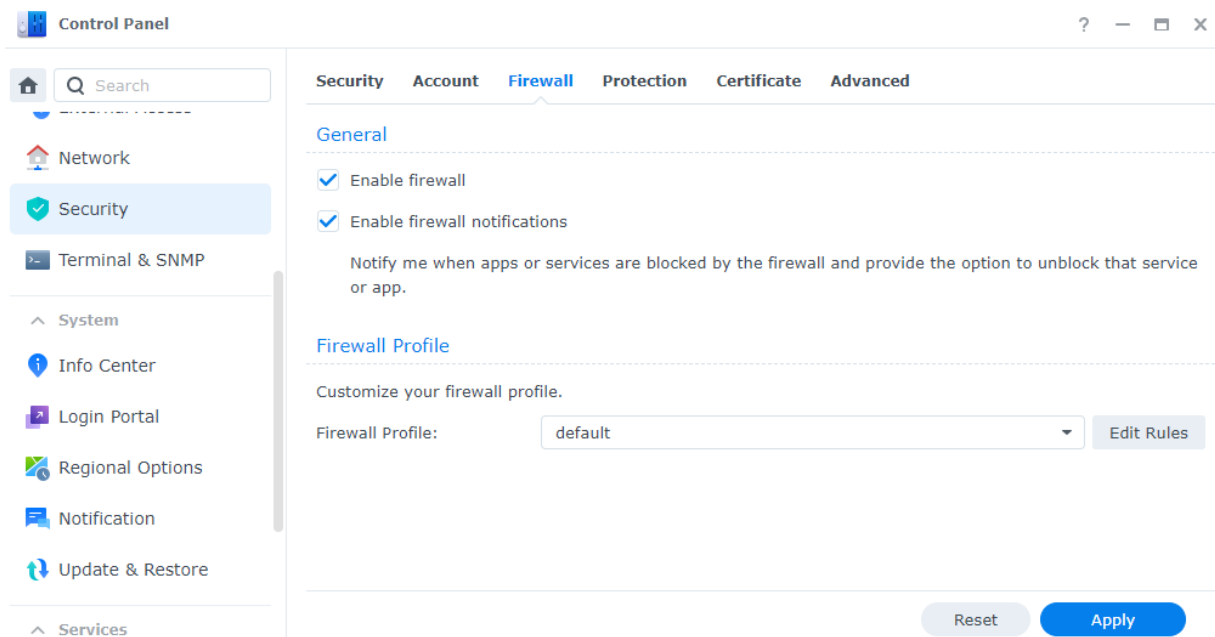
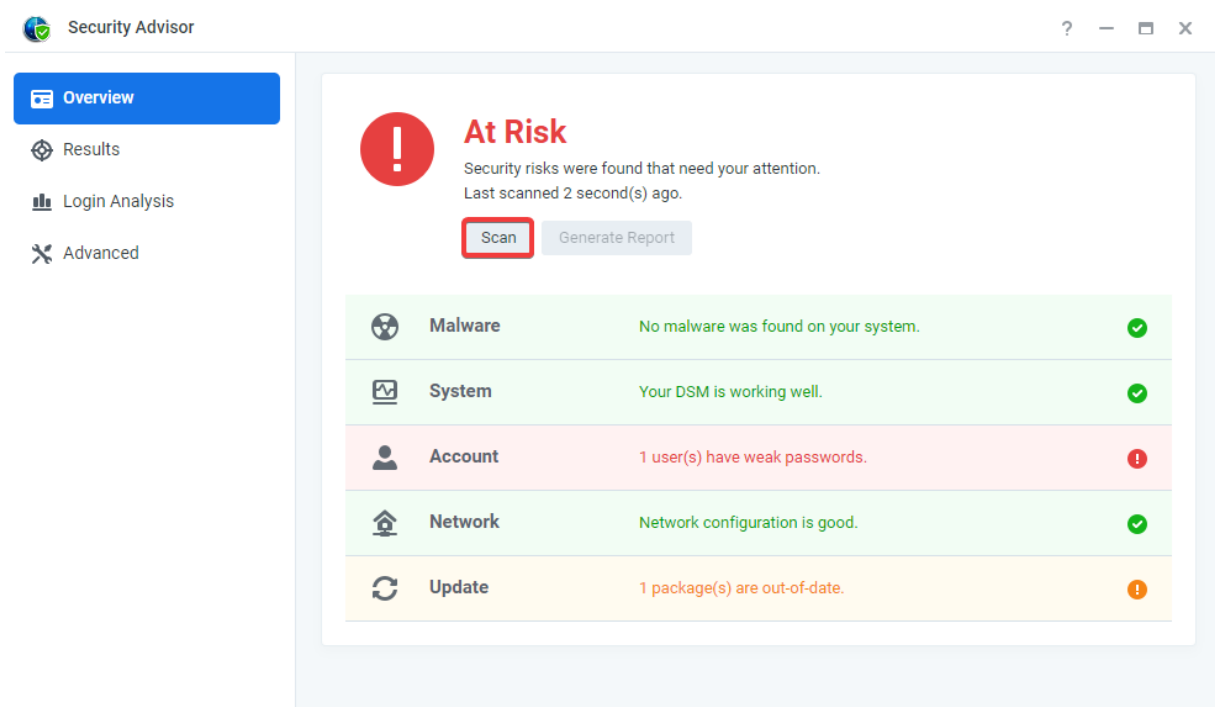## Leverage Security Advisor

Security Advisor is a built-in application that scans your Synology NAS, checks your DSM settings, and provides advice on how to address security weaknesses. Keep your Synology NAS secure by doing the following:
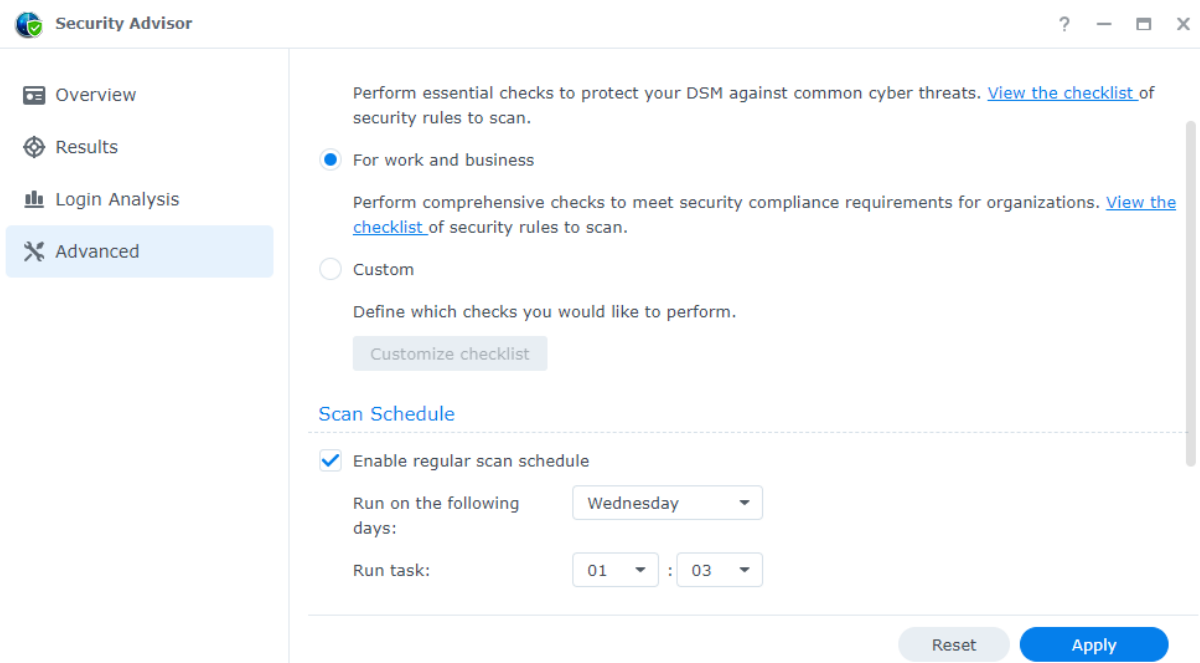
Scan your Synology NAS immediately

1. Go to **Security Advisor** > **Overview**.
2. Click **Scan**.

3. Fix the security weaknesses according to the results.

Set up an automatic scan schedule

1. Go to **Security Advisor** > **Advanced**.

2. Tick **Enable regular scan schedule** under the **Scan Schedule** section. Select the time to run scans from the drop-down menus.

3. Click **Apply** to save the settings.

Learn more about Security Advisor.

Protect your account with 2-factor authentication

2-factor authentication provides additional security for your DSM account. Once this option is enabled, you will need to enter a one-time authentication code with your password when signing in to DSM. This code can be obtained through authenticator apps (e.g., Synology Secure SignIn and Google Authenticator) installed on your mobile device.

To enable 2-factor authentication for your account, go to **DSM** > **Personal** > **Security** and click **2-Factor Authentication** to launch the setup wizard. Enter your password to continue.

Learn more about 2-factor authentication.

Enable auto block, Account Protection, and DoS protection

You can safeguard DSM through these three mechanisms: auto block, Account Protection, and DoS protection.

Auto block unauthorized access

1. Go to **Control Panel** > **Security** > **Protection** > **Auto Block**.

2. Tick **Enable auto block**.

23

3. Enter a value in the **Login attempts** field and a value in the **Within (minutes)** field. An IP address will be blocked when it exceeds the number of failed login attempts within the specified duration.

4. Tick **Enable block expiration** and enter a value in the **Unblock after (days)** field to unlock a blocked IP address after the specified number of days.

5. Click **Apply** to save the settings.

Enable Account Protection to prevent login attacks

1. Go to **Control Panel** > **Security** > **Account** > **Account Protection**.

2. Tick **Enable Account Protection**.

3. Enter a value in the **Login attempts** field and a value in the **Within (minutes)** field. An untrusted client will be blocked if it exceeds the number of failed login attempts within the specified duration.

4. For **Untrusted clients**, enter a value in the **Cancel account protection (minutes later)** field. The account protection will be canceled after the specified duration.

5. For **Trusted clients**, enter a value in the **Unblock (minutes later)** field. The account protection will be canceled after the specified duration.

6. Click **Apply** to save the settings.
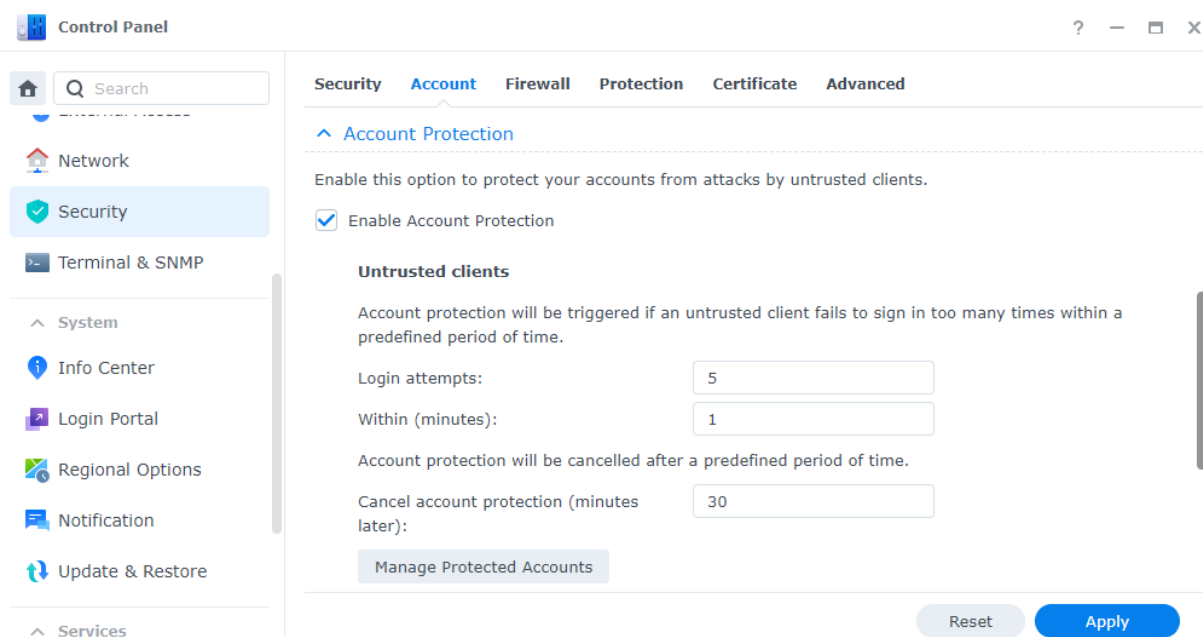
Defend against DoS attacks

A Denial-of-Service (DoS) attack is a malicious attempt to render network services unavailable by disrupting service functionality. To avoid this type of cyberattacks, follow the steps below:

1. Go to **Control Panel** > **Security** > **Protection** > **Denial of Service (DoS) Protection**.

2. Tick **Enable Dos Protection** and click **Apply**.
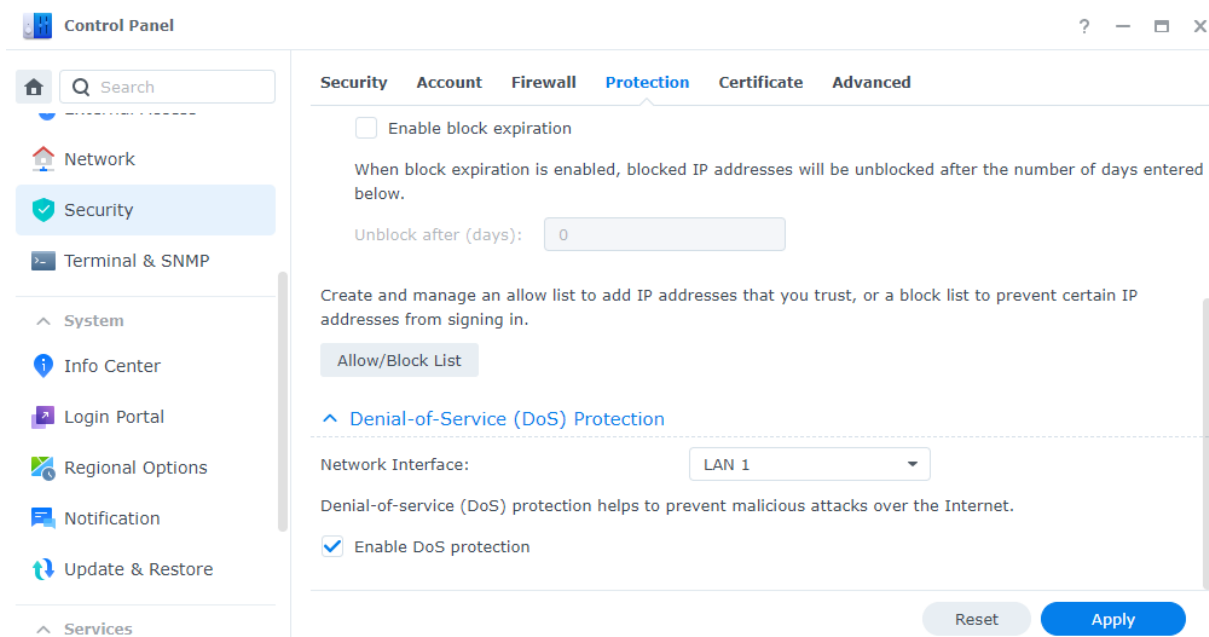
Learn more about auto block, Account Protection, and DoS protection.

Keep your DSM updated

Synology frequently releases DSM updates that may include new features, function improvements, and performance enhancements. This section guides you through the configuration of DSM updates.

> **Notes:**
> - After a DSM update, you cannot downgrade to previous versions.
> - Available updates and the latest versions may vary depending on your DSM configurations.

Perform a manual DSM update

1. Go to Synology's Download Center.
2. Select your product type and model.
3. Scroll down to **Operating System** and download the update file.
4. Go to **DSM** > **Control Panel** > **Update & Restore** > **DSM Update**.
5. Click **Manual DSM Update**.

6. In the pop-up window, click **Browse** to upload the file.
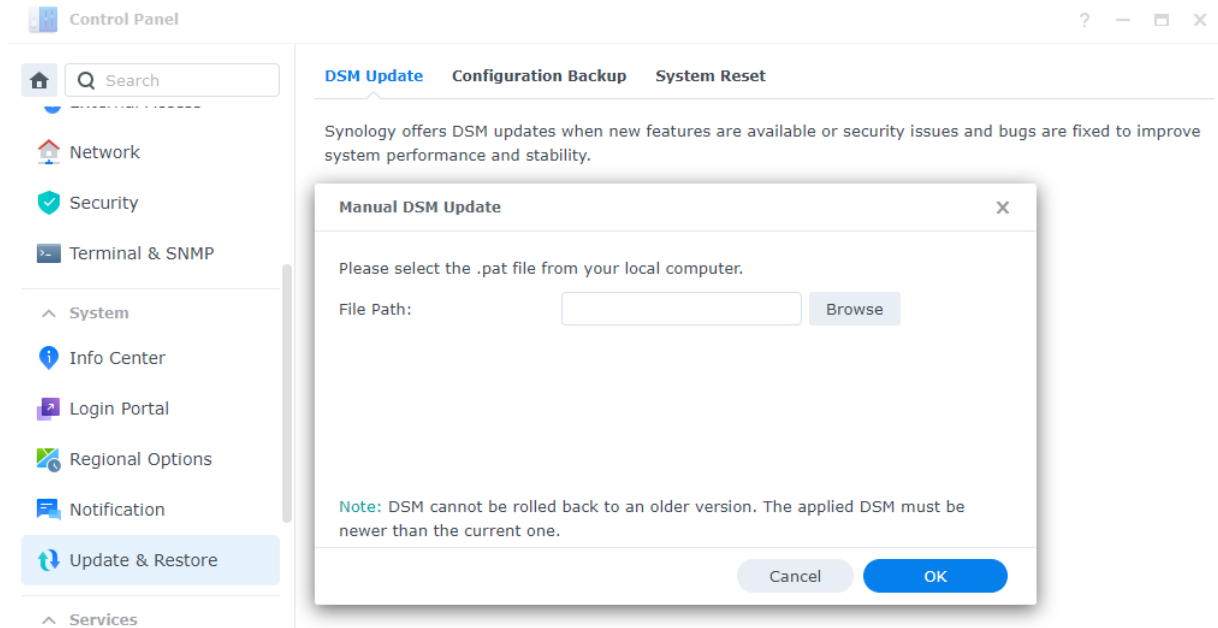
7. Click **OK** and wait for the file to be uploaded.

8. After reading through the update information and ticking the confirmation checkbox, click **Update**.

9. Click **Yes** in the confirmation box. The installation can take 20 to 40 minutes. Do not shut down the system during the update.

10. The system will restart all services and packages once the update is complete.

Set up automatic DSM updates

1. Go to **DSM** > **Control Panel** > **Update & Restore** > **DSM Update**.

2. Click **Update Settings**.

3. In the pop-up window, you can configure the following settings to check for DSM releases in Synology's Download Center.

   - **Automatically install important updates that fixed critical security issues and bugs (Recommended)**: Allow the system to automatically install important DSM updates. To ensure that your system is always protected, we recommend enabling this option.

   - **Automatically install the latest update**: Allow the system to automatically install new DSM updates when the system finds new updates.

   - **Notify me and let me decide whether to install the new update**: Have the system notify you via desktop notifications when there is a new DSM update available. You can choose whether or not to download the update after receiving the notification.

   - **Check schedule**: Decide when the system should check for available updates. Specify the check time from the drop-down menus.
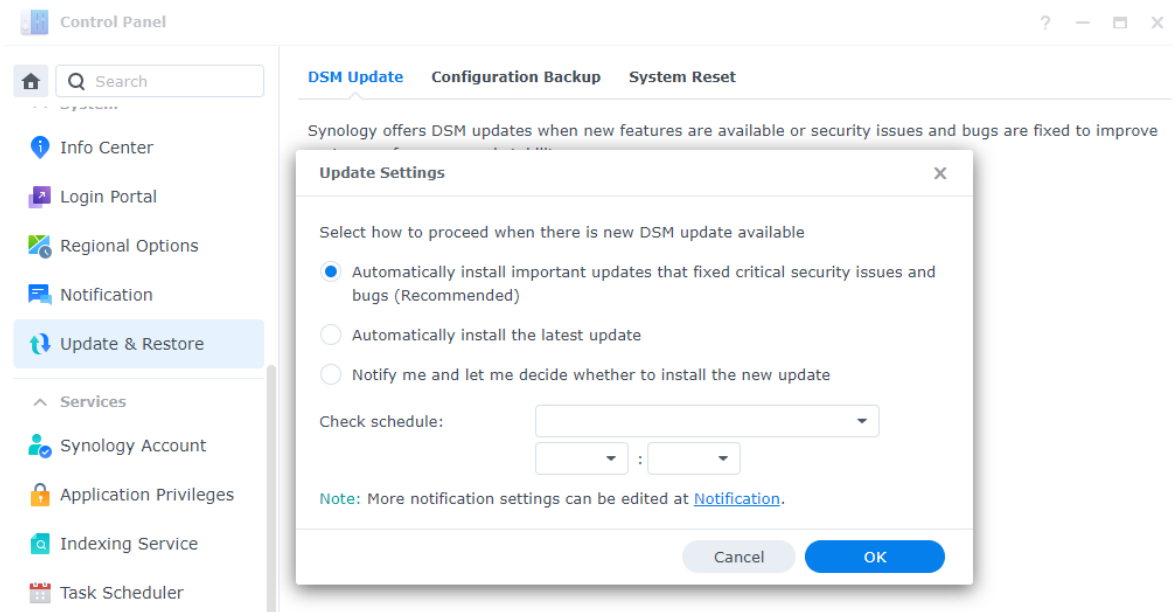
Learn more about DSM system updates.

> **Notes:**
>
> - Automatic updates only apply to minor updates, not major updates. Generally, minor updates consist of bug fixes and security patches, major updates include brand-new features and performance enhancements in addition to bug fixes and security patches, and important updates contain fixes for critical security issues or bugs.

Chapter 3: Account & Privileges

Account & privileges

You can create user accounts to share DSM access with others and set up user groups to simplify account and permissions management. To create users and groups, refer to the Create local users and groups section.

You can assign each user shared folder access, application permissions, storage quotas, or access speed limits. You can also grant access privileges to individual users or groups. For more detailed information, refer to the User and Group articles.

Role delegation (**Control Panel** > **User & Group** > **User** > **Delegate** > **Delegated Administration**) allows you to assign management duties to users or groups that do not have administrator rights. Task specific users with managing user accounts, shared folders, or system services, or assign system monitoring duties.

> **Further reading:**
> - Video tutorial: How to Manage User Privileges on Your Synology NAS

Directory clients

In **Control Panel** > **Domain/LDAP**, you can join your Synology NAS to an existing directory service such as Microsoft Active Directory, Synology Directory Server, or JumpCloud LDAP service. As a

28

directory client, you can manage directory users' access permissions to shared folders, home folders, and DSM services.

Learn how to join your Synology NAS to a directory service.

You can also turn your Synology NAS into a Single Sign-On (SSO) client. With your Synology NAS acting as an SSO client, users can access services provided by your Synology NAS once they sign in to an SSO server. Learn how to set up your Synology NAS as an SSO client.

> **Further reading:**
>
> - How can I implement an SSO solution on Synology NAS with Azure AD Domain Services?

Synology Directory Server

Manage your domain accounts and resources using **Synology Directory Server**. It supports the following commonly used Windows Active Directory features:

- Classifying objects with organizational units (OUs)
- Applying group policies for device management
- Using Kerberos for authentication
- Joining diverse client devices

Synology Directory Server allows you to securely store your directory database and manage user accounts. You can use it to deploy devices based on your organization structure and even migrate an existing Windows Server domain to your Synology NAS. Additionally, you can join your Synology NAS to Synology Directory Server's domain as a secondary read-write or read-only domain controller.

Learn how to set up a domain via Synology Directory Server.

> **Further reading:**
>
> - Synology Directory Server Quick Start Guide
> - Synology Directory Server Administrator Guide
> - Why are there "sysvol" and "netlogon" folders?

LDAP Server

Run an account authentication service with **LDAP Server**. LDAP (Lightweight Directory Access Protocol) is a cross-platform protocol used to consolidate and govern access to centrally stored directory information over IP networks.

Different lists of users within your organization can be merged into one LDAP directory, reducing the number of databases for you to manage.

With LDAP Server set up, you can:

- Build a Provider-Consumer server architecture.
- Specify connection settings to restrict access by anonymous, non-encrypted, or idle clients.
- Create and organize users and groups according to your needs.
- Customize sign-in and password settings to secure accounts.
- Back up and restore your LDAP database and package settings.
- Turn your Synology NAS into an identity provider for Google Workspace domains.

Learn how to set up LDAP Server.

> **Further reading:**
> - How to join Mac client computers to the Synology LDAP directory service
> - How can I sync Synology's LDAP Server with Google Workspace via Google Cloud Directory Sync?
> - LDAP Server documents

SSO Server

If your organization is using several applications (such as Microsoft 365 or Synology MailPlus), it's worth your while to set up a single sign-on (SSO) service on your NAS. Synology's **SSO Server** provides a variety of SSO solutions for your apps, including OIDC, SAML, and Synology SSO. Both you and your users can benefit from the convenience and speed it brings:

- Users only need to remember a single set of sign-in credentials without needing to sign in to different apps separately.
- You can centralize your app management without keeping credentials of the same user in different databases.
- The minimized database reduces sign-in issues.

Learn more about SSO Server.

RADIUS Server

RADIUS Server is an add-on package that offers centralized authentication, authorization, and accounting (AAA) for wired and wireless network connections via the Remote Authentication Dial-In User Service (RADIUS) protocol. RADIUS Server lets you:

- Flexibly deploy wireless routers, VPN servers, and network switches with RADIUS support on your network.

- Unify the security regulation process of different connection types.

- Choose between various authentication methods (e.g., PAP, MS-CHAP, PEAP, EAP-MSCHAPv2, or EAP-TTLS).

- Import existing local DSM, domain, or LDAP user lists.

- Configure detailed restrictions for users and groups.

- Keep track of access statuses with detailed reports.

Learn more about RADIUS Server.

Chapter 4: Storage & Virtualization

Storage Manager

Storage Manager allows you to organize the storage units on your Synology NAS, monitor overall storage use, and inspect the health of all your drives.

Key Terms

Before using Storage Manager, it can help to familiarize yourself with the following terms:

- **Storage Pool**:

  - A storage pool is a single storage unit made up of a one or more drives. A storage pool can be configured to be protected by a data storage technology known as Redundant Array of Independent Disks (RAID).

- **RAID**:

  - RAID is a data storage technology that aggregates multiple physical drives into one or more logical units for improved fault tolerance, performance, and storage capacity.

  - Supported RAID types vary according to your Synology NAS model. For details, refer to RAID type overview and the product specs of your Synology NAS.

- **Volume**:

  - Volumes are created on top of storage pools and provide the basic storage space on your Synology NAS. All of your shared folders, documents, and package data will be stored here.

Storage Pools and Volumes

Create at least one storage pool and volume to start storing data on your Synology NAS. For more information, refer to the instructions in the Configure storage space section.

You can go to **Storage Manager** > **Overview** to find key information about your storage system, such as overall system status, volume usage, drive information, and scheduled tasks.
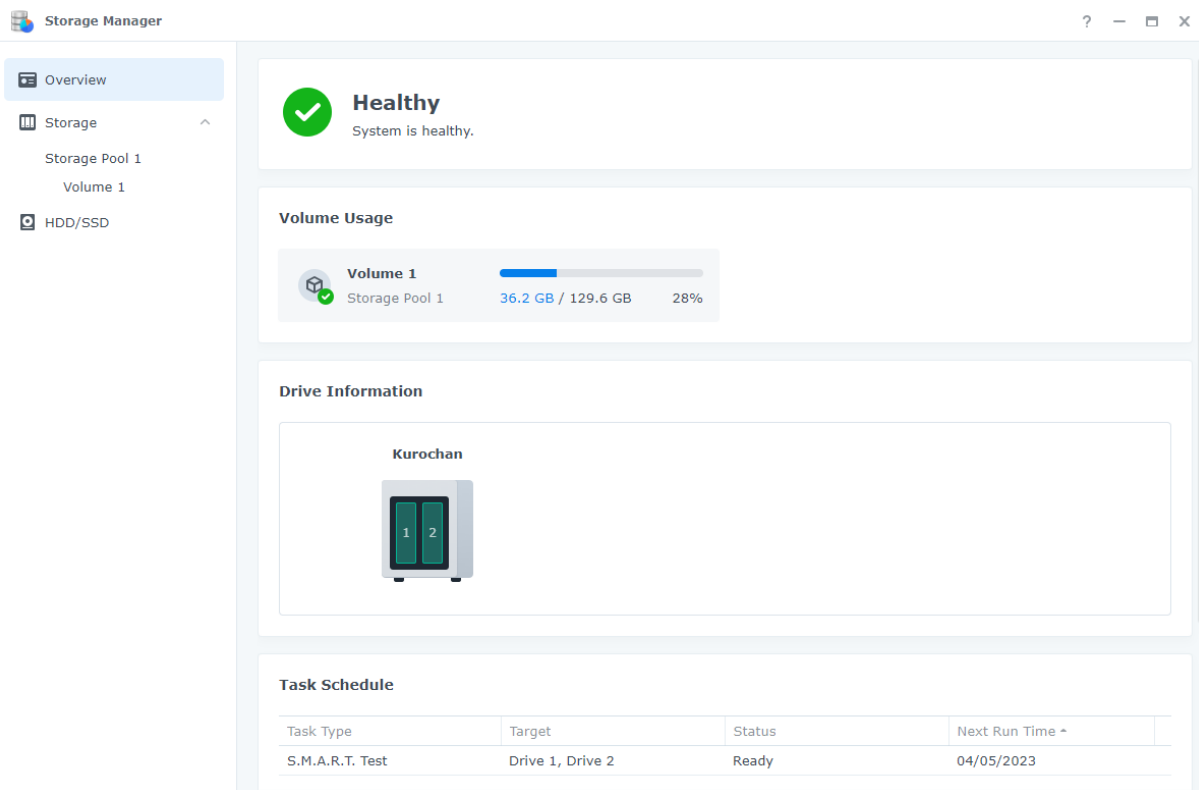
View and manage all your storage pools and volumes at **Storage Manager** > **Storage**. The actions you can perform here depend on your Synology NAS model and configurations:

- Change the RAID type of a storage pool without losing existing data.
- Add or replace drives to expand the capacity of a storage pool and volume.
- Enable volume encryption to safeguard your data.
- Enable SSD TRIM to optimize the performance of an SSD-only storage pool.
- Perform or schedule data scrubbing on a storage pool to maintain data consistency.
- Perform file system defragmentation to improve a volume's file access performance.

Learn more about storage pools and volumes.

> **Further reading:**
>
> - Storage Manager Quick Start Guide

Hot Spare

Hot spare drives are standby drives that allow your Synology NAS to automatically repair degraded storage pools. You can assign hot spare drives to protect storage pools with a drive fault tolerance of one or more drives at **Storage Manager** > **Storage** > **Hot Spare**.

When a drive crashes and causes a storage pool to degrade, the hot spare drive replaces the crashed drive, allowing the storage pool to recover.

Learn more about hot spare drives.

> **Notes:**
> - The RAID type of the storage pool must have a fault tolerance of 1 or more drives (i.e., RAID 1, RAID 5, RAID 6, RAID 10, RAID F1, and SHR comprising at least two drives).
> - The capacity of the hot spare drive must be equal to or larger than the capacity of the smallest drive in a RAID 1, RAID 5, RAID 6, RAID 10, or RAID F1 storage pool.
> - The capacity of the hot spare drive must be larger than or equal to the capacity of the largest drive in an SHR storage pool.
> - HDDs and SSDs can each only be assigned as hot spares to storage pools of the same drive type. Only SSD hot spares can protect SSD storage pools, and only HDDs can protect HDD pools.

SSD Cache

SSD cache is a cost-effective way to improve the performance of HDD arrays. It improves random access by storing frequently accessed data on the SSDs of an SSD cache mounted on a volume or LUN. Note that this feature is only available on specific models. Find out if your Synology NAS supports SSD cache.

There are two types of SSD cache:

- A **read-only cache** uses one or more SSDs to store frequently read data and accelerate random read performance. No data loss will occur in the event of SSD failure because this cache mode only stores copies of data from the volume.

- A **read-write cache** uses at least two SSDs to create a fault-tolerant cache. The read-write cache first writes data to the SSDs to improve the random read/write performance and accelerate data access speed.

Both types or modes of SSD cache can consist of up to 6 SSDs and must be comprised of drives of the same type.

Learn more about SSD cache and its requirements.

If you are unsure what is the best SSD cache size for your use case, we strongly recommend running an analysis in **Storage Manager** > **Storage** > **SSD Cache Advisor** beforehand.

SSD Cache Advisor analyzes your current data use patterns and recommends a suitable SSD cache size for your selected volume. Allow the initial analysis to run for at least seven days for more accurate results.

Learn more about SSD Cache Advisor.

HDD/SSD

Inspect the health of your drives and take follow-up actions at **Storage Manager** > **HDD/SSD**. Depending on your storage setup and Synology NAS model you can:

- Examine your drives' health information, including location, drive status, allocation role, temperature, serial number, and firmware version.

- Schedule and run S.M.A.R.T. tests to examine the status of your drives.

- Assign drives to create, manage, or repair a storage pool or SSD cache.

- Enable SSD estimated endurance notifications and request a warning whenever an SSD's estimated life expectancy reaches a specified value.

- Enable write cache support to boost the system performance of your Synology NAS.

Learn more about [HDDs and SSDs in DSM](#).

Storage expansion

You can pair your Synology NAS with additional expansion units or external devices to scale up your storage.

Expansion units

Scale up your Synology NAS with an [expansion unit](#) to increase your overall storage or use the expansion unit server as a backup location. Expansion units are designed to work automatically once connected to a Synology NAS and let you seamlessly upgrade your storage space.

You can create and manage storage spaces that span across your main Synology NAS and connected expansion units. However, we recommend keeping each storage space on one device for better performance.

External devices

Manage the external devices (e.g., SD cards or USB devices) connected to your Synology NAS device at **Control Panel** > **External Devices**. Connected external devices will appear as system-created shared folders that allow you to access their drive capacity.

You can install the **USB Copy** package to copy files between your Synology NAS and external storage devices in multiple ways. Synology NAS only recognizes certain file systems over USB: Btrfs, ext3, ext4, FAT32, exFAT, HFS Plus, and NTFS. External drives with other file systems must be formatted before use.

Learn more about external devices.

If you need to access data stored on exFAT file systems, you can install the **exFAT Access** package.

Learn how to install exFAT on your Synology NAS.

Storage Analyzer

Storage Analyzer allows you to monitor the overall use trends of your Synology NAS. You can create reporting tasks to obtain detailed reports on volume usage that help you manage your system and optimize your settings.

Learn more about Storage Analyzer.

SAN Manager & Storage Console

Make your Synology NAS a storage extension for your devices with **SAN Manager**. You can divide a part of a volume to create LUNs and connect to them using storage area networking (SAN) services.

Synology NAS provides certified storage for VMware®, Microsoft®, and other virtualization platforms. For better management efficiency, install **Synology Storage Console for VMware** or **Windows** to manage your storage systems right in the hypervisor.

With SAN Manager and Storage Console, you can:

- Choose between iSCSI and Fibre Channel as the protocol to deploy your own SAN storage. Deploying Fibre Channel requires an adequate switch and adapter.

- Create Thick-provisioned or Thin-provisioned LUNs as block-level data storage.

- Protect block-level storage with snapshot and replication features.

Learn more about configuring iSCSI or Fibre Channel services.

Learn more about Synology Storage Console for VMware and Windows.

Virtual Machine Manager

Virtual Machine Manager is a full-fledged hypervisor for Synology NAS. You can run virtualized Windows or Linux services on your Synology NAS and create virtual instances of DSM.

The clustering architecture of Virtual Machine Manager allows you to manage virtual machines and operations across multiple Synology NAS from a single portal. You can allocate available hardware resources and migrate virtual machines between different Synology NAS whenever needed.

For data protection, secure your virtual machines with snapshot and replication protection plans. There's also the built-in high-availability feature to minimize system downtime.

Learn more about [Virtual Machine Manager](#).

Container Manager

Container Manager is a lightweight virtualization environment that allows you to build and run applications inside an isolated software container. The hugely popular built-in image repository, Docker Hub, allows you to find shared applications from other talented developers. Synology has developed an optimized Docker container management GUI for users to create and manage containers in DSM.

Learn more about [Container Manager](#).

Chapter 5: File-Sharing & Sync

Shared Folder

Synology offers two types of shared folders for general storage purposes and multi-site file access.

Create Shared Folder

A **Shared Folder** is a basic directory to store files and folders on your Synology NAS. You need to create at least one shared folder before storing any data.

Store data in private shared folders, or share them with specific users or user groups by configuring custom access permissions. You can also encrypt shared folders for an additional layer of protection.

To learn how to create a shared folder and start sharing files, refer to the Create a shared folder and start sharing filessection or the Shared Folder article.

Shared folders also include the following advanced options:

- Cloning shared folders to create near-instantaneous copies (only available on Btrfs volumes).
- Enabling the **Recycle Bin** feature in shared folders to store deleted files and folders you want to retrieve.
- Using **Key Manager** to manage encryption keys of shared folders and to decrypt multiple shared folders at a time.
- Protecting shared folders with **WriteOnce**, which adopts WORM (Write Once, Read Many) technology to avoid unauthorized changes to your data. WriteOnce provides Enterprise mode and Compliance mode to best fit your needs.

Mount Hybrid Share Folder

Hybrid Share combines the performance of Synology NAS with the scalability of C2 Storage, Synology's public cloud solution. You can mount a Hybrid Share folder on-premises for multiple NAS devices at different locations to share files.

Once the Hybrid Share folder is mounted on your Synology NAS, you can view all the cloud-based data locally and cache only the most recently accessed files on the local site. Hybrid Share can help you achieve the following:

- **Multi-site file access**: Access your centrally stored data at anytime and from anywhere by mounting the same Hybrid Share folder on multiple Synology NAS devices.
- **Disaster recovery**: Protect your Hybrid Share folder and achieve near-instantaneous data recovery with Hybrid Share's snapshot feature in C2 Storage.

To get started, you will need the following:

- A subscription to the C2 Storage-Advanced Plan

- A Synology NAS running DSM 7.0.1 or above

- A Btrfs volume on which to mount the Hybrid Share folder

- Connection to an external network

Learn how to set up a Hybrid Share folder.

> **Further reading:**
>
> - Hybrid Share Quick Start Guide
>
> - Hybrid Share documents

Encryption

Synology NAS uses AES-256 encryption to protect shared folders and Hybrid Share folders against unauthorized access.

- Shared folders: Encryption is optional for shared folders. Learn more about shared folder encryption.

- Hybrid Share folders: To ensure data security, data are always encrypted on your NAS before being transferred to C2 Storage. You need an encryption key to mount and decrypt any Hybrid Share folder. Data remain encrypted during upload and while they are stored on C2 Storage. Learn more in the Synology Hybrid Share White Paper.

Permissions

You can implement **Windows Access Control List (ACL)** permissions settings for shared folders and Hybrid Share folders. This also allows you to customize permissions for individual files and subfolders in Windows ACL.

File services

SMB, AFP, and NFS

Configure the **SMB**, **AFP**, and **NFS** networking protocols on your Synology NAS to use it as a file-sharing center. Manage files in DSM shared folders from client computers as if you were using local storage.

DSM supports the most common protocols to provide seamless file access from Windows, Mac, and Linux devices:

39

- For Windows: SMB/CIFS

- For Mac: SMB, AFP

- For Linux: NFS, SMB

Each operating system has a native file-sharing protocol that delivers the best performance for that platform. SMB supports all three types of operating systems but may be slower than NFS and AFP. Each protocol also has different security implications.

To enable one or more file-sharing protocols, go to **Control Panel** > **File Services**.

Learn more about SMB, AFP, and NFS.

FTP

FTP is a convenient way to share files with known or anonymous users. Users can access an FTP server from their computers using web browsers or FTP clients. You can level up your transfer security with FTP over SSL (FTPS) and SSH FTP (SFPT).

Learn more about FTP.

File Station

File Station is a built-in file manager for users to access and manage files easily. Share files securely with customizable access permissions and temporary share links. You can centrally view all your files, including photos, songs, and even backups.

With File Station, you can:

- Centralize file access by mounting remote folders and public cloud storage to File Station.

- Create file requests for non-DSM users to upload files to Synology NAS.

- Access files from anywhere with its mobile application, DS file.

- Apply and modify WriteOnce settings to files, such as locking files, extend the retention period, or convert the lock state.

Learn more about File Station.

Synology Drive Server

Synology Drive Server is a comprehensive file management and collaboration solution that allows you to easily manage, share, and collaborate on files with others. Its package includes three components — **Synology Drive Admin Console**, **Synology Drive**, and **Synology Drive ShareSync**.

In **Synology Drive Admin Console**, administrators can appoint team folders, monitor client connections, and manage service settings. The **Synology Drive web portal** allows users to

browse, manage, share, and collaborate on files and folders with others. **Synology Drive ShareSync** is an application that synchronizes files in Synology Drive across multiple Synology NAS.

Synology Drive also comes with a desktop utility, **Synology Drive Client**, and a mobile app. These applications are available on all mainstream platforms.

With Synology Drive, you can achieve:

- **Local file backup**: Sync and back up files on your client device.

- **Version control**: Retain up to 32 versions per file. Synology Drive's Intelliversioning helps you keep the most important changes.

- **Offline accessibility**: Pin important files to your client device for continuous accessibility, even when your client device is offline.

- **Multi-site exchange**: Synchronize files and folders across multiple sites to simplify local access and enhance cross-office file collaboration. It also provides additional file redundancy.

- **Real-time collaboration**: Integration with Synology Office and Synology Chat to increase productivity. Collaborate using documents, spreadsheets, or slides and initiate discussions as you work.

Learn more about Synology Drive Server.

> **Further reading:**
> - Synology Drive Quick Start Guide for administrators
> - Synology Drive Quick Start Guide for users
> - Synology Drive documents

Cloud Sync

Connect your Synology NAS with Google Drive, Dropbox, and other public cloud services to create your own hybrid cloud with **Cloud Sync**. Choose between one-way or two-way synchronization to back up or sync data between your private NAS and public clouds.

You can use one-way synchronization to back up data from your Synology NAS to public clouds, or the other way around. File changes on the destination side of the synchronization will not affect the source.

Meanwhile, two-way synchronization keeps files on your Synology NAS and in the public cloud identical, automatically uploading and downloading changes on both sides.

One folder can be synced to more than one public cloud or to several accounts on the same cloud to create multiple backups of your files. You can select exactly which files on your Synology NAS or the public cloud you wish to synchronize, and in which direction.

To prevent unauthorized access to files in the cloud, you can protect synced files with AES-256 encryption.

By scheduling sync tasks, capping traffic, or limiting system resource use, you can prevent Cloud Sync from affecting other applications or processes.

Learn more about Cloud Sync.

> **Further reading:**
>
> - Cloud Sync documents

WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) is an extension of the HTTP protocol that allows users to manage files stored on remote servers. Common client programs supporting WebDAV include Windows File Explorer, macOS Finder, and many Linux file managers.

After setting up WebDAV Server, you can mount and access shared folders on Windows, macOS, or Linux devices.

WebDAV has the following advantages over other file access protocols:

- Provides better performance than CIFS/SMB over VPN
- Supports editing files on client devices
- Takes advantage of HTTPS security

> **Further reading:**
>
> - How do I access files on Synology NAS with WebDAV?
> - How do I import calendars from WebDAV Server to Synology Calendar?

Chapter 6: Data Backup

Active Backup Suite

Synology NAS, PC, Server, and VM backup solution

Active Backup for Business

Your Synology NAS can be a backup destination for your other Synology NAS, personal computers, physical servers, file servers, and virtual machines.

Active Backup for Business is an all-in-one business data protection solution that allows you to easily manage, deploy, and monitor multiple customized backup tasks for multiple devices in one centralized location.

Active Backup for Business consists of an admin console and a recovery portal. The admin console allows you to deploy and track the protection of multiple devices. The recovery portal allows admin users and end-users delegated by the server admin to access, browse, download and restore backed-up data.

Maximize backup efficiency with Active Backup for Business with global deduplication, data compression, and incremental backup technologies, so that even when data are backed up from different platforms, storage space consumed by the same backup data can be greatly reduced.

Moreover, various restoration methods for backed-up devices, such as full device restoration and instant restoration to virtual platforms, are provided to satisfy different IT needs. When an IT disaster strikes, you can retrieve your backup data in a flash to shorten service downtime and ensure business continuity.

Active Backup for Business supports the backup of the following devices:

- Synology NAS
- Windows computers
- Mac computers
- Windows physical servers
- Linux physical servers
- VMware vSphere virtual machines
- Microsoft Hyper-V virtual machines
- SMB protocol file servers
- Rsync protocol file servers

Learn more about Active Backup for Business.

SaaS backup solution

Active Backup for Microsoft 365

With Active Backup for Microsoft 365, you can back up the following data of your organization: OneDrive for Business, Exchange Online, SharePoint Online, and Microsoft Teams. The following Microsoft 365 plans are supported: Business, Enterprise, Education, and Exchange Online.

Active Backup for Microsoft 365 consists of an admin console and a recovery portal. The admin console provides a centralized interface where admins can create backup tasks, monitor backup statuses, and manage storage usage. The recovery portal allows users to restore their own data, without relying on admins.

Active Backup for Microsoft 365 keeps your backup data up-to-date with its continuous backup mode. In the event of a emergency data recovery, granular restores and exports are available, allowing you to easily restore specific data to its original location or download it to your local device.

Active Backup for Microsoft 365 supports the backup of the following services and data:

- **OneDrive for Business**: Files, file-sharing permissions, and corresponding metadata.

- **Exchange Online**: Mailboxes including mails, folder structure, email attachments, contacts, and calendars along with event attachments.

- **SharePoint Online**: Document libraries and lists of Sites, Personal Sites, and Team Sites.

- **Microsoft Teams**: Team posts, team objects, and chat files.

Learn more about Active Backup for Microsoft 365.

Active Backup for Google Workspace

With Active Backup for Google Workspace, you can back up the following data of your organization: Google Drive, Gmail, Google Contacts, and Google Calendar.

Active Backup for Google Workspace consists of an admin console and a recovery portal. The admin console provides a centralized interface where admins can create backup tasks, monitor

backup statuses, and manage storage usage. The recovery portal lets users restore their own backup data, without relying on the admins.

Active Backup for Google Workspace keeps your backup data up-to-date with its continuous backup mode. In the event of a emergency data recovery, granular restores and exports are available, allowing you to easily restore specific data to its original location or download it to your local device.

Active Backup for Google Workspace supports the backup of the following services and data:

- **Google Drive**: Files, file-sharing permissions, and corresponding metadata in My Drive and shared drives.
- **Gmail**: Mailboxes including labels and email attachments.
- **Google Contacts**: Contact data.
- **Google Calendar**: Calendars including calendar events and their attachments.

Learn more about Active Backup for Google Workspace.

> **Further reading:**
>
> - Active Backup for Google Workspace Quick Start Guide

USB Copy

USB Copy lets you copy data between a Synology NAS and a USB storage device or SD card.

For storage efficiency, you can configure the following settings for a copy task to ensure that only targeted data are exchanged and only important copy versions are retained:

- Customized filters according to file types and extensions.
- Incremental, mirroring, and multi-versioned copy modes.
- Version rotation for the multi-version copy mode.

You can customize a copy task for each USB/SD storage device. When a device once used for a copy task is connected to the Synology NAS, it automatically recognizes and applies the previous settings of the device.
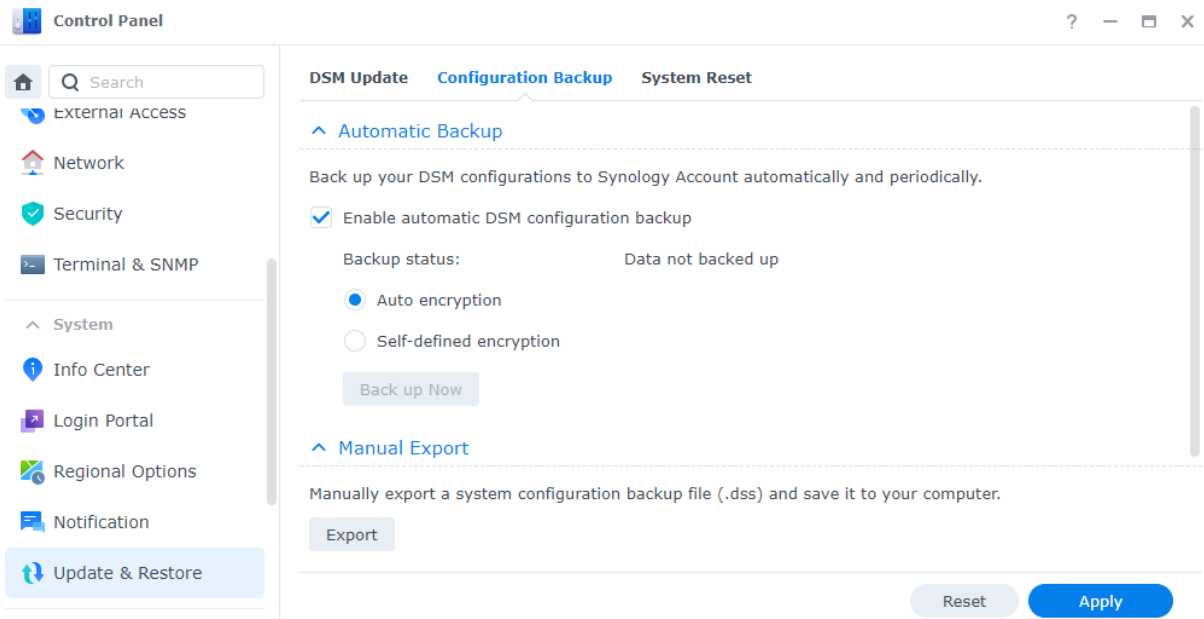
Learn more about USB Copy.

> **Notes:**
>
> - All the USB/SD storage devices in the following Synology supported file systems are allowed to copy data from or to a Synology NAS: FAT32, NTFS, ext3, ext4, and exFAT.

Chapter 7: NAS Protection

DSM configuration backup

Regularly backing up system configurations lets you quickly retrieve and restore your settings with ease. You can set up DSM to automatically back up system configurations to your Synology Account in **Control Panel** > **Update & Restore** > **Configuration Backup**. Backups can also be performed manually with the data saved to your computer.

Learn more about configuration backup.

Hyper Backup

Hyper Backup allows you to back up and restore all data on your Synology NAS, including system configurations, permission settings, applications, folders, files, LUNs, or even the entire system. With a wide selection of backup destinations, including local folders, remote NAS, rsync file servers, and multiple cloud service providers, you get more flexibility when planning a backup strategy.

Multiple data backup versions can be retained to keep important information handy and easy to track. Backup data are kept in an encrypted database and can be easily browsed, downloaded, or restored using **Hyper Backup Explorer** on DSM, Windows, Mac, or Linux platforms.

Learn how to create backup tasks in Hyper Backup.

46

Snapshot Replication

Snapshot Replication allows you to protect your NAS with schedulable and near-instantaneous snapshot and replication plans. A snapshot is the state of your NAS at a certain point in time. Compared to full backups, snapshots use minimum storage space and can be taken within seconds with the help of Btrfs.

With Snapshot Replication, you can:

- Recover your lost or damaged data and save multiple versions of your data.

- View and restore earlier versions of files in File Station or Windows File Explorer.

- Customize a retention policy to automatically delete unneeded old snapshots and free up storage space.

- Safeguard your data by taking immutable snapshots that cannot be deleted via any method within a specified period.

If you have more than one Synology NAS that supports Snapshot Replication, you can replicate snapshots to a remote NAS to further secure your data. Configure replication schedules to regularly take snapshots of your share folders/LUNs and transfer snapshots to the other NAS. When the replication source is not accessible, you can perform a failover to ensure file access on the other NAS. Ensuring that you always have access to the data on your NAS is beneficial when creating a disaster recovery plan.

Learn more about Snapshot Replication.

Synology High Availability

High Availability refers to a server layout solution designed to reduce interruption of services caused by server malfunctions. With two Synology NAS, you can leverage **Synology High Availability** to establish a "high-availability cluster" where one server assumes the role of an "active server" and the other acts as a standby "passive server".

Using a real-time data mirroring mechanism, all the data stored on the active server are replicated to the passive server in real-time. This ensures that all replicated data are quickly accessible after incidents of hardware failure, minimizing your service downtime.

Learn more about Synology High Availability.

Further reading:

- Synology High Availability Quick Start Guide

- Synology High Availability documents

Chapter 8: Security

Security settings

Protect your Synology NAS from unauthorized logins with firewall rules, Auto Block, and Account Protection in **Control Panel**. Proper firewall settings let you control which IP addresses or services have access to DSM.

The **Auto Block** and **Account Protection** features help make sure that your Synology NAS is safe from brute-force attacks. These features ensure that IP addresses or DSM accounts with too many failed login attempts within a specified period will be blocked. When there are attempts to sign in to your NAS or its services from a specific IP with random username/password combinations, Auto Block prevents users of that IP address from gaining access to the NAS. Account Protection works the same way but focuses on individual accounts, blocking users' access to specific accounts.

Certificates from Let's Encrypt or other certificate authorities help secure connections to and from DSM. When you connect to DSM through a web browser, certificates encrypt the information sent between DSM and the browser to prevent any possible information interception.

Security settings can be configured at **Control Panel** > **Security**.

Learn more about firewalls, protection, and certificates.

> **Further reading:**
>
> - Security Measures Quick Start Guide

Secure SignIn

Secure SignIn Service improves the overall security of DSM accounts while offering easy-to-use and flexible login options. With the use of a single-tap prompt (Approve sign-in) or a hardware security key, you can sign in without the fuss of manually typing in the password.

To further safeguard your account, enable the 2-factor authentication option. After entering the password, as the second step of identity verification, select from either one-time verification codes (OTP), Approve sign-in, or hardware security key for a seamless login experience.

Synology offers a mobile authenticator app, **Synology Secure SignIn**, for approving sign-in requests and receiving OTP codes.

Learn more about Sign-In Methods.

Security Advisor

Security Advisor offers a comprehensive security checkup on the system settings of your Synology NAS. It scans for security weaknesses and provides recommendations for you to take action on.

With Security Advisor, you can perform the following security checks to ensure data and system security:

- Detecting and removing malware.

- Checking for password strength.

- Scanning system and related network settings.

- Analyzing suspicious login activities.

- Checking for available DSM and package version updates.

You can run a manual/scheduled system checkup based on a preferred security baseline or customize a checklist to meet your needs. The results can be consolidated into a daily/monthly report by configuring the settings at **Security Advisor** > **Advanced** > **Report Settings**. To receive the reports via email, go to **Control Panel** > **Notification** and enable notifications.

Refer to the Fortify security section for setup instructions.

Learn more about Security Advisor.

Antivirus

Antivirus protects your Synology NAS from malicious threats. You can run a full system scan, scan specific folders, or schedule automatic scan tasks. Virus definitions will be automatically updated to ensure maximum security.

Two antivirus packages are available in the Package Center: Antivirus Essential (free, based on the ClamAV scanning engine) and Antivirus by McAfee (paid service, powered by the McAfee scanning engine).

Learn more about Antivirus Essential and Antivirus by McAfee.

Chapter 9: Network

External Access

If your Synology NAS is located on a private network (e.g., connected to a router as a client), you can configure external access settings to allow your Synology NAS to be accessible from anywhere over the Internet. This section explains the basics regarding three approaches to external access: QuickConnect, DDNS, and port forwarding.

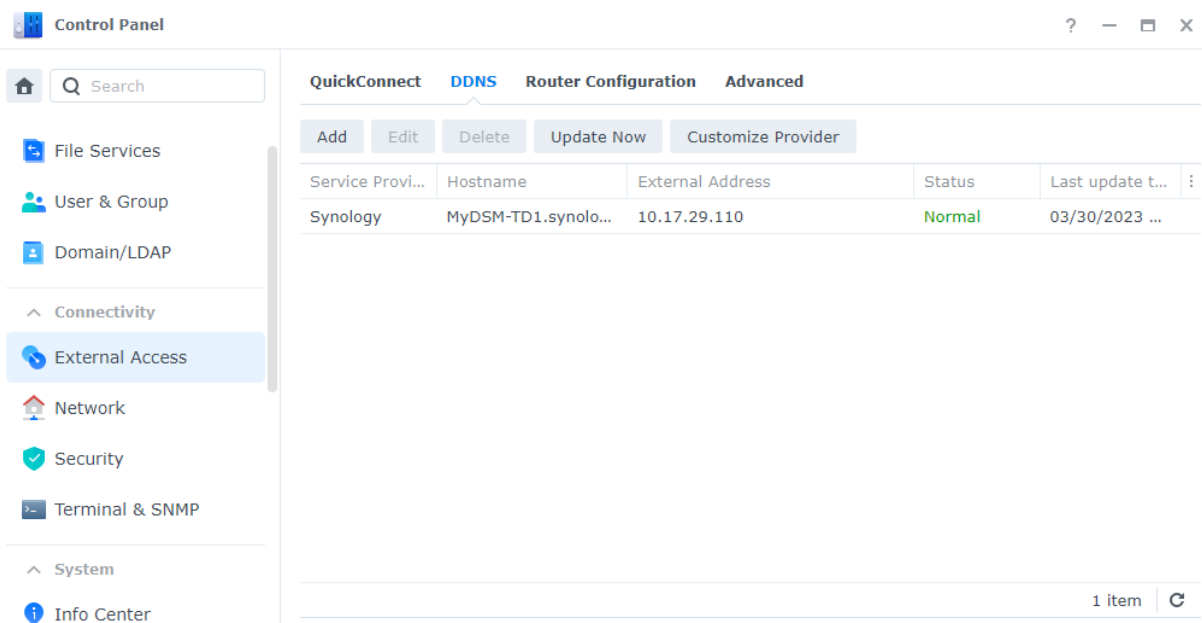Learn how to configure external access for your Synology NAS.

QuickConnect
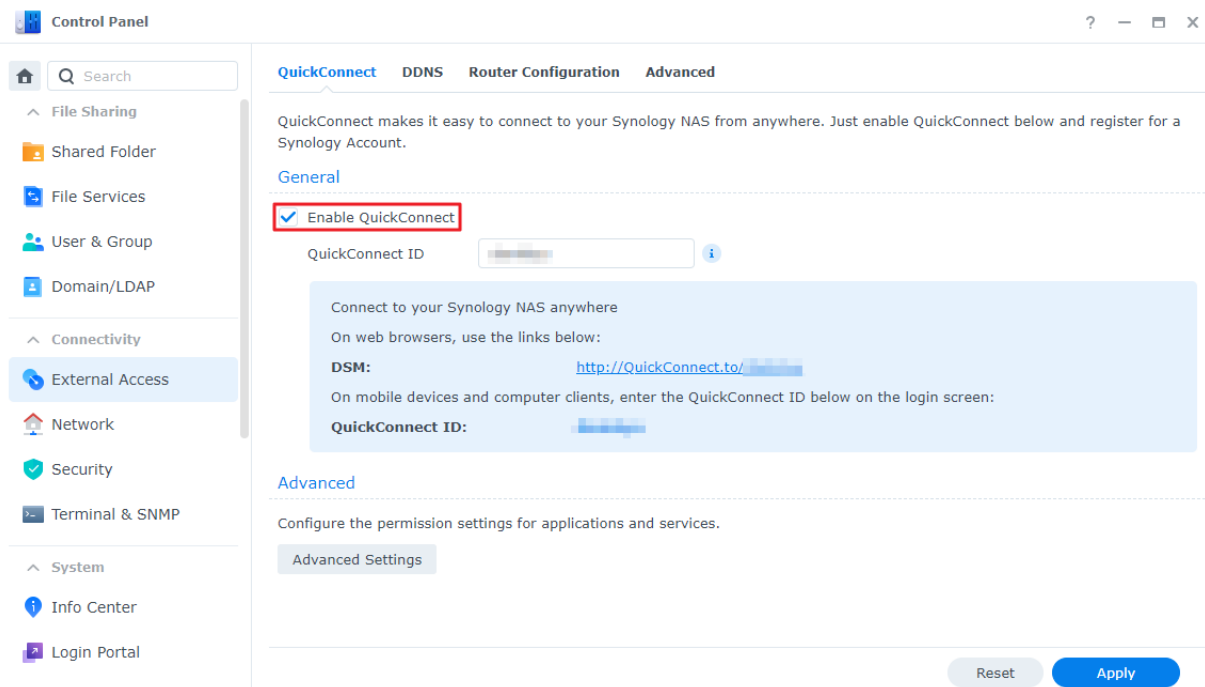
QuickConnect is designed to make connections to your Synology NAS quick and easy from outside of your local network. With a customized QuickConnect ID, you can access your Synology NAS without configuring a static external IP address, or switch between WAN/LAN addresses when your Synology NAS is moved to another location.

QuickConnect can be configured at **Control Panel** > **External Access** > **QuickConnect**. Learn more about QuickConnect.

DDNS

DDNS (Dynamic Domain Name System) is an efficient way to allow external access to your Synology NAS. It simplifies connections to your Synology NAS over the Internet by mapping a hostname to its IP address. For example, you can access your Synology NAS using a DDNS hostname (e.g., "www.john.synology.me") instead of using an IP address (e.g., "10.17.1.1").

DDNS hostnames can be configured at **Control Panel** > **External Access** > **DDNS**.

Learn more about DDNS.

Port forwarding

Port forwarding allows external devices to access resources within a local area network. It works by redirecting network packets from a NAT device (e.g., a router) to the IP address/port

combination of a local device.

Port forwarding rules can be configured at **Control Panel** > **External Access** > **Router Configuration**.

Learn more about [port forwarding mechanisms](#) or how to [set up port forwarding rules](#) in DSM.

> **Further reading:**
> - [What network ports are used by DSM services?](#)
> - Video tutorial: [How to Configure Port Forwarding to Remotely Access Your Synology NAS](#)

Network Settings

In most cases, you can start exploring services on your Synology NAS right after installing DSM without needing to configure network settings. If you do need to customize these settings, go to **Control Panel** > **Network**.
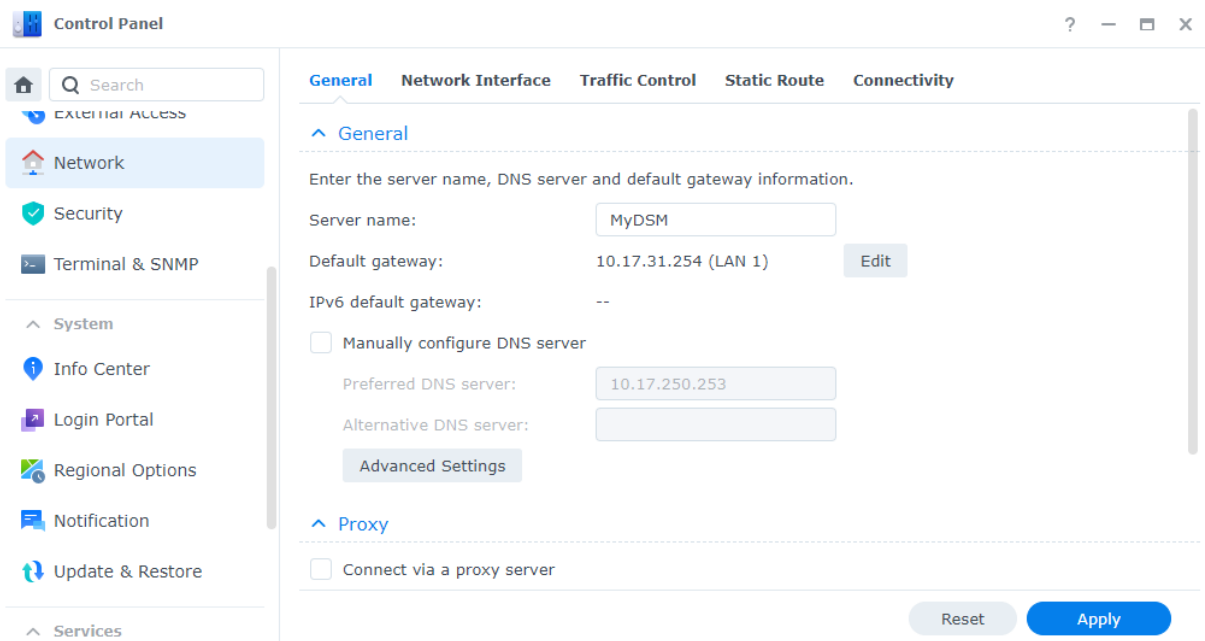

The following list introduces some generic network options available at **Control Panel** > **Network** > **General**:

- **Change the hostname**: A hostname is a unique and absolute label for a device on a network and is used to identify the device during network communication. To edit the hostname of your Synology NAS, enter a new name in the **Server name** field.

- **Assign the default gateway**: A gateway connects multiple different networks so that the data from your Synology NAS can be transmitted to other networks. The default gateway will be the device used if no alternative routes are specified. To assign the default gateway, click the **Edit** button beside **Default gateway** and arrange the priority order of connected gateways.

- **Specify DNS servers**: The Domain Name System (DNS) resolves easy-to-remember Internet addresses to the numeric addresses that Internet-connected devices use. When your Synology NAS connects to a domain name such as "www.synology.com", its DNS server is responsible for querying the site's IP address "210.61.203.200", allowing your Synology NAS to access the website's information. Under the **General** section, you can tick **Manually configure DNS server** and specify a preferred DNS server along with an alternative one.
- **Connect via a proxy server**: A proxy server functions on behalf of client devices to access resources on the Internet. To specify a proxy for your Synology NAS, tick **Connect via a proxy server** under the **Proxy** section, enter the **Address** and **Port**, and then click **Apply**.

Learn more about general network settings.

Manage network interfaces
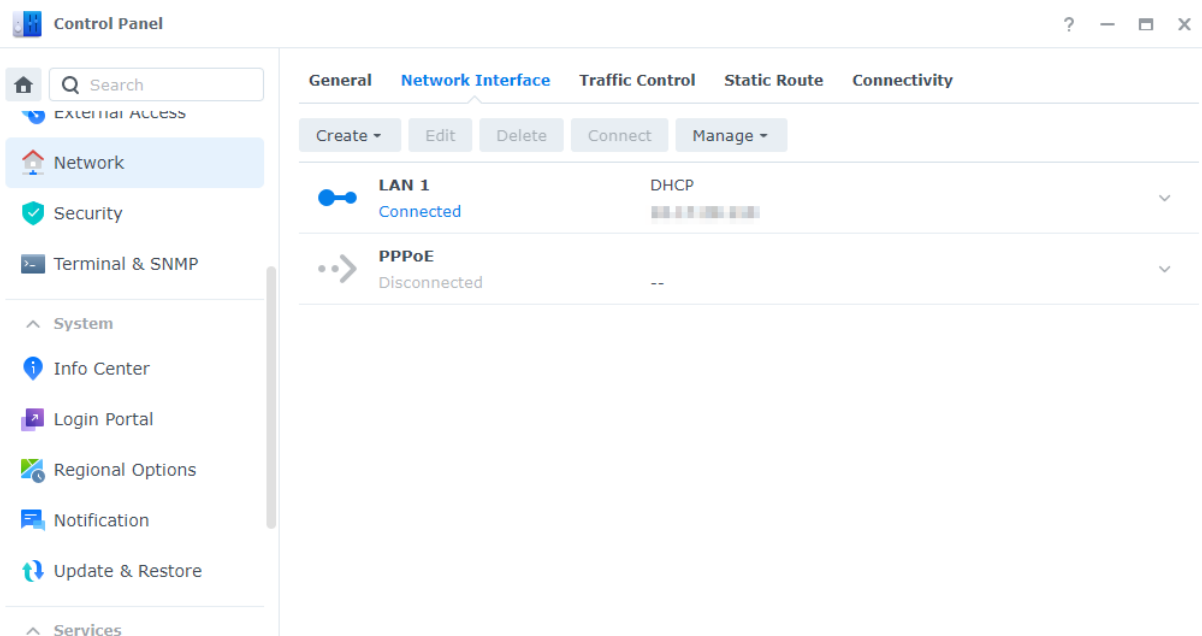
A **network interface** serves as a medium that connects your Synology NAS to local networks or the Internet. The following list provides the three connection types for network interfaces that you can configure at **Control Panel** > **Network** > **Network Interface**:

- **Dynamic IP**: Your Synology NAS will obtain a dynamic IP address automatically from a DHCP (Dynamic Host Configuration Protocol) server (e.g., a router) after DSM has been installed. If you have changed the connection type of Synology NAS, but would like to use dynamic IP mode again, select the specified network interface, click **Edit**, and tick **Get network configuration automatically (DHCP)** on the **IPv4** tab.
- **Static IP**: If you already have some fixed IP addresses, you can adopt this connection type for network interfaces. For enterprise use, we suggest assigning a static IP address to your Synology NAS because this makes it easier for IT administrators to mange. Learn how to set up a static IP address in DSM.
- **PPPoE**: If your Synology NAS connects to the Internet via a DSL or cable modem and you have purchased a PPPoE (Point to Point Protocol over Ethernet) service from your ISP, you can

adopt this connection type to allow your NAS to directly connect to the Internet without a router. Learn how to enable PPPoE connections in DSM.

At **Control Panel** > **Network** > **Network Interface**, you can configure more settings related to the network interfaces of your Synology NAS, including IPv6 connections, VPN client settings, and Link Aggregation. The following sections will briefly introduce these options and guide you on their configurations.

Set up IPv6 connections

Besides connections to the Internet via the **IPv4 protocol**, DSM also supports IPv6 address structure through the following two strategies (they can be adopted simultaneously):

- **Dual stack**: An IPv4/IPv6 dual-stack configuration lets you configure your Synology NAS with both an IPv4 and an IPv6 address. Use this approach to access resources across IPv4 and IPv6 network environments.
- **Tunneling**: Tunneling involves transmitting one protocol inside another through encapsulation. This method allows your Synology NAS to encapsulate IPv6 packets in IPv4 packets and send them across IPv4 networks.

Learn more about IPv6-integrated network interfaces.

> **Further reading:**
>
> - What services on Synology NAS support IPv6?

Turn your Synology NAS into a VPN client

A **VPN (Virtual Private Network)** service allows you to access resources confidentially through your private network, no matter where you are. VPNs can also be used to safeguard the network connections of your Synology NAS via encrypted tunnels.

With DSM, you can easily connect to a VPN server with your Synology NAS via PPTP, OpenVPN, or L2TP/IPSec protocols. If multiple VPN sources are available, you can also switch between different servers by using VPN profiles.

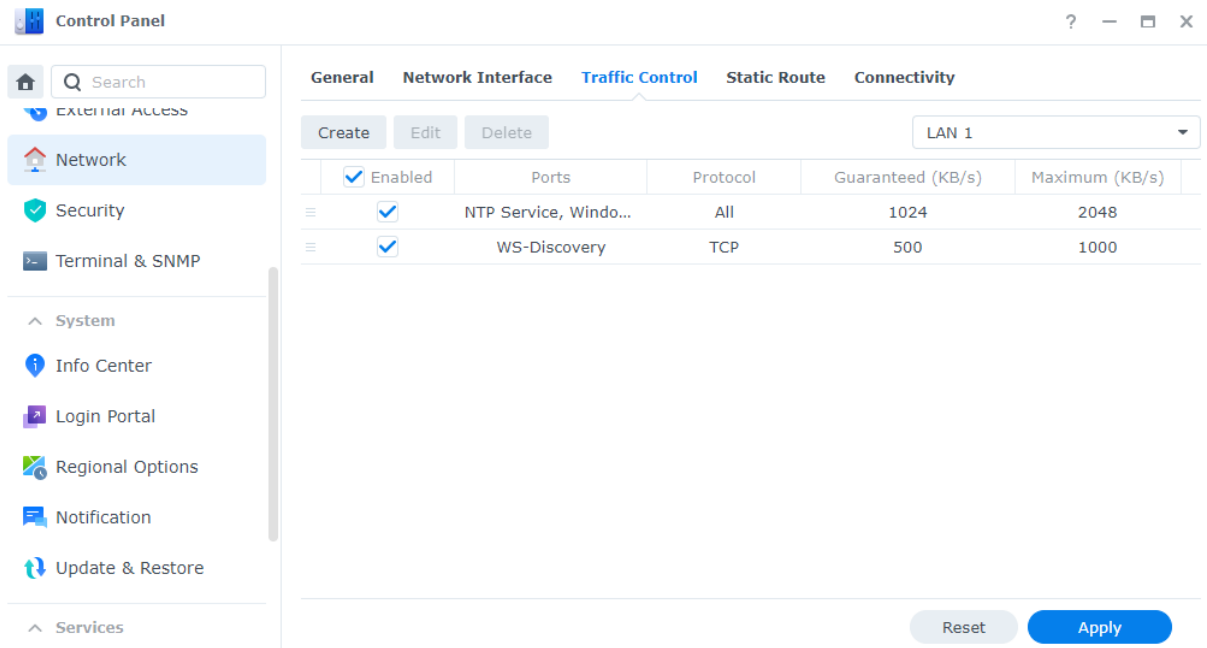Learn how to create VPN profiles in DSM.

Combine LANs with Link Aggregation

Link Aggregation increases the bandwidth of your Synology NAS by aggregating multiple network interfaces and provides traffic failover to ensure uninterrupted network connections.

Learn how to combine multiple LANs with Link Aggregation.

Control network traffic

At **Control Panel** > **Network** > **Traffic Control**, you can control the outbound network traffic of DSM services to prevent latency, congestion, and packet loss. If you want to limit the traffic of a specific service, you can specify its guaranteed and maximum bandwidths on this page.

Learn how to create a traffic control rule.

Configure static routes

At **Control Panel** > **Network** > **Static Route**, you can add static routes to the routing table in DSM.

By doing so, service traffic on your DSM can be transmitted via different paths according to network destinations, which improves the routing efficiency of gateway devices in your network environment.

Learn how to set up static routing.

Proxy Server
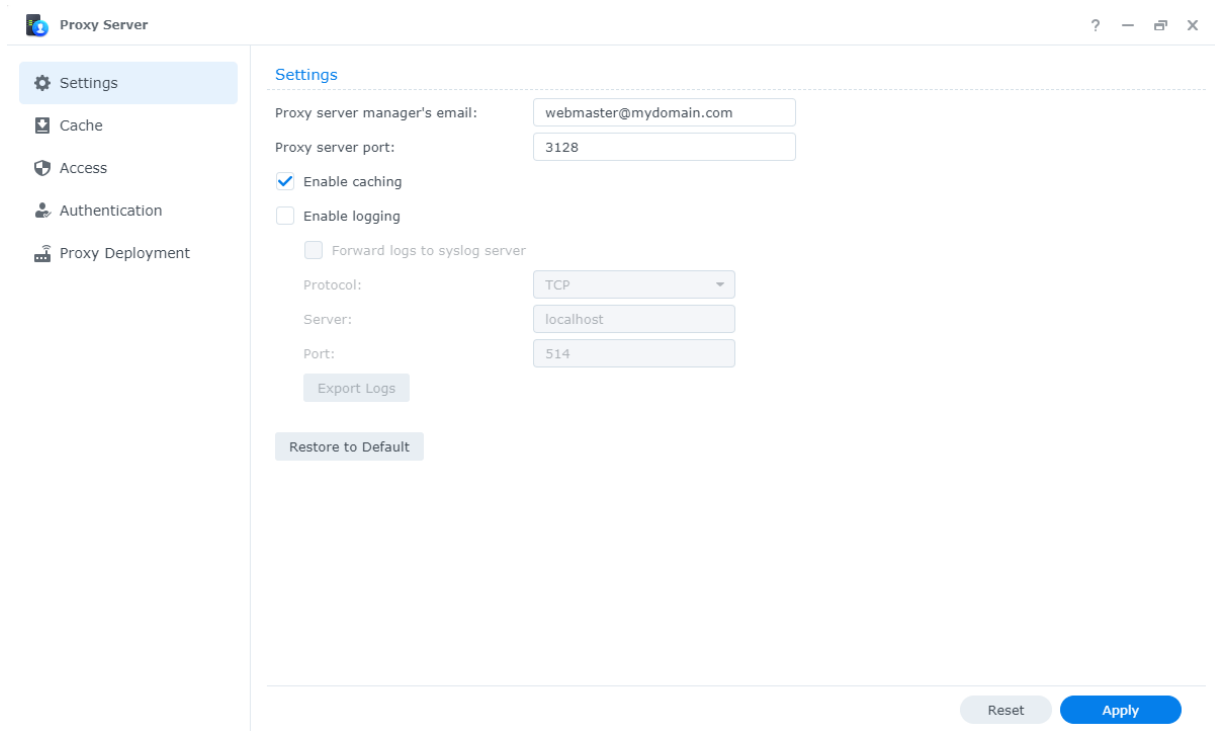
A **proxy server** acts as a gateway that forwards web requests and data between clients on your network and servers on the internet.

You can use a proxy server as a firewall, to filter web traffic, to manage shared network connections, and to speed up responses for common web requests.
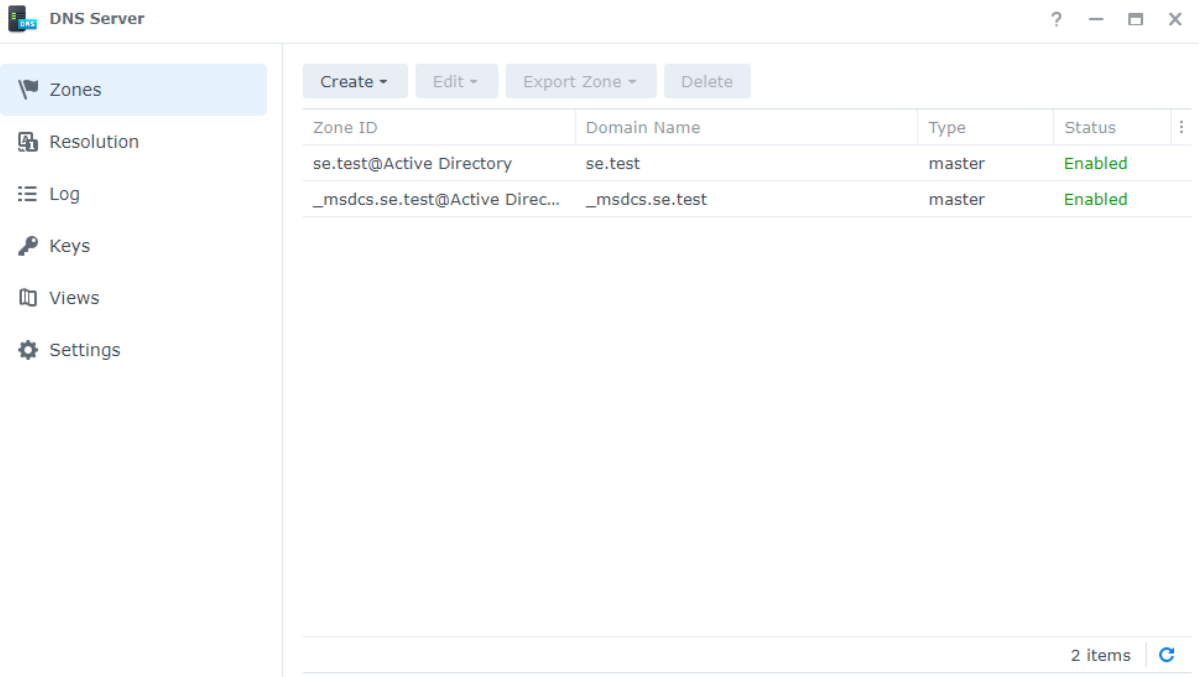
Proxy Server can be downloaded and installed from the Package Center.

Learn more about proxy servers.

> **Further reading:**
>
> - To learn how to connect your Synology NAS via a proxy server, refer to Connecting via Proxy Server.

DNS Server

DNS (Domain Name System) is an address book of the Internet. It maps meaningful names (i.e., domain names such as "www.synology.com") into IP addresses (e.g., "210.61.203.220"), allowing users to easily access web pages, computers, or other resources across networks.

In DSM, DNS services can be set up via **DNS Server**. This package is recommended for website hosting and is necessary for Active Directory domain services.

DNS Server includes the following features:

- **Primary and secondary zones**: The DNS boundaries that allow granular control of DNS components. You can store DNS information in one primary zone (containing a read/write copy of data) and multiple secondary zones (containing read-only copies of data) to ensure the high availability of DNS service.

- **DNS forwarding**: An alternative method of DNS resolution that will be used when DNS Server cannot find matching IP addresses in your zones.

- **TSIG keys**: Safeguard the synchronization of your DNS files with encryption.

- **Split-horizon DNS**: A function that provides each client with customized DNS information. This helps improve the security and privacy management of DNS zone records.

Learn more about DNS servers.

> **Further reading:**
>
> - How do I set up a DNS server on my Synology NAS?

DHCP Server
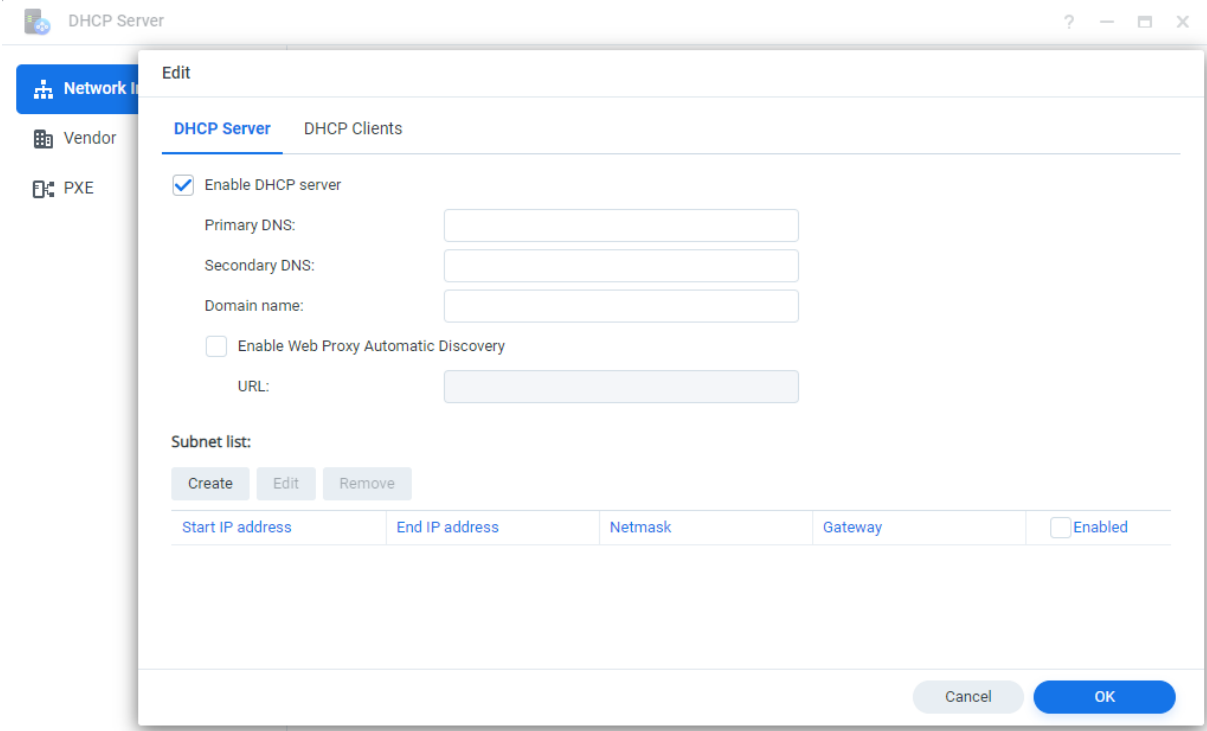
A **DHCP server** automatically assigns IP addresses and network parameters (e.g., subnet mask, DNS server, etc.) to client devices located within the same local area network. By doing so, the administrator does not need to manually configure the network settings for each client device.

Learn more about DHCP servers.

VPN Server
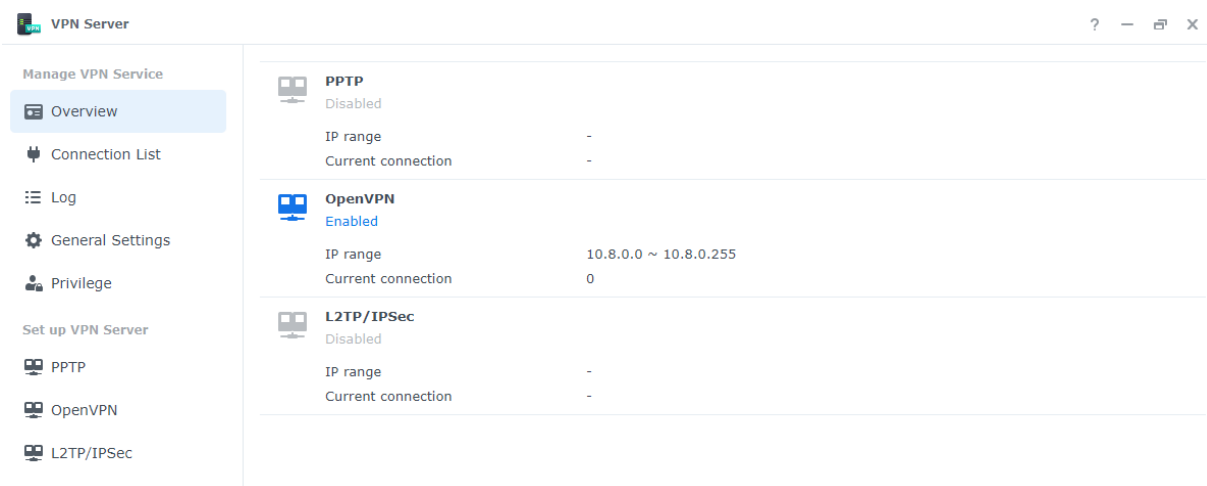
You can turn your Synology NAS into a **VPN (Virtual Private Network)** server, allowing DSM users to securely connect to the local area network that the Synology NAS belongs to no matter where they are.

Supported VPN protocols:

- **L2TP/IPSec**: A combination of protocols that offers secure VPN connections and is supported by most clients (such as Windows, Mac, Linux, and mobile devices).

- **OpenVPN**: An open-source protocol for reliable and secure VPN connections. This protocol protects VPN connections with SSL/TLS encryption.

- **PPTP**: An older VPN protocol supported by most clients, including Windows, Mac, Linux, and Android devices.

Learn how to set up VPN services.

> **Further reading:**
> - How do I connect to Synology's VPN Server via Windows PC?
> - How do I connect to Synology's VPN Server via Mac?
> - How do I connect to Synology's VPN Server via an Android device?
> - How do I connect to Synology's VPN Server via an iOS device?
> - Frequently asked questions regarding VPN services on Synology NAS

Chapter 10: Management

Hardware & Power Settings
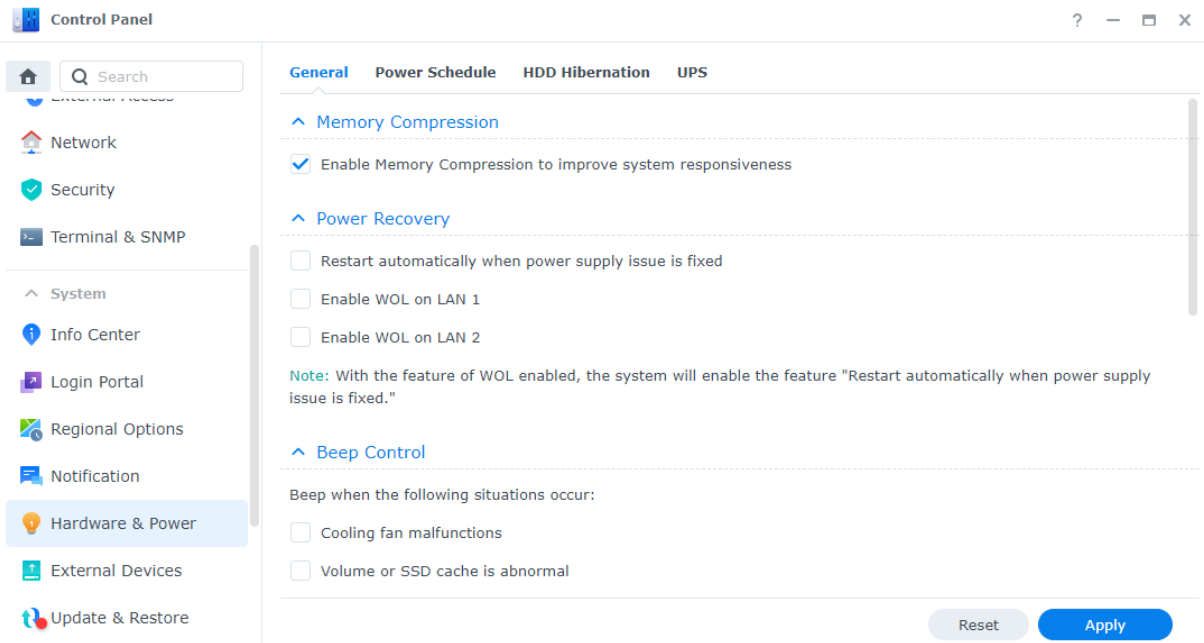
Hardware Settings

General hardware settings of your Synology NAS can be configured at **Control Panel** > **Hardware & Power** > **General**, including the following:

- Memory Compression
- Power Recovery
- Beep Control
- Fan Speed Mode

Power Settings

The power settings of your Synology NAS can be configured at **Control Panel** > **Hardware & Power** under the following tabs:

- **Power Schedule**: Specify a time for DSM to automatically start up and shut down.
- **HDD Hibernation**: Specify the idle time before drives enter hibernation. This function helps you limit power consumption and extend the lifespans of your drives.
- **UPS**: Enable UPS support to extend the operation of your Synology NAS upon an unexpected power outage. This will give DSM enough time to execute a normal shutdown.

61
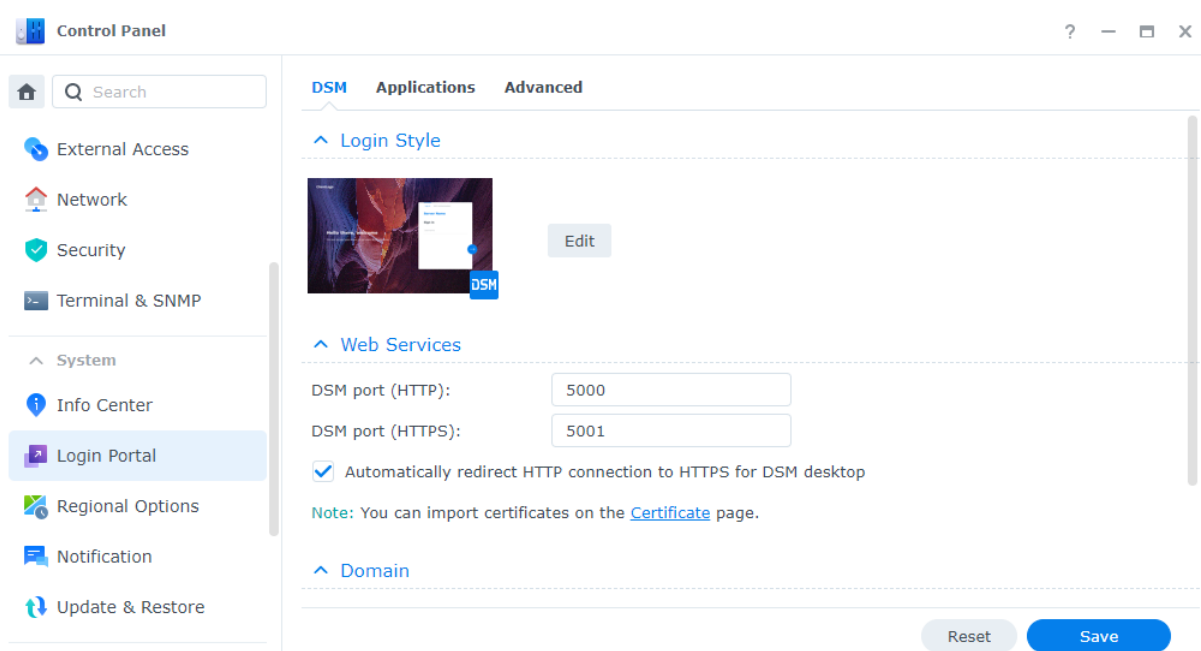
Login Portal

You can customize the login web portals for DSM and various applications (e.g., File Station), change their login background and appearance, and manage network settings at **Control Panel** > **Login Portal**.

The HTTP/HTTPS port, domain name, and alias for your DSM or applications can be customized. This allows users to access your NAS via custom URLs. For example, instead of launching an application after users sign in to DSM, a custom URL takes them to the application interface directly. This not only allows for quick logins when running specific applications, but it also lets you grant other users the permission to access certain applications on your DSM.

Network settings management helps ensure the security of your Synology NAS. Configuring access control rules restricts users of denied IP addresses from accessing your Synology NAS, whereas configuring reverse proxy rules allows trusted users from sensitive ports to access your Synology NAS.

Learn more about Login Portal.

Resource Monitor

Monitor the CPU usage, memory usage, disk utilization, and network flow of your Synology NAS in real-time using the built-in **Resource Monitor**.

You can view historical data to compare system usage over a specific period and customize performance alarms to promptly notify you of resource anomalies.

Managing the services running on your DSM and the users connected to your Synology NAS can help ensure optimal system performance and control memory usage. For example, you can stop services that have reached pre-configured speed limits from transferring files, force users to sign out of DSM, or stop connected users from accessing data on your NAS.

Learn more about Resource Monitor.

Log Center

Log Center centralizes the management of system logs. You can configure notification settings to inform administrators when certain events occur.
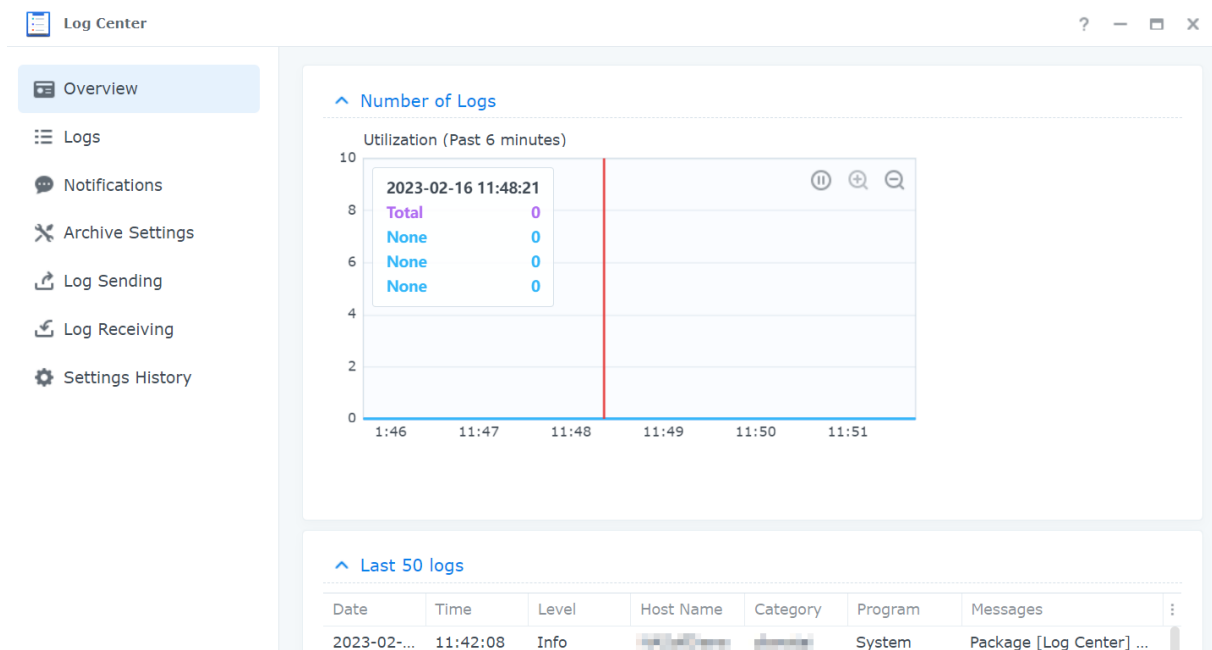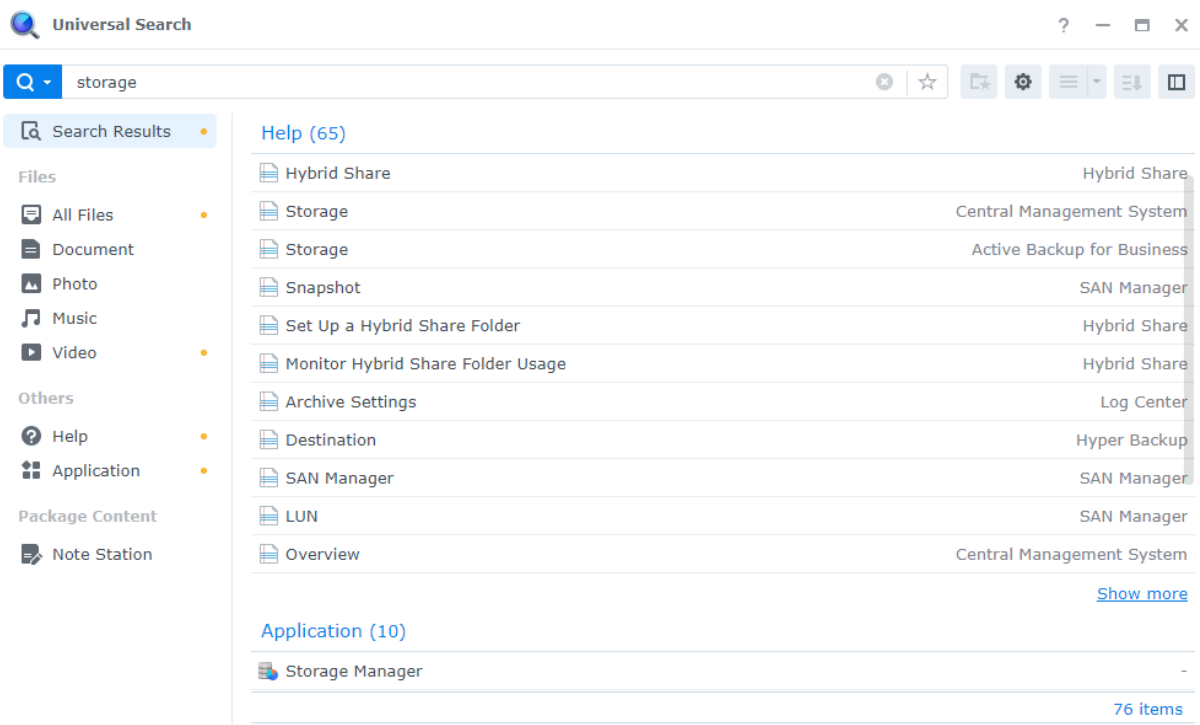

Log Center is activated by default when DSM is set up. For advanced features, such as remote log transfer and log archiving, you can install the **Log Center** package from the **Package Center**.

To learn how to use Log Center, refer to the following articles:

- Log Center (built-in function)
- Log Center (add-on package)

Universal Search

Using **Universal Search**, perform keyword searches or advanced searches in the search box to find applications, folders, and files on your Synology NAS in just a few clicks. You can index folders or file contents for fast and accurate searches, manage searches by marking your favorite searches, specify a maximum number of search records, and more.

Universal Search covers the following items:

- Files (including images, music, and videos) in indexed folders
- Package-specific files:
    - Notes in Note Station
    - Spreadsheets and documents in Synology Office
- Offline DSM Help documents
- Applications

Learn more about Universal Search.

Central Management System
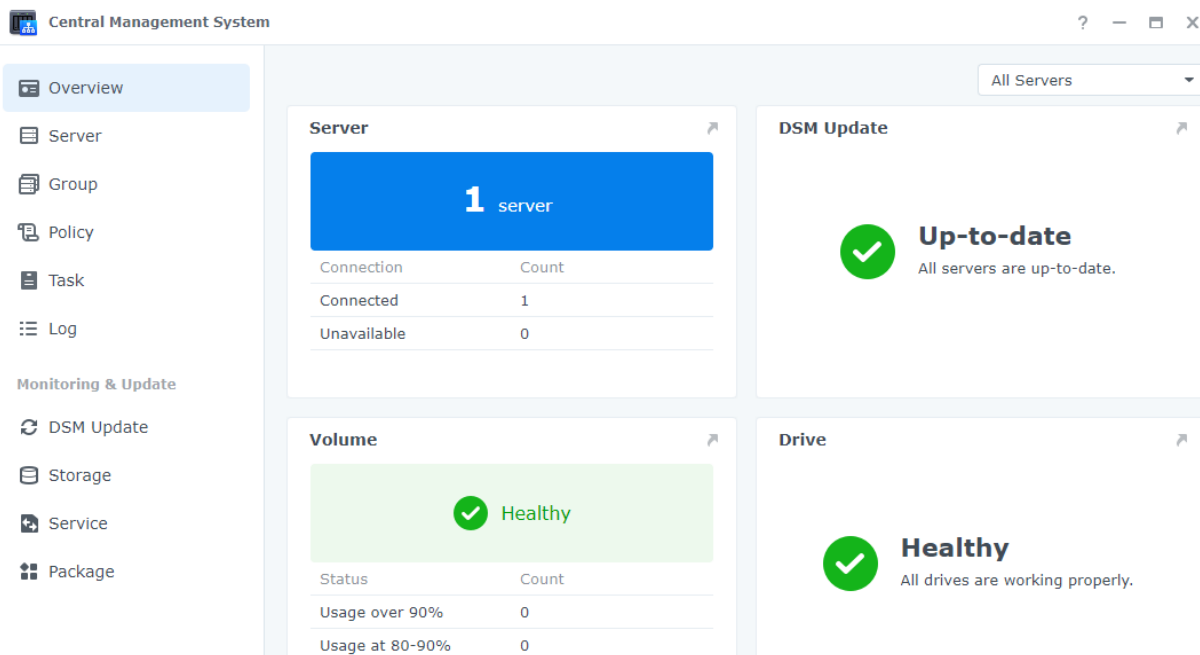
With **Central Management System**, you can centrally and simultaneously manage multiple Synology NAS by designating a NAS as a host server and other NAS as managed servers. On the host server, IT admins responsible for the mass deployment of multiple NAS can apply policies (e.g., enable traffic control and firewall) to managed servers and run tasks (e.g., enable Wake on LAN) or customized scripts (e.g., create users or install packages) on these servers. This ensures that configurations across all servers are the same and simplifies management.

On the unified dashboard, you can monitor the overall information (e.g., connection status and storage usage) of the managed servers, delegate administrator permissions to specific users or groups, install DSM versions and packages, perform updates on managed servers, and more.

Learn more about Central Management System.

Active Insight

Synology **Active Insight** is a cloud-based service that provides real-time system monitoring for your Synology NAS. Active Insight helps with the maintenance of your NAS through the following services:

- **Cloud monitoring**: This service continuously monitors the health, performance, backup tasks, and access activities of your Synology NAS. It displays the top-rated NAS for each performance metric/topic so that you can quickly recognize abnormalities from unexpected high values.

- **Centralized management**: Through a dedicated web portal, Active Insight provides an informative overview of all your Synology NAS devices and actively checks update availability. This can help lighten the workload of your IT personnel since they won't have to check up on each Synology NAS and everything can be seen in one central location.

- **Self-service troubleshooting**: When a system abnormality occurs, Active Insight will deliver a notification by email and a push notification in the mobile app with detailed troubleshooting advice. Following the provided steps will reduce the time needed to find the cause of abnormal events.

You can enable Synology Active Insight in DSM.

Learn how to use Active Insight on your Synology NAS.

System reset

You can reset DSM to its factory default settings at **Control Panel** > **Update & Restore** > **System Reset**. All user data and system configurations will be deleted and DSM will be restored to its default settings.

Learn how to reset DSM.

Chapter 11: Productivity

Synology Office

Synology Office is a suite of tools that allows for interactive collaboration in real-time. With Synology **Document**, **Spreadsheet**, and **Slides**, you can use editing tools to create, edit, and share your work and ideas. Because all work files are saved online, they can be accessed anytime, anywhere using different devices, including computers, mobiles, and tablets.

Your sensitive documents in Synology Office can be protected using file encryption. Additionally, when Synology Chat is installed on the same Synology NAS, it allows for instant and interactive collaboration at your fingertips.

Learn more about Synology Office.

> **Further reading:**
> - What types of files can I import into Synology Office?
> - How do I import files on my Synology NAS into Synology Office?
> - Synology Chat Plugin

Note Station

Note Station is a note-keeping application that allows you to add, view, manage, and share your content-rich notes. For every note you take, you can easily add elements such as reference links or audio recordings. You can also save clipped texts/graphics using Synology Web Clipper in your Chrome browser. Easily manage your notes by grouping them by tags or categorizing them into notebooks or shelves.

Note Station is available in web browsers, as a desktop utility, and in mobile app formats. Learn more about Note Station.

> **Further reading:**
> - How can I enhance my personal productivity in Note Station?

Synology Chat

Synology Chat is an instant messaging service that can be set up for both personal and workplace communication. You can send one-on-one messages, encrypt messages for privacy, or create channels for group discussions.

In **Synology Chat Admin Console**, administrators can manage channel settings, set content deletion interval, and view logs. The Synology Chat web portal offers various features to help increase efficiency, including pinning messages, bookmarks, scheduling messages, reminders, and chatbots.

The service can be integrated with **Synology Office**, **Synology Drive**, and **Synology Calendar** to enhance workplace collaboration. For example, users can send messages, view conversations, or link folders to a Chat channel when using Synology Office without having to switch windows.

Synology Chat is available in web browsers, as a desktop utility, and in mobile app formats. Learn more about Synology Chat Server.

> **Further reading:**
> - Synology Chat Quick Start Guide for Administrators
> - Synology Chat Quick Start Guide for Users

Synology Calendar

With **Synology Calendar**, you can set up personal calendars and share them with others. You can create events and edit their details, including descriptions, time, location, and alerts, as well as share and invite guests.

Advanced management options are available, such as repeating events, adding event colors, attaching files to events, editing guest lists, switching between calendars, and exporting calendars. Additionally, when Synology Calendar is installed on the same Synology NAS as **Synology MailPlus**, information sync across services is available.

Learn more about Synology Calendar.

> **Further reading:**
> - How do I import calendars from WebDAV Server to Synology Calendar?

Synology Contacts

With **Synology Contacts**, you can create contacts, personalize labels for identification, and share address books with members of your organization. The default group address book, **Team**

Contacts, will automatically include all users from the selected account system (local, domain, or LDAP users), reducing the need for manual effort.

Additionally, Synology Contacts can serve as a contact management add-on for **Synology MailPlus** when they are installed on the same Synology NAS. It can suggest email recipients when sending emails through Synology MailPlus.

Learn more about Synology Contacts.

> **Further reading:**
> - Synology Contacts Quick Start Guide for Administrators
> - Synology Contacts Quick Start Guide for Users
> - How do I import contacts from a CardDAV server to Synology Contacts?
> - How do I sync Synology Contacts with CardDAV clients?

Synology MailPlus

With **Synology MailPlus**, you can host a privately owned mail service on your Synology NAS. The MailPlus suite consists of the following two packages: **Synology MailPlus Server** and **Synology MailPlus**.

Synology MailPlus Server

Synology MailPlus Server is an administration console where you can centrally manage and monitor your mail server. It includes the following key features:

- **Flexible anti-spam and antivirus protection**: MailPlus Server offers a variety of security engines for your choice, including free open-source options like Rspamd and ClamAV, as well as paid third-party options like McAfee and Bitdefender. You can customize the auto-learning, DNSBL, and quarantine settings to tailor the protection to your needs.

- **Full-fledged authentication**: The following mail authentication protocols are supported by MailPlus Server to block fraudulent messages and protect against identity theft: SPF, DKIM, DMARC, and DANE.

- **Multiple domain management**: MailPlus Server allows the setup of multiple domains at no extra cost. You can customize the following settings for each domain: aliases, auto BCC, usage limits, and disclaimers.

- **MailPlus high-availability**: Two Synology NAS can form a high-availability cluster to prevent service disruptions caused by server malfunctions or overloads. The cluster will perform two-way synchronization to keep mail data consistent between both servers, reducing the risk of data loss and minimizing server downtime.

Synology MailPlus

Synology MailPlus is a versatile online mail client that works with all popular web browsers. It includes the following key features:

- **Email, calendar, and contact integration**: With Synology MailPlus, Synology Calendar, and Synology Contacts running on the same Synology NAS, data can be synchronized across different services. For example, mail content can be added to Synology Calendar as an event, while Synology Contacts can provide recipient suggestions for Synology MailPlus.

- **Shared mailbox**: A personal mailbox can be shared with other internal users to collaborate and keep track of projects together.

- **Custom mail filter**: Multiple filter rules can be set up to automatically apply labels or move certain emails to a specific mailbox, streamlining mail management.

- **Block and allow lists**: Emails from specific senders can be filtered by adding their email addresses or domains to the personal block or allow lists.

Learn how to set up a mail server with Synology MailPlus.

> **Further reading:**
>
> - How do I best deploy Synology MailPlus and select a suitable Synology NAS?
> - Synology MailPlus Quick Start Guide for administrators
> - Synology MailPlus Quick Start Guide for users
> - Frequently asked questions about Synology MailPlus
> - Synology MailPlus documents

Web Station
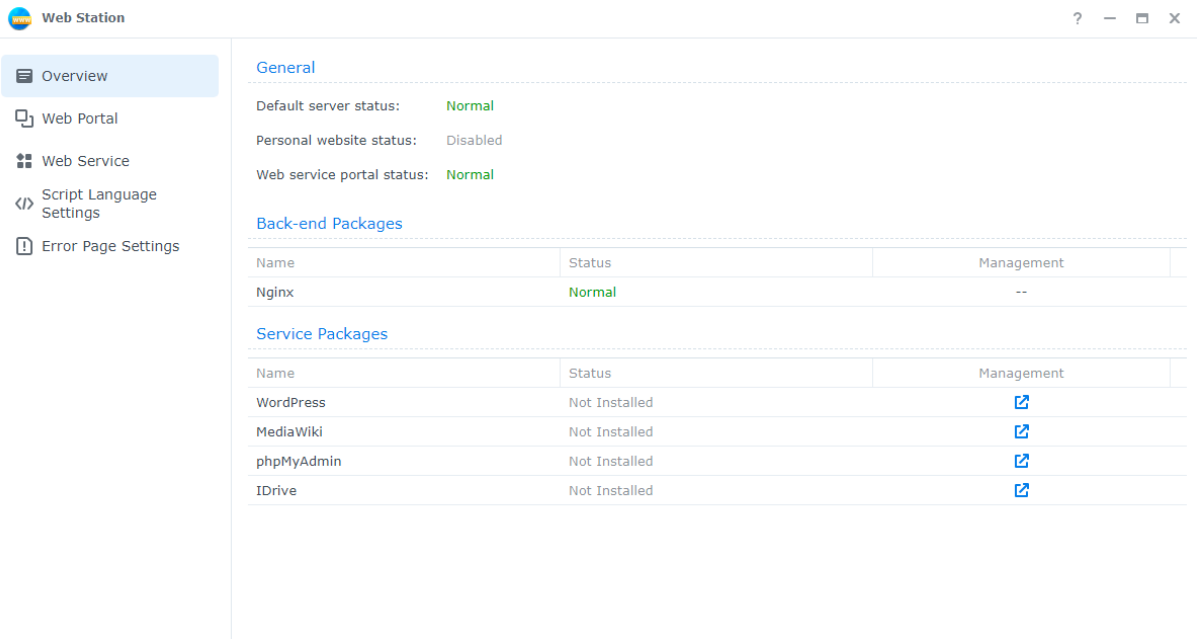
Web Station allows you to host websites on Synology NAS. With support for PHP, MySQL, Nginx, Apache HTTP Server, containerized services, and a variety of third-party packages, you can manage dynamic and database-driven web entrances for your personal or business needs.

The following features make website management flexible and easy:

- **Web service**: You can create multiple static websites and various other types of websites for your personal use or business.

- **Web portal**: You can assign each local, domain, and LDAP user an independent web portal, which allows them to host their own website.

- **Script language settings:** You can define profiles for PHP and Python environments.

- **Error pages settings:** You can define profiles for error pages of websites.

Learn more about Web Station.

> **Further reading:**
>
> - How do I host a website on my Synology NAS?
>
> - How should I set access permissions to folders used for hosting websites?

Chapter 12: Multimedia

DSM's multimedia applications allow everyone to smart-manage their photos, organize videos, and enjoy music anytime, anywhere. This chapter highlights some of the key features that allow you to enjoy entertainment content on your Synology NAS.

Synology Photos

Synology Photos collects and displays photos and videos saved on your Synology NAS. With its flexible arrangement options and detailed share settings, users can tailor photo management to their liking.
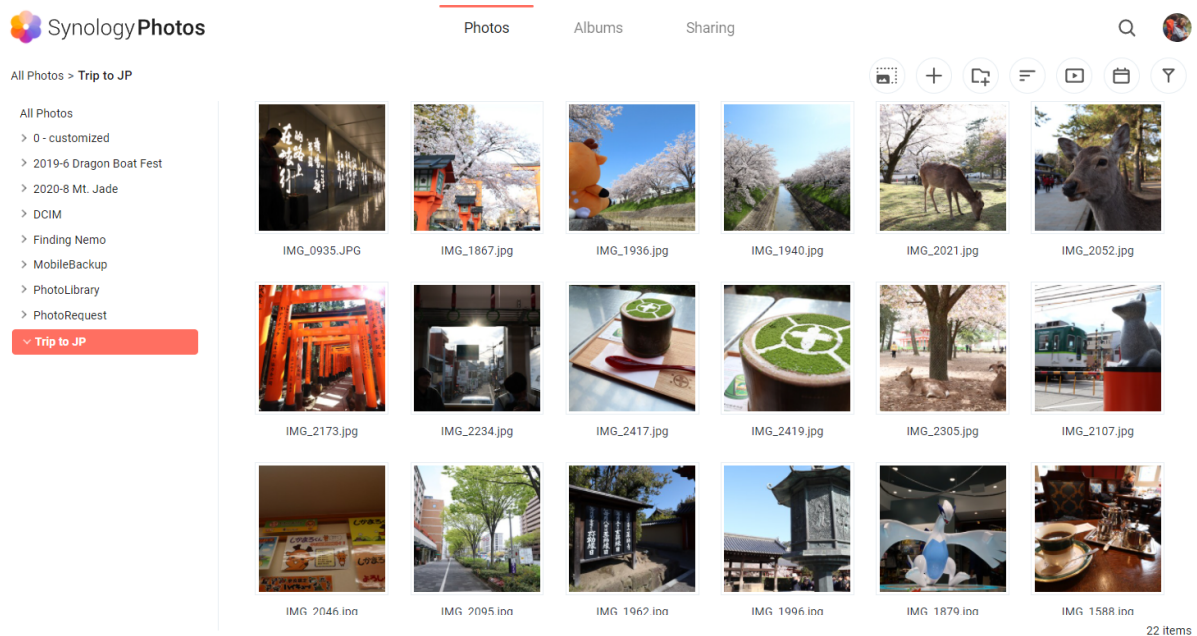
Each tab of Synology Photos represents one key feature:

- **Photos** allows users to manage photos and videos with folders. Users can choose to operate alone in their Personal Space or open up Shared Space and invite others to work together.

- **Albums** are virtual, and allows users to create different collections of their photos without taking up extra storage space.

- **Sharing** lists the albums shared to the user and shared with others.

The Synology Photos mobile application is available on iOS and Android, and is built for effortless browsing, organizing, and back up. You can also view photos on the big screen via Synology Photos TV app, available on Apple TV and Android TV, or by casting through AirPlay or Google Chromecast.

Learn more about using Synology Photos on web browsers and mobile devices.

Video Station

Organize your video collections with **Video Station**. Manage movies, TV shows, or home videos on your Synology NAS and stream them to various devices, including computers, DLNA/UPnP-compliant DMAs, AirPlay devices, and mobile devices.

Learn more about Video Station.

Audio Station

Centralize your music collections with **Audio Station**. You can access music on your NAS using a web browser or mobile device, or stream it to various devices for playback.

Learn more about Audio Station.

Media Server

Turn your Synology NAS into a multimedia server. With **Media Server**, you can stream multimedia content from your Synology NAS to DLNA/UPnP-compliant DMAs (e.g., stereo systems, TV sets, or gaming consoles). By connecting these devices to your home network, you can view photos, listen to music, and watch videos without installing any applications or devices on them.

Learn more about Media Server.

Indexing Service

The indexing service provides a way to automatically scan and index multimedia files from specified shared folders in File Station. Once indexed, these files will be accessible from your DMAs and will be displayed in multimedia packages, including Synology Photos, Video Station, Audio Station, and Media Server.

By default, new files in the photo, music, and video folders are automatically indexed. To create an indexed folder, go to **Control Panel** > **Indexing Service**. On this page, you can edit/remove indexed folders, set the thumbnail quality for photos and videos, or manage conversion settings for videos.

Learn more about the indexing service in DSM.

> **Notes:**
>
> - Mounted shared folders from remote servers cannot be added as indexed folders.
>
> - You can add up to 100 indexed folders on your Synology NAS.

Advanced Media Extensions

Equip packages a better file browsing experience for particular formats. With Advanced Media Extensions, packages such as Audio Station, Surveillance Station, Synology Photos, and Video Station may have the ability to view High-Efficiency Video Coding (HEVC) files stored on Synology NAS.

To learn more about Advanced Media Extensions, refer to its software specifications.

Chapter 13: Surveillance

Surveillance Station is a professional security solution that can adapt to different environments. The clean web interface and extensive device support let you watch live feeds and recordings, receive instant alerts, and operate a multi-site surveillance system. For security management on the go, download the dedicated mobile app, DS cam.

> **Further reading:**
>
> - [Surveillance Station Quick Start Guide](#)
> - [Surveillance Station documents](#)

IP Camera

The Synology Camera series provides exclusive analytics and image adjustment features. It is the choice for users who are looking for a one-site solution that can grow with their needs. You can also choose from the 8,300 compatible 3rd party cameras including PTZ, fisheye, multi-lens, and other specialized models.

Based on your deployment, when adding cameras, choose between auto-discovering devices in the network and manually entering the IP address or IP range. To add cameras in batch, copy the settings of existing cameras or import a pre-filled .xlsx list or configuration file.

Video recording can be scheduled or triggered by events so that only valuable videos take up storage space.
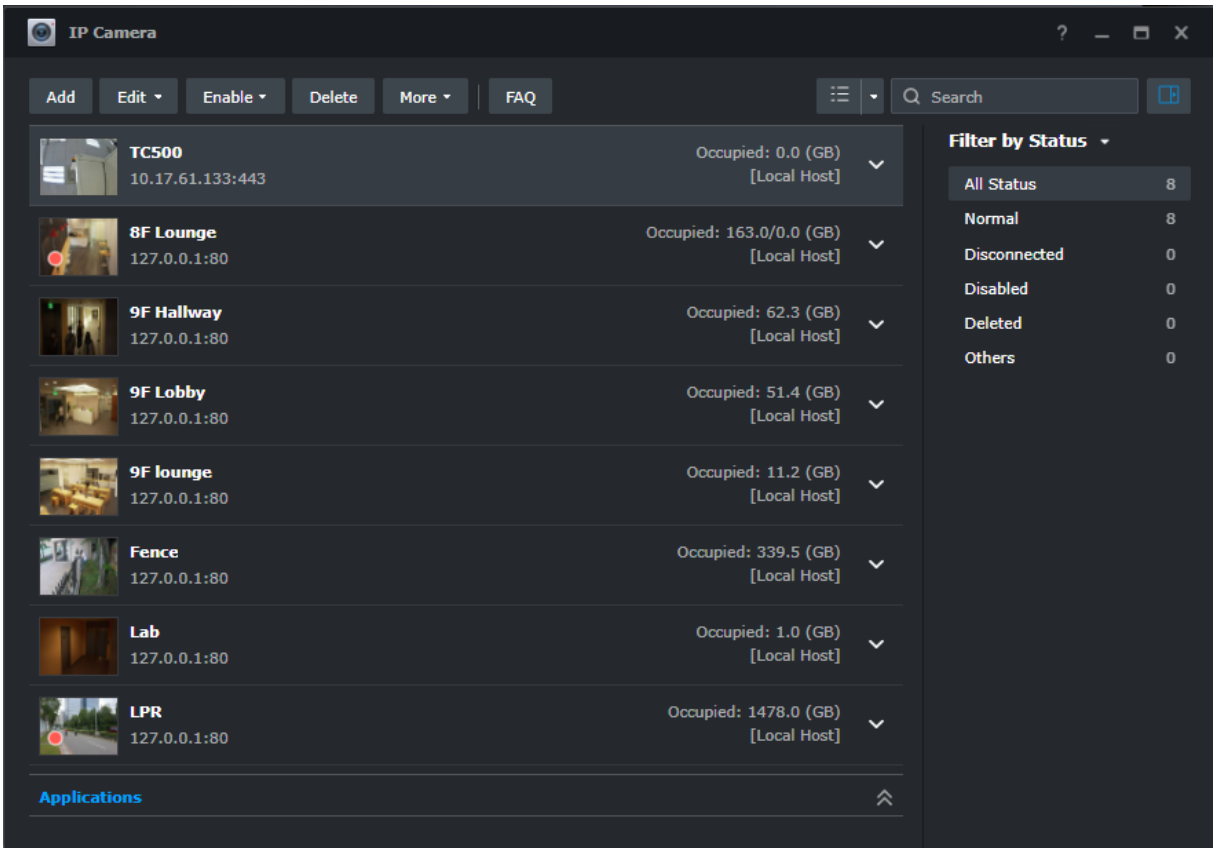
Monitor Center

Monitor Center is where you watch camera feeds, both live and recorded. Simply drag-and-drop items to customize layouts and monitor up to 100 channels. You can directly operate cameras and trigger I/O devices, find and play specific recordings with the timeline, and check the alert panel to track all unusual movements.
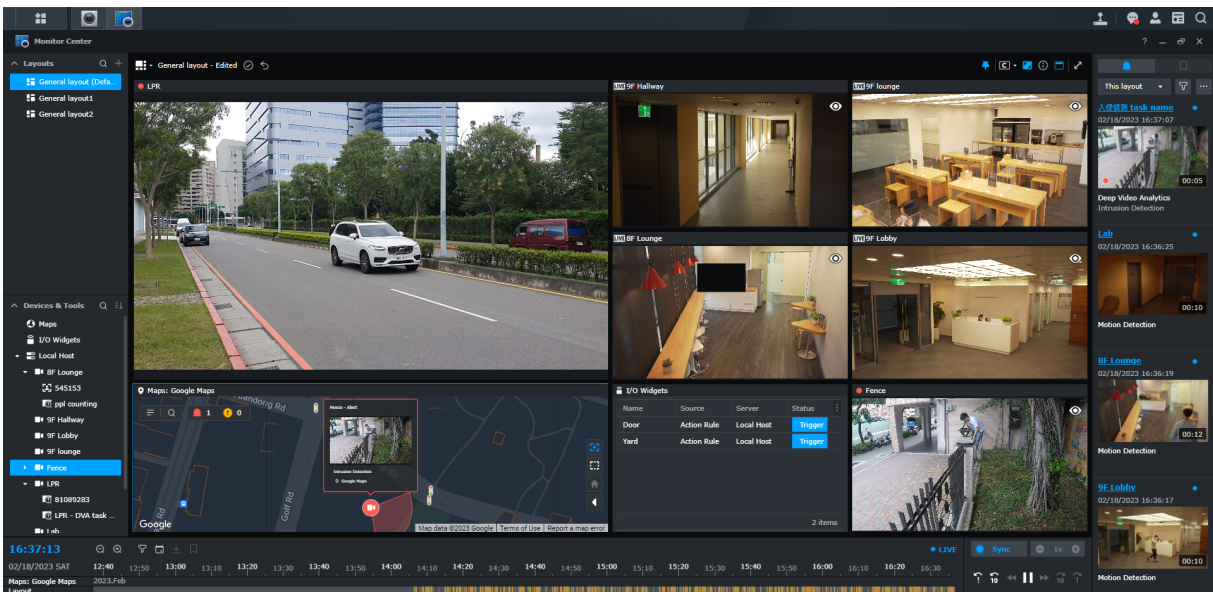
Recording

The **Recording** application saves recordings, event results, and bookmarks separately. You can configure the recording storage, set up independent retention rules for recordings and event results, and download with a customized time range and watermark. Simply click on the thumbnails in any application for playback.
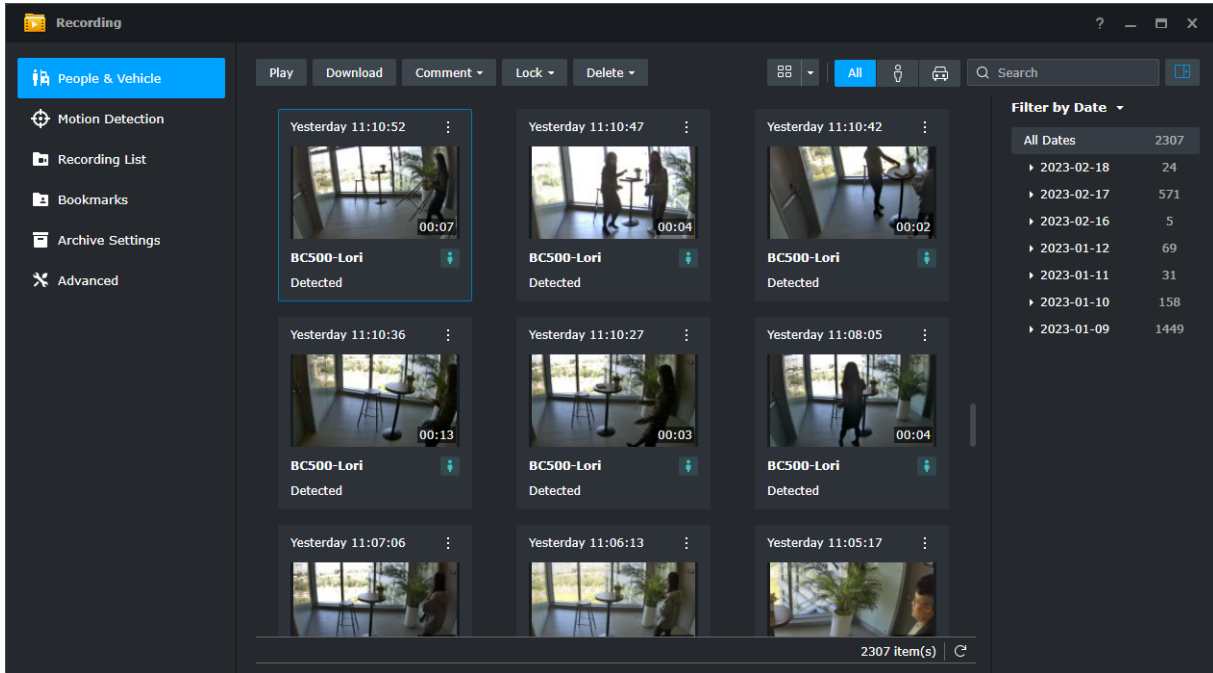
Comprehensive Management Features

Administrators can extend their management beyond IP cameras and recordings. For instance:

- Action Rules automate a series of surveillance functions according to set rules, such as setting schedules for your cameras to patrol.

- Privilege Profiles grant users with different administrative Manager/Spectator permissions to Surveillance Station applications.

- System logs provide a full record of Surveillance Station activities while event logs list detected events.

- Notifications can be customized to send instant alerts to security personnel.

Centralized Management System

Surveillance Station **Centralized Management System (CMS)** allows you to host a multi-site and multi-server surveillance system. With a single portal, you can update remote servers, manage their applications, view and operate cameras and recordings, and migrate devices across the system. The automatic failover and backup services ensure uninterrupted video surveillance.

C2 Surveillance

Secure camera footage by saving recordings to the Synology C2 cloud. This allows investigation even if the Synology NAS is stolen or physically damaged. With the intuitive web portal, you can access and share recordings anywhere, anytime.

Learn more about C2 Surveillance.