NAS Management System

User Manual

Manual Version: V1.02

Software Version: DX-B1101.8.0

Contents

1 System Introduction 1

1.1 System Login 1

1.2 Home Page 2

1.3 Quick Guide 3

2 Personalization 3

3 Control Panel 5

3.1 Account Manager 5

3.1.1 User Group 5

3.1.2 User 9

3.1.3 Domain 12

3.2 System Settings 14

3.2.1 Network 14

3.2.2 Interface Bonding 17

3.2.3 NTP 18

3.2.4 External Access 19

3.2.5 Hardware and Power 20

3.3 Task Manager 24

3.3.1 S.M.A.R.T. 24

3.3.2 Rsync 25

3.3.3 Data Scrubbing 27

3.3.4 Snapshot 28

3.4 Security Manager 29

3.4.1 Service 29

3.4.2 Firewall 30

3.4.3 Certificate 32

4 Storage Manager 33

4.1 Overview 33

4.2 Storage 33

4.2.1 Storage Pool Information 33

4.2.2 Create Storage Pool 34

4.2.3 Manage Storage Pool 35

4.2.4 Rename Storage Pool 36
4.2.5 Delete Storage Pool 36
4.3 Cache 36
4.4 Disk 37
5 Sharing Manager 38
5.1 Shared Folder 39
5.1.1 Add Shared Folder 39
5.1.2 Properties Manager 40
5.1.3 Snapshot 42
5.1.4 Lock/Unlock 46
5.1.5 Delete Shared Folder 47
5.2 Sharing Configuration 47
5.2.1 Share with Windows 47
5.2.2 Share with Linux 50
5.2.3 Share with Mac 51
5.2.4 Share by WebDAV 51
5.2.5 Share by FTP 52
6 Block Sharing 53
6.1 Overview 53
6.2 Host 54
6.2.1 Add Host 54
6.2.2 Edit Host 56
6.2.3 View Initiator 56
6.2.4 Delete Host 56
6.3 LUN 56
6.3.1 Add LUN 57
6.3.2 Edit LUN 57
6.3.3 Snapshot 58
6.3.4 Delete LUN 58
6.4 Target 58
6.4.1 Add Target 59
6.4.2 Edit Target 61
6.4.3 Delete LUN Mapping 61
6.4.4 Delete Link 61
6.4.5 Delete Target 61

6.5 Use NAS Resource on the Host 62
6.5.1 Windows Host 62
6.5.2 VMware ESXi Host 63
6.5.3 Linux Host 64
7 File Manager 65
7.1 File Manager 65
7.1.1 New Folder 65
7.1.2 Upload Files 65
7.1.3 Share Files 66
7.1.4 Download File 67
7.1.5 File Management Actions 67
7.2 Share Links 67
7.3 Recycle Bin 68
8 NVR 68
8.1 Log in to the NVR 68
8.2 Add a Camera 69
8.3 Storage 69
8.4 Live View 71
8.5 Playback 71
9 System Maintenance 72
9.1 Update and Restore 72
9.1.1 System Update 72
9.1.2 Backup and Restore 72
9.2 Log Center 73
9.2.1 Alarm Logs 73
9.2.2 Operation Logs 74
10 Acronym and Abbreviations 74
Disclaimer and Safety Warnings 76

1 System Introduction

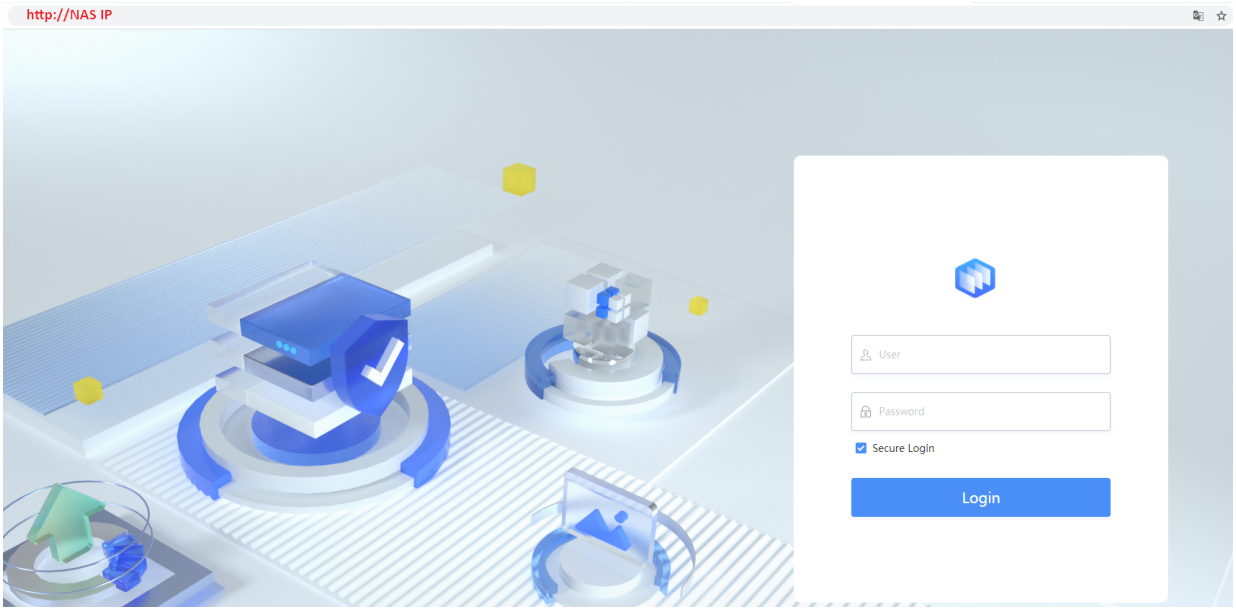
The desktop Network Attached Storage (NAS) is a powerful storage device with high-capacity file storage and data protection.

You can log in to the NAS management system from a computer to configure and manage your NAS device.

1.1 System Login

Follow the steps to log in to the NAS management system:

1. Make sure the computer and the NAS device are connected via network. If the IP address of the NAS device and that of the computer are on different networks, you need to use a router to connect them.
2. Use a browser to visit http://*NAS IP*. The login page appears.



NOTE!

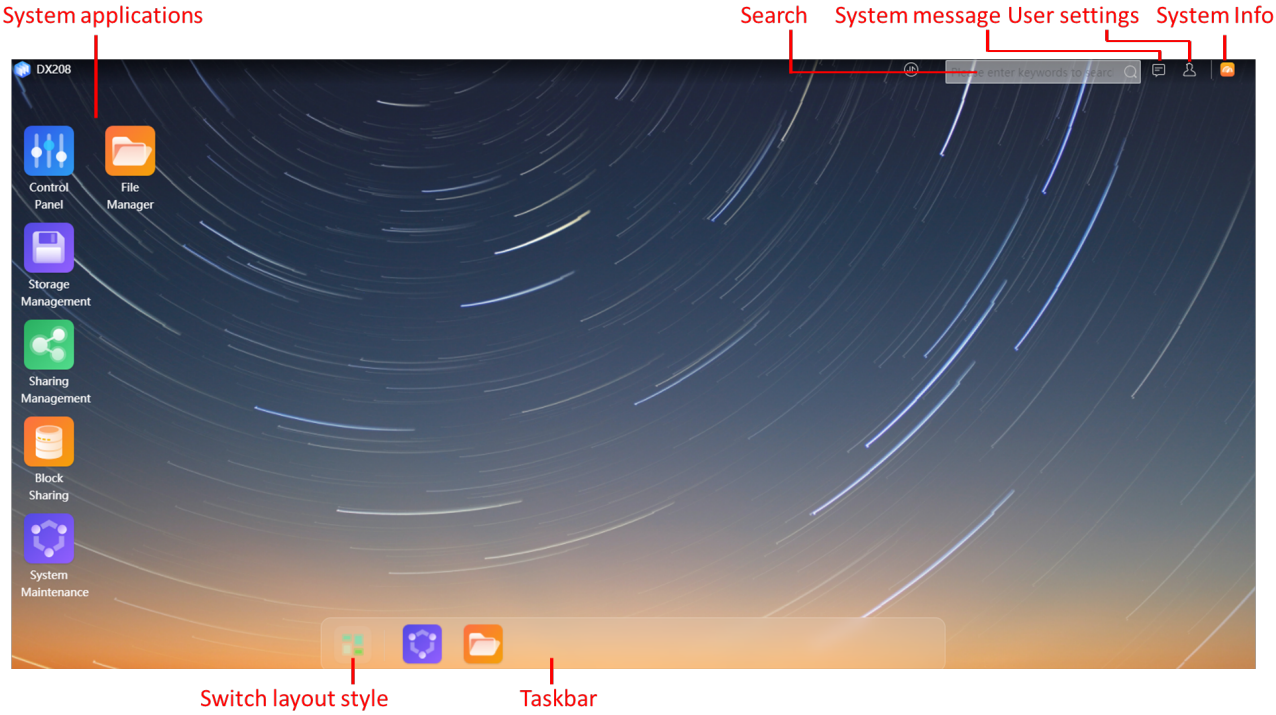
To use a secure connection via HTTPS, select the **Secure Login** checkbox.

3. Enter the username and password, and then click **Login**.

NOTE!

- The default username/password: nas/nas
- For data security please change the default username/password after your first login. A strong password is recommended: at least nine characters including uppercase and lowercase letters, digits, and special characters. See Personalization.
- For first-time use, follow the steps to change the NAS device IP to the actual IP on the LAN.
  (1) Connect one end of the network cable to the network interface on the NAS, and connect the other end to your computer.
  (2) Use a browser to visit the NAS device IP (http://192.168.0.1) to access the NAS management system.
  (3) Go to **Control Panel** > **System Settings > Network**, change the IP address. See Network.
  (4) Connect the NAS device to the networking device (switch, router) using a network cable.

1.2 Home Page



Functional Module	Description
System applications	Click an icon to open the application page.
Switch layout style	Click at the bottom to switch the layout style: landscape or portrait.
Taskbar	Shows icons of running applications.
Search	Type keywords in the field and then click to search for a function, and then click to open the application page.
System message	Click to see system errors, warnings, and alerts.
User settings	Click to view user information, to personalize, restart, turn off, or log out of the NAS device.

System Info	Click to view system operation status.

1.3 Quick Guide

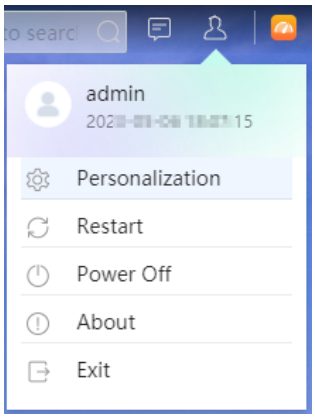
For first-time use, follow the steps to configure the NAS device before using it to store your files.

1. Create storage pool and cache: Add hard disks to a storage pool to create storage space; use SSD to create cache space.
2. Configure shared folder and service: Create shared folders to store files and manage subfolders; configure sharing service to allow data access from other clients.
3. Create groups/users: Create accounts for family or enterprise members, set permissions, and assign storage space.
4. Use NAS to store files : Upload files to the NAS device, view, download, and share files on the NAS device.
5. Use NAS as local disk: Allocate storage space, so the local host (e.g., computer) can use the allocated space as a local disk.

2 Personalization

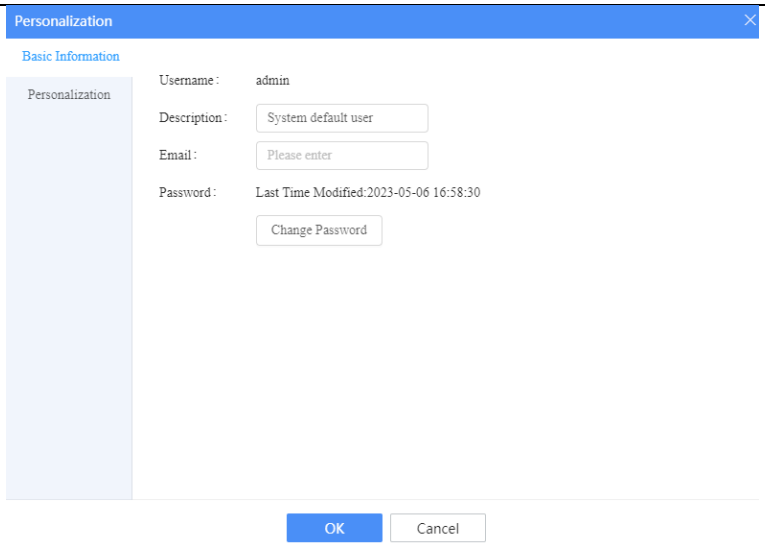
View personal information and storage quota, and personalize settings such as email, password, and UI style.

1. Click in the upper right corner.

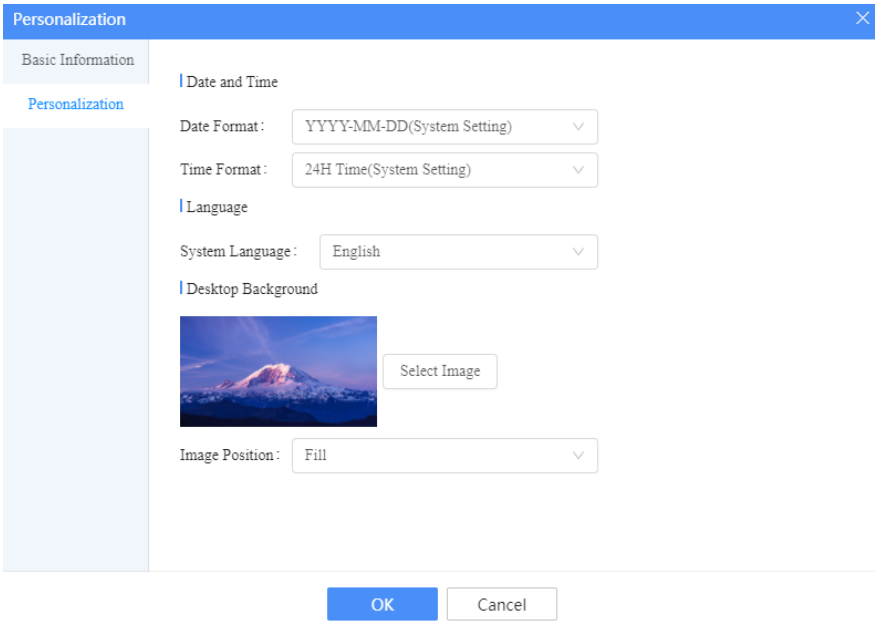


2. Click **Personalization**.
3. View or edit settings as described below.

Item	Description
Basic Information	Basic information

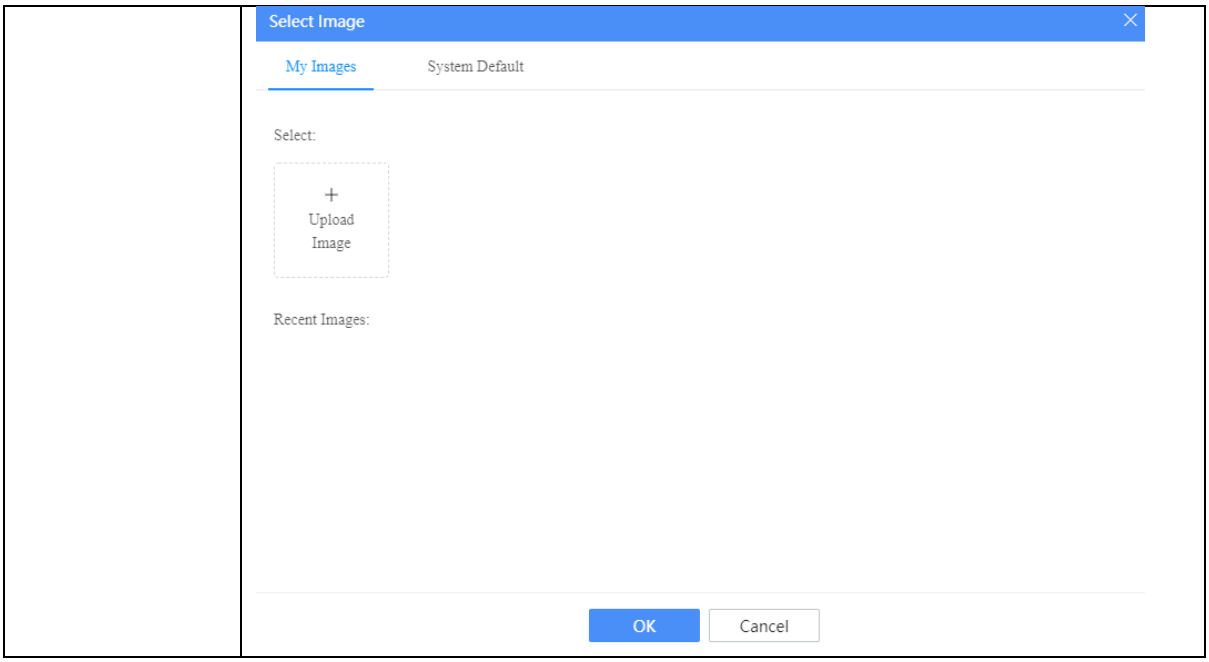
<table>
<tr>
<td></td>
<td>


Description: Type a personal description.
Email: Input your personal email address to receive system messages and retrieve password in case you forget it.
Password: Click Change Password to set a new password. After changing the password, you need to log in with the new password.
Note: Privileged user can allow or forbid other users to change password (Control Panel > User, see User).

</td>
</tr>
<tr>
<td>Personalization</td>
<td>
Personalize the system according to your preferences.


Date and Time: Choose the date and time format.
Language: Choose the system language.
Desktop Background: Click Select Image, and choose an image from your computer, or choose from default images in the system.
Image Position: Set how the image will be displayed (fill or tile).

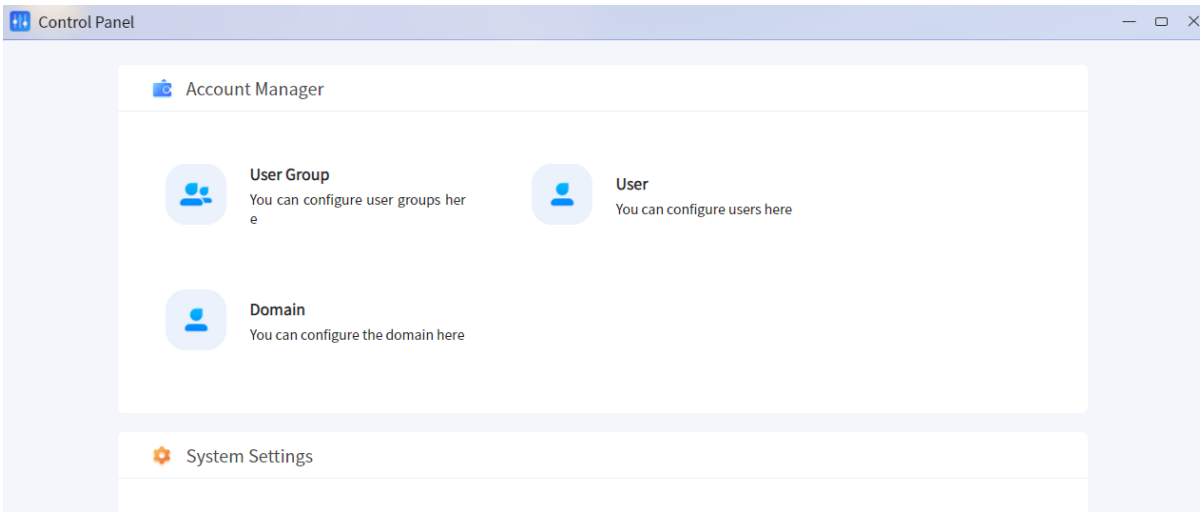
</td>
</tr>
</table>



4. Click **OK** to save the settings.

3 Control Panel

On the **Control Panel** page, click a menu to enter the corresponding configuration page.

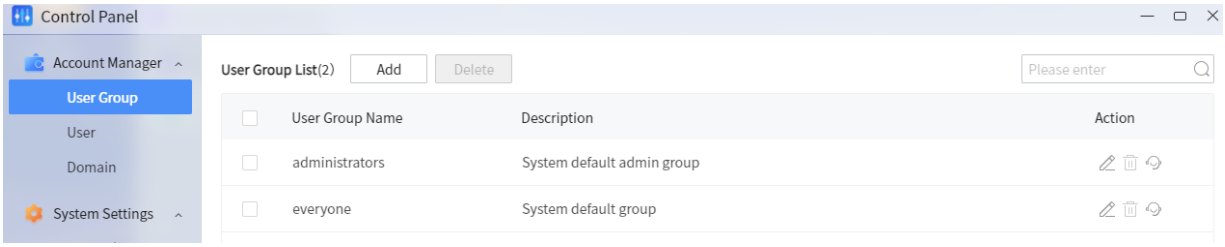


3.1 Account Manager

3.1.1 User Group

If the NAS device is used by multiple users, it is recommended to create user groups and manage user attributes in batches by setting group attributes.

Go to **Control Panel** > **Account Manager** > **User Group**.



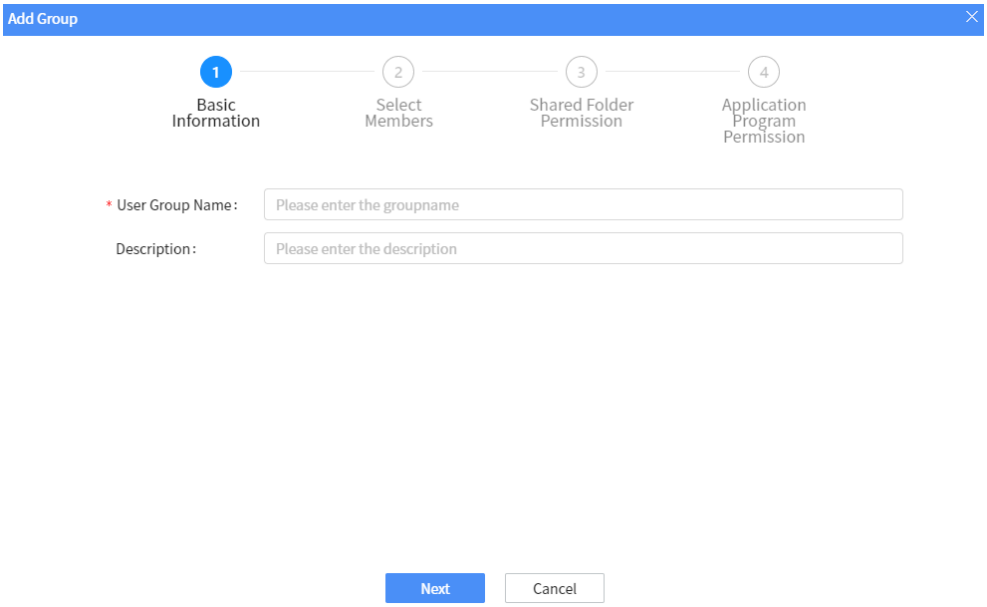
NOTE!

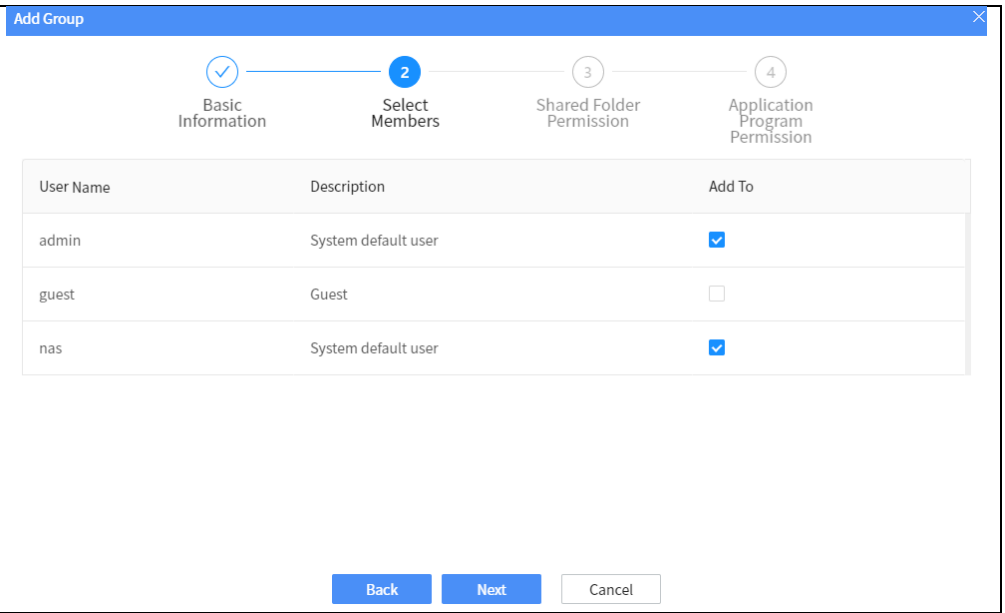
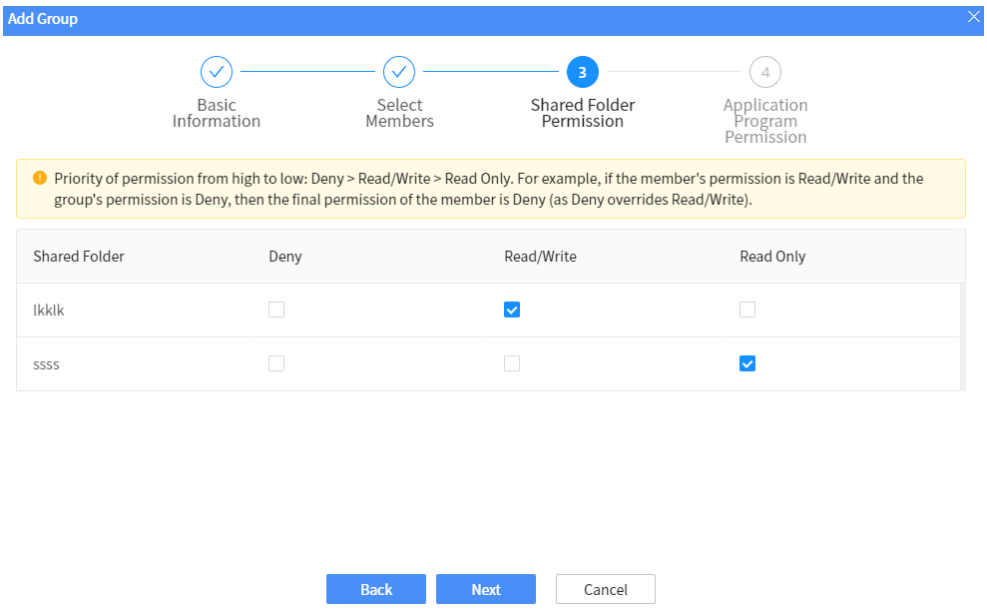
The system includes two default user groups:

- administrators: This group includes the default administrators (nas and admin) in the system.
- everyone: This group includes the common users in the system.

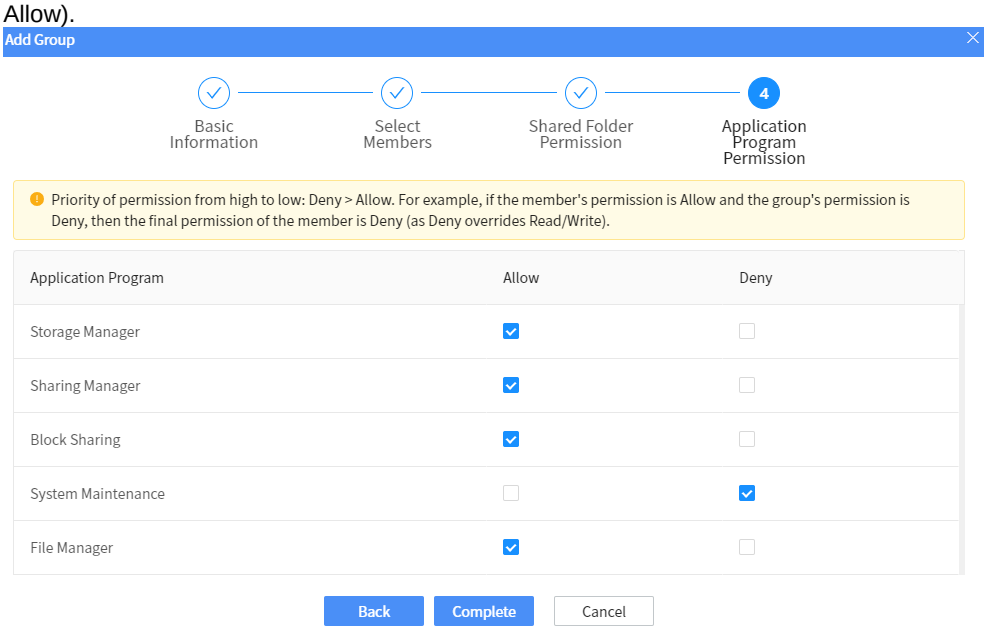
Add a Group

1. Click **Add**.
2. Follow on-screen instructions to complete the group information. Click **Next** to proceed, or click **Back** to return to the previous step.

Item	Description
Basic Information	Input the group name and description.  ● User Group Name: Input the group name. The name contains 4-16 characters and allows letters, digits, and underscore (_). ● Description: Input a description of the group for differentiation.
Select Members	Add users to the group. (To add users, see User). ● Select users you want to add to the group. ● If you haven't created any user, you may skip this step and add later.

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Shared Folder Permission</td><td>Set permission for group members to access the shared folder.
Priority of permission from high to low: Deny > Read/Write > Read Only. For example, if user permission is Read/Write and group permission is Deny, then the final permission of the user is Deny (as Deny overrides Read/Write).
 
</td></tr>
<tr><td>Application Program Permission</td><td>Set permission for group members to access the application program.
Priority of permission from high to low: Deny > Allow. For example, if user permission is Allow and group permission is Deny, then the final permission of the user is Deny (as Deny overrides</td></tr>
</table>

Allow).



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

Edit a Group

In the user group list, click for the group you want to edit. You may change the group description, group members, and group permission.

Delete a Group

In the user group list, click for the group you want to delete and then confirm the deletion.

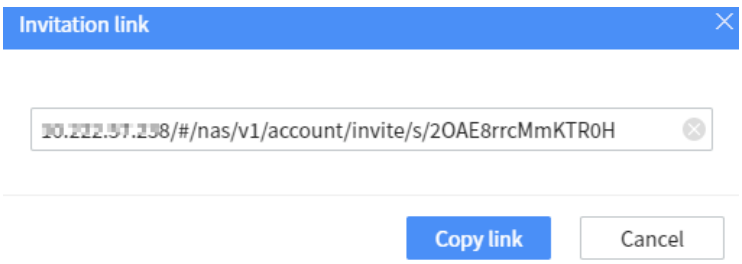
NOTE!
Default system groups cannot be deleted.

Generate an Invitation

Generate an invitation for a group, so other users can join the group through the link.

1. Generate an invitation link and share it with other users.

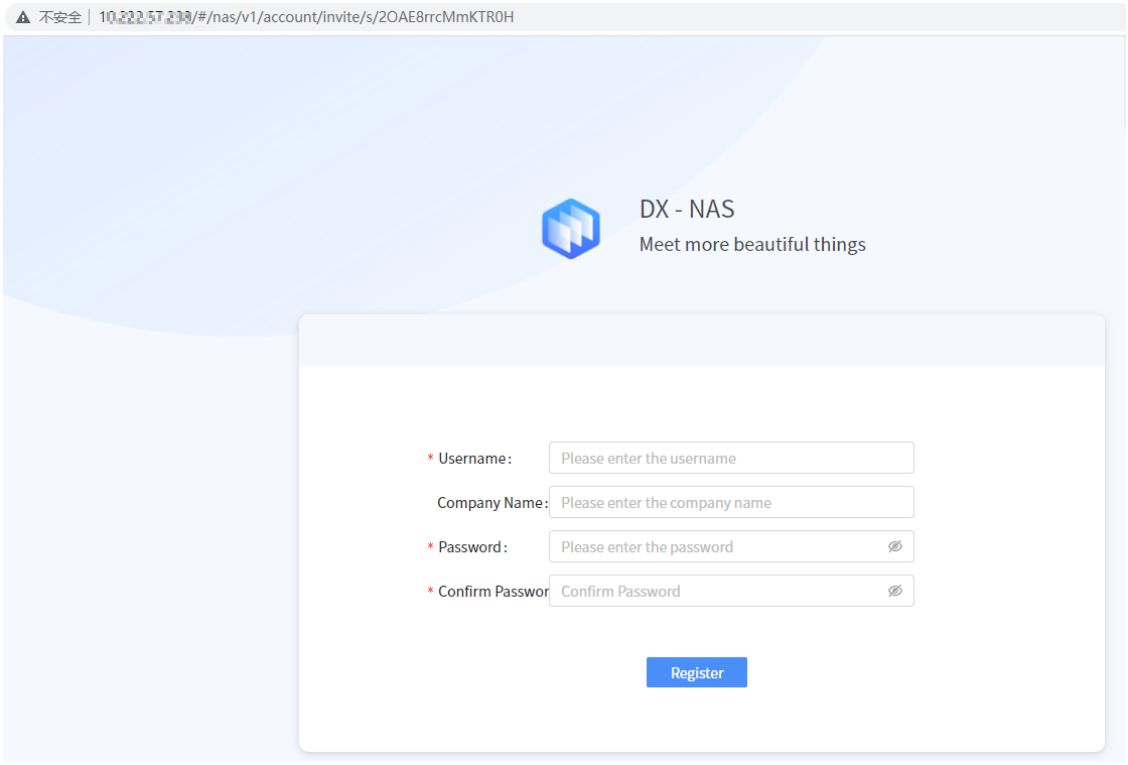
   (1) In the user group list, click the corresponding to generate an invitation link.



   (2) Click **Copy link**, and send the link to other users.

2. Other users join the group through the link.

   (1) Use a browser to open the link and enter the user registration page.



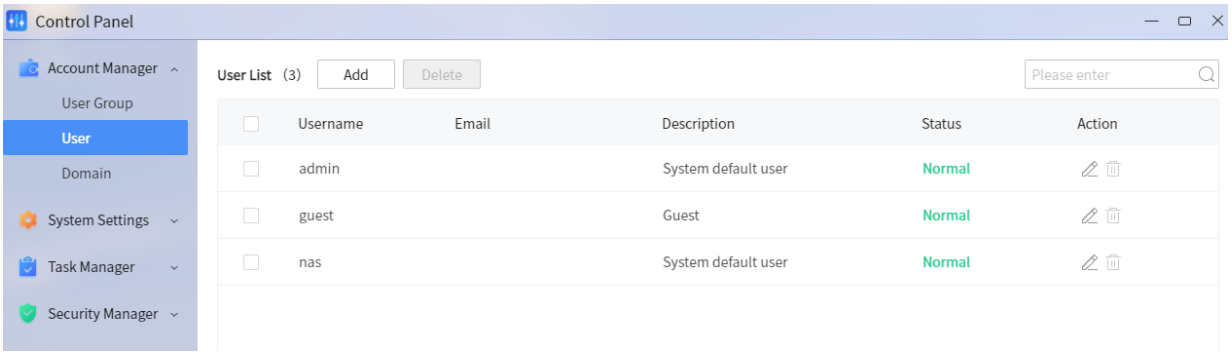
(2) Enter the username, password, company information, and then click **Register**.

(3) After completing the registration, the user automatically joins the group and logs in to the NAS management system.

3.1.2 User

Create a user account for each family or enterprise member, set permission for each member, for example, set access to shared folders and a limit for storage/shared folder.

Go to **Control Panel** > **Account Manager** > **User**.



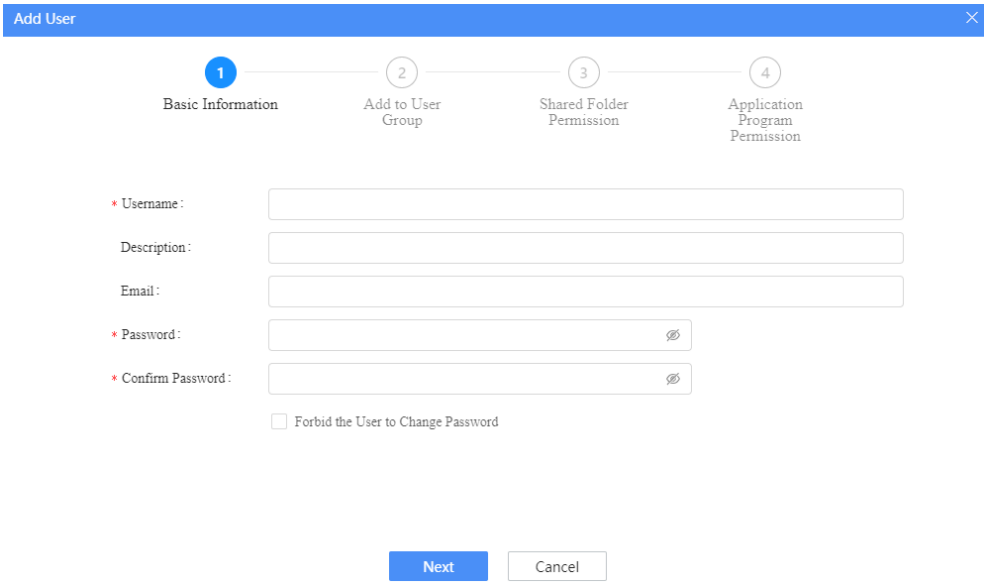
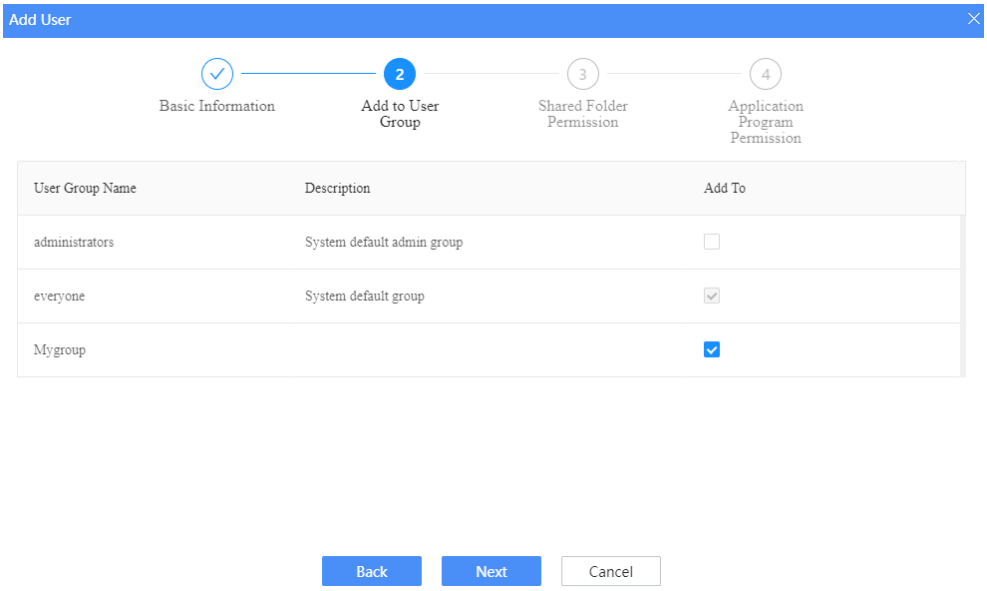
NOTE!

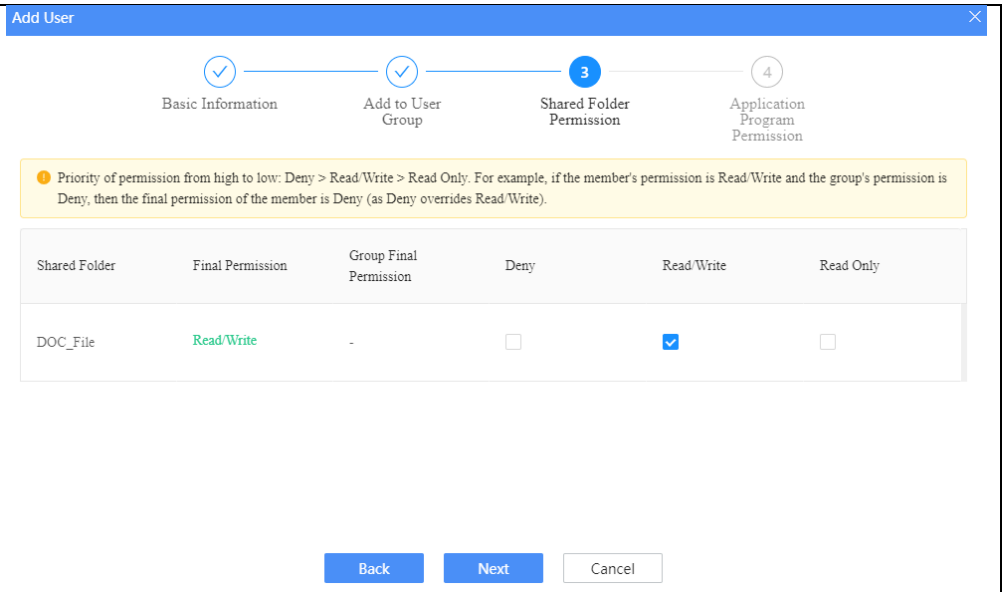
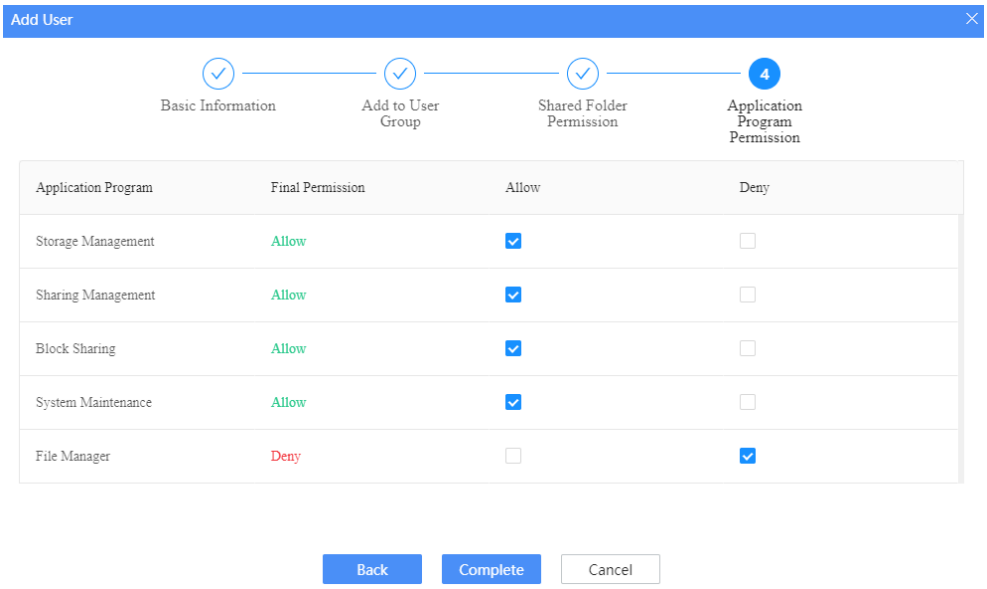
The system has 3 default users:

- nas: System administrator with maximum permissions. The default password is “nas”.
- admin: System administrator with maximum permissions. The default password is “admin”.
- guest: Guest user with only the file management permission (see File Manager). The default password is “guest”.

Add a User

1. Click **Add**.
2. Follow on-screen instructions to complete user information. Click **Next** to proceed, or click **Back** to return to the previous step.

Parameter	Description
Basic Information	Enter the username, password, etc.  ● Username: Set a unique username. The username must be 4-16 characters long and include letters, digits, and underscores (_). ● Description: Input a description of the user. ● E-mail: Used to receive account information. ● Password: Enter a password for the user and then enter again to confirm. ● Forbid the User to Change Password: If selected, the user cannot change his/her own password.
Add to User Group	Add the user to a user group (see User Group). ● If the user group already exists, choose it to add the user. ● Or skip this step and add later. 
Shared Folder Permission	Set permission for the user to access shared folders. Priority of permission from high to low: Deny > Read/Write > Read Only. For example, if user permission is Read/Write and group permission is Deny, then the final permission of the user is Deny (as Deny overrides Read/Write).

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Application Program Permission</td><td>Set permission for the user to access application programs.
Priority of permission from high to low: Deny > Allow. For example, if user permission is Allow and group permission is Deny, then the final permission of the user is Deny (as Deny overrides Allow).
 
</td></tr>
</table>

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

Edit a User

In the user list, click for the user you want to edit. You may change the user description, email, password, group, and permission.

Delete a User

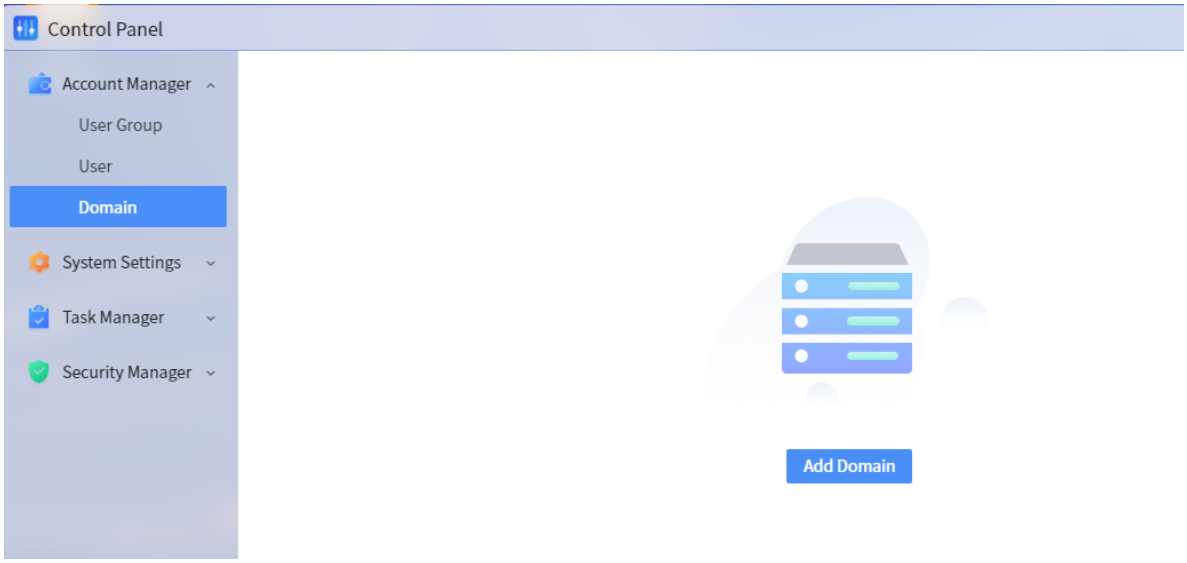
In the user list, click for the user you want to delete and then confirm the deletion.

NOTE!
The default system users (nas, admin, guest) cannot be deleted.

3.1.3 Domain

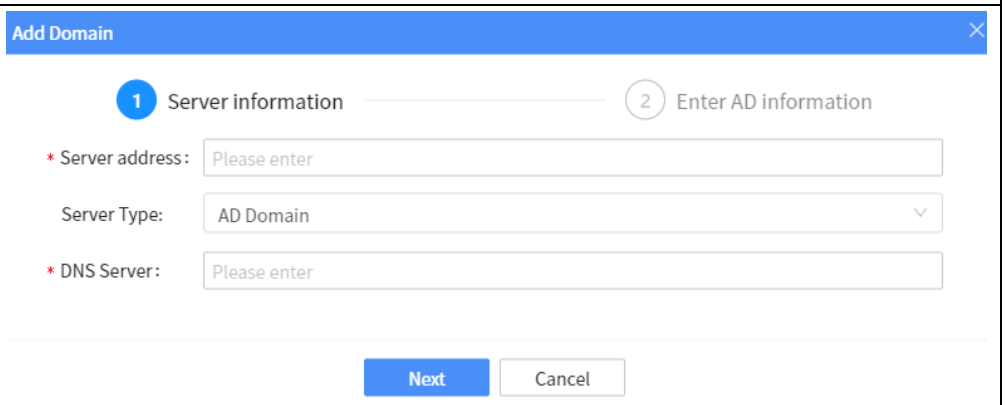
Add NAS to directory service. When your NAS becomes a directory client, you can manage AD domain user's access to files, folders, and services on the NAS. You can also assign administrative privileges and home directories to domain users.

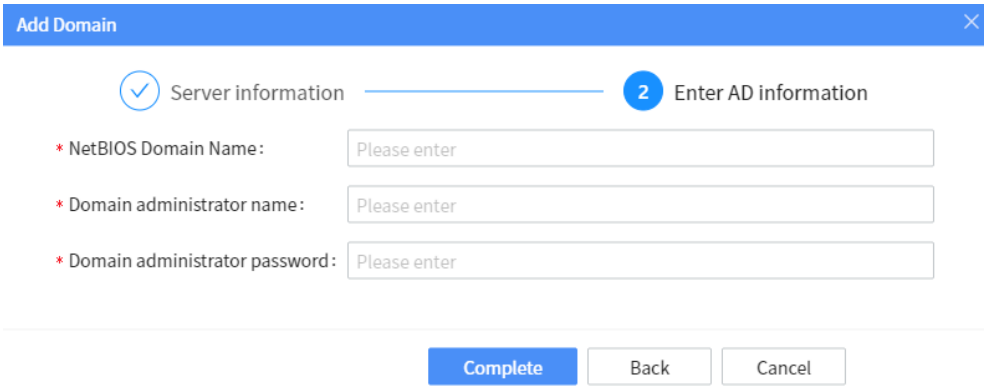
Go to **Control Panel** > **Account Manager** > **Domain**.



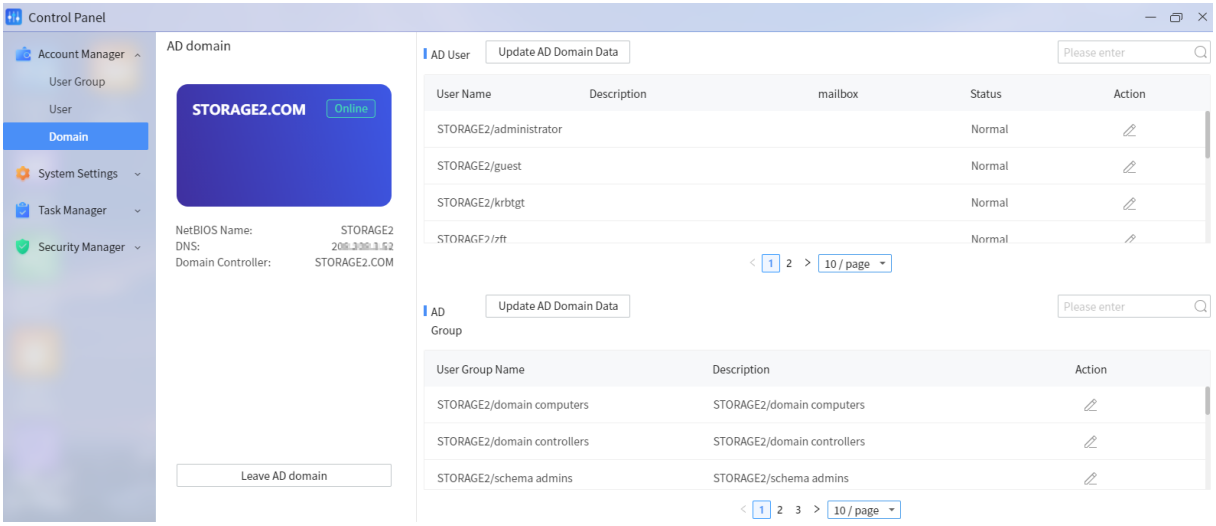
Add a Domain

1. Click **Add Domain**.
2. Follow on-screen instructions to complete the information. Click **Next** to proceed, or click **Back** to return to the previous step.

Item	Description
Server information	 ● Server address: Domain name of the AD domain server, for example, XXX.com. ● Server Type: Choose **AD Domain** (Active Directory is a directory service for Microsoft servers). ● DNS Server: Enter the IP address of the DNS server used to resolve domain names.

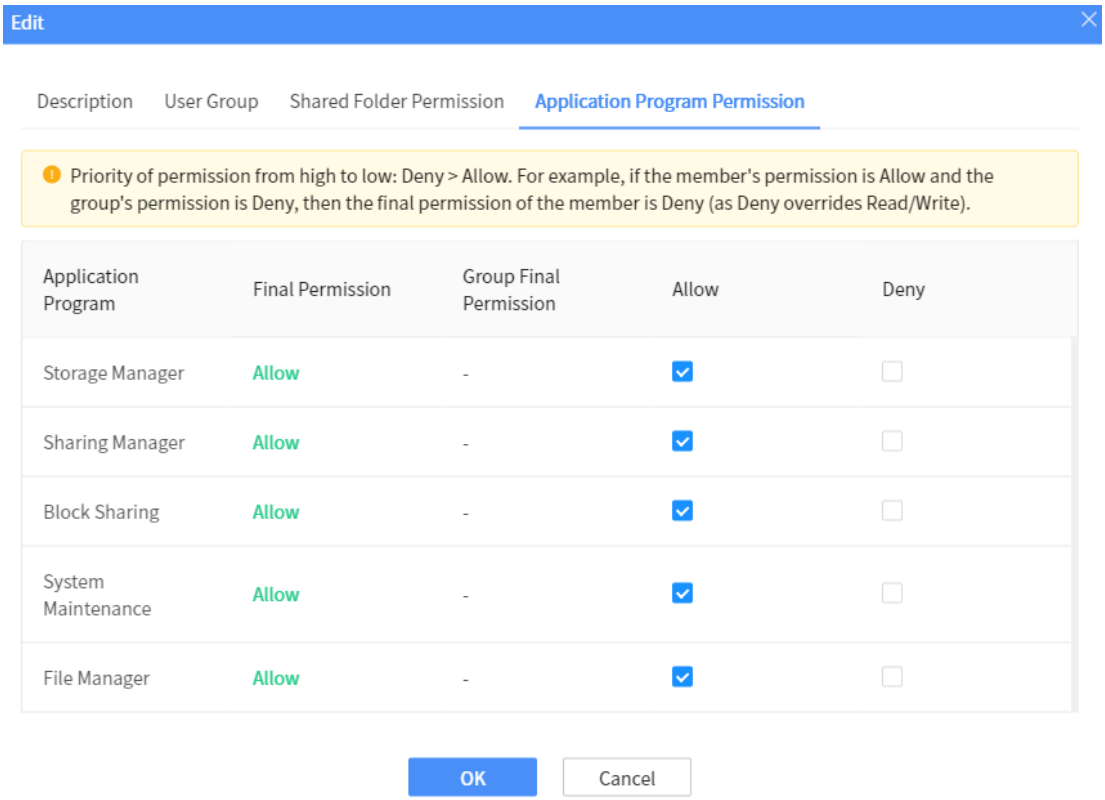
Enter AD information	 ● NetBIOS Domain Name: Enter the distinguished name of the domain server. If the server address is XXX.com, then enter XXX. ● Domain administrator name: Enter the administrator name of the AD domain. ● Domain administrator password: Enter the administrator password of the AD domain.

3. Click **Complete** to save the settings, then you can use the AD domain service.



Set Permission for AD Domain User or User Group

1. Click for the AD domain user/group to edit the access of the user/group to specified shared folders or application programs, etc.



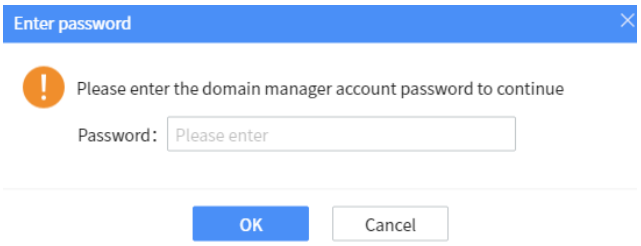
2. Log in to the NAS device as an AD domain user. The user has access to permitted shared folders and application programs.

Update AD Domain Data

If any AD domain user or user group has changed, click **Update AD domain data** to update the data.

Leave AD Domain

1. Click **Leave AD domain** and confirm. A dialog box as shown below appears.



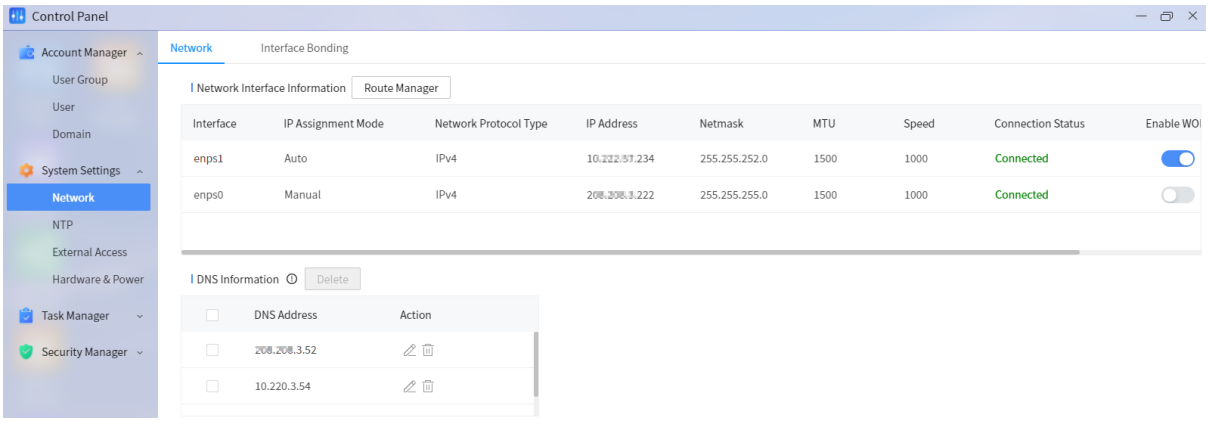
2. Enter the administrator password, and then click **OK** to leave the AD domain.

3.2 System Settings

3.2.1 Network

Configure the IP, route, and DNS server information so the NAS device can connect to network.

Go to **Control Panel** > **System Settings** > **Network**.

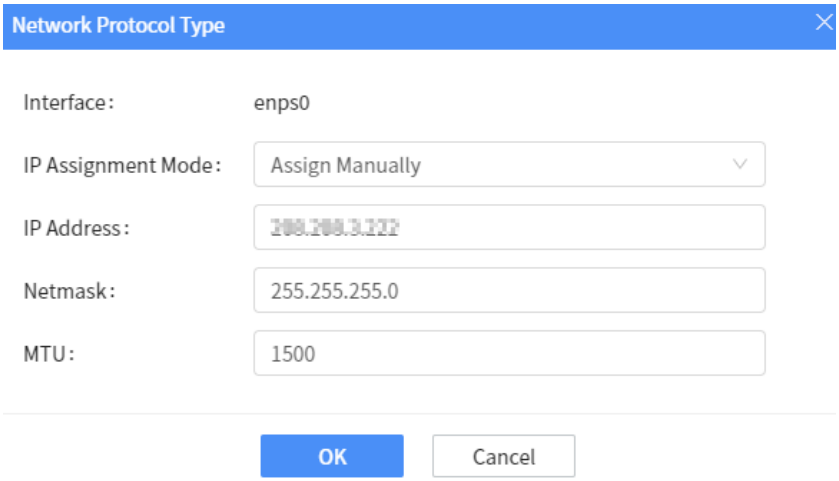


Network Interface Information

View the number of network interfaces, IP address, and connection status of the NAS device.

- To change a network interface IP, follow the steps below:

1. Click for the network interface.



2. Choose the IP assignment mode (Assign Manually or Assign Automatically). If Assign Manually, set IP address, netmask, and MTU. The recommended MTU is 1500.
3. Click **OK** to save the settings.

- Wake On LAN (WOL)

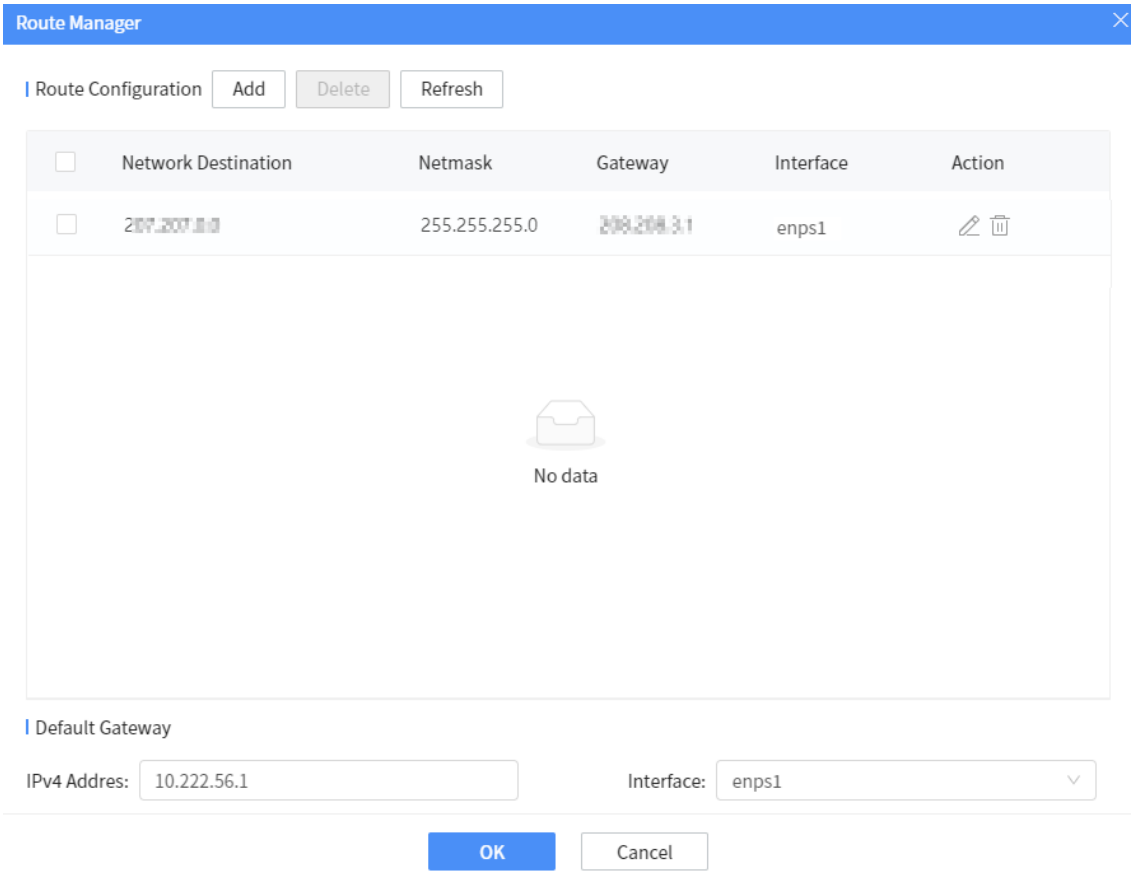
1. When Wake On LAN is enabled, you can wake the NAS and restore its running status or switch it to standby mode from shutdown by sending a command to its IP via the Ethernet, even if it is sleeping or powered off.

2. Enable or disable this function as needed. means “enabled”, means “disabled”.

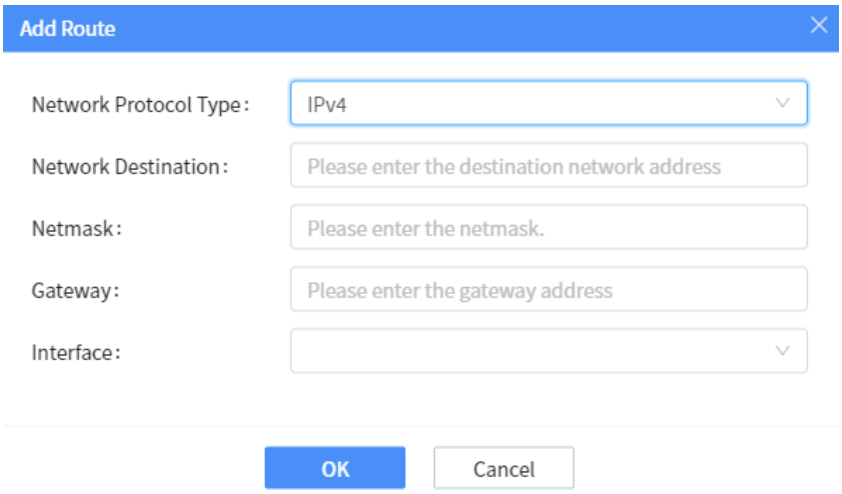
Route Manager

Configure a route for the NAS device so it can communicate with other network devices.

1. Click **Route Manager**.



2. If a route already exists and you want to edit it, click . To add a new route, click **Add**.

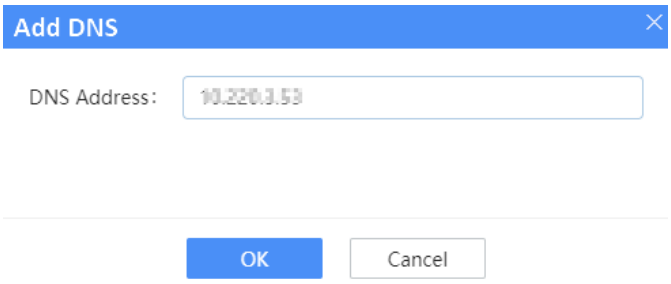


3. Click **OK** to save the settings.

DNS Information

The DNS translates a domain name into a digital address for a networking device. To use DNS, you need to configure a DNS server first.

1. Click **Add**, input the DNS server IP address.

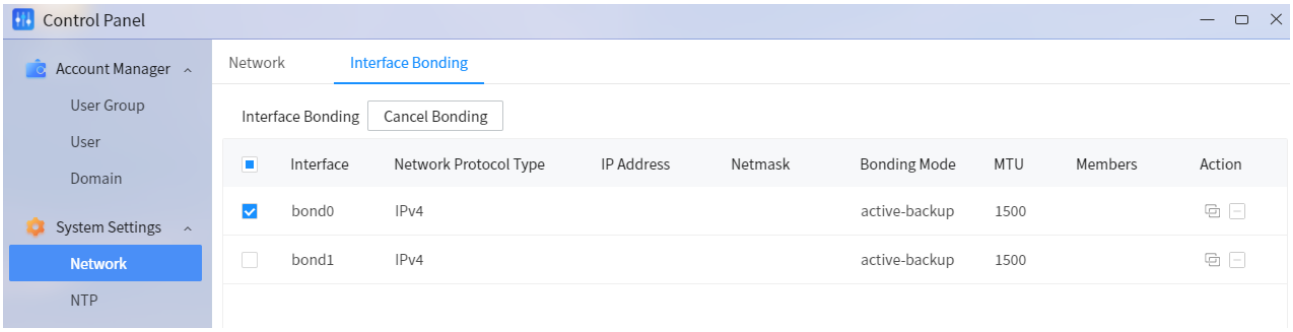


2. Click **OK** to save the settings.

3.2.2 Interface Bonding

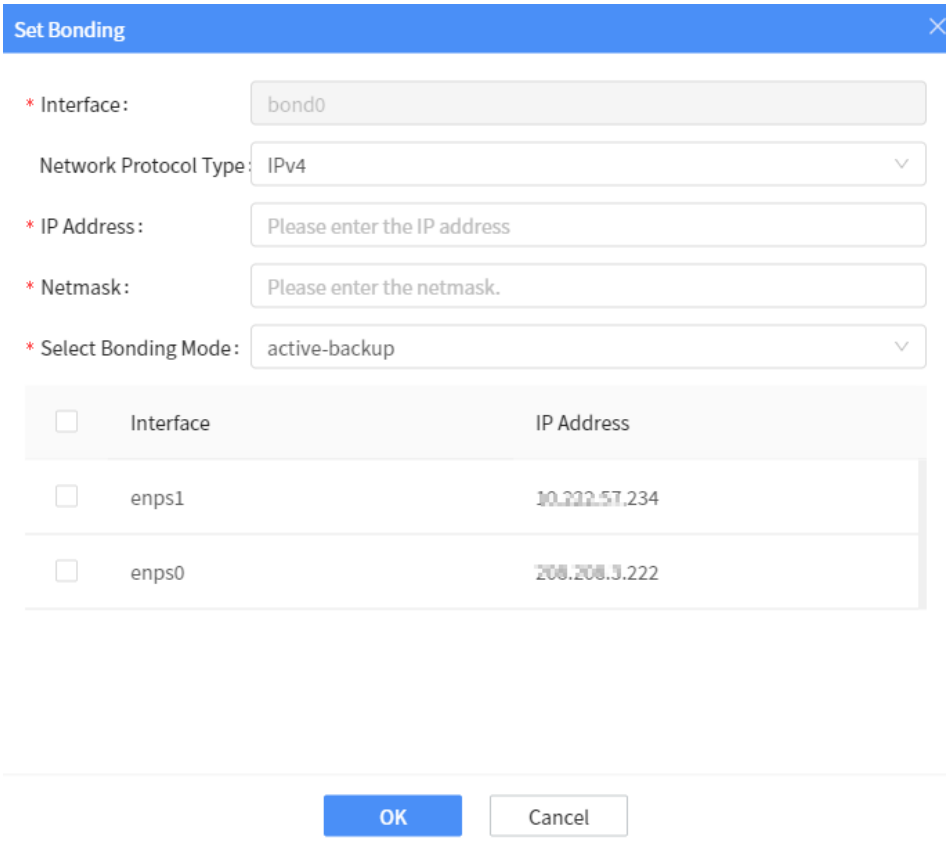
Configure interface bonding to increase bandwidth and achieve link redundancy.

Go to **Control Panel** > **System Settings** > **Network**> **Interface Bonding**.



Set Bonding

1. Click in the **Action** column. A page as shown below appears.



2. Complete the required information, and choose member interfaces.
3. Click **OK** to save the settings.

Interface bonding modes are described in the table below:

Bonding Mode	Description	Pros	Cons
Active-backup	One interface is active, and the other interface is standby. Traffic is processed on the active link. If the active interface fails, the standby interface takes over.	Provides fault tolerance.	Low resource utilization (1/N).
Balance-RR	Transmits packets in sequential order (that is, transmits the first packet through eth0, the second through eth1, the third through eth0, ..., till the last packet is transmitted).	Provides load balancing and fault tolerance.	Packets sent from different interfaces may arrive out of order and may require resending, causing decreased throughput.
Balance-XOR	Transmits packets based on the selected transmit hash policy.	Provides load balancing and fault tolerance.	_
Broadcast	Transmits the same packets on both interfaces to ensure successful transmission.	High availability.	Wasting resources.
802.3ad	Creates link aggregation using all the interfaces according to 802.3ad specification.	Provides load balancing.	It is required to enable IEEE 802.3ad on the switch. All the interfaces share the same speed and duplex settings.
Balance-TLB Adaptive transmit load balancing.	Chooses an interface to transmit packets according to the current load on each interface.	Provides load balancing and fault tolerance.	The interface driver needs to allow ethtool to get speed status.
Balance-ALB Adaptive transmit load balancing.	Includes Balance-TLB mode, supports receive-load balancing for IPv4 traffic and does not require any special switch support.	Provides load balancing and fault tolerance.	The interface driver needs to allow ethtool to get speed status.

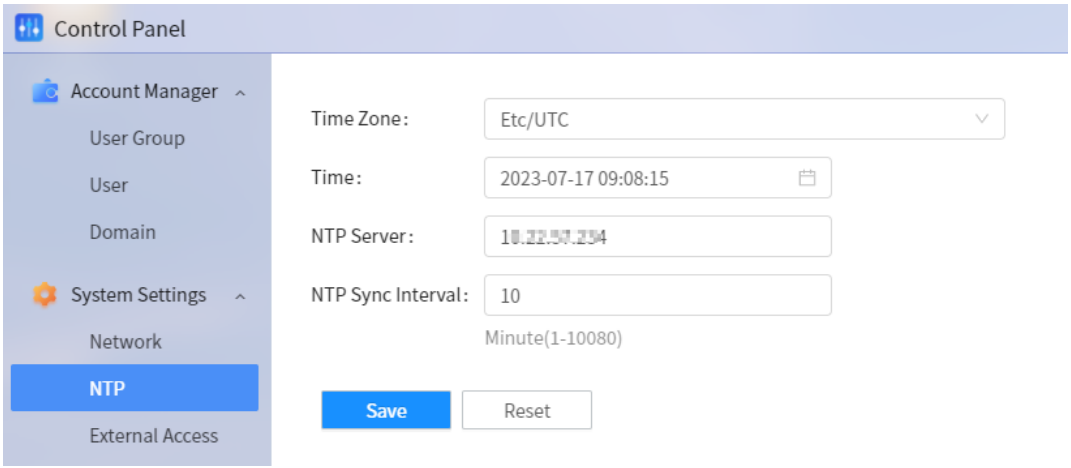
Cancel Bonding

Select the bonding you want to cancel, click **Cancel Bonding**, and then confirm.

3.2.3 NTP

Set time for the NAS device to ensure correct time of the stored data.

Go to **Control Panel** > **System Settings** > **NTP**. You can set time manually or use an NTP server (if configured).



Set Time Manually

1. Configure time zone and time.
   - Time Zone: Choose a time zone according to the geographic location of the NAS device.
   - Time: Click and set the current time.
2. Click **Save** to save the settings.

Sync Time with an NFT Server

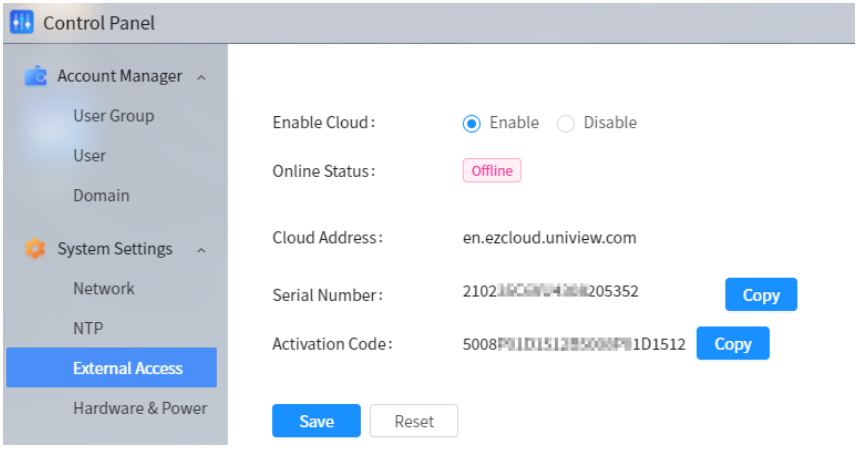
3. Set the NTP server IP and a time synchronization interval.
4. Click **Save** to save the settings.

CAUTION!
Make sure the time zone and time settings of your computer are consistent with those of the NAS; otherwise, records such as snapshots and logs will have inconsistent timestamps between the computer and NAS.

3.2.4 External Access

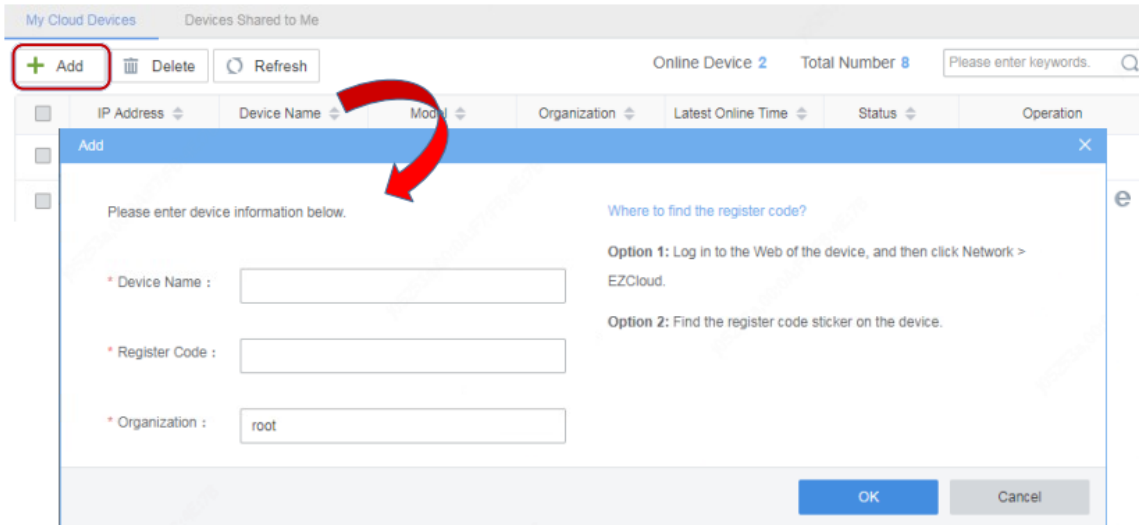
If you have Internet access, you can add the NAS device to EZCloud and then access the NAS device from the Internet.

Go to **Control Panel** > **System Settings** > **External Access**.

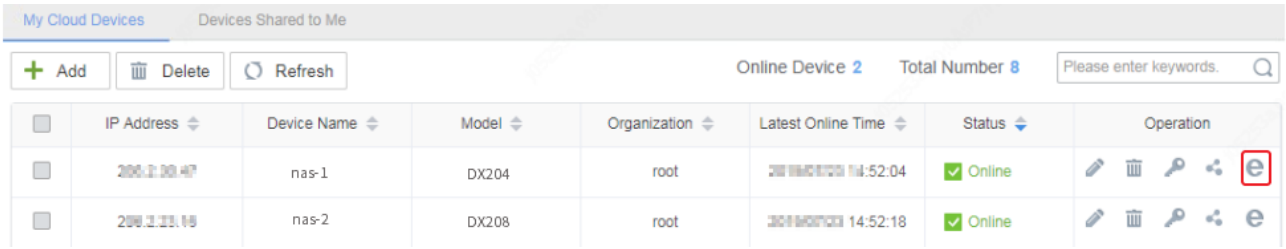


1. Click **Enable**, then click **Save**.
2. Click **Copy** behind the Activation Code to copy the activation code of the NAS device.

3. Go to https://en.ezcloud.uniview.com/ using a web browser and log in. If you do not have an EZCloud account, click **Register** and then follow on-screen instructions to sign up for an account.
4. On the **My Cloud Devices** page in EZCloud, Click **Add**. A page as shown below appears. Paste the activation code you just copied in the **Register Code** field, complete other required information, and then click **OK**. The NAS device is added to EZCloud.



5. After the NAS status changes to **Online**, you can click the e icon to access the NAS device via EZCloud.

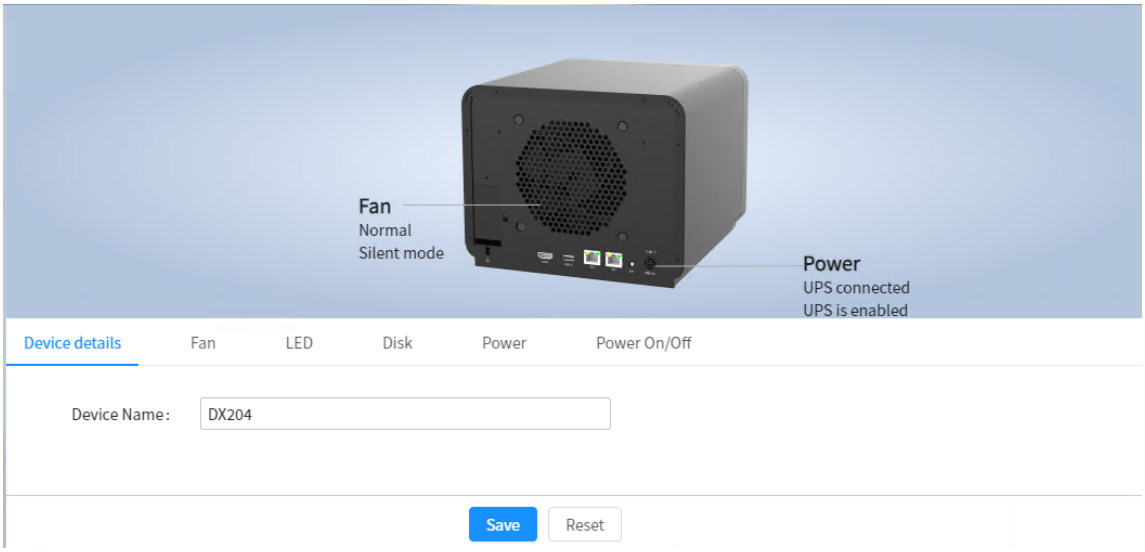


3.2.5 Hardware and Power

Go to **Control Panel** > **System Settings** > **Hardware and Power**

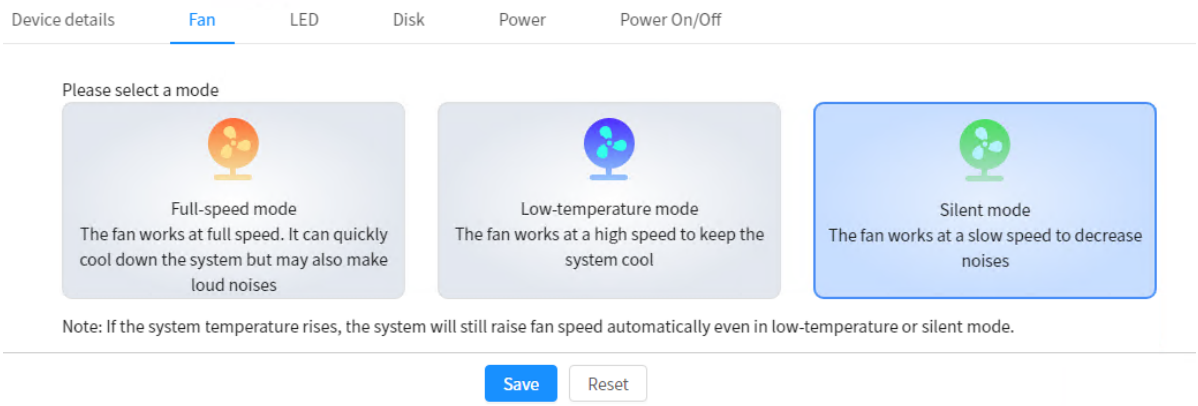
1. Device details

View the device name. To change the device name, enter the new name and then click **Save**. The device name displayed on the login page and in the system's upper left corner will update automatically.



2. Fan

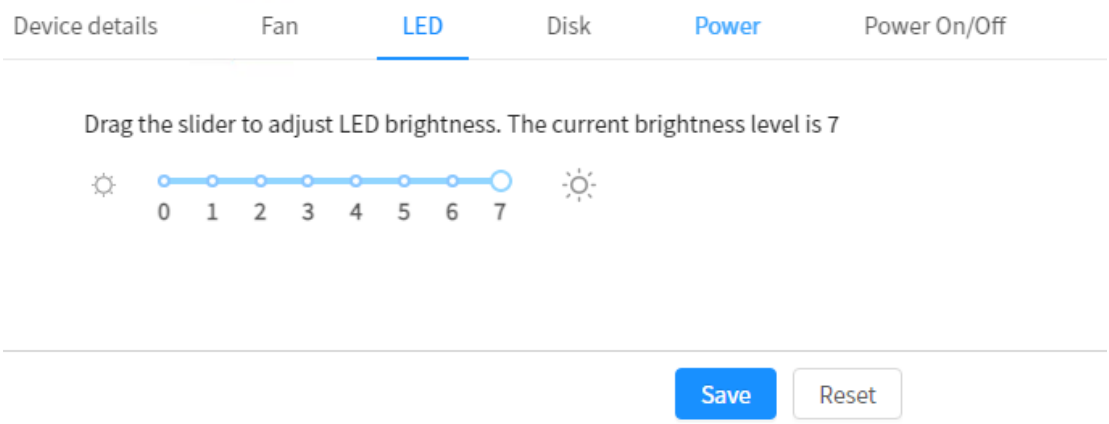
Choose an operation mode for the fan according to the on-screen instructions. Click **Save** to save the settings.



3. LED

Adjust the brightness of LED indicators on the NAS device.

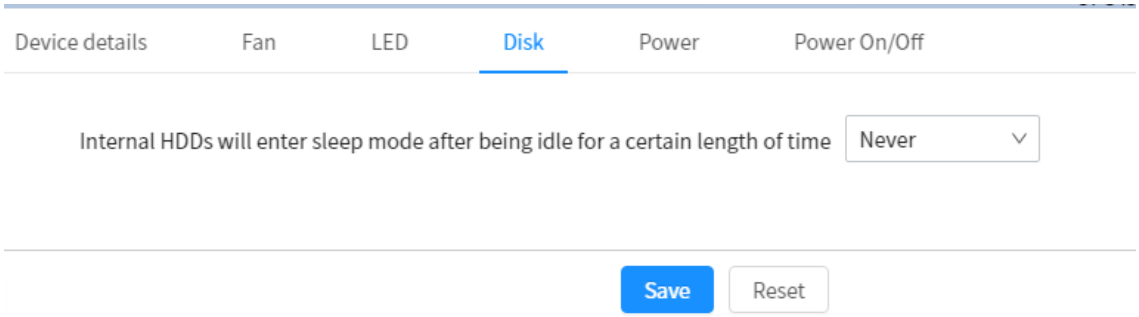
1. Drag the slider to adjust brightness.
2. Click **Save** to save the settings.



4. Disk

Set the length of idle time before the HDD enters sleep mode. In sleep mode, the HDD stops operation to save power and lifetime.

1. Set an idle time for internal HDD, external SATA HDD, and USB HDD. The NAS device does not sleep if **Never** is selected.
2. Click **Save** to save the settings.

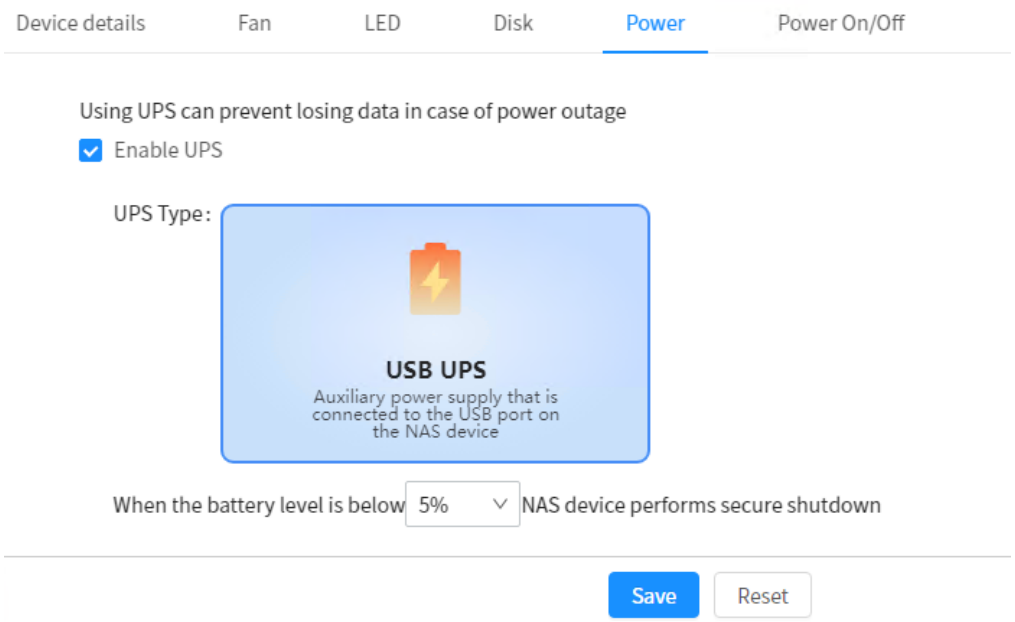


5. Power

Use UPS to prevent losing data due to a power outage.

To enable UPS, follow the steps:

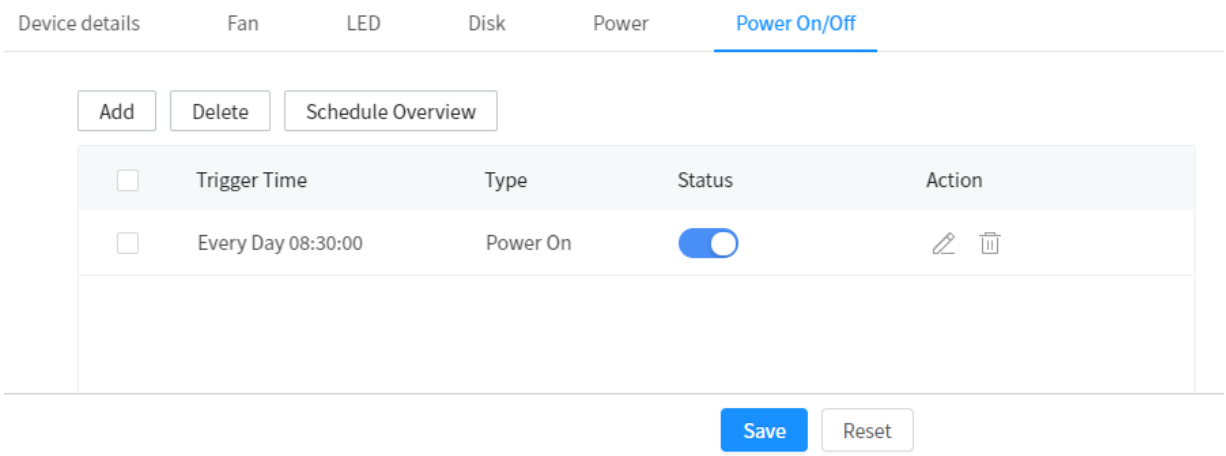
1. Connect the UPS device to the USB port on the NAS device.
2. Select the **Enable UPS** checkbox. Set the NAS device to perform a secure shutdown when the UPS battery level drops below a certain threshold.



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

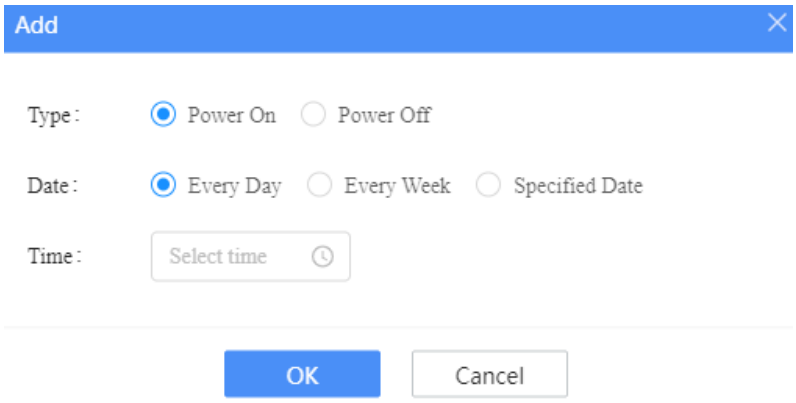
6. Power On/Off

Set a power-on/off schedule to automatically turn on or off the NAS device at a specified time. If another scheduled task is running at the time of a scheduled shutdown, the scheduled power-off task will be cancelled.



- Add a power-on/off schedule

1. Click **Add**.
2. Set a schedule.



   - Type: Choose **Power On** or **Power Off**.
   - Date and Time: Set if the task will repeat every day (power-on/off occurs at the same time every day), every week (power-on/off occurs at the same time on the same day every week), or on a specified date (according to the date and repetition cycle you set).

3. Click **OK**. New schedules are enabled by default.

- Schedule management operations

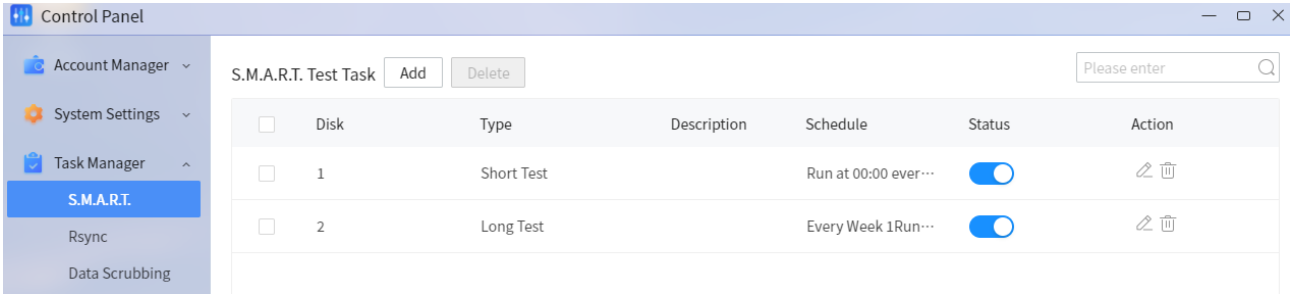
Enable/disable Schedule	Click / to enable or disable the schedule.
Edit Schedule	Click to edit the schedule.
Delete Schedule	• Delete: Click to delete a schedule. • Batch delete: Select the schedules you want to delete and then click **Delete**.
Schedule Overview	Click **Schedule Overview** to view all the exiting schedules.

3.3 Task Manager

3.3.1 S.M.A.R.T.

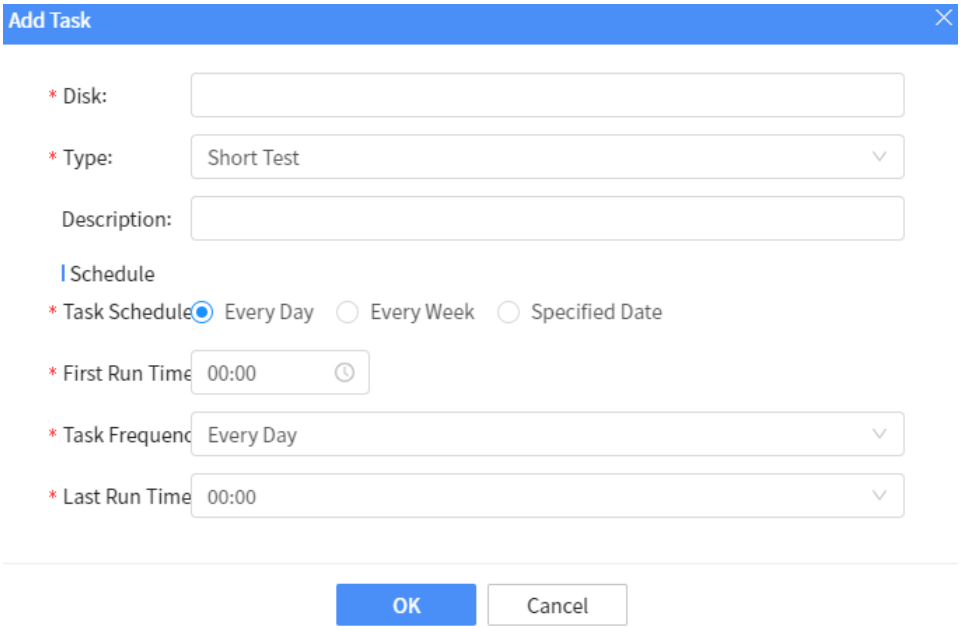
Create a S.M.A.R.T. test task to check HDD health regularly. If an exception is detected, the system will alert you through LED indicators and system messages and automatically repair to ensure data safety.

Go to **Control Panel** > **Task Manager** > **S.M.A.R.T.**.



Add a Task

1. Click **Add**.



2. Complete the settings. See the table below for descriptions.

Parameter		Description
Disk		Choose the HDD you want to test.
Type		● Short Test: The test only tests key items and takes a short time. ● Long Test: The test tests all items and takes a long time.
Schedule	Task Schedule	Choose a repetition mode for the schedule. ● Every Day: The task will be run at the same time every day. ● Every Week: The task will be run at the same time on the same day every week. ● Specified Date: You need to specify a date and the repetition cycle, so the task will be run at the same time on the same day according to the set cycle.

	First Running Time	The first time when the task will be run.
	Task Frequency	How often to run the task.
	Last Running Time	The last time when the task will be run. Options are determined by “First Run Time + Task Frequency * Number of tasks”.

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

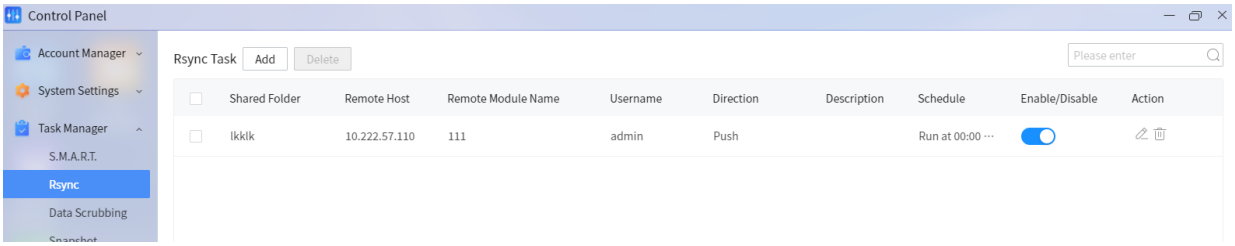
3.3.2 Rsync

Create a Rsync task so the NAS device can automatically back up data to a remote host or download data from a remote host according to a schedule.

NOTE!

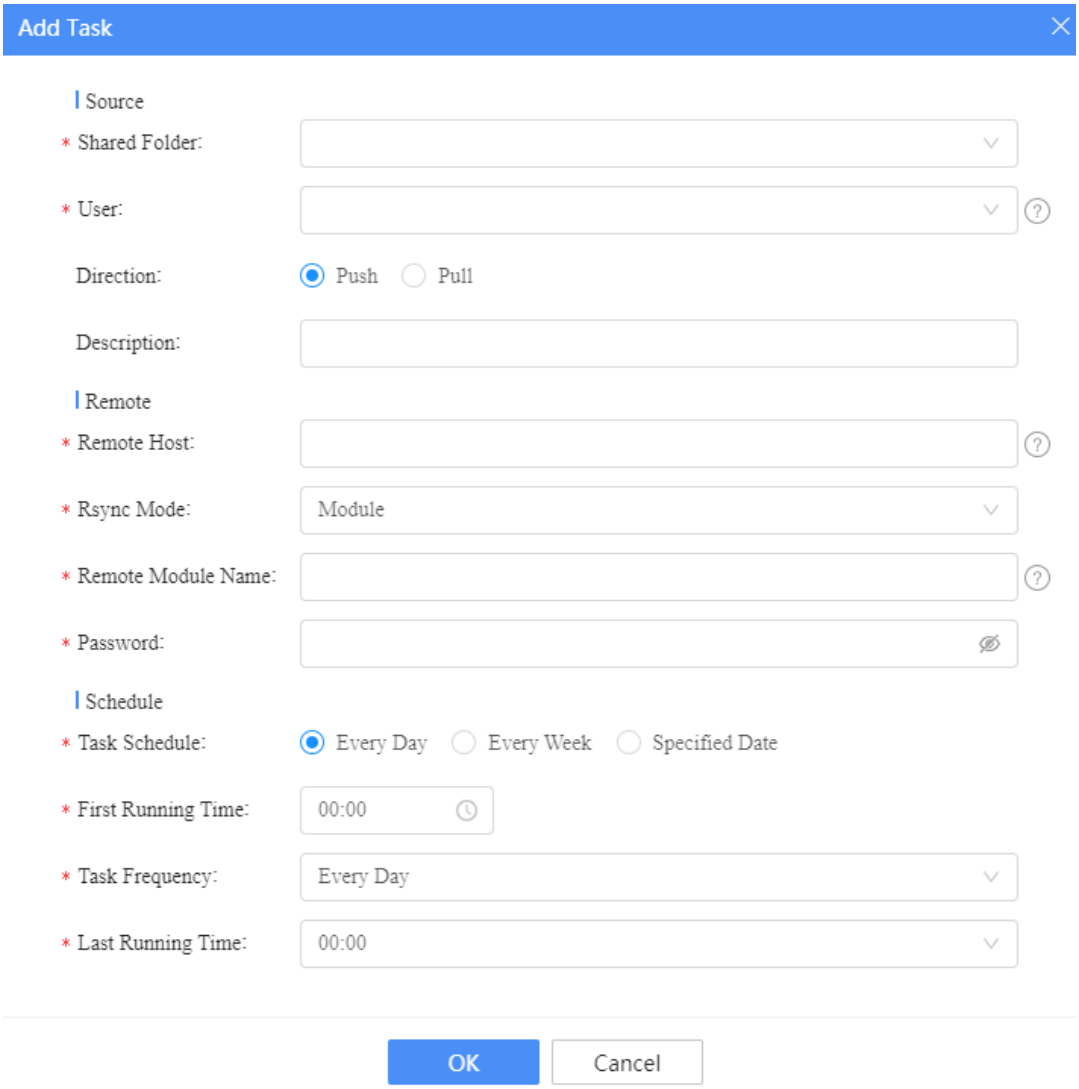
You need to enable rsync under **Control Panel** > **Security Manager** > **Service** first. See Service.

Go to **Control Panel** > **Task Manager** > **Rsync**.



Add a Task

1. Click **Add**.



2. Complete the settings. See the table below for descriptions.

Parameter		Description
Source	Shared Folder	Choose the shared folder containing the data you want to back up.
	User	Choose the user that will perform the Rsync task. **Note**: The user must have permission to write data to the specified folder on the remote host.
	Direction	● Push: Back up data on the NAS device to the remote host. ● Pull: Download data from the remote host to the NAS device.
	Description	Input a description of the task.
Remote	Remote Host	Input the IP or name of the remote host.
	Rsync Mode	● Module: After choosing this option, you need to configure the remote module name. ● SSH: After choosing this option, you need to configure the port and path for the remote host.
	Password	Input the password of the remote host.
Schedule	Task Schedule	Choose a repetition mode for the task. ● Every Day: The task will be run at the same time every day. ● Every Week: The task will be run at the same time on the same day every week.

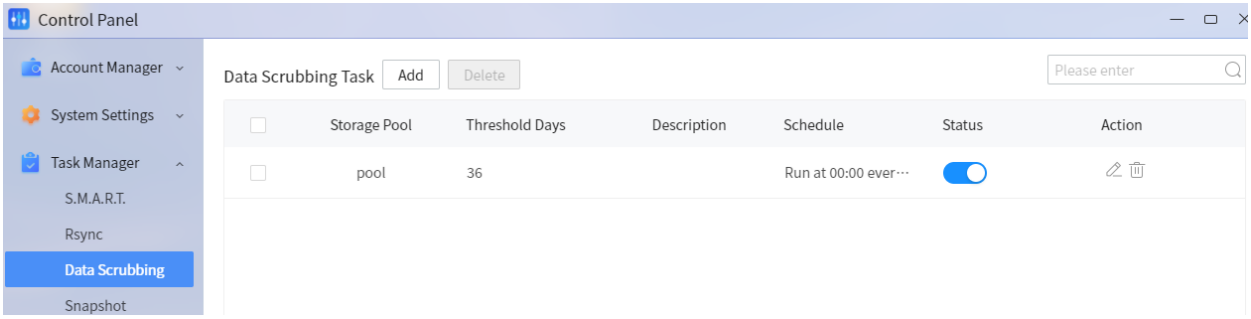
		● Specified Date: You need to specify a date and the repetition cycle, so the task will be run at the same time on the same day according to the set cycle.
	First Running Time	The first time when the task will be run.
	Task Frequency	How often to run the task.
	Last Running Time	The last time when the task will be run. Options are determined by “First Run Time + Task Frequency * Number of tasks.

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

3.3.3 Data Scrubbing

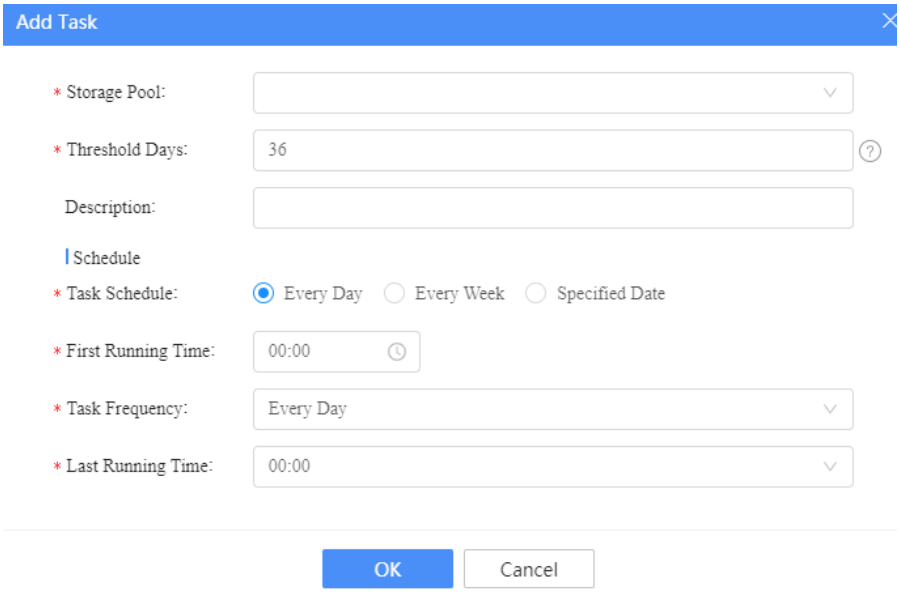
Data scrubbing is a maintenance function that deletes or repairs data in incorrect or incomplete storage pools. It is recommended to perform data scrubbing regularly to ensure data consistency and avoid losing data due to a disk failure.

Go to **Control Panel** > **Task Manager** > **Data Scrubbing**.



Add a Task

1. Click **Add**.



2. Complete the settings. See the table below for descriptions.

Parameter	Description
Storage Pool	Choose the target storage pool.

Threshold Days	Time interval between two data scrubbing tasks. After completing a data scrubbing task, the system continues checking the storage pool and performs the next data scrubbing task after the set threshold days is over.
Description	Input a description of the task.
Task Schedule	Choose a repetition mode: ● Every Day: The task will be run at the same time every day. ● Every Week: The task will be run at the same time on the same day every week. ● Specified Date: You need to specify a date and the repetition cycle, so the task will be run at the same time on the same day according to the set cycle.
First Running Time	The first time when the detection task will be run.
Task Frequency	How often to run a detection task.
Last Running Time	The last time when the detection task will be run. Options are determined by “First Running Time + Task Frequency * Number of tasks”.

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

3.3.4 Snapshot

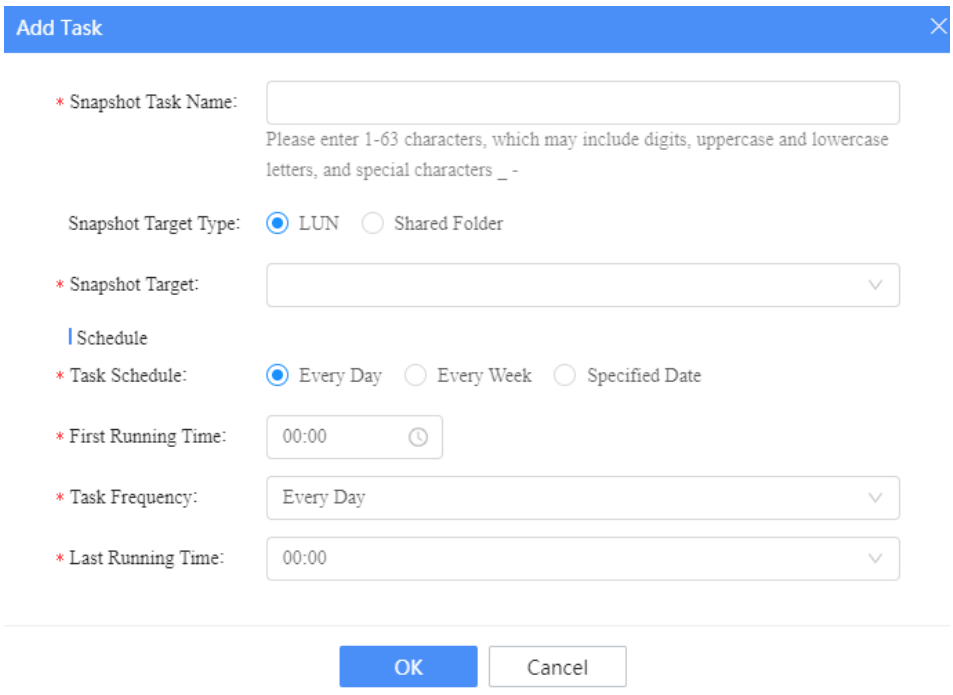
The snapshot is the data state of the NAS system at a certain point in time. You can create a snapshot of a shared folder or a LUN, and use the snapshot to restore data if the data is lost accidentally. Snapshots use a small storage space compared to backups.

It is recommended to add a schedule to create snapshots regularly in case you need to restore data to an earlier version.

Go to **Control Panel** > **Task Manager** > **Snapshot**.

Add a Task

1. Click **Add**.



2. Complete the settings. See the table below for descriptions.

Parameter	Description
Snapshot Task Name	Input a task name that is easy to recognize.
Snapshot Target Type	Choose the snapshot target type: LUN or Shared Folder.
Snapshot Target	Choose the target for the snapshot target type.
Task Schedule	Choose a repetition mode for the schedule: ● Every Day: The task will be run at the same time every day. ● Every Week: The task will be run at the same time on the same day every week. ● Specified Date: You need to specify a date and the repetition cycle, so the task will be run at the same time on the same day according to the set cycle.
First Running Time	The first time when the snapshot task will be run.
Task Frequency	How often to run a snapshot task.
Last Running Time	The last time when the snapshot task will be run. Options are determined by “First Running Time + Task Frequency * Number of tasks”.

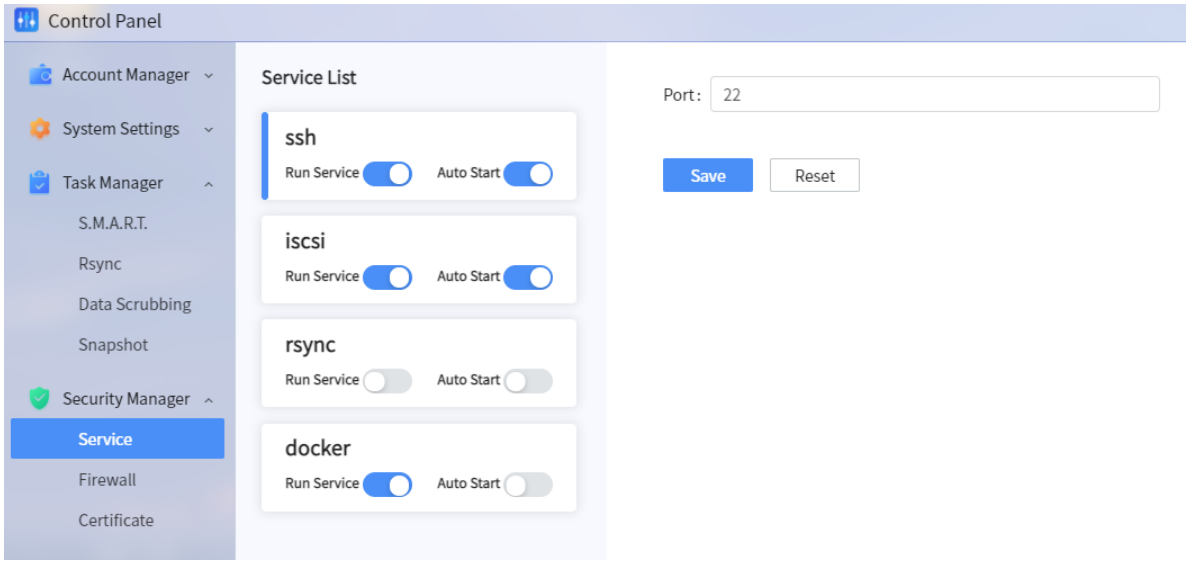
3. Click **OK** to save the settings.

3.4 Security Manager

3.4.1 Service

You can enable or disable services and automatic service startup.

Go to **Control Panel** > **Security Manager** > **Service**.



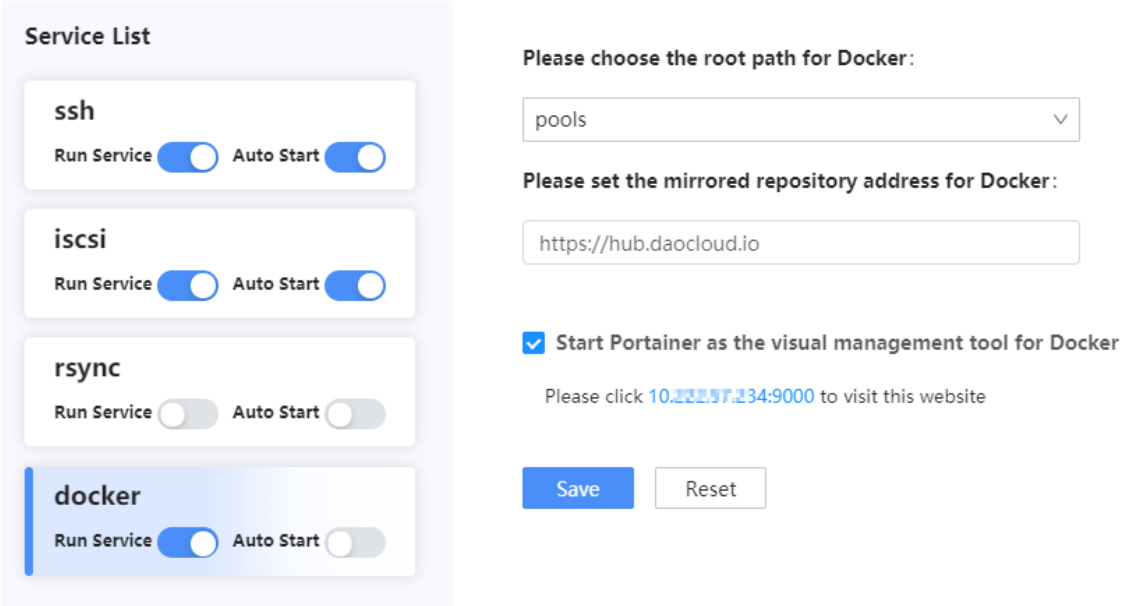
NOTE!

The service functions are described below:

- The ssh service is used to improve data transmission security.
- The iscsi service is used to provide efficient data storage.
- The rsync service is used to back up data on the NAS device to a remote host, or download data from a remote host to the NAS device.
- The docker service is used to containerize other applications on the NAS device as needed.

1. Flip the toggle switch to enable or disable a service.

- After enabling ssh/iscsi/rsync service, configure a port for the service.
- After enabling the docker service, choose the root path (storage pool), set mirrored repository address and enable Portainer as the visual management tool for the service. You can access Portainer by clicking the website http://NAS IP:9000 on the interface, install docker image and manage the docker container.

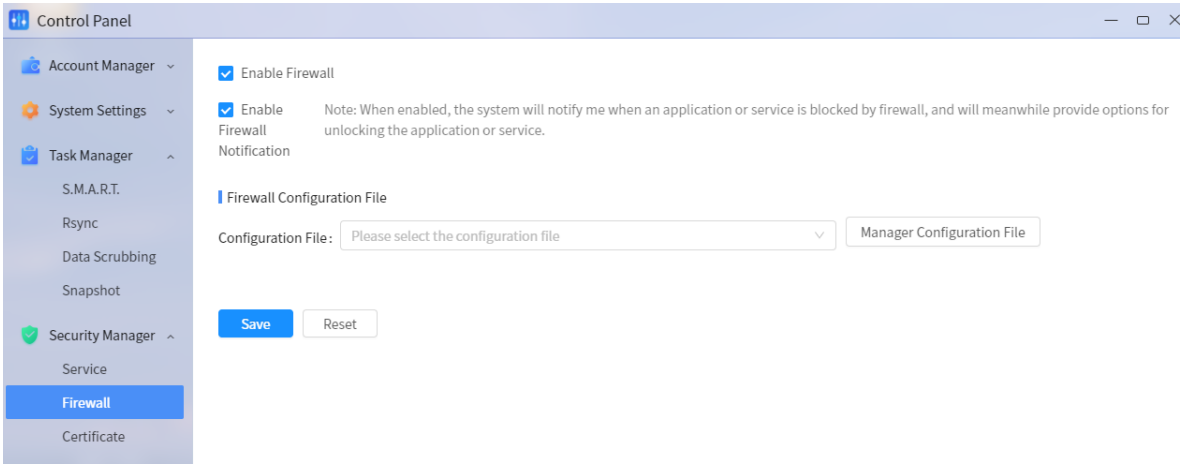


2. To enable a service to restart automatically after the NAS device restarts, turn on **Auto Start** for the service.
3. Click **Save** to save the settings.

3.4.2 Firewall

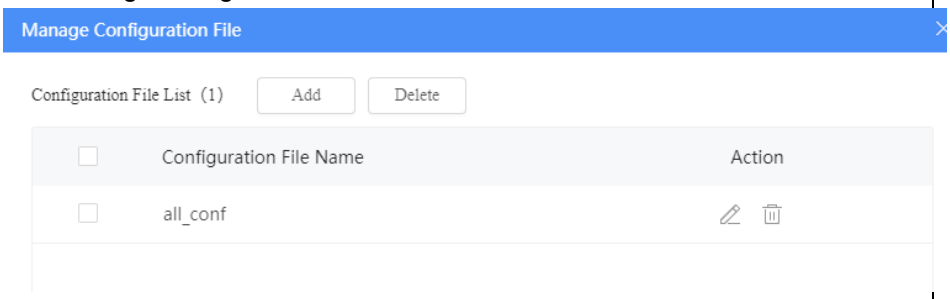
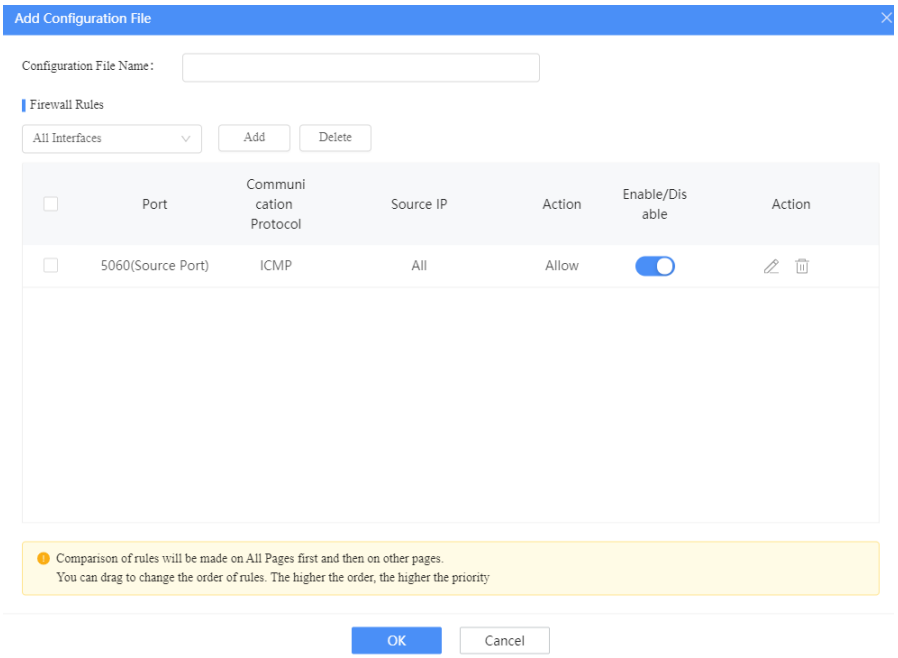
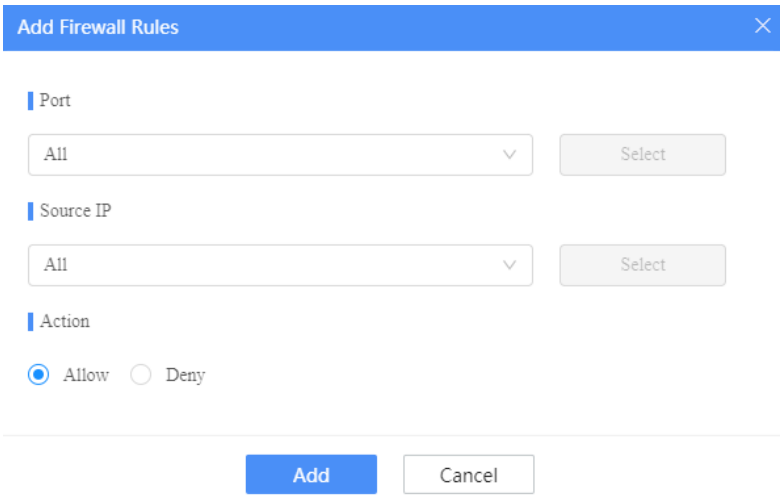
Enable firewall to prevent unauthorized login and control service access. You may also allow or deny access to certain network interfaces from specified IP addresses.

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



1. Complete the settings. Refer to the table below for parameter descriptions.

Parameter	Description
Enable Firewall	To enable firewall, select the checkbox.

Enable Firewall Notification	To enable firewall notification, select the checkbox. If enabled, the system will notify user when an application or service is blocked by firewall and provide unlock options.
Firewall Configuration File	You can set different configuration files to quickly apply different firewall rules according to security needs. ● If the configuration file is already created, choose it from the drop-down list. ● Otherwise, follow the steps to add one: 1. Click **Manage Configuration File**.  2. Click **Add**. On the page as shown below, input the file name, and choose a firewall rule from the list.  If the firewall rule is not created, click **Add** to create it.  ➢ Port: All (default), Custom (you need to specify a port or a port range).

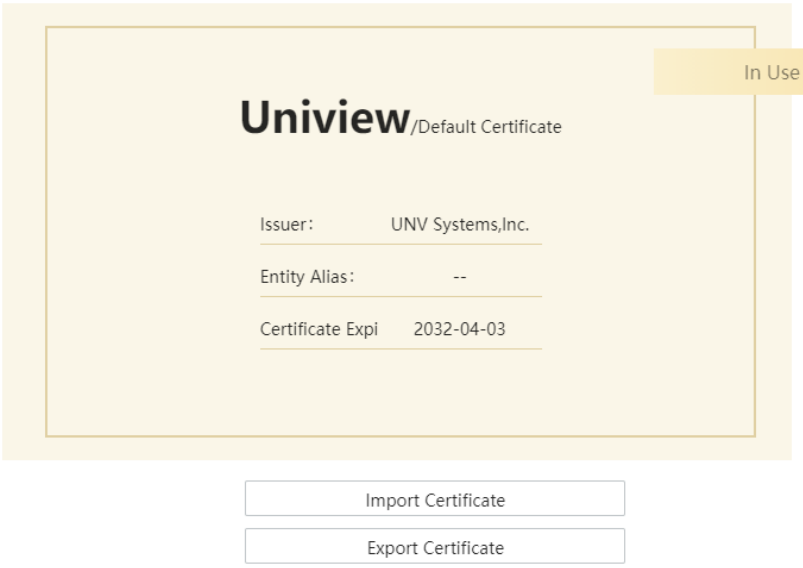
	➢ Source IP: All (default), Specified IP (you need to specify an IP address or an address range). ➢ Action: Allow (allow access from specified port and IP), Deny (deny access from specified port and IP). 3. Click **OK** to save settings on the pop-up windows one by one.

2. Click **Save** to save the settings.

3.4.3 Certificate

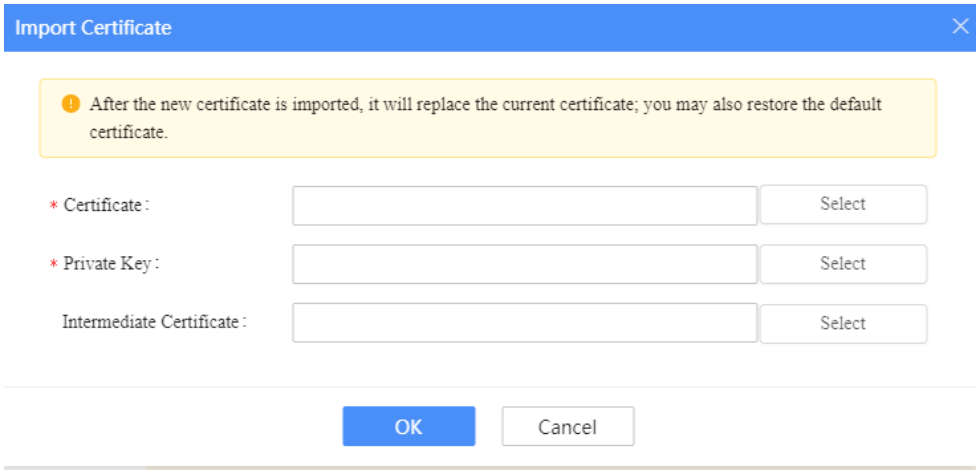
Certificates are used by SSL to protect the NAS, for example, webpage (all HTTPS service), email, or FTP. Certificates can verify server and admin identity before user sends confidential messages.

Go to **Control Panel** > **Security Manager** > **Certificate**.



Import a Certificate

1. Click **Import Certificate**. A page as shown below appears.



2. Click **Select** and choose a certificate, a private key, and an intermediate certificate from your computer.
3. Click **OK** to save the settings.

Export a Certificate

Click **Export Certificate**.

4 Storage Manager

Manage the HDDs, storage pool, and cache of the NAS device.

4.1 Overview

Go to **Storage Manager** > **Overview** to view hard disk slots, disk status (normal, abnormal, no disk), and usage of storage space.

Click to select a storage pool to view the disks in the pool (identified by a white box on the device diagram).

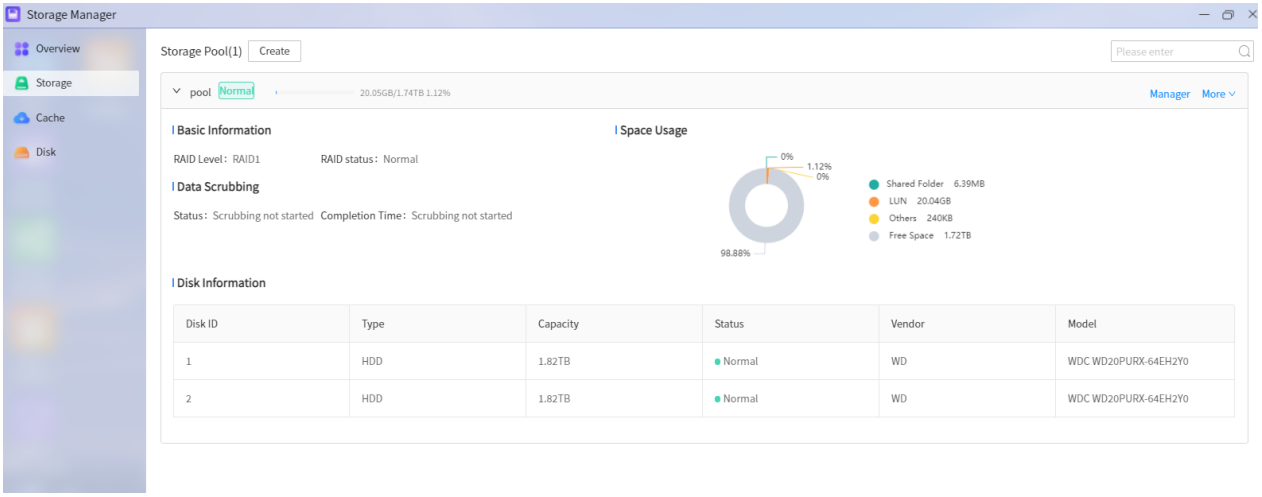
4.2 Storage

A storage pool is one or several sets of RAID-protected HDDs used to store data. Different RAID types provide different levels of data protection.

Go to **Storage Manager** > **Storage**.

4.2.1 Storage Pool Information

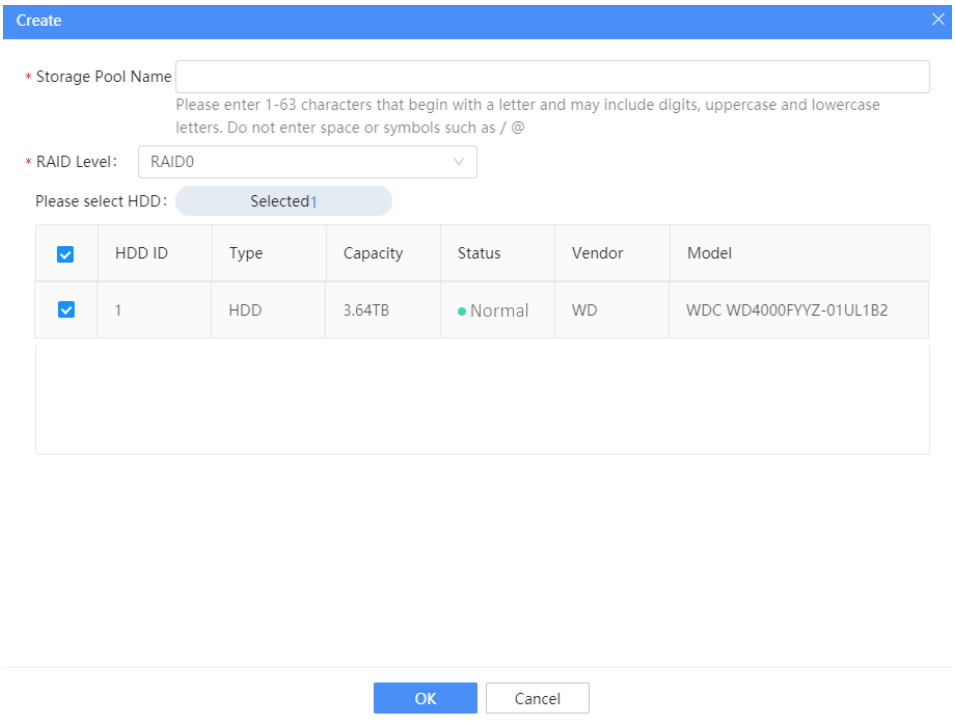
After creating a storage pool, you can view its overall status, space utilization, and disk information on the **Storage** page.



4.2.2 Create Storage Pool

Follow the steps to create a storage pool:

1. Click **Create**.



2. Input a name for the storage pool.
3. Choose a RAID level. Refer to the table below for RAID descriptions.

Level	Min. Number of Disks (N)	Data Storage Mode	Storage Capacity Provided
RAID0	≥1	Stripes data across multiple disks without redundancy.	=Total disk capacity
RAID1	2	Stores two identical copies of data on two disks for redundancy.	=Capacity of the smallest disk
RAID5	≥3	Stripes data across multiple disks with parity and provides redundancy.	= (N-1) * Capacity of the smallest disk
RAID6	≥4	Performs dual parity and uses the capacity of two disks to store parity data.	= (N-2) * Capacity of the smallest disk

RAID10	≥4 (must be even)	Provides the performance of RAID0 and the protection of RAID1. Uses two identical RAID0 arrays to store two identical copies of data.	= (N/2) * Capacity of the smallest disk
RAID50	≥6	Provides the performance of RAID0 and the protection of RAID5. Stripes data across two disk groups with parity. The number of disks in each group must be the same and ≥3.	= (N-2) * Capacity of the smallest disk
RAID60	≥8	Provides the performance of RAID0 and the protection of RAID6. Stripes data across 2 disk groups with dual parity. The number of disks in each group must be the same and ≥3.	= (N-4) * Capacity of the smallest disk
RAIDTP	≥5	Performs triple parity and uses the capacity of three disks to store parity data.	= (N-3) * Capacity of the smallest disk

4. Select the required number of HDDs according to the RAID level.

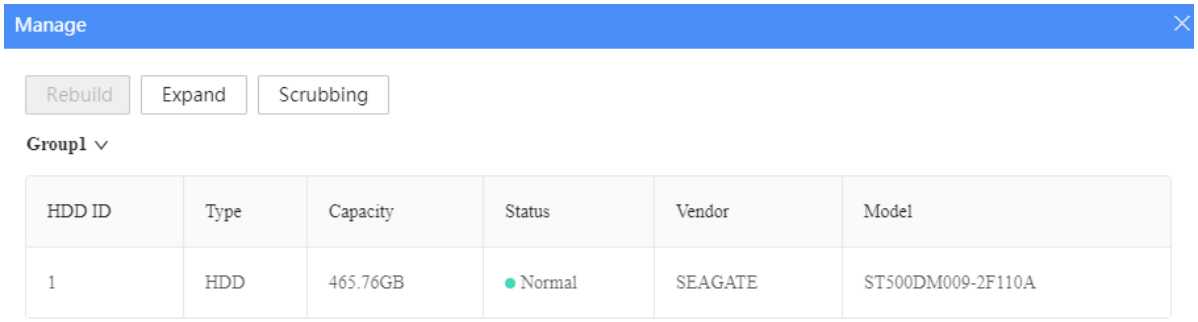
CAUTION!
Before creating a storage pool, be sure to back up data stored on the HDDs that are used to create the storage pool. All the data on the HDDs will be erased during the creation of the storage pool.

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

4.2.3 Manage Storage Pool

Rebuild, expand, and scrub a storage pool.

On the **Storage** page, click **Manager** for the storage pool. A page as shown below appears.



1. Rebuild

Rebuild the RAID if any HDD in it is damaged.

Select the faulty HDD and then click **Rebuild**.

2. Expand

Add HDDs to a storage pool to expand the capacity.

NOTE!

Expansion rules for different RAID levels:

- **RAID0**: Supports expansion with any number of HDDs (1-n). RAID level does not change after expansion.
- **RAID1**: The number of HDDs used for expansion must be the same as the current HDD number (2, in this case). RAID level changes to RAID10 after expansion.
- **RAID5**: The number of HDDs used for expansion must be the same as the current HDD number. RAID level changes to RAID50 after expansion.
- **RAID6**: The number of HDDs used for expansion must be the same as the current HDD number. RAID level changes to RAID60 after expansion.
- **RAIDTP**: Expansion is not available due to system capacity.
- **RAID50/RAID60**: Expansion is not available due to system capacity.
- **RAID10**: Supports expansion with 2 HDDs only.

Follow the steps to expand the storage pool:

1. Install expansion HDDs on the NAS device.
2. Click **Expand**.
3. Select the HDDs to be added to the storage pool.
4. Click **OK** to save the settings.

3. Scrubbing

Scrubbing can delete or repair corrupted or incomplete data in the storage pool to ensure data consistency.

Click **Scrubbing**.

4.2.4 Rename Storage Pool

1. On the **Storage** page, click **More** for the storage pool, and then choose **Rename**.
2. Change the storage pool name.
3. Click **OK** to save the settings.

4.2.5 Delete Storage Pool

CAUTION!

The stored data may be lost after the storage pool is deleted.

1. On the **Storage** page, click **More** for the storage pool, and then choose **Delete**.
2. A dialog box appears. Click **OK** to confirm the deletion.

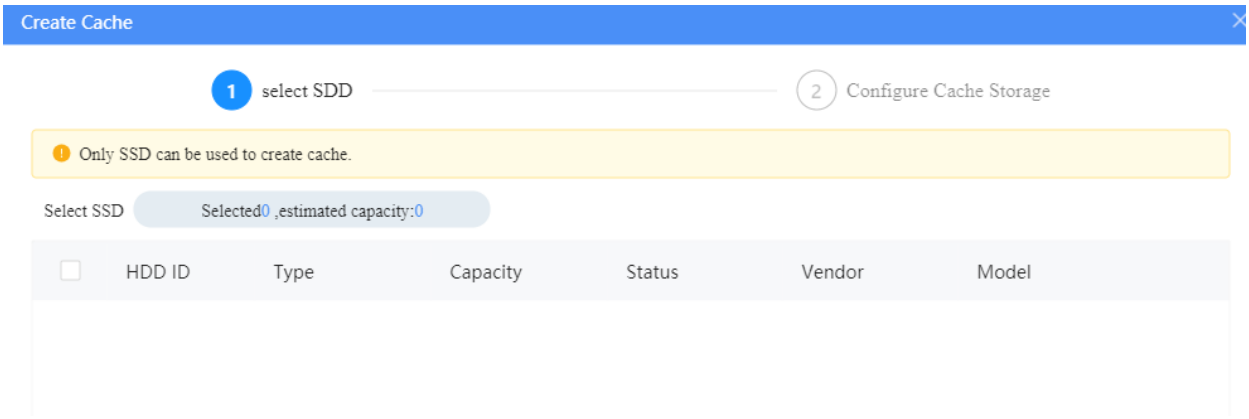
4.3 Cache

Create cache using the SSD installed on the NAS device. SSD cache can improve read and write speed when the NAS device handles many random read and write operations (such as re-reading previously accessed files).

Go to **Storage Manager** > **Cache**.

Add Cache Device

1. Click **Add Cache Device**. A page as shown below appears.

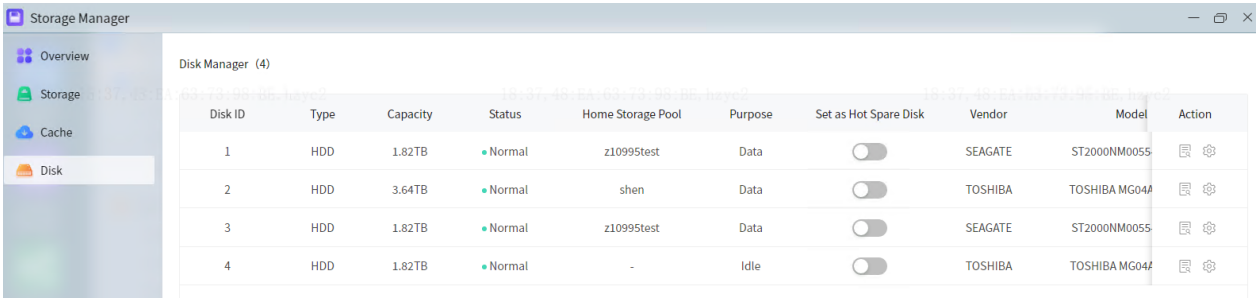


2. Choose SSDs, and then click **Next**.
3. Configure cache storage.
4. Click **OK**.

4.4 Disk

View information about HDDs installed on the NAS device, including the type, capacity, status, home storage pool, usage, manufacturer, model, and whether is a hot spare disk.

Go to **Storage Manager** > **Disk**.



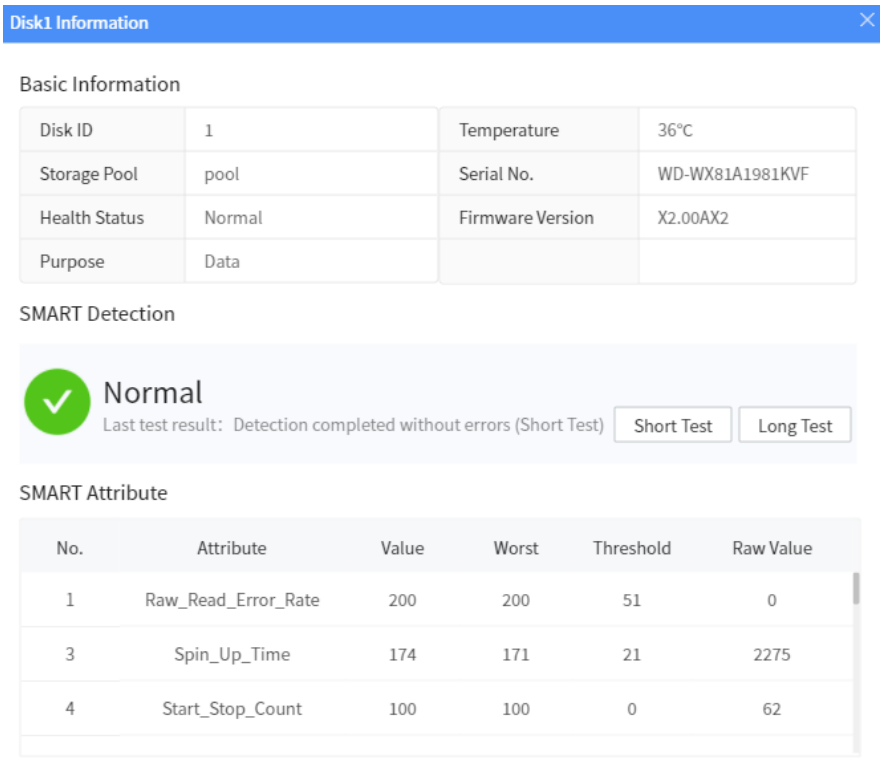
- Set as a hot spare disk:

A hot spare disk offers extra protection by functioning as a backup and replacing the damaged HDD in the RAID.

Flip the toggle switch for an HDD to set it as a hot spare disk.

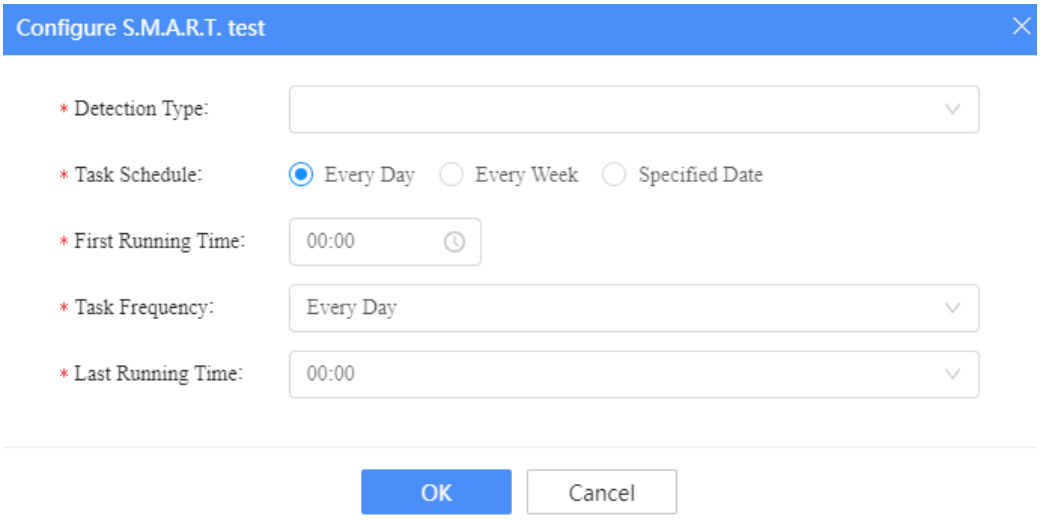
- View HDD details:

Click for the HDD.



- Configure a S.M.A.R.T. test task:

Click ⚙ to configure a S.M.A.R.T. test task for an HDD. See S.M.A.R.T. Test Task for more information.



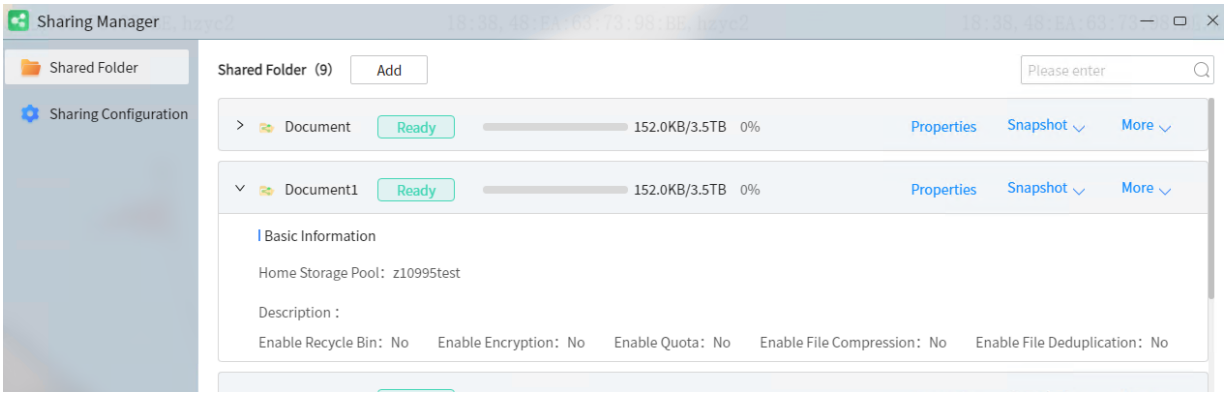
5 Sharing Manager

Sharing Manager allows you to configure shared folders and sharing services to turn the NAS device into an accessible and safe file sharing center.

5.1 Shared Folder

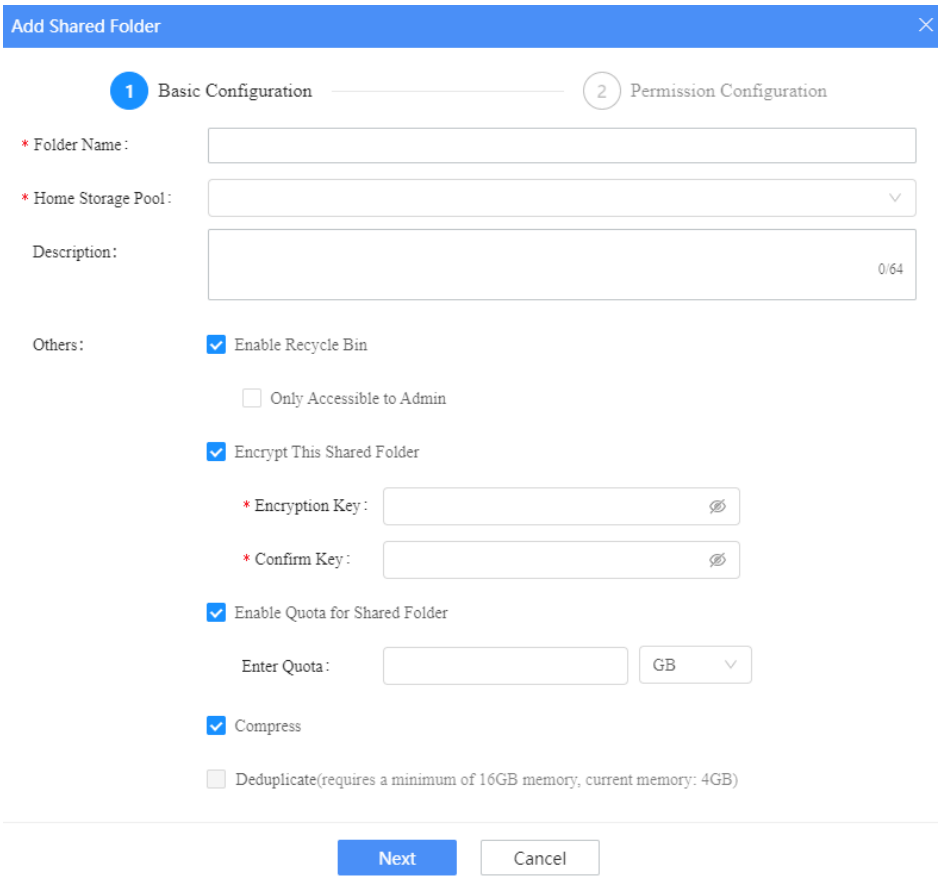
The shared folder is the basic directory for storing files and folders. You need to create at least one shared folder to store data on the NAS device. You can set different access permissions for the shared folder, for example, set it as “private” or accessible only to certain users or user groups.

Go to **Share Manager** > **Shared Folder** to view shared folders, including folder information and space usage.



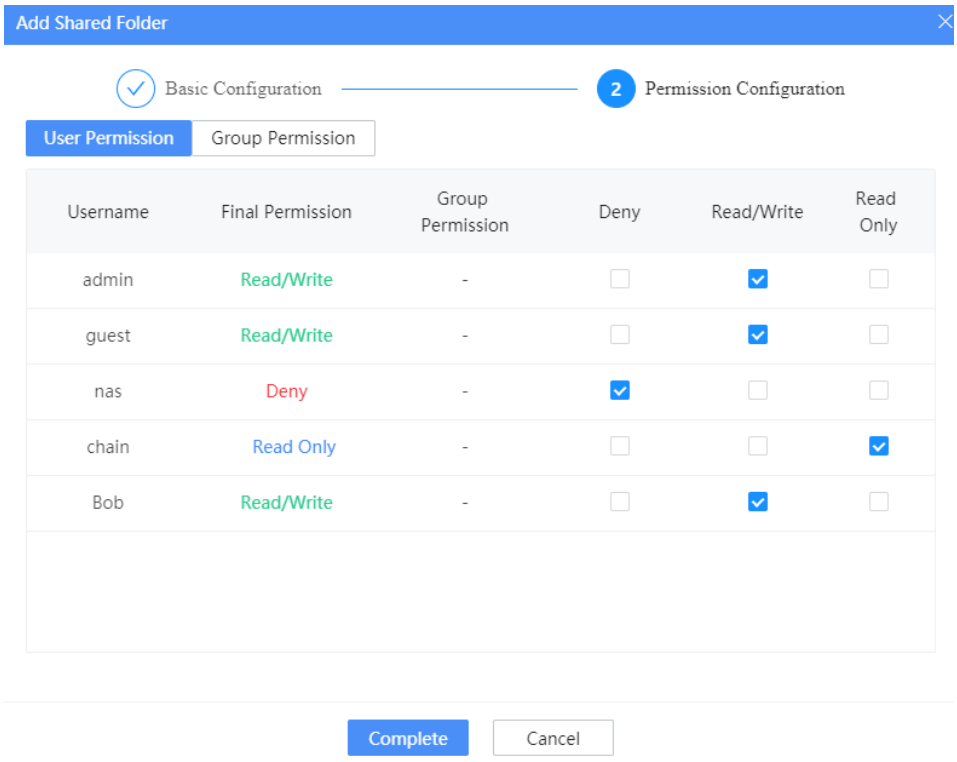
5.1.1 Add Shared Folder

1. Click **Add**.
2. Complete the basic information and then click **Next**.



Item	Description
Folder Name	Input a name for the shared folder. Only letters and digits are allowed.
Home Storage Pool	Select a storage pool for the folder.
Description	Input a description of the folder, for example, its usage.
Others	Select the items you want to use. ● Enable Recycle Bin: When enabled, the deleted files will be kept in the recycle bin until being restored or permanently deleted. To allow only admin to access the recycle bin, select the **Only Accessible to Admin** checkbox. ● Encrypt This Shared Folder: When enabled, you need to set a private key to encrypt the shared folder. Other users must decrypt the folder using the private key before they can view the folder contents. ● Enable Quota for Shared Folder: When enabled, you need to set a space limit for the shared folder. ● Compress: When enabled, the system automatically compresses data in the shared folder to save space. Compressed data will be extracted automatically when you search or use them. ● Deduplicate: When enabled, the system will check for duplicate data and keep one copy only by deduplication.

3. Configure access permission for users and user groups. Permission includes Deny, Read/Write, Read Only. Select the checkbox(es) to assign permission.



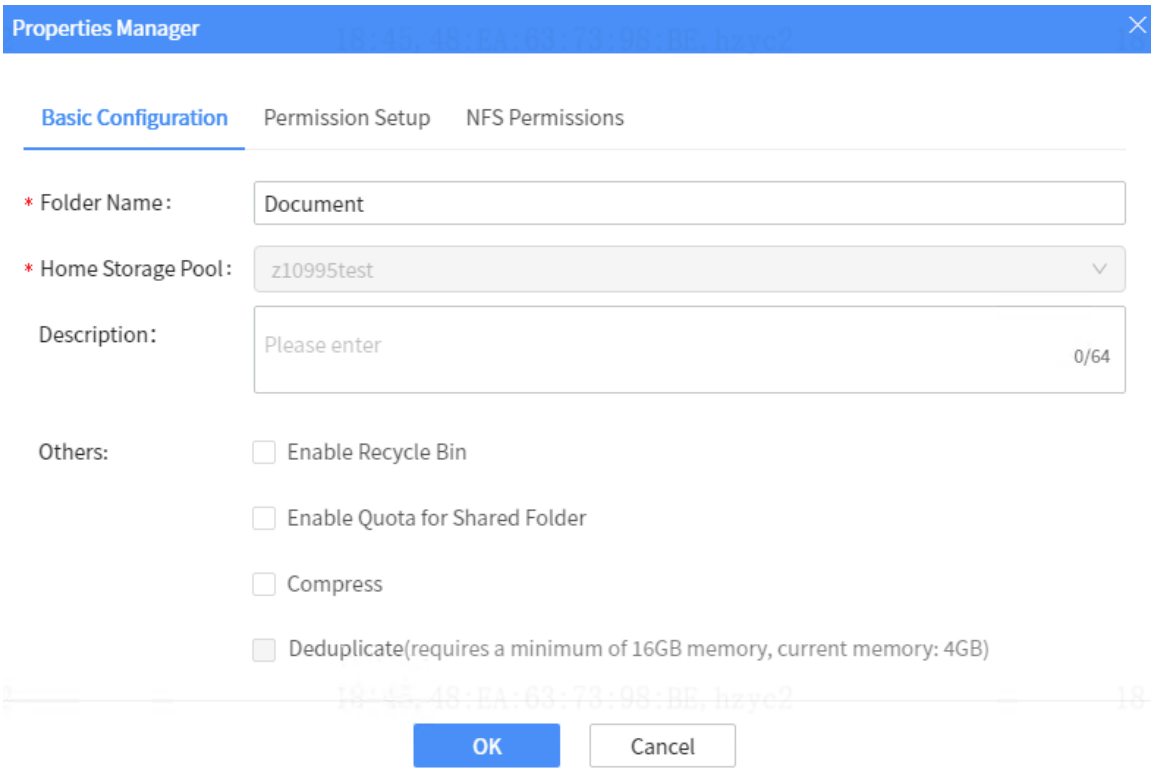
4. Click **Complete**. The shared folder is added.

5.1.2 Properties Manager

Edit the basic configuration and read/write permission for a shared folder, and set NFS permissions to share the folder with Linux clients.

1. Edit Configuration and Permission

1. Click **Properties Manager** for the shared folder you want to edit.



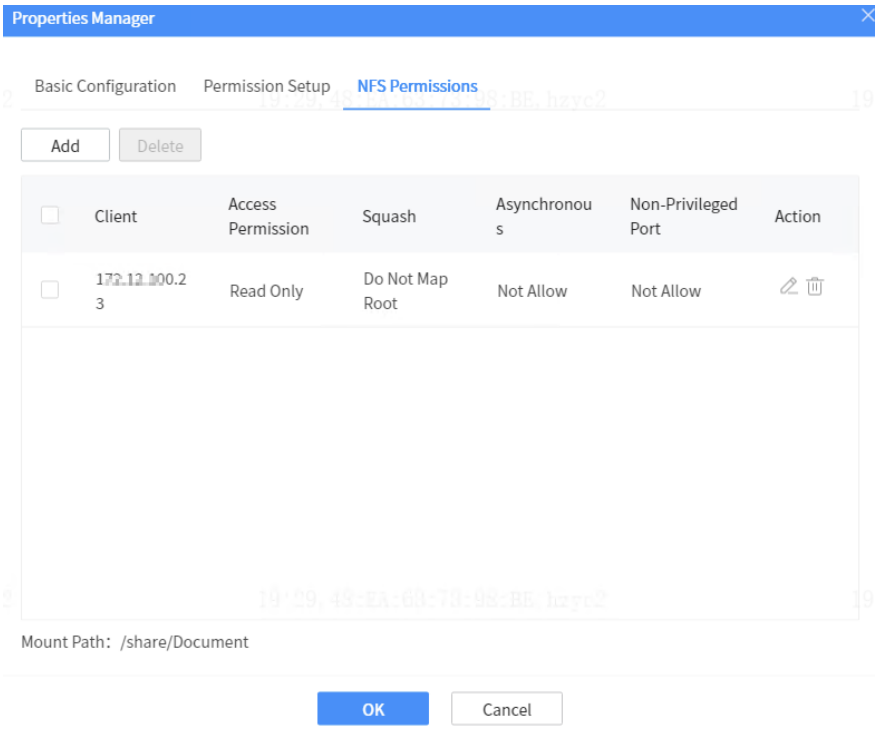
2. On the **Basic Configuration** tab, edit the basic settings for the shared folder. On the **Permission Setup** tab, set read/write permissions for the shared folder. For parameter descriptions, see Add Shared Folder.
3. Click **OK** to save the settings.

2. Configure NFS Permissions

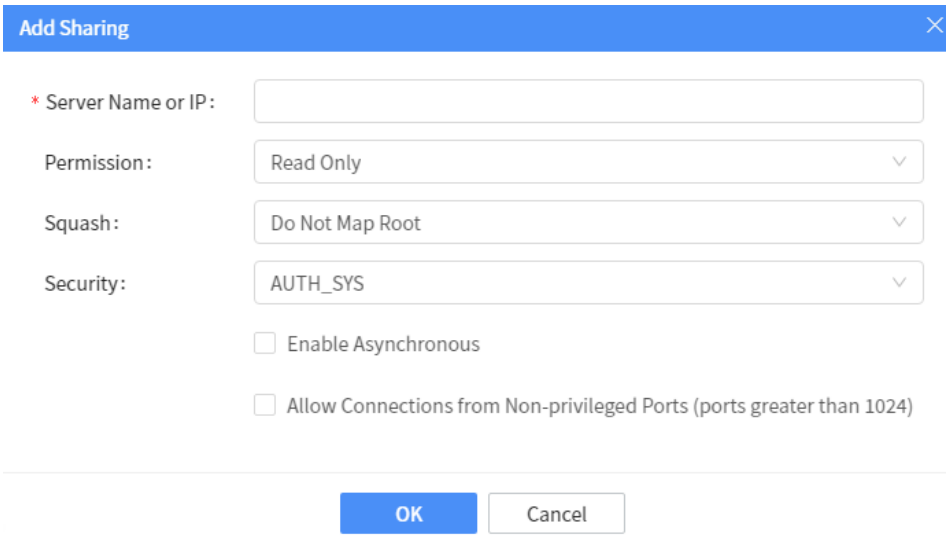
Configure NFS permissions to allow Linux clients to access the shared folder.

NOTE!
You need to enable NFS service first. See Share with Linux.

1. Click **Property** > **Properties Manager** > **NFS Permissions** for the shared folder you want to edit.



2. Click **Add Sharing**. A page as shown below appears.

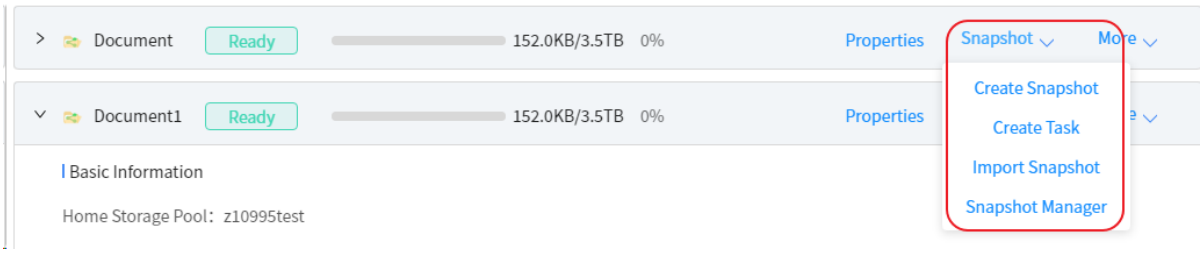


3. Enter the Linux server's name or IP address, and set other configurations as needed.
4. Click **OK**.

5.1.3 Snapshot

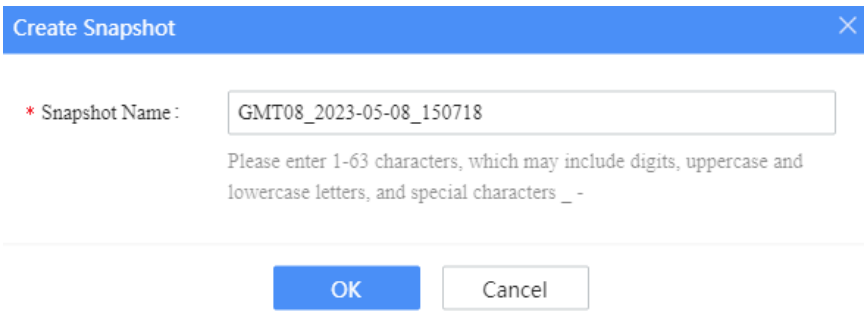
Create a snapshot to make a duplicate of a shared folder at a given time in case you need to restore data after data is lost accidentally. Snapshots use a small storage space compared to backups.

On the **Shared Folder** page, click **Snapshot** of the shared folder and then choose options as you need.



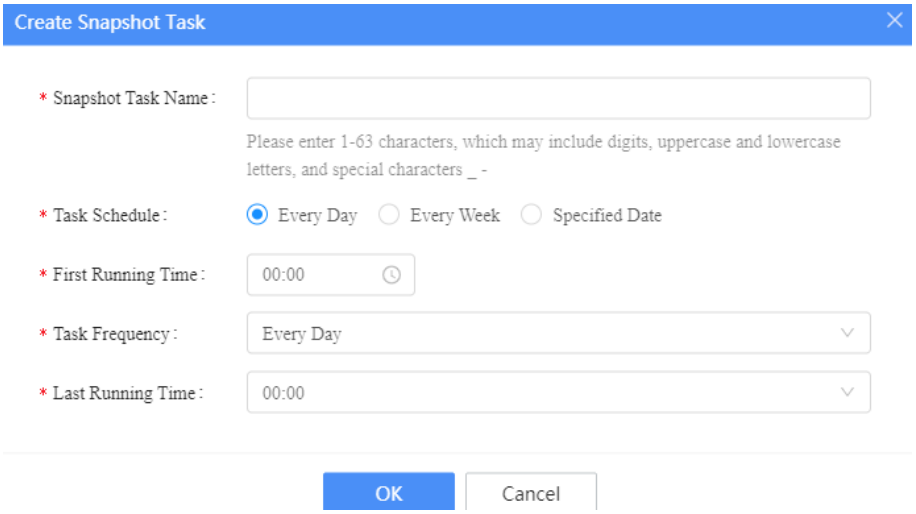
1. Create Snapshot

Input the snapshot name (the current time by default), and then click **OK.** A snapshot of the shared folder at the current time is created.



2. Create Task

It is recommended to create a periodical snapshot task to automatically save the snapshot at a given time to improve security



1. Complete the settings. See the table below for descriptions.

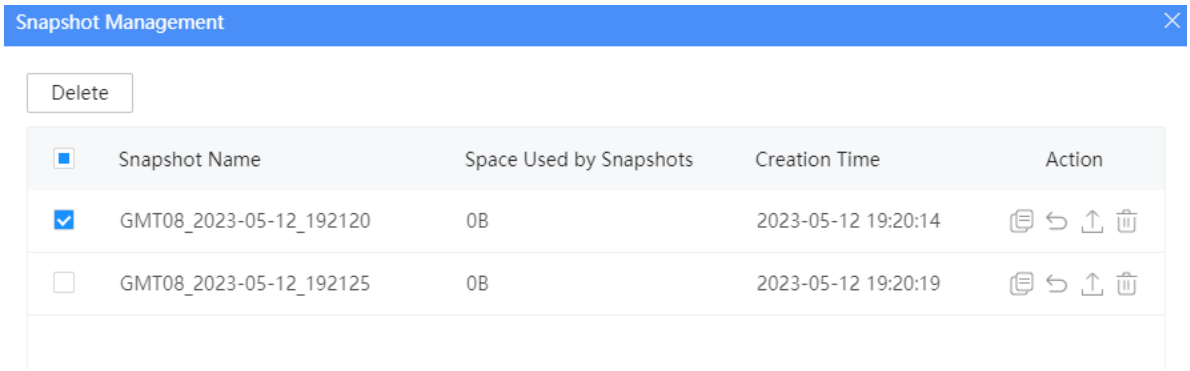
Parameter	Description
Snapshot Task Name	Input a task name that is easy to recognize.
Task Schedule	Choose a repetition mode for the schedule: ● Every Day: The task will be run at the same time every day. ● Every Week: The task will be run at the same time on the same day every week. ● Specified Date: You need to specify a date and the repetition cycle, so the task will be run at the same time on the same day according to the set cycle.
First Running Time	The first time when the snapshot task will be run.
Task Frequency	How often to run a snapshot task.

Last Running Time	The last time when the snapshot task will be run. Options are determined by “First Running Time + Task Frequency * Number of tasks”.

2. Click **OK** to save the settings.

3. Snapshot Manager

View the snapshots created for the shared folder.

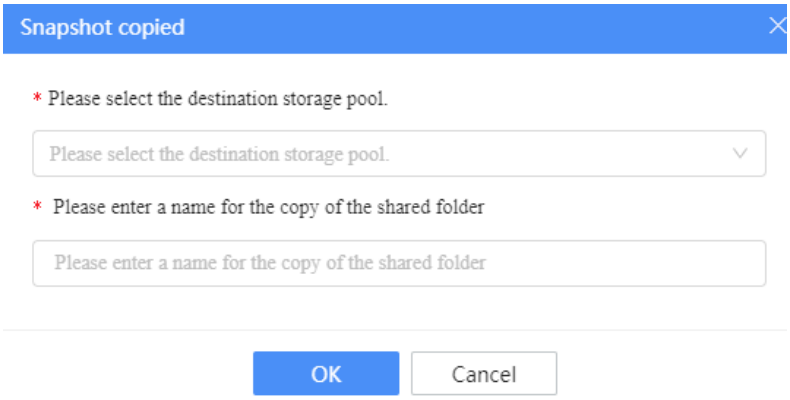


The following operations are supported:

- **Copy**: Copy the shared folder at the time of the snapshot, that is to create a copy of the shard folder, which will not affect the current shared folder.

  (1) Click .

  (2) Select the destination storage pool, and input the name for the copy of the shared folder.



  (3) Click OK to copy the shared folder. You can view the copy of the shared folder on the Shared Folder page.

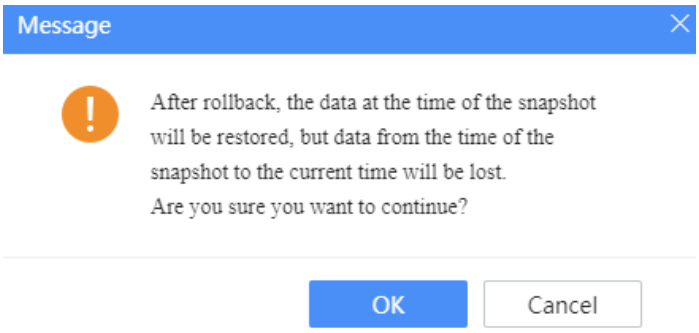
NOTE!
The copy of the shared folder has no user permissions by default. You need to set permission first, then you can access the shared folder.

- **Rollback**: Restore the data to the previous version at the time of the snapshot.

WARNING!
After rollback, the data from the time of the snapshot to the current time will be lost.

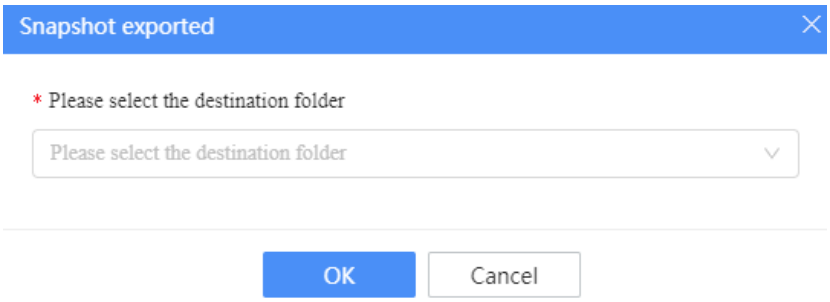
(1) Click .

(2) Click **OK** on the pop-up interface to rollback the data.



- **Export**: Export the snapshot to the shared folder.

(1) Click .



(2) Select the destination folder.

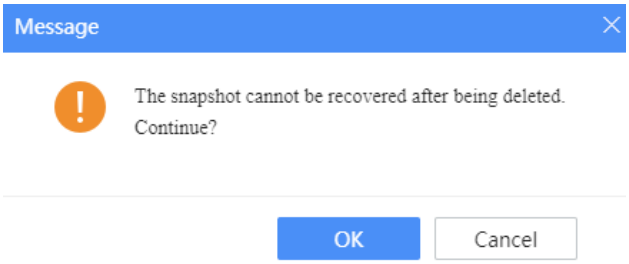
(3) Click **OK** to export the snapshot.

You can view the exported snapshot from the shared folder on the **File Manager** page.

- **Delete**: Delete the snapshot.

(1) Click .

(2) Click **OK** on the pop-up interface to delete the snapshot.



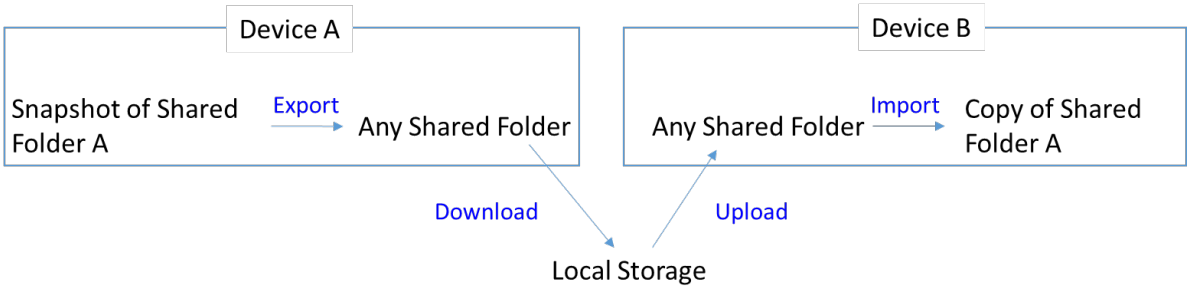
4. Import Snapshot

Import a snapshot to make a duplicate of a shared folder at a given time.

Snapshots can be imported to the current device or other devices.

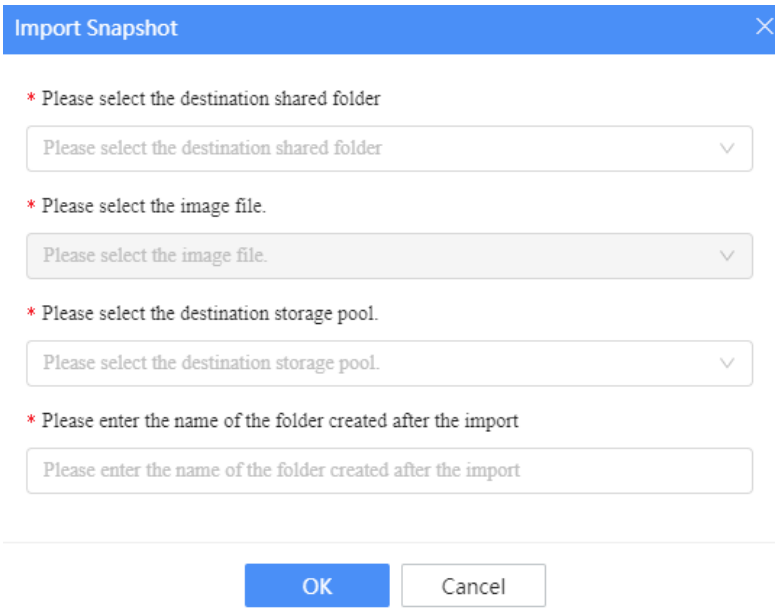
- Import a snapshot to the current device

- Import a snapshot to other devices



Follows the steps to import the snapshot:

1. Click **Import Snapshot**.



2. Select the destination shared folder, image file and destination storage pool, and input the name of the folder created after the import.
3. Click OK to import the snapshot. You can view the created folder on the Shared Folder page.

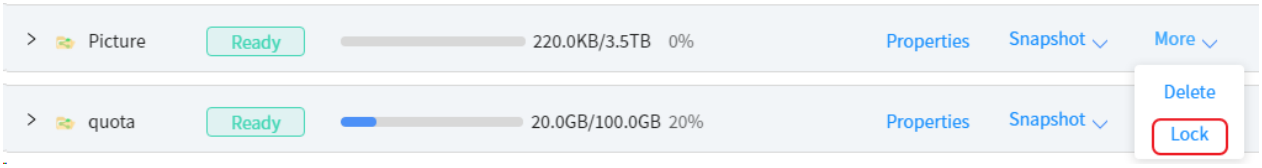
NOTE!
The imported shared folder copy has no user permissions by default. You need to set permission first so authorized users can access the shared folder.

5.1.4 Lock/Unlock

You can lock a shared folder if you have enabled encryption and set a private key for the shared folder. Users need to enter a key in order to access the shared folder.

- Lock

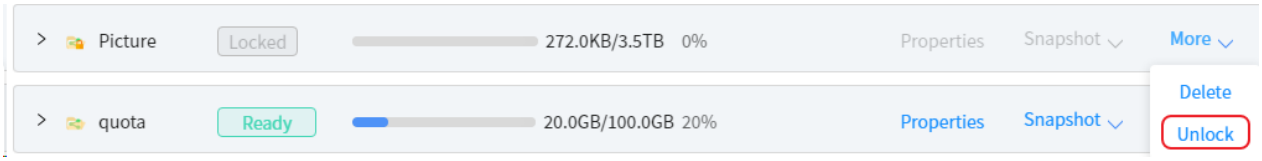
1. Click **More** for the folder you want to lock and then choose **Lock**.



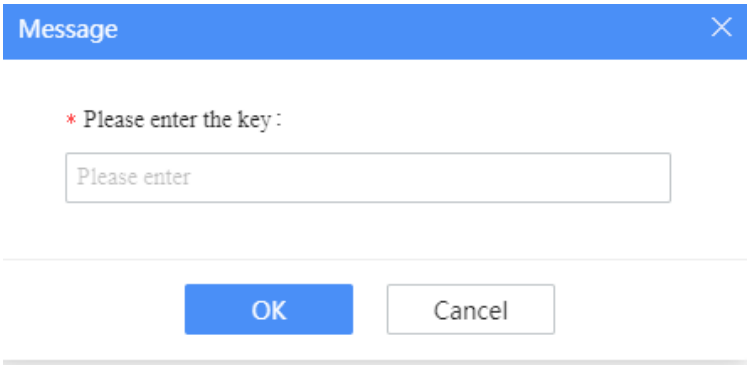
2. After the shared folder is locked, users cannot edit, upload or download files, or create a snapshot for the shared folder.

- Unlock

1. Click **More** for the folder you want to unlock and then choose **Unlock**.



2. Enter the key, click **OK**, and then the folder will be unlocked after the key is verified.



5.1.5 Delete Shared Folder

Follow the steps to delete a shared folder:

CAUTION!
A shared folder will be permanently deleted if recycle bin is disabled. If recycle bin is enabled, the deleted folder will be kept in the recycle bin until you delete it permanently.

1. Click **More** for the shared folder you want to delete and then choose **Delete**.
2. Click **OK** to confirm the deletion.

5.2 Sharing Configuration

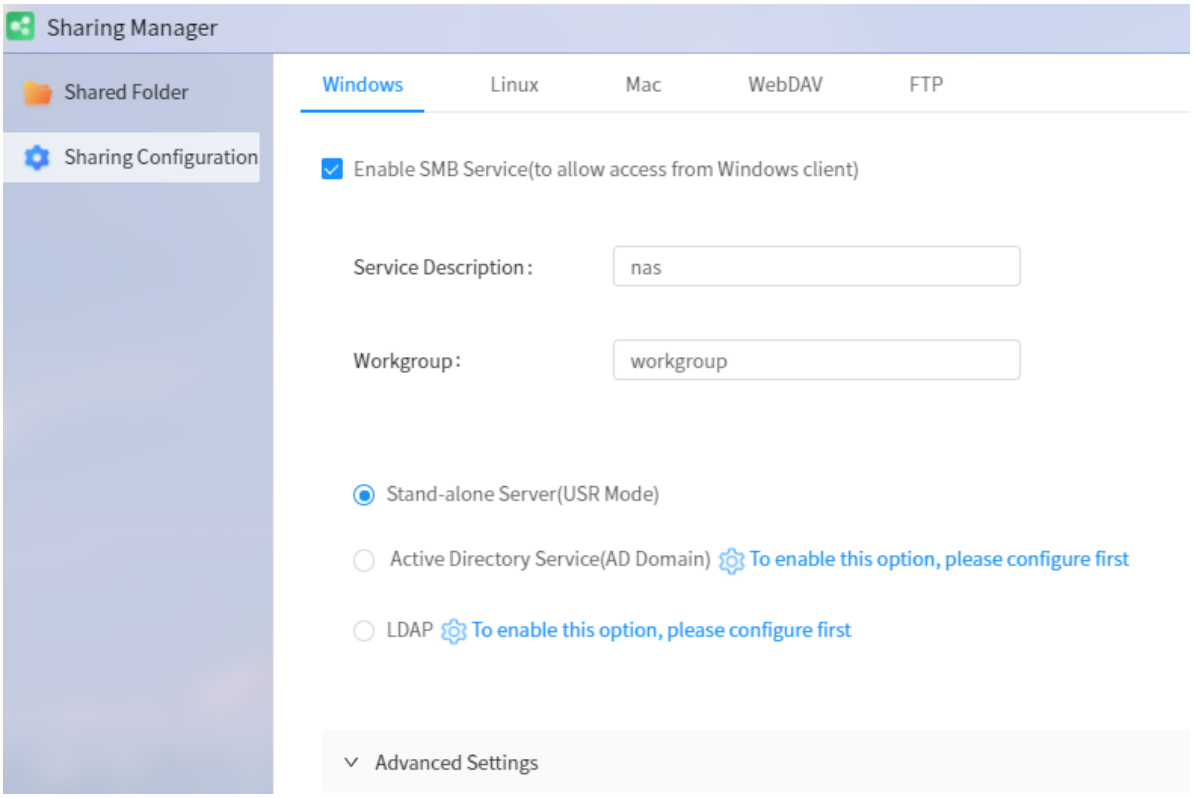
Go to **Sharing Manager** > **Sharing Configuration** and configure sharing service parameters for different sharing modes, so users can access files on the NAS device from different types of clients, including Windows, Linux, Mac, WebDAV, and FTP clients.

5.2.1 Share with Windows

Windows users can use File Explorer to access shared files on the NAS device or mount a shared folder on the NAS as a network disk.

1. Enable SMB

You need to enable SMB to allow access from a Windows client.

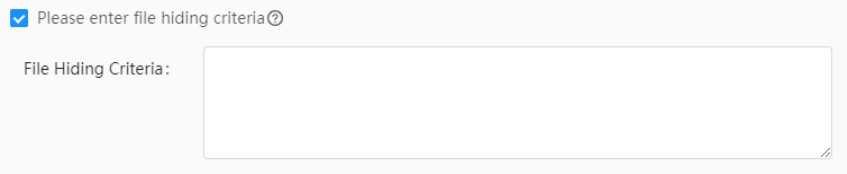


See the table below for descriptions.

Item	Description
Enable SMB	Select the checkbox to enable the Server Message Block (SMB) service.
Service Description	Service name of the NAS device on the LAN, for example, nas.
Workgroup	Workgroup that the NAS device belongs to on the LAN, for example, workgroup.
Stand-alone Server (USR Mode)	Choose this option if the Windows computer functions as a stand-alone server. Users can access the NAS device as a current NAS user.
Active Directory Service (AD Domain)	AD users can access the NAS device when AD domain is enabled. To enable this option, add AD domain in **Control Panel** > **Account Manager** > **Domain**.
LDAP	LDAP users can access the NAS device when LDAP domain is enabled. To enable this option, add AD domain in **Control Panel** > **Account Manager** > **Domain**.

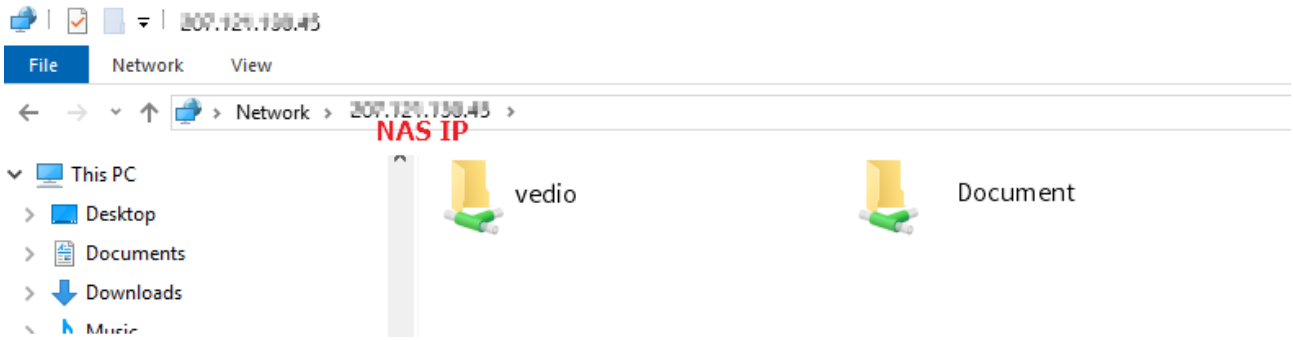
If you have higher security and performance requirements on the sharing, click **Advanced Settings** to expand it. Refer to the table below for more information.

Item	Description
Enable WINS Server	The WINS server is used for domain name resolution. This option is required when your network doesn't have a WINS server and some computers are in different subdomains. Make sure there's only one WINS server on the network and all the computers on the network are set to use this WINS server.
Use Specified WINS Server	Input the IP address of the specified WINS server.

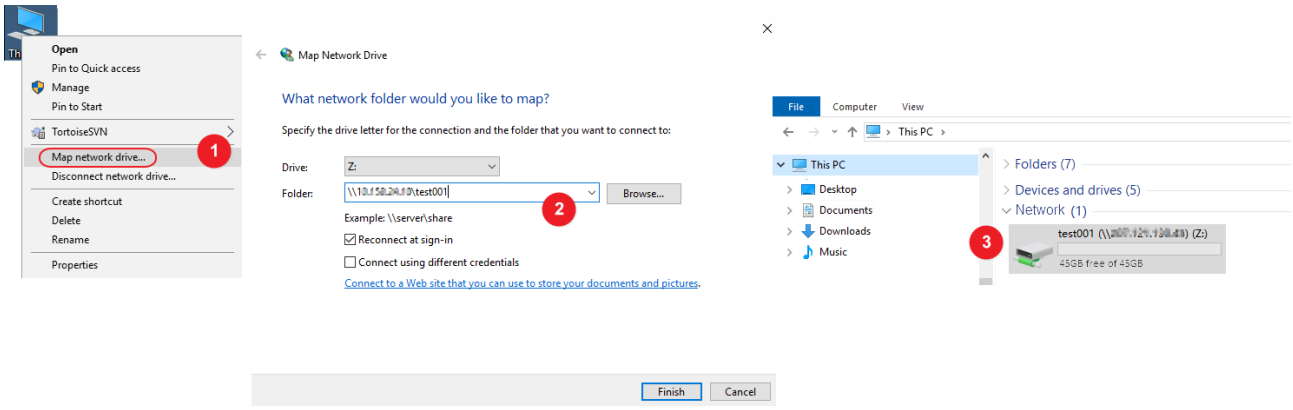
Domain Name Resolution Order	Choose the name resolution order: WINS First, or DNS First.
Set as Domain Master Browser	When enabled, the NAS device can be used as the local master browser. The local master browser is responsible for maintaining the device list in the network workgroup.
Allow NTLMSSP Authentication Only	When enabled, only NTLMSSP authentication will be allowed. Make sure all the computers on the network support NTLMSSP authentication. When disabled, NTLM authentication will be applied and provide lower security.
Alternative Login Method	When enabled, users can access the NAS device through Domain\Username instead of Domain+Username.
Enable DNS Auto Update	This option is available when AD Domain is enabled. When enabled, the NAS device can be registered on the DNS server, so the NAS device will automatically update its IP on the DNS server after the NAS device IP is changed.
Enable Trusted Domain	This option is available when AD Domain is enabled. When enabled, trusted users from AD domains can be added.
Enable Asynchronous IO Mode	This mode can improve SMB performance through asynchronous I/O. Asynchronous I/O refers to the I/O on the CIFS protocol. **Note**: If this option is enabled, you need to use UPS in case of a power outage.
Enable WS-Discovery	When enabled, Web Services Dynamic Discovery is available, and the NAS device will appear in File Explorer on the Windows 10 computer.
Highest SMB Version Lowest SMB Version	Choose the highest and lowest SMB protocol versions used on your network. **Note**: SMB3 is supported since Windows 8 and Windows Server 2012; and SMB2 is supported since Windows Vista.
Allow Symbolic Link in Shared Folder	When enabled, a link (path) to shared file B can be included in shared file A, so Windows users can visit shared file B when visiting shared file A.
Restrict Anonymous Access to SMB Shared Folder	Choose whether identity verification is required when anonymous user wants to access the shared folder via SMB. ● Disable: Everyone can view the shared folder list without identity verification. Visitors can access the permitted folders. ● Enable: Users who pass identity verification can view the shared folder list. Visitors can access the permitted folders without identity verification. ● Enable (Strict): Users who pass identity verification can view the shared folder list. Visitors cannot access any folder.
Hide Files	When enabled, the system can hide files from users accessing the NAS device via SMB. Files with the name matching the configured rules will be hidden from the user. Select the checkbox and then input the rules. 

2. Access NAS from a Windows Computer

- Option 1: On Windows File Explorer, input ***NAS IP***, press **Enter**, and then input the NAS username and password to access folders on the NAS device.



- Option 2: (Take Win10 as an example). Right-click **This PC**, click **Map network drive**. Input ***\\NAS IP\Shared Folder***, click **Finish**. Input the NAS username/password to connect to the NAS device. Open **This PC**, and you can see the shared folder has been mapped to the computer as a network drive.

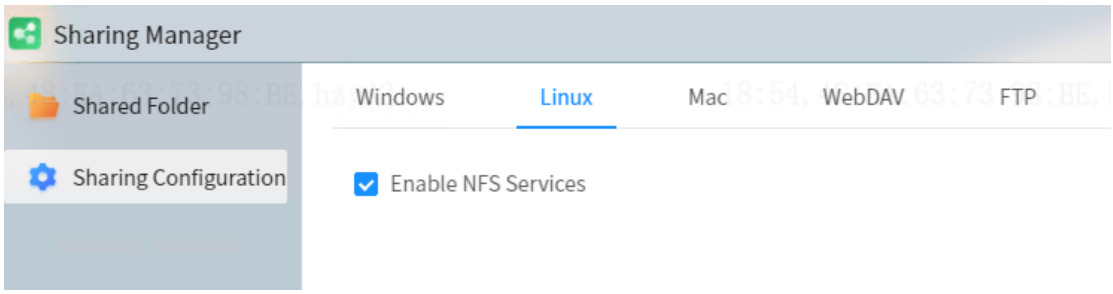


5.2.2 Share with Linux

Linux users can use NFS to mount shared folders on the NAS device and access the shared folders from the Linux client like local folder.

1. Enable NFS

Select the **Enable NFS Services** checkbox to allow access from a Linux client.



2. Configure Linux Client

Configure the Linux client that is allowed to access the shared folder. See Configure NFS Permissions.

3. Access NAS from a Linux Client

Log in to the Linux client as the root user, and then run the following command to mount the shared folder on the NAS device.

mount –t nfs [NAS IP]:/[shared folder][space][target folder]

NOTE!
For example, NAS IP is 192.168.0.1. To mount a shared folder named **Public** on the NAS device to the **/mnt** directory on the Linux client, run this command:
mount –t nfs 192.168.0.1:/Public /mnt

To unmount the shared folder, use this command:

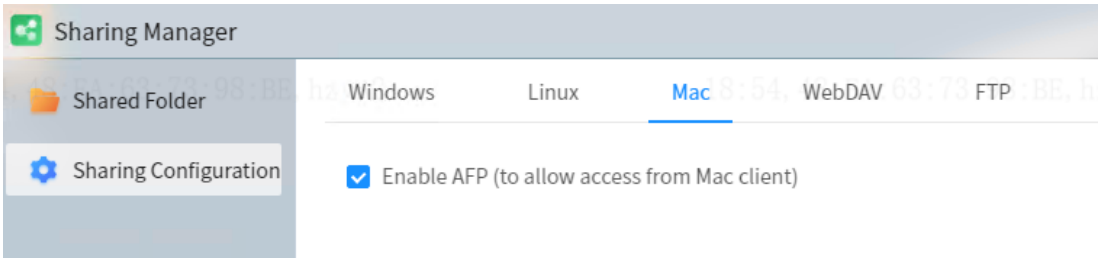
umount /[shared folder]

5.2.3 Share with Mac

Mac users can use Finder to browse shared files on the NAS device or mount a shared folder on the NAS as a network disk.

1. Enable AFP

Select the **Enable AFP** checkbox to allow access from a Mac computer.



2. Access NAS from a Mac Computer

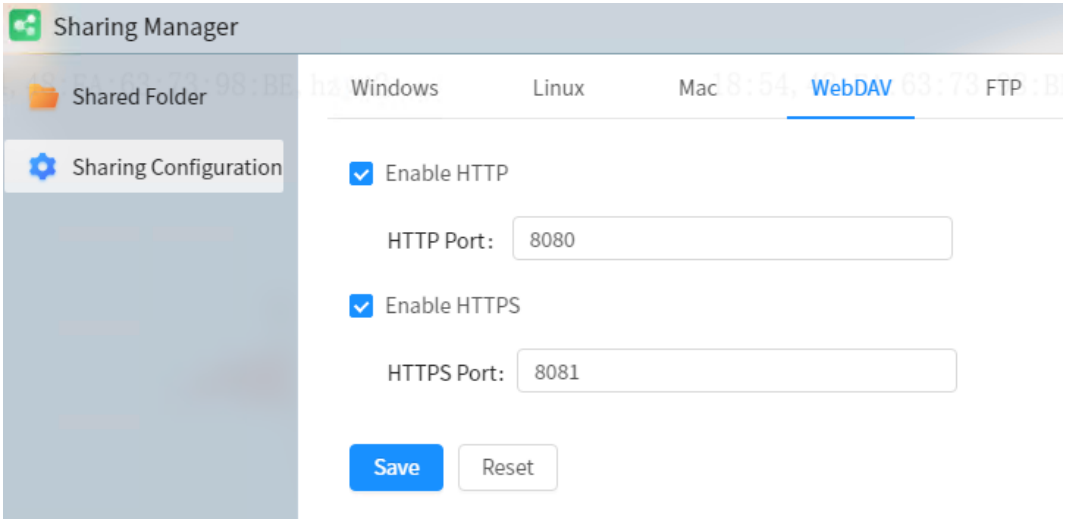
On the Mac computer, go to **Finder** > **Go** > **Connect to Server**, type **afp://*NAS IP*** in the **Server Address** field and then click **Connect.**

5.2.4 Share by WebDAV

WebDAV stands for Web Distributed Authoring and Versioning and can enable a Web server to function as a standard network driver.

1. Enable HTTP/HTTPS

Select the **Enable HTTP** or **Enable HTTPS** checkbox and input the corresponding service port to allow access by WebDav.



2. Access NAS by WebDAV

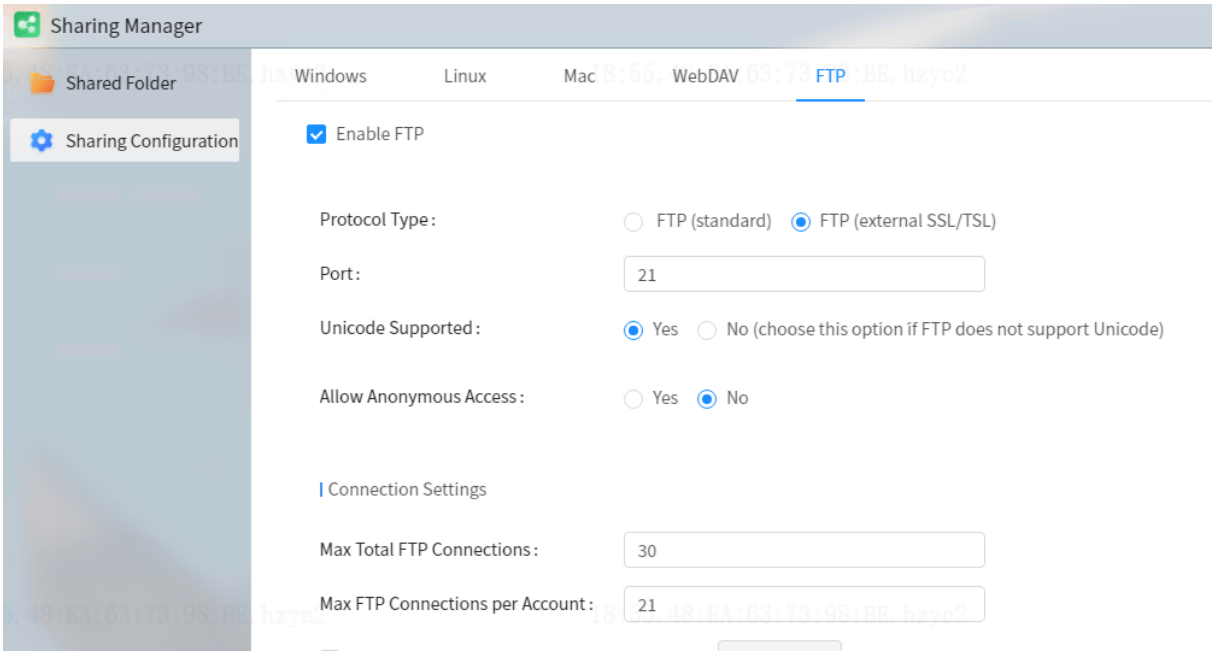
Use a Web browser or a WebDAV client to access the NAS device at **http://*NAS IP:port*** or **https://*NAS IP:port***.

5.2.5 Share by FTP

File Transfer Protocol (FTP) is used to upload and download files. When FTP is enabled, users can upload data to or download data from the NAS device via FTP.

1. Enable FTP

Select the **Enable FTP** checkbox to allow access to the NAS device via FTP.



Item	Description
Enable FTP	Select the checkbox to enable the FTP service.
Protocol Type	Choose an FTP protocol type. ● FTP (standard): Standard network protocol used to transfer files. This option does not provide encryption for session information but offers a faster transmission speed and consumes less system resources.

	• FTP (external): An extension of the standard FTP which supports TLS and SSL. This option provides session information encryption but offers slower transmission speed and consumes more system resources.
Port	Input the FTP service port. The default is 21.
Unicode Supported	Set whether Unicode is supported. This setting helps the FTP client correctly display characters in files. • The default is **Yes**. • Choose **No** if the FTP client does not support Unicode.
Allow Anonymous Access	Set whether to allow anonymous users to access the NAS device.
Max Total FTP Connections	Set the maximum number of users that can access the FTP server simultaneously.
Max FTP Connections per Account	Set the maximum number of connections per user.
Max. Upload Speed	Set the highest speed for uploading files from the FTP client to the NAS device.
Max. Download Speed	Set the highest speed for downloading files from the NAS device to the FTP client.

2. Access NAS via FTP

- Method 1: Use an FTP client program (such as FileZilla) to connect the NAS IP and configured port to access the shared folder.
- Method 2: Use a Web browser to visit the NAS device at **ftp://*NAP IP*** to access the shared folder.
- Method 3: Use a Linux client to connect **ftp NAS IP** to access the shared folder.

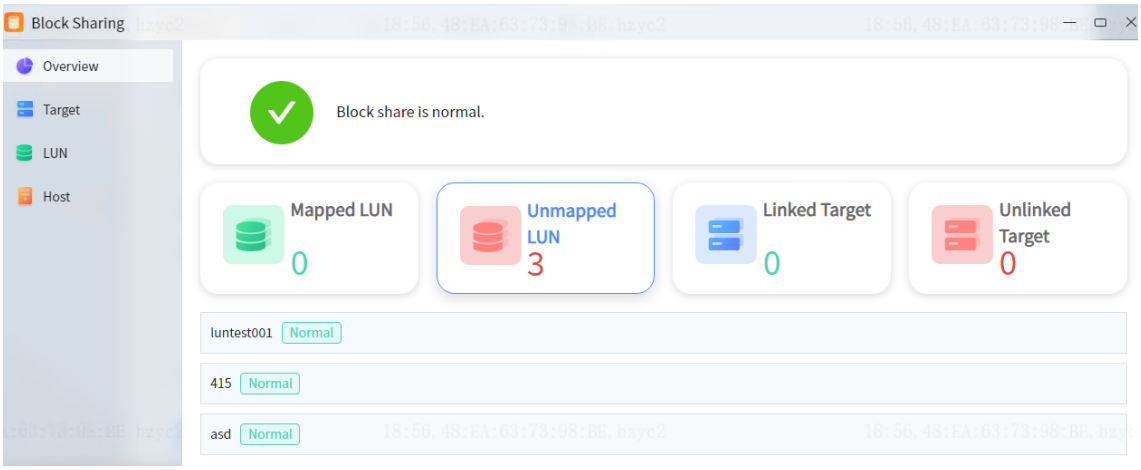
6 Block Sharing

Block sharing allocates storage space on the NAS device to other hosts, for example, to a computer as its local disk.

NOTE!
To use this function, enable iscsi service in **Control Panel** > **Security Manager** > **Service** first.

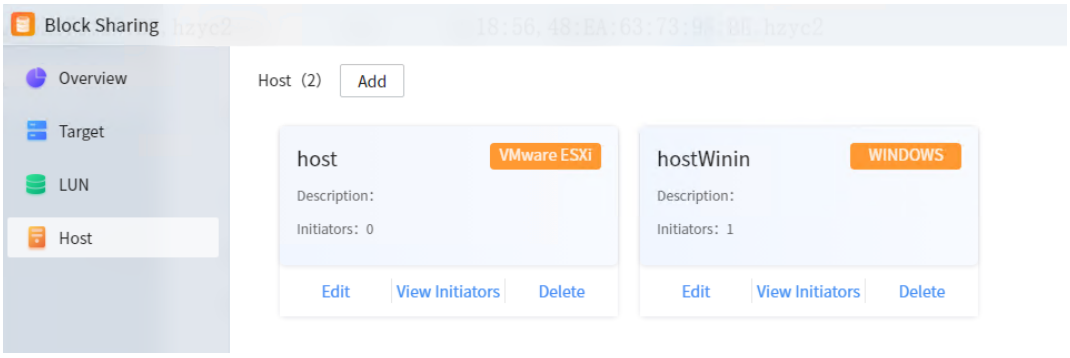
6.1 Overview

View the created resources. Click a resource card to view resource details.



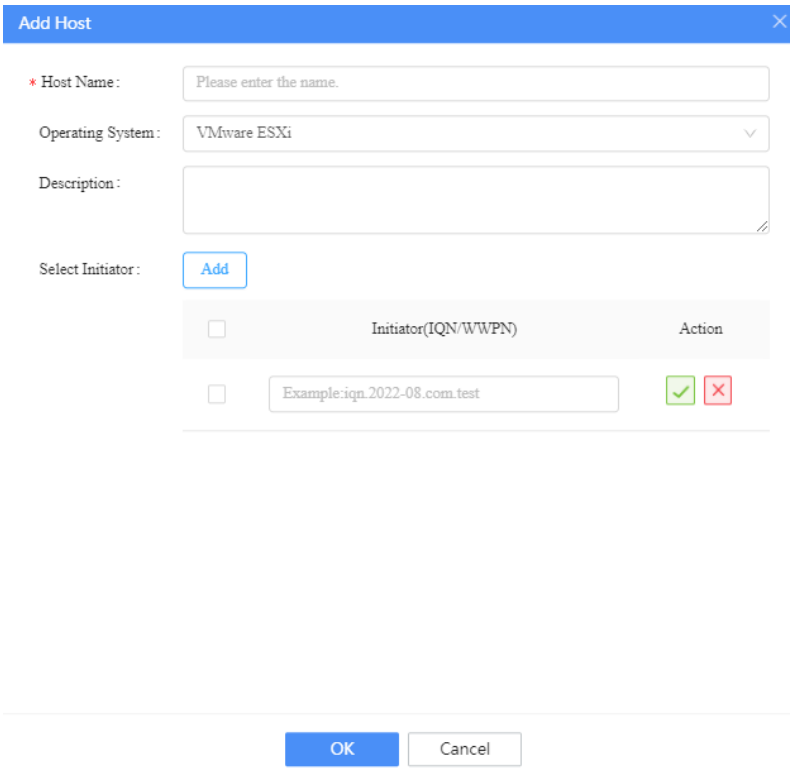
6.2 Host

A host is a device that uses storage resources on the NAS device and supports VMware ESXi (e.g., virtual machine), Windows (e.g., personal computer) or Linux (e.g., server).

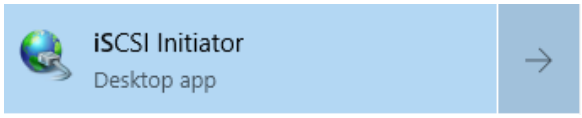
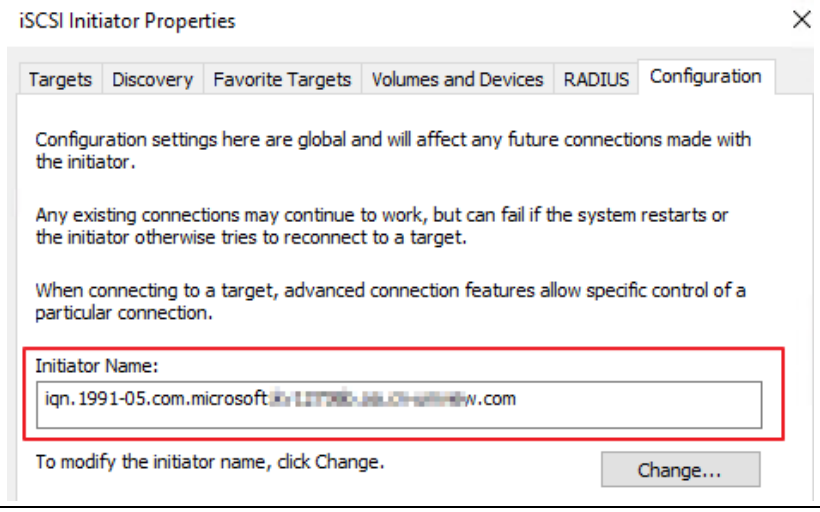


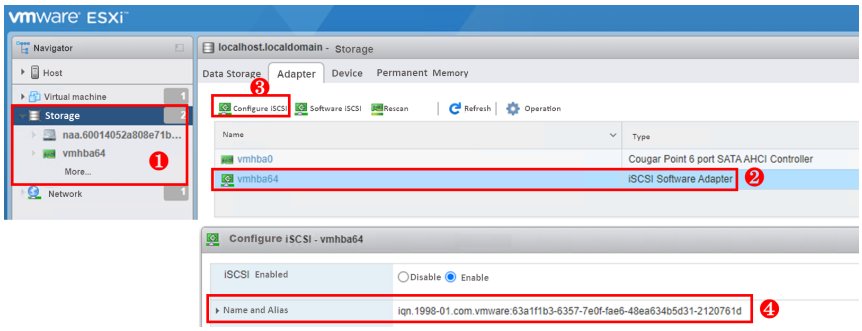
6.2.1 Add Host

1. Click **Add**.



2. Complete the required settings. See the table below for descriptions.

Item	Description
Host Name	Give a name that is easy to recognize. The device name (computer name) is recommended.
Operating System	Choose the host's operating system: VMWare ESXi, Windows, or Linux.
Select Initiator	Click **Add**, add an initiator (IQN), and then select it. Standard format: **iqn.[date].[domain].[device identifier]**. Follow the steps to get the initiator name. The figures below are for reference only. ● Windows (1) Type **iSCSI Initiator** in the search field and open the app.  (2) On the **iSCSI Properties** page, find the initiator name on the **Configuration** tab. 

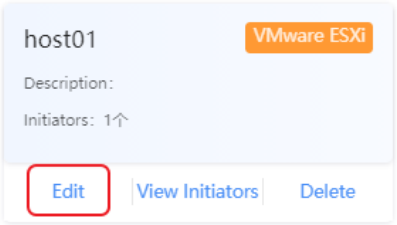
	• VMware ESXi (1) Open a web browser, type the VMware ESXi host IP in the address bar to open the VMware ESXi management portal. (2) Go to **Storage** > **Adapter**, choose the iSCSI adapter, click **Configure iSCSI**, find the initiator name next to **iSCSI name and Alias**.  • Linux (1) Use an SSH tool to log in to the management portal of the Linux host. (2) Run the following command to get the initiator name: **iscsiadm –m discovery –t st –p [IP address]**

3. Click **O**K. The host is added.

6.2.2 Edit Host

Follow the steps to edit host information:

1. Click **Edit** on the card.



2. Edit the host.
3. Click **OK** to save the settings.

6.2.3 View Initiator

Click **View Initiators** on the card to view the added initiators.

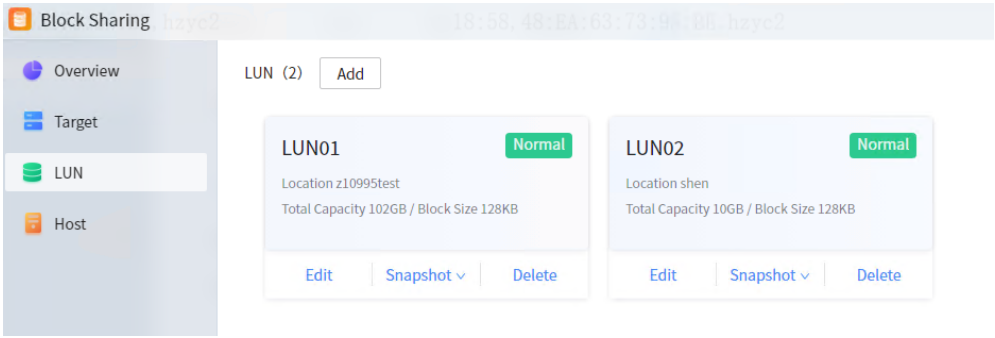
6.2.4 Delete Host

NOTE!
Before deleting a host, you need to remove the link with the target first. See Remove Link.

Click **Delete** on the card, and then confirm the deletion.

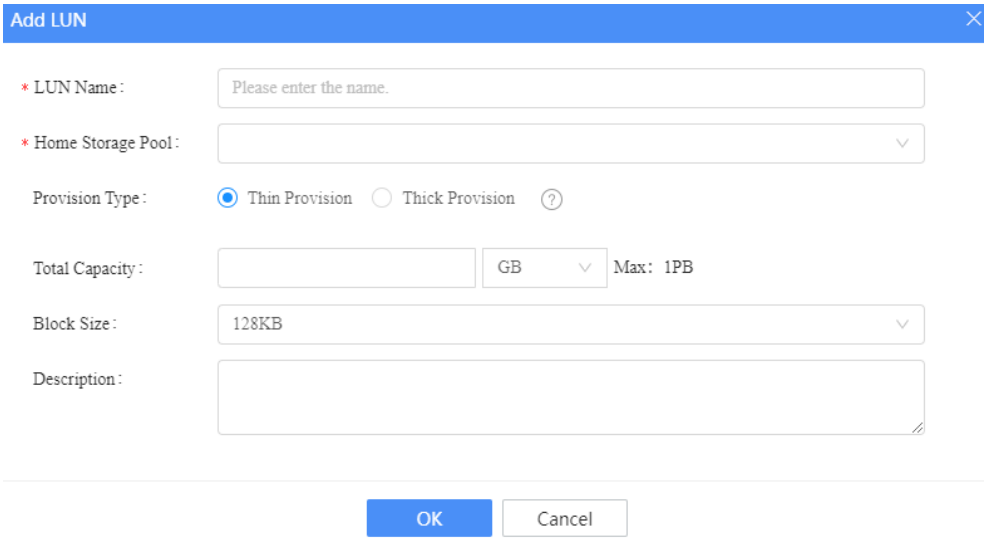
6.3 LUN

An iSCSI LUN is a logical unit of storage.



6.3.1 Add LUN

1. Click **Add**.



See the table below for descriptions.

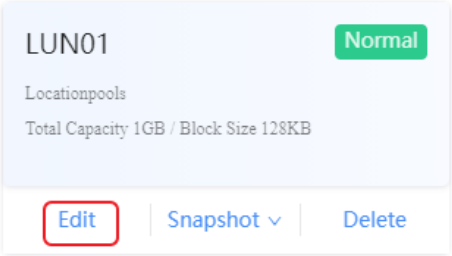
Item	Description
LUN Name	Set a LUN name as needed.
Home Storage Pool	Choose a storage pool and allocate space to the LUN.
Provision Type	● Thin Provision: The system allocates pool space on demand when writing data to the LUN. It may cause corrupted file system if the LUN space is insufficient. ● Think Provision: The system allocates pool space when creating the shared folder to ensure availability of space.
Total Capacity	Set the LUN's storage capacity. The valid range is 1GB to 1PB.
Block Size	Choose the block size. The default value 128K is recommended.

2. Click **O**K. The LUN is added.

6.3.2 Edit LUN

Follow the steps to edit LUN:

1. Click **Edit** on the card.

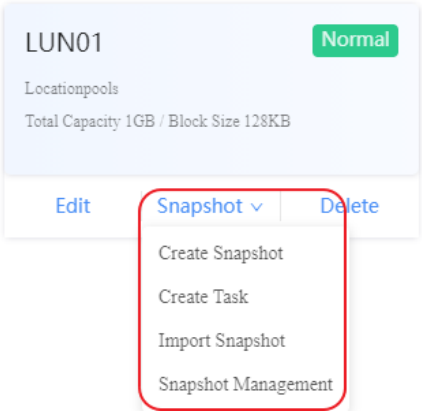


2. After you complete the modification, click **OK**.

6.3.3 Snapshot

Create a snapshot to make a duplicate of a LUN at a given time in case you need to restore data after data is lost accidentally. Snapshots use a small storage space compared to backups.

Click **Snapshot** on the LUN card, and then choose options as needed.



The operations are similar to the snapshot management of the shared folder. See Snapshot for details.

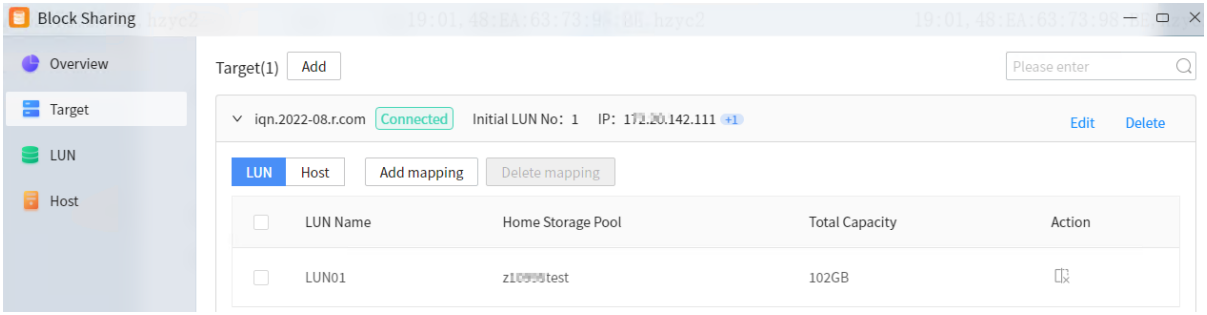
6.3.4 Delete LUN

NOTE!
Before deleting a LUN, you need to delete its mapping with the target first. See Remove Link.

Click **Delete** on the card, and then confirm the deletion.

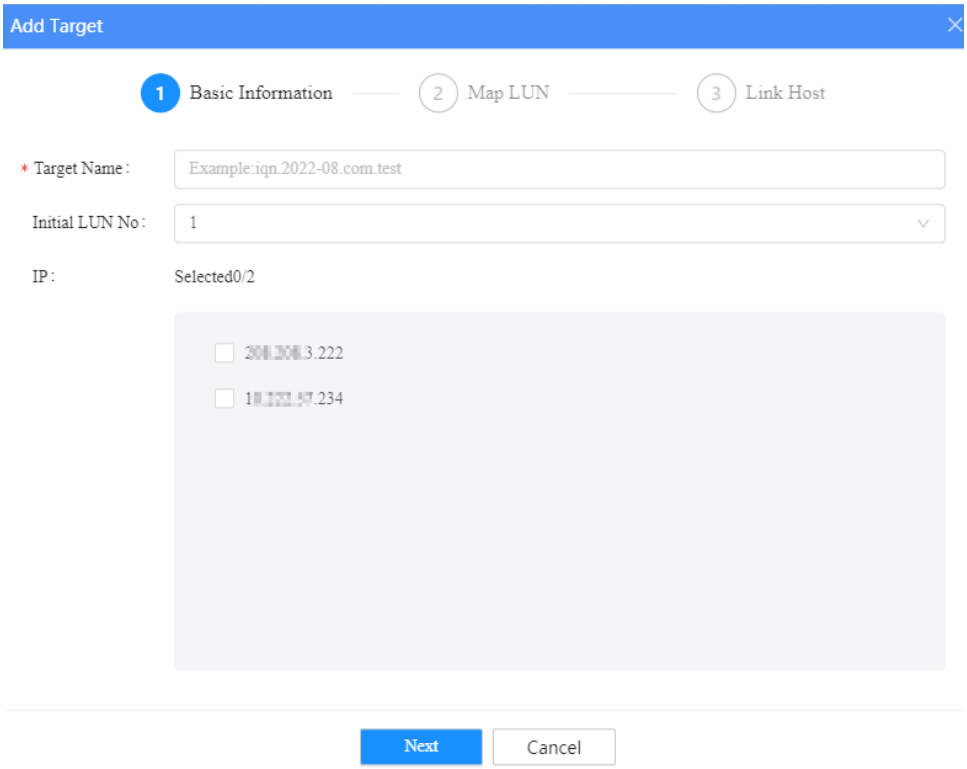
6.4 Target

Create a Target and link it to the host.

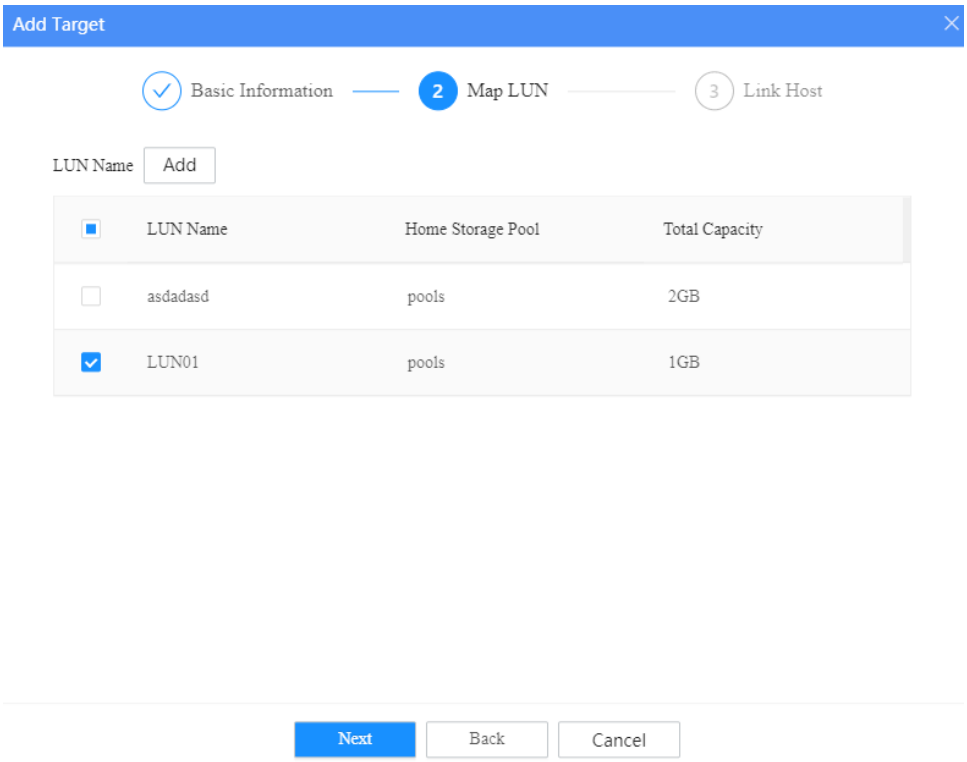


6.4.1 Add Target

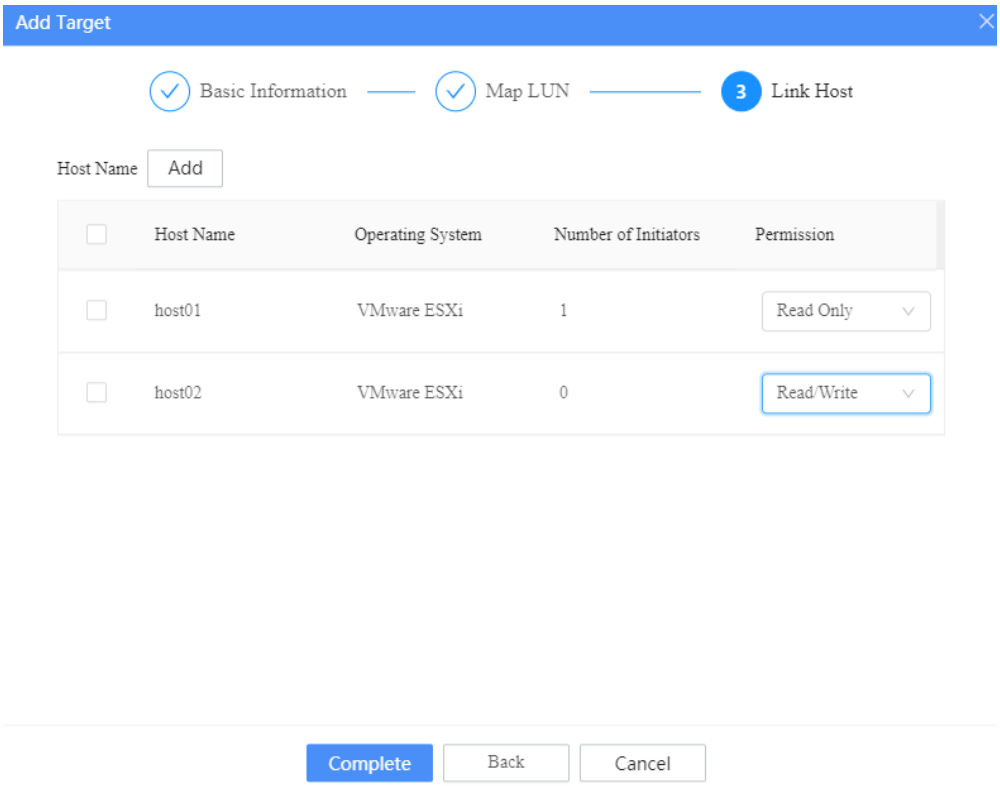
1. Click **Add**.
2. Complete the basic information.
   - Target Name: Set as needed. Standard format: **iqn.[date].[domain].[device identifier]**. The name must be unique.
   - Initial LUN No.: Choose a LUN number. The default is 1.
   - IP Address: Choose the NAS IP address. If no IP address is selected, all the listed IP addresses will be used to provide sharing service.



3. Click **Next**. Choose the LUN that the Target maps to (for information about creating a LUN, see LUN).



4. Click **Next**, choose the host that the target links to, and set read/write permission for the host to access the storage resource.



NOTE!

Disk partitioning requires read/write permission. So usually it is recommended to set read/write permission to allow disk configuration.

5. Click **Complete**. The Target is added.

6.4.2 Edit Target

To change the IP address of the Target, follow the steps below:

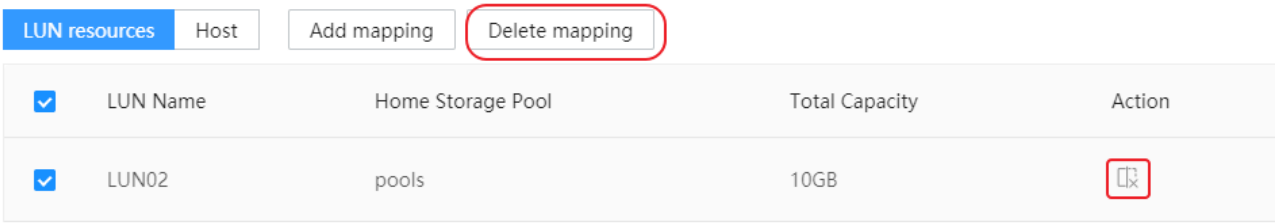
1. Click **Edit** for the Target.

2. After you complete the modification, click **OK**.

6.4.3 Delete LUN Mapping

Follow the steps to delete the mapping between the LUN and the Target:

1. Select the LUN, and then click **Delete Mapping**; or click the for the LUN.

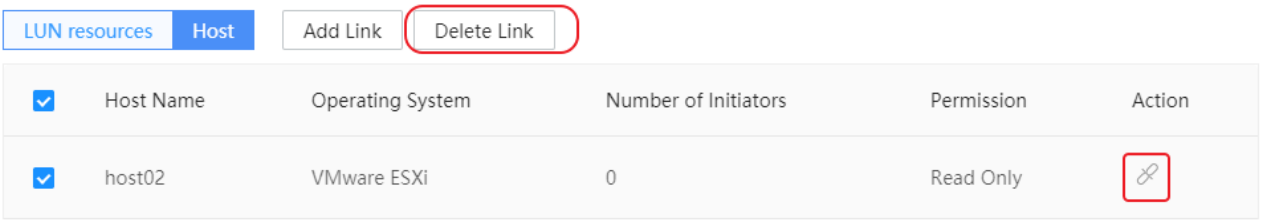


2. Confirm to delete the mapping.

6.4.4 Delete Link

Follow the steps to delete the link between a host and a LUN.

1. Select the host, click **Delete Link**, or click for the host.



2. Confirm to delete the link.

NOTE!

If the host is already linked with the Target, you need to remove the link on the host first (see Use NAS Resource on the Host) before you can remove the link on this page.

6.4.5 Delete Target

NOTE!

When deleting a target, you need to delete the mapping between the LUN and the target and remove the link between the host and the target.

Click **Delete** for the target and then confirm the deletion.

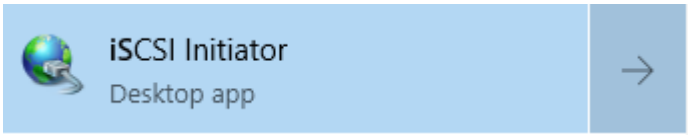
6.5 Use NAS Resource on the Host

After a link is established between the host and the Target, the host has access to LUN resource that the Target is mapped to and can use the LUN as a local disk.

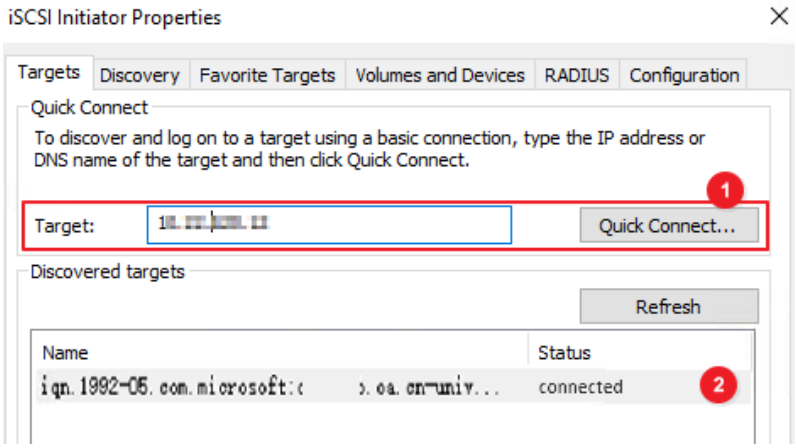
6.5.1 Windows Host

Follow the steps to create a local disk using NAS resource on a Windows host:

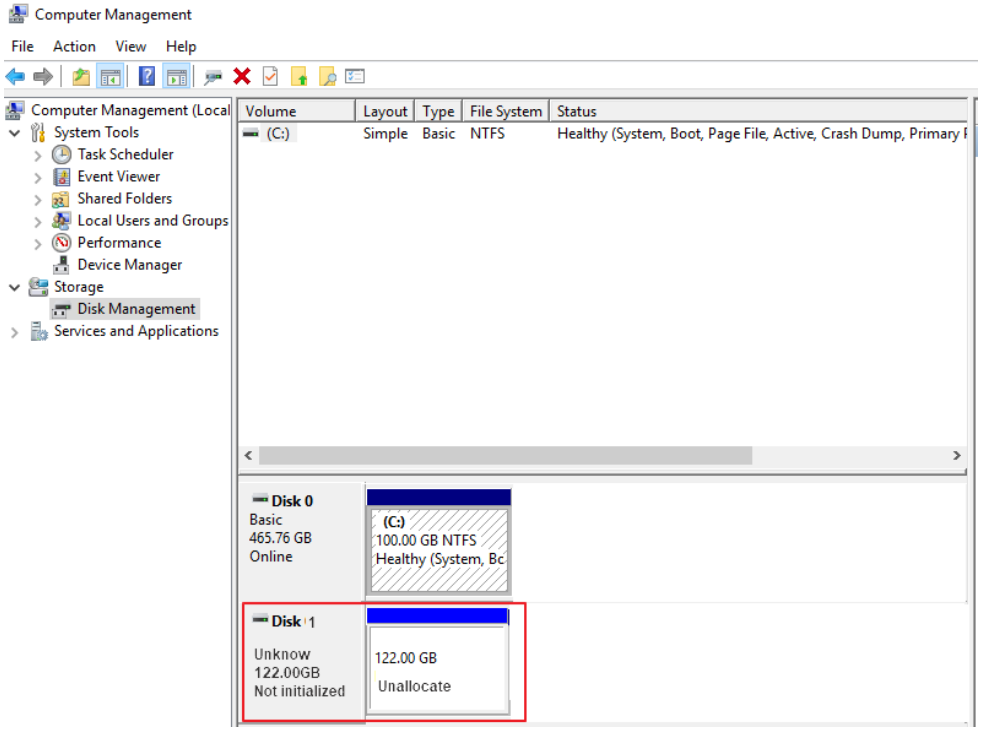
1. Type iSCSI Initiator in the search field and open the app.



2. In the **Properties** dialog box, click the **Targets** tab. Enter the NAS IP in the **Target** filed, and then click **Quick Connect**. When the status is changed to “connected”, the NAS device is connected successfully.

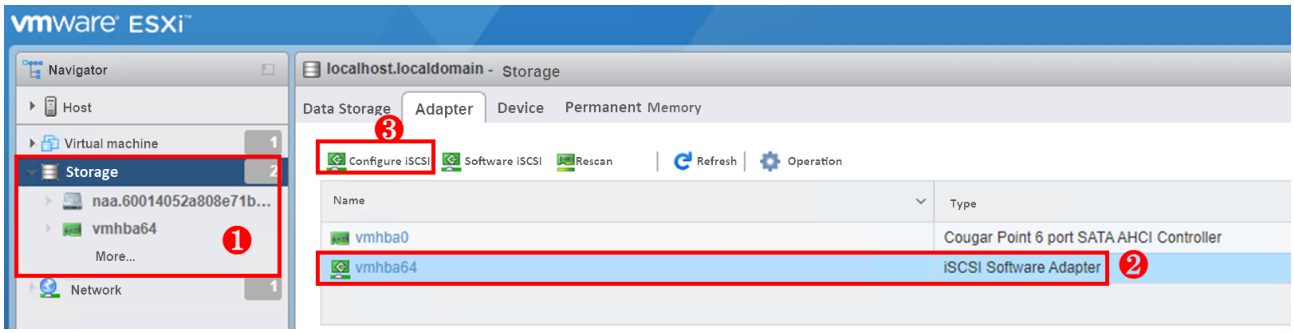


3. Take a Win10 computer as an example. Right-click **This PC**, click **Manage**. The **Computer Management** page appears. You may also type **compmgmt.msc** in the **Run** field to open this page.
4. Choose **Storage** > **Disk Management** to view the storage space (unallocated status) from the NAS device, and then initialize the disk in accordance with Windows system rules.

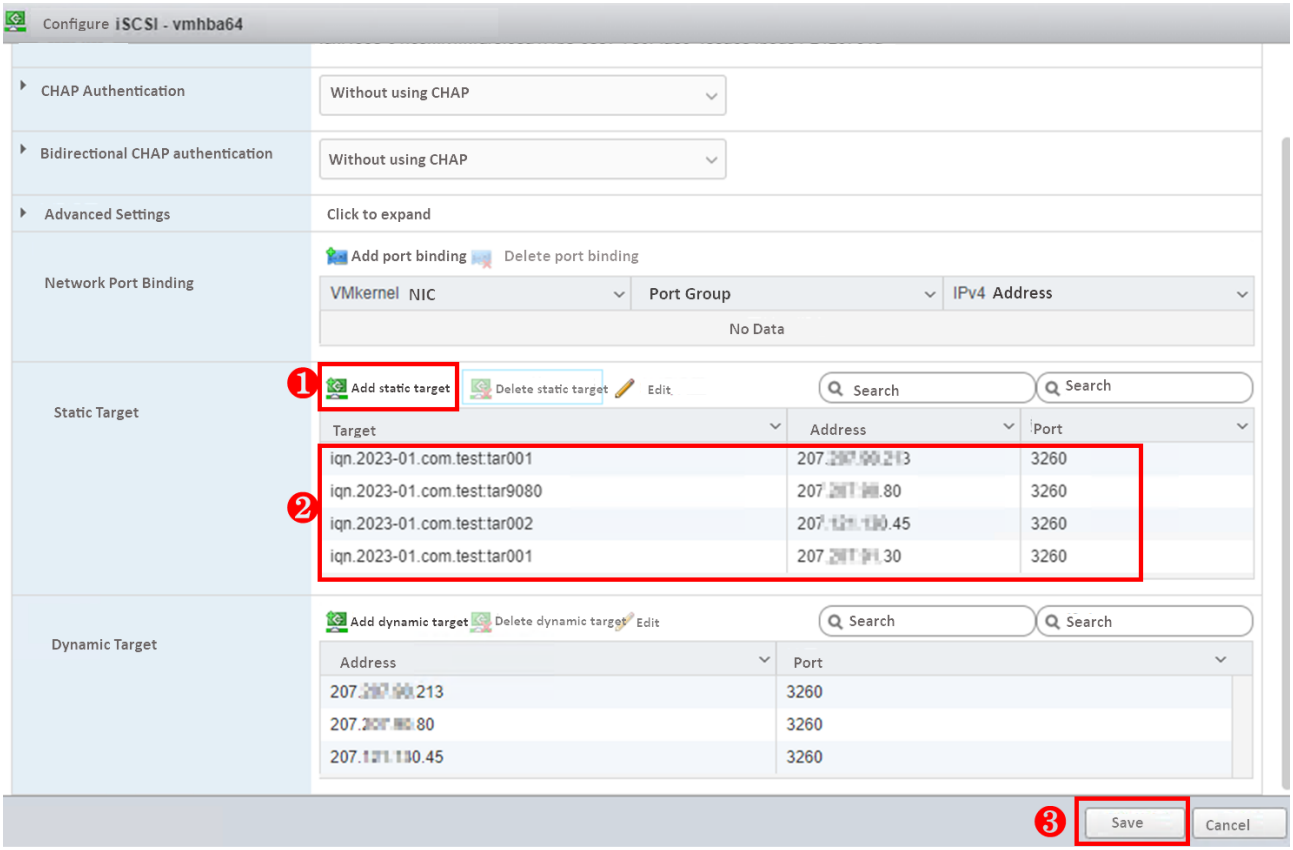


6.5.2 VMware ESXi Host

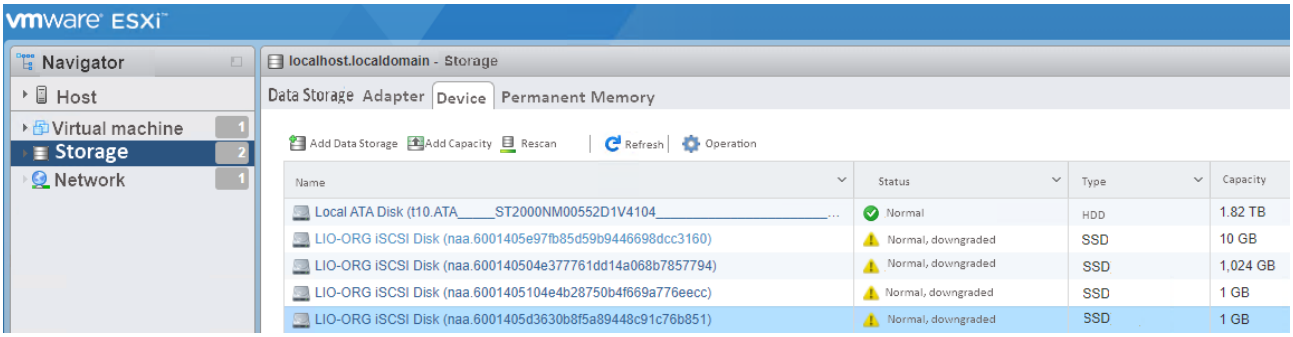
1. Open a Web browser, type the VMware ESXi host IP in the address bar to open the VMware ESXi management portal.
2. Go to **Storage** > **Adapter**, choose the iSCSI adapter, click **Configure iSCSI**.



3. Add a static Target including the Target name and NAS IP, and then save the settings.



4. Choose **Storage** > **Device** to view the allocated space.



6.5.3 Linux Host

1. Use an SSH tool to log in to the management portal of the Linux host.
2. Use the **iscsiadm** command to connect to the Target on the NAS device.

   iscsiadm –m node –targetname“[Target name]”-portal“[Target IP:3260]”-login

   Example:

   iscsiadm –m node –targetname“iqn.2023-01.com.test:tar001”-portal“192.168.0.1:3260”-login
3. Use the **fdisk** command to create partitions.

   fdisk –l // Searches available disks

   fdisk disk path // Creates partitions

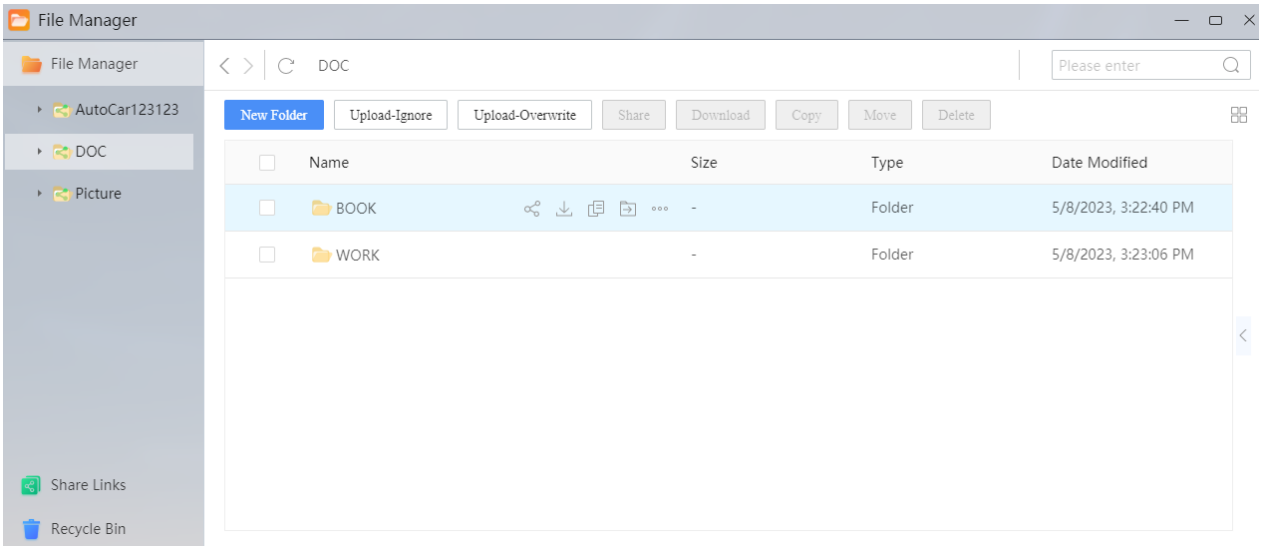
7 File Manager

On **File Manager**, you can upload files of different types to the storage space on the NAS device, visit, download, and manage files stored on the NAS device, and share files in a secure way with other users via custom access permissions and temporary links.

7.1 File Manager

On the **File Manager** page, click **File Manager** on the left to view the shared folders on the NAS device and their sub-folders and files.

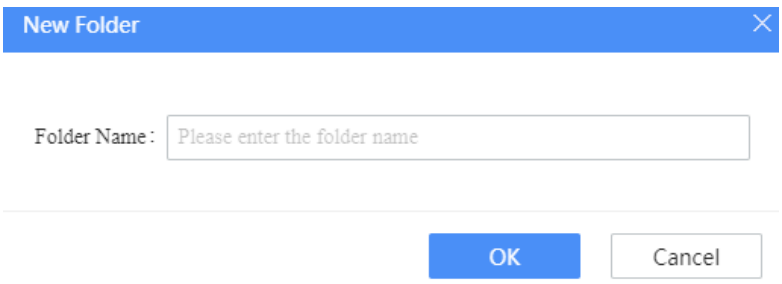
To view files in a folder, expand the left-side tree and select the folder.



7.1.1 New Folder

Folders are used to manage files by type. To achieve quick search, it is recommended to create folders according to the file types you want to store.

1. On the **File Manager** page, click **File Manager** on the left.
2. Select a shared folder, click **New Folder**. A dialog box appears. To create a folder under an existing folder, select the folder and then click **New Folder**.



3. Enter the folder name, and then click **OK**.

7.1.2 Upload Files

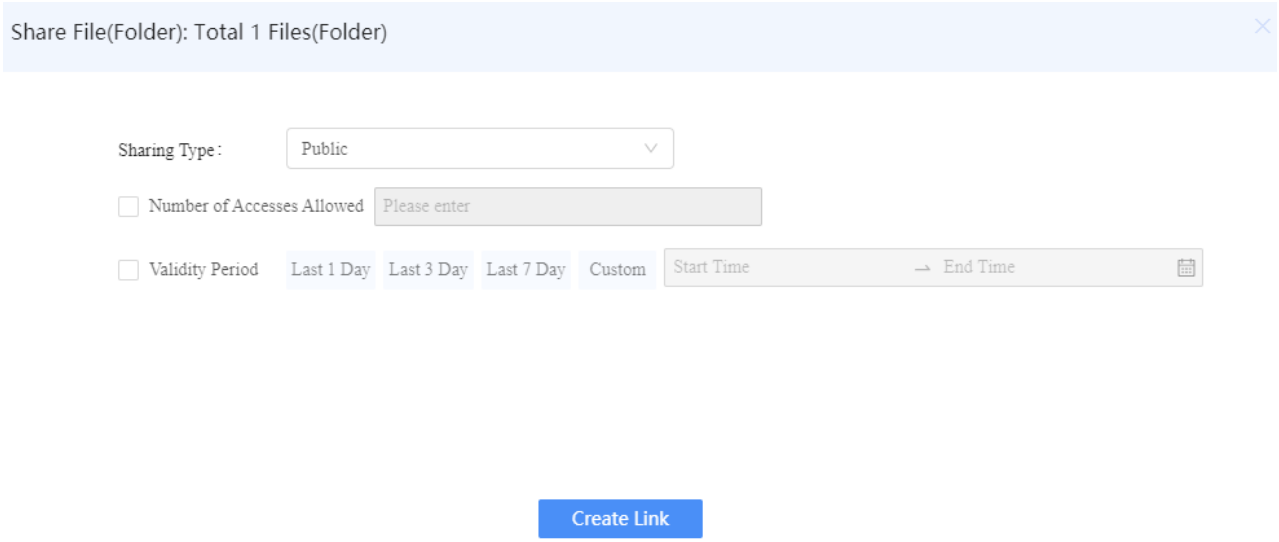
Follow the steps to upload files to the NAS device.

1. On the **File Manager** page, click **File Manager** on the left, and then select the destination folder for the files you want to upload.
2. Click **Upload-Ignore** or **Upload-Overwrite** in case a file with the same name as the file you want to upload already exists in the destination folder.
   - Upload-Ignore: Upload will be cancelled.
   - Upload-Overwrite: The uploaded file will overwrite the existing file in the folder.
3. Select the file you want to upload, and then click **OK** to start upload.

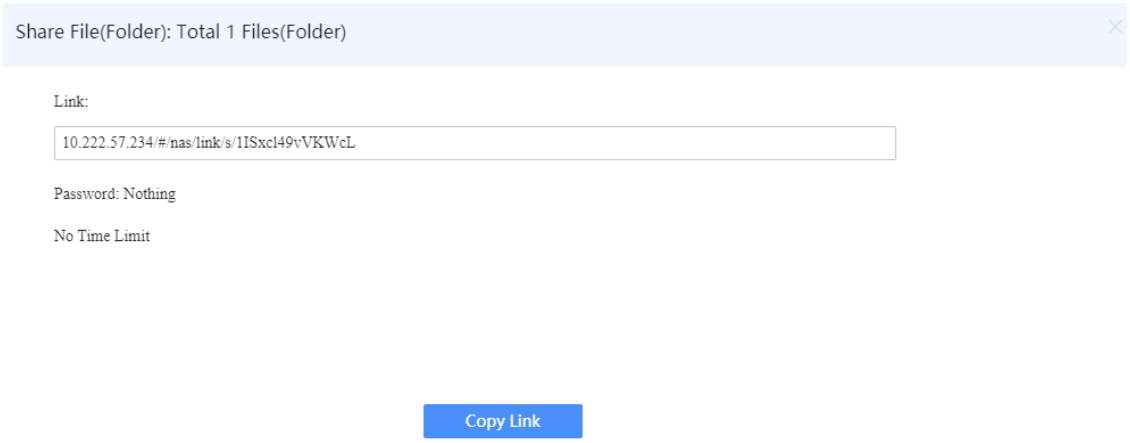
7.1.3 Share Files

Share files (including folders) with other users of the NAS system, so they can view or download the shared files.

1. On the **File Manager** page, click **File Manager** on the left.
2. On the file list, select the file or folder you want to share, and then click **Share**.
3. Choose a type (public, password protection, shared by internal account), set the number of accesses allowed, and validity period.



4. Click **Create Link** to generate a link to share the file or folder.



5. Click **Copy Link** to copy the link and then send it to the intended users.

NOTE!
Users who receive the link can paste the link in a web browser to download the shared files.

7.1.4 Download File

Download files (including folders) from the NAS device to your computer.

1. On the **File Manager** page, click **File Manager** on the left.
2. On the file list, select the file or folder you want to download, and then click **Download**.
3. You can view the downloaded files on your computer after the download is completed.

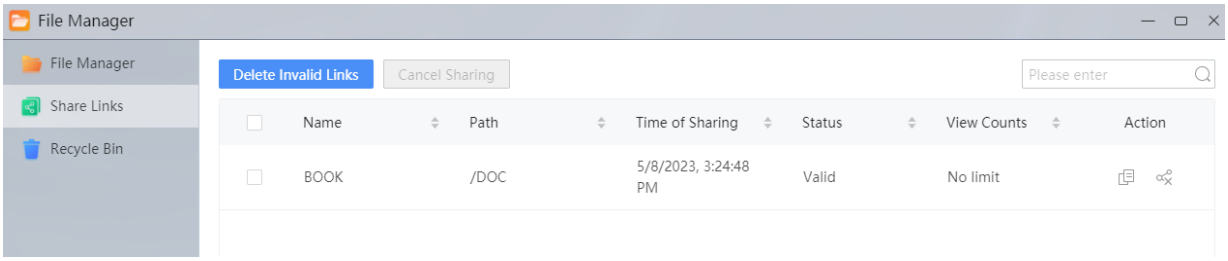
7.1.5 File Management Actions

You can copy, move, delete, rename files on the NAS device and save files to favorites folder.

Action	Purpose	Steps
Copy	Copy a file to a different folder for backup.	1. On the file list, select the file/folder and then click **Copy**. 2. Choose the destination folder, and then click **OK**.
Move	Move a file to a different folder.	1. On the file list, select the file/folder and then click **Move**. 2. Choose the destination folder, and then click **OK**.
Delete	Delete a file from the NAS device.	1. On the file list, select the file/folder and then click **Delete**. 2. Click **OK** in the pop-up window to confirm the deletion. **Note:** The deleted files will be moved to **Recycle Bin** and can be restored to the previous paths.
Rename	Change the name of a file.	1. On the file list, click ⋯ for the file/folder and then choose **Rename**. 2. Input the new name and then click **OK**.

7.2 Share Links

On the **Share Links** page, you can view the shared files, including the filename, time of sharing, expiration time, and the number of times that the file has been viewed and downloaded. You can also copy links, cancel sharing, and delete expired links.

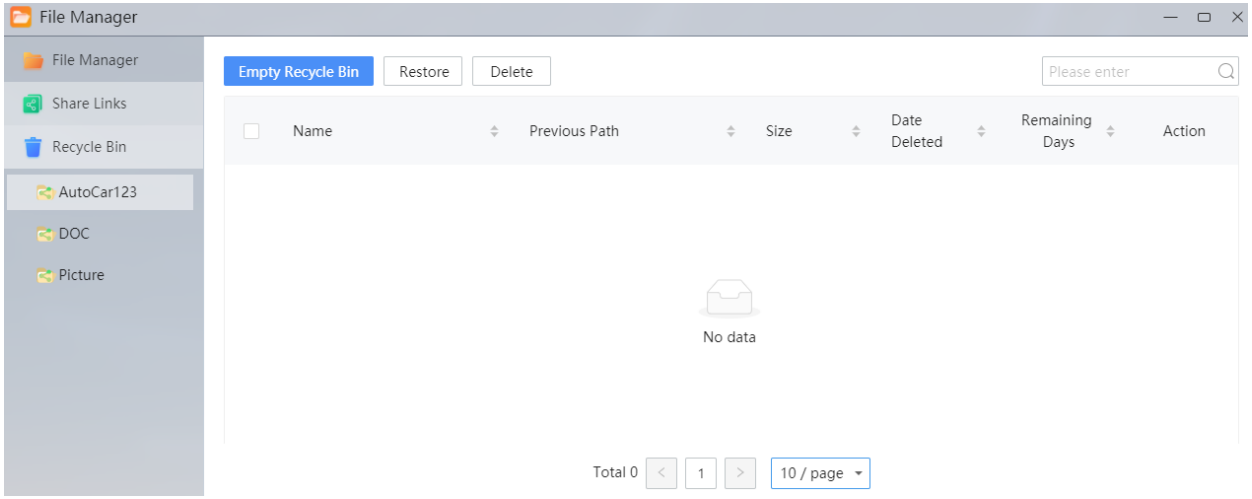


Action	Purpose	Steps
Copy Link	Copy and send a link to other users. Users who receive the link can click the link to access the shared file.	1. Click . 2. Paste the link to an app such as file editor, chatting tool, and Web browser.
Cancel Sharing	Stop sharing a file, so other users can no longer access the file.	1. On the shared file list, select the file. 2. Click **Cancel Sharing**.

Delete Invalid Links	Delete links of expired sharing.	1. On the shared file list, select the file. 2. Click **Delete Invalid Links**.

7.3 Recycle Bin

The recycle bin is used to retain files that deleted from **File Manager**. You can restore files or permanently delete files from the NAS device.



- Restore: Restore files to the previous paths.
  - Batch Restore: Select the files you want to restore and then click **Restore**.
  - Restore: Click to restore a file.
- Delete: Delete files from the recycle bin.

WARNING!
This operation will permanently files from the NAS device. This operation cannot be undone.

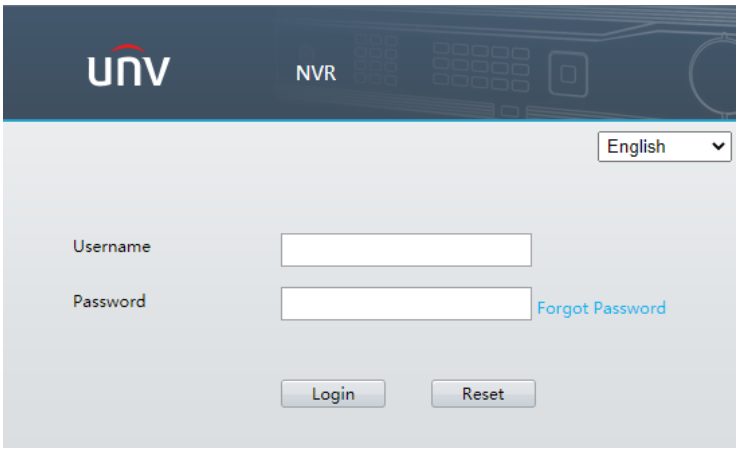
  - Empty Recycle Bin: Click **Empty Recycle Bin** to delete all files from the recycle bin.
  - Batch delete: Select the files you want to delete and then click **Delete**.
  - Delete: Click to delete a file.

8 NVR

The NAS can be used as an NVR (Network Video Recorder) to connect cameras for video surveillance and recording storage.

8.1 Log in to the NVR

1. Click NVR on the desktop to go to NVR configuration page.
2. Enter the username and password of NVR, then click **Login**.



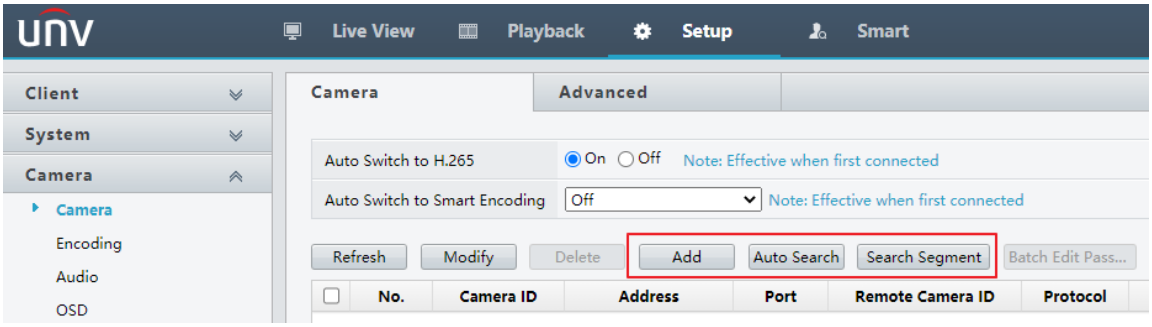
NOTE!

- The default username/password: admin/Admin123-.
- For data security, please change the default username/password after your first login. A strong password is recommended: at least nine characters including uppercase and lowercase letters, digits, and special characters.

8.2 Add a Camera

Add camera(s) to the NVR for management.

1. Go to **Setup** > **Camera** > **Camera**, click the **Camera** tab.



2. Choose a way to add cameras.

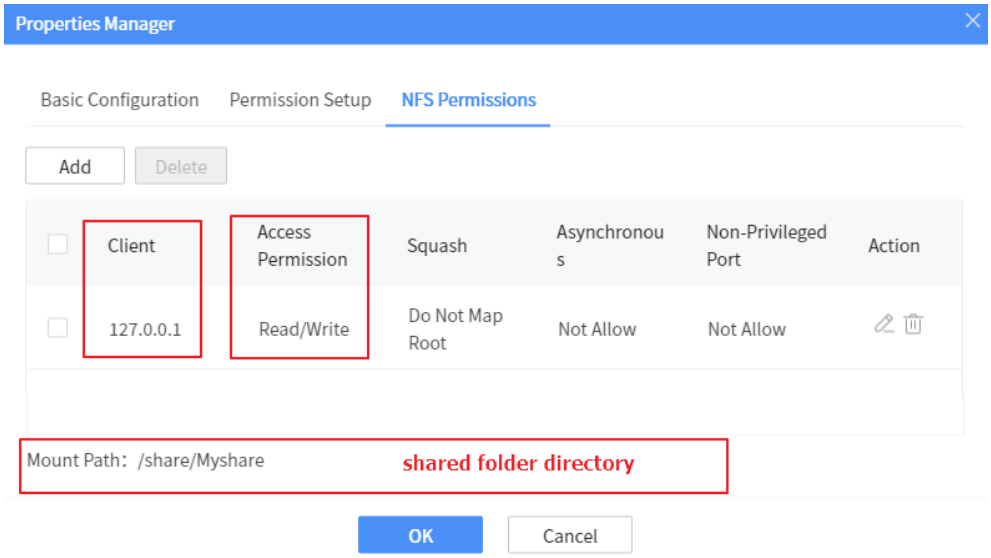
- Add one by one: Click **Add**, enter the exact IP address to add the camera.
- Auto Search: Click **Auto Search**, NVR will automatically search cameras in the network, then select the desired cameras to add.
- Search Segment: Click **Search Segment**, set the network segment to search for cameras, then select the desired cameras to add.

8.3 Storage

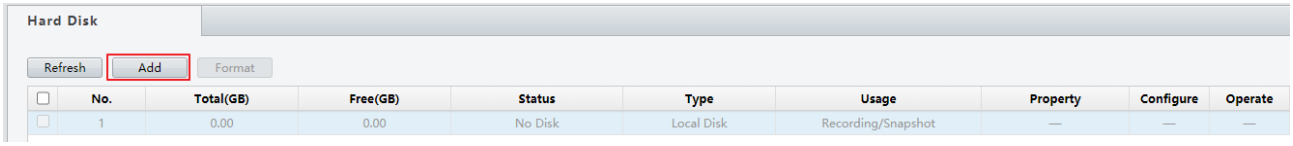
Mount the NAS's shared folder in the NVR.

NOTE!

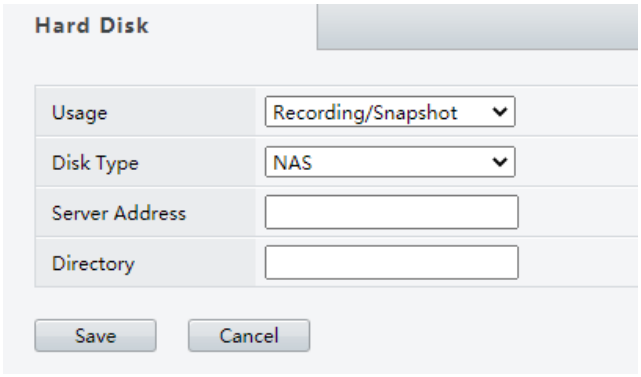
Configure sharing with Linux clients in **Sharing Manager**. Set Linux client IP as 127.0.0.1, and set access permission to Read/Write. See Sharing with Linux.



1. Go to **Setup** > **Hard Disk** > **Hard Disk**.

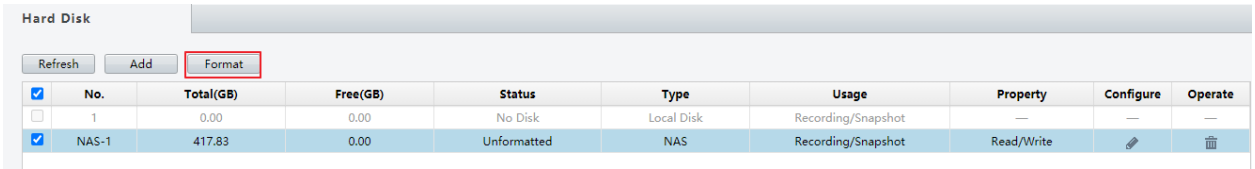


2. Click **Add** to add the shared folder.



- Server Address: NAS's IP address.
- Directory: NAS shared folder directory. Standard format: /share/*shared folder name*.

3. Click **Save**.



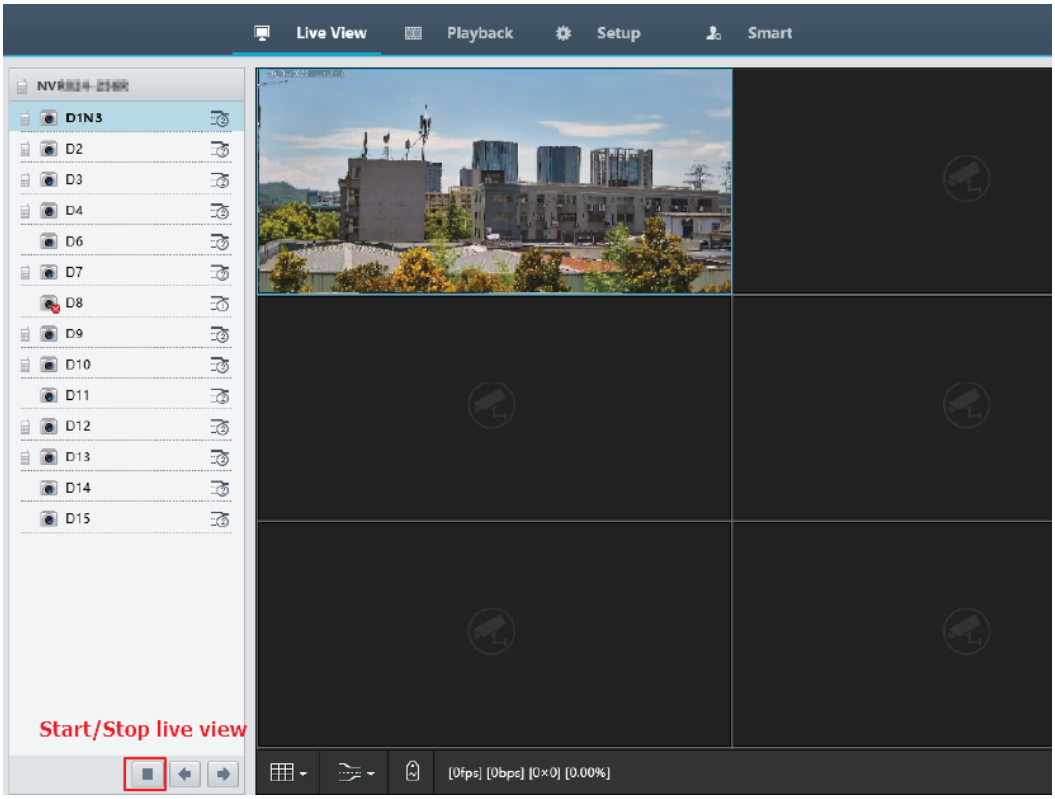
4. On the **Hard Disk** page, select the mounted NAS storage space, then click **Format** to create the qualified directory.

NOTE!

The formatting operation does not affect data already stored on the NAS.

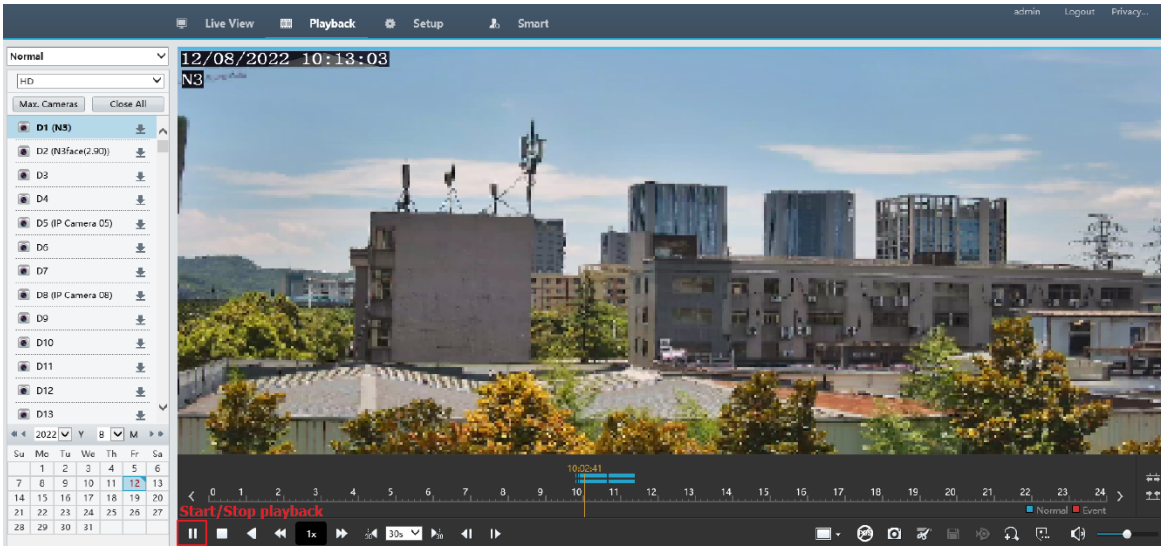
8.4 Live View

On the **Live View** page, select the desired camera on the left, then click to view the live video.



8.5 Playback

On the **Playback** page, select the desired camera and the date on the left, then click to start playback.



9 System Maintenance

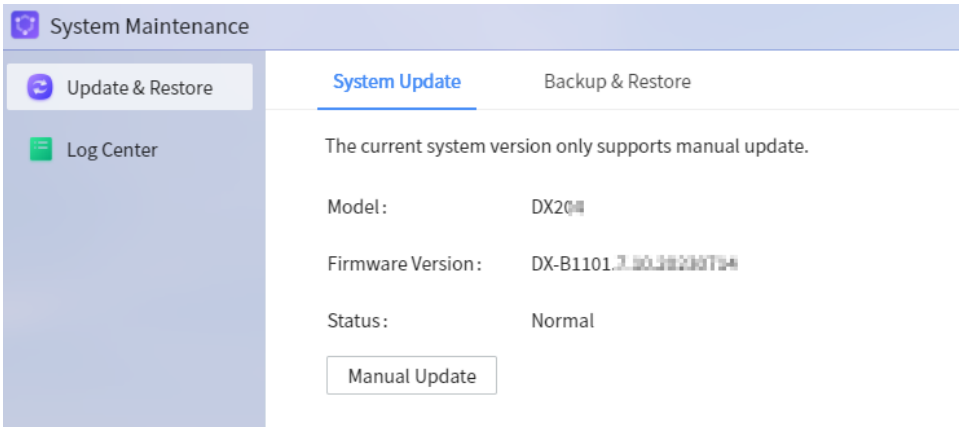
9.1 Update and Restore

Upgrade the system to the latest version, or restore it to a previous version using a backup file.

9.1.1 System Update

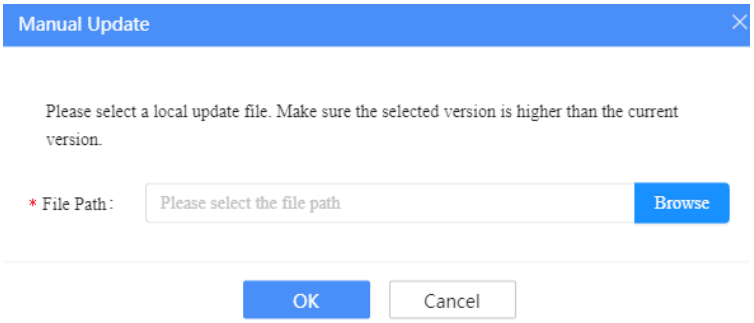
The system supports automatic version update.

Go to **System Maintenance** > **Update and Restore** > **System Update** to view the current version.



To update the version manually, follow the steps below:

1. Click **Manual Update**. A page as shown below appears.

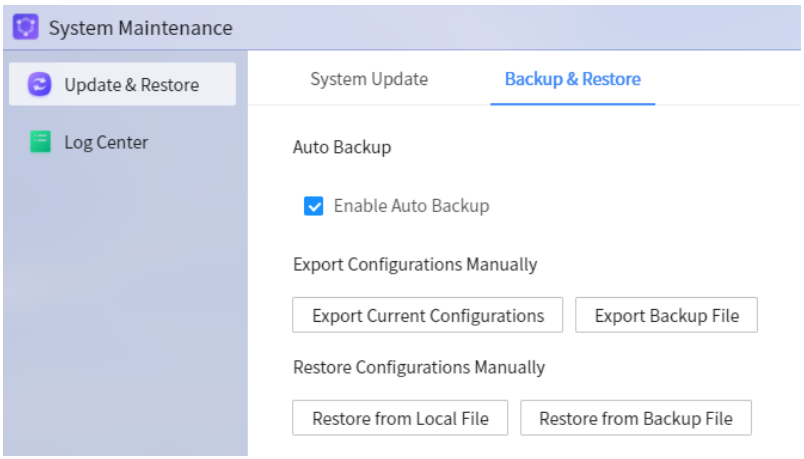


2. Click **Browse** and locate the upgrade file on your computer.
3. Click **OK**.

9.1.2 Backup and Restore

It is recommended to enable system backup, so you can restore the system using the backup file when necessary.

Go to **System Maintenance** >**Update and Restore** > **Backup and Restore**.



System Backup

- Auto backup: Select the checkbox to enable automatic backup.
- Export Configurations Manually
  - Click **Export Current Configurations** to export the current backup of the system.
  - Click **Export Backup File** to export a historical backup of the system.

Restore System

Use a backup file to restore the system to an earlier version.

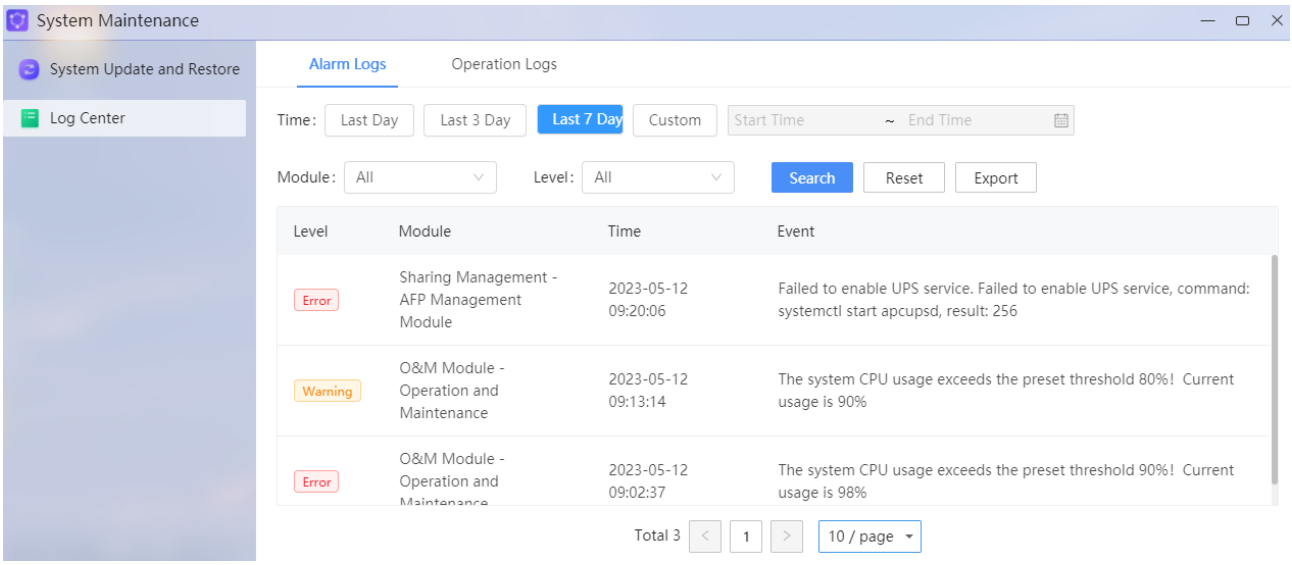
- Restore from a local file: Click **Restore from Local File**, and then locate the backup file from your computer.
- Restore from a backup file: Click **Restore from Backup File**, and then locate the backup file on the NAS device.

9.2 Log Center

View system alarm logs and operation logs.

9.2.1 Alarm Logs

Go to **System Maintenance** > **Log Center** > **Alarm Logs** to view alarm records in the system.

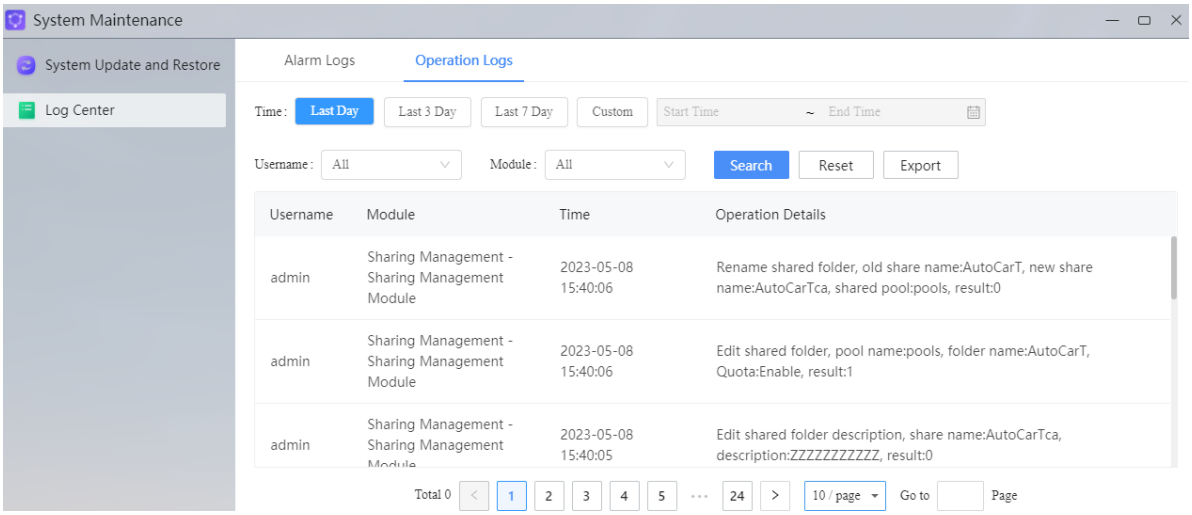


Set search criteria including time, alarm level, and module, and then click **Search** to view needed alarm records.

Click **Export** to export alarm logs to a **.csv** file.

9.2.2 Operation Logs

Go to **System Maintenance** > **Log Center** > **Operation Logs** to view user operation records in the system.



Set search criteria including time, username, module, and then click **Search** to view specific operation records.

Click **Export** to export operation logs to a **.csv** file.

10 Acronym and Abbreviations

The table below lists some acronyms and abbreviations in this document.

Acronym	Full Name	Description
AD	Active Directory	A directory service created by Microsoft to manage Windows domain networks.
AFP	Apple Filing Protocol	A network protocol used to provide file service for Mac computers.
DNS	Domain Name System	A service that provides domain name-IP address mappings to allow user to visit a website conveniently using its domain name.
FTP	File Transfer Protocol	Used to upload or download files on a network.
IQN	iSCSI Qualified Name	Unique name of each iSCSI Target.
iSCSI	Internet Small Computer Systems Interface	A storage technology based on IP network and SCSI-3 protocol.
LDAP	Lightweight Directory Access Protocol	Enables reading/writing data in the correct location in the information directory.
LUN	Logical Unit Number	An LUN is a logical unit of storage.
MTU	Maximum Transmission Unit	The maximum size of a packet or frame in network transmission, usually in unit of Byte. If the MTU size is too large, packets or frames may be discarded by the router; if the MTU size is too small, the actual size of data transmitted will be too small.

Acronym	Full Name	Description
NAS	Network Attached Storage	Refers to our NAS device.
NFS	Network File System	A network file system protocol based on TCP/IP. Users can use NFS client to access shared resources on the NFS server like accessing a local directory.
NTLM	NT LAN Manager	A standard security protocol in an early version of Windows NT.
NTLMSSP	NT LAN Manager Security Provider	A security support interface protocol provided by Microsoft, which specifies the encryption method for SMB-based sharing.
NTP	Network Time Protocol	A server that provides time source for other devices on the network to keep the time of all the devices synchronized.
RAID	Redundant Arrays of Independent Disks	A data storage technology that combines multiple hard drives into a single storage space with reliable storage.
rsync	remote sync	A data image backup tool for Linux systems, which supports remote data synchronization with other SSH and rsync hosts.
S.M.A.R.T.	Self-Monitoring Analysis and Reporting Technology	An automatic hard disk status monitoring and warning system.
SMB	Server Message Block	A protocol that allows SMB/CIFS-enabled Windows clients to access data stored on NAS.
SSH	Secure Shell	A protocol that provides security for Telnet sessions and other network services.
Target	Target	Storage resource on the iSCSI server.
UPS	Uninterruptible Power Supplies	An uninterruptible power supply device used to provide stable and uninterrupted power in case of power outage.

Disclaimer and Safety Warnings

Copyright Statement

©2023 Zhejiang Uniview Technologies Co., Ltd. All rights reserved.
No part of this manual may be copied, reproduced, translated or distributed in any form or by any means without prior consent in writing from Zhejiang Uniview Technologies Co., Ltd (referred to as Uniview or us hereafter).
The product described in this manual may contain proprietary software owned by Uniview and its possible licensors. Unless permitted by Uniview and its licensors, no one is allowed to copy, distribute, modify, abstract, decompile, disassemble, decrypt, reverse engineer, rent, transfer, or sublicense the software in any form or by any means.

Trademark Acknowledgements

unv uniarch are trademarks or registered trademarks of Uniview.

HDMI HIGH-DEFINITION MULTIMEDIA INTERFACE The terms HDMI, HDMI High-Definition Multimedia Interface, HDMI trade dress and the HDMI Logos are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.

All other trademarks, products, services and companies in this manual or the product described in this manual are the property of their respective owners.

Export Compliance Statement

Uniview complies with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abides by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, Uniview asks you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

EU Authorised Representative

UNV Technology EUROPE B.V. Room 2945,3rd Floor,Randstad 21-05 G,1314 BD,Almere,Netherlands.

Privacy Protection Reminder

Uniview complies with appropriate privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information. Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

About This Manual

- This manual is intended for multiple product models, and the photos, illustrations, descriptions, etc, in this manual may be different from the actual appearances, functions, features, etc, of the product.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Uniview cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Uniview reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will Uniview be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. Uniview strongly recommends that users take all necessary measures to enhance the protection of network, device, data and personal information. Uniview disclaims any liability related thereto but will readily provide necessary security related support.
- To the extent not prohibited by applicable law, in no event will Uniview and its employees, licensors, subsidiary, affiliates be liable for results arising out of using or inability to use the product or service, including, not limited to, loss of profits and any other commercial damages or losses, loss of data, procurement of substitute goods or services; property damage, personal injury, business interruption, loss of business information, or any special, direct, indirect, incidental, consequential, pecuniary, coverage, exemplary, subsidiary losses, however caused and on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise) in any way out of the use of the product, even if Uniview has been advised of the possibility of such damages (other than as may be required by applicable law in cases involving personal injury, incidental or subsidiary damage).
- To the extent allowed by applicable law, in no event shall Uniview's total liability to you for all damages for the product described in this manual (other than as may be required by applicable law in cases involving personal injury) exceed the amount of money that you have paid for the product.

Network Security

Please take all necessary measures to enhance network security for your device.
The following are necessary measures for the network security of your device:

- **Change default password and set strong password**: You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
- **Keep firmware up to date**: It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit Uniview's official website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly**: Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL**: Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering**: Allow access only from the specified IP addresses.
- **Minimum port mapping**: Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features**: If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely**: Avoid using the username and password of your social media, bank, email account, etc, as the username and password of your device, in case your social media, bank and email account information is leaked.

- **Restrict user permissions**: If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP**: When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP**: Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast**: Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs**: Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection**: Keep the device in a locked room or cabinet to prevent unauthorized physical access.
- **Isolate video surveillance network**: Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

Learn More

You may also obtain security information under Security Response Center at Uniview's official website.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Protect the device from liquid of any kind.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting Uniview first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use a UL certified power supply that meets LPS requirements if an adapter is used.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Use Caution

- When battery is used, avoid:
  - Extremely high or low temperature and air pressure during use, storage and transportation.
  - Battery replacement.
- Use the battery properly. Improper use of the battery such as the following may cause risks of fire, explosion or leakage of flammable liquid or gas.
  - Replace battery with an incorrect type;
  - Dispose of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery;
- Dispose of the used battery according to your local regulations or the battery manufacturer's instructions.

Avertissement de l'utilisation de la batterie

- Lorsque utiliser la batterie, évitez:
  - Température et pression d'air extrêmement élevées ou basses pendant l'utilisation, le stockage et le transport.
  - Remplacement de la batterie.
- Utilisez la batterie correctement. Mauvaise utilisation de la batterie comme celles mentionnées ici, peut entraîner des risques d'incendie, d'explosion ou de fuite liquide de gaz inflammables.
  - Remplacer la batterie par un type incorrect;
  - Disposer d'une batterie dans le feu ou un four chaud, écraser mécaniquement ou couper la batterie;
- Disposer la batterie utilisée conformément à vos règlements locaux ou aux instructions du fabricant de la batterie.
- **Personal safety warnings:**
  - Chemical Burn Hazard. This product contains a coin cell battery. Do NOT ingest the battery. It can cause severe internal burns and lead to death.
  - Keep new and used batteries away from children.
  - If the battery compartment does not close securely, stop using the product and keep it away from children.
  - If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- **Avertissements de sécurité personnelle:**
  - Risque de brûlure chimique. Ce produit contient une batterie de cellules. N'ingérer pas la batterie. Si la batterie de cellule est avalée, elle peut causer de graves brûlures internes en seulement 2 heures et peut entraîner la mort.
  - Gardez les batteries nouvelles ou utilisées à l'écart des enfants.
  - Si le compartiment de la batterie ne se ferme pas en toute sécurité, cessez d'utiliser le produit et gardez-le à l'écart des enfants.
  - Si vous pensez que des piles ont pu être avalées ou placées à l'intérieur d'une partie du corps, consultez immédiatement un médecin.

Regulatory Compliance

FCC Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Visit http://en.uniview.com/Support/Download_Center/Product_Installation/Declaration/ for SDoC.

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

LVD/EMC Directive

This product complies with the European Low Voltage Directive 2014/35/EU and EMC Directive 2014/30/EU.

WEEE Directive–2012/19/EU

The product this manual refers to is covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

Battery Directive-2013/56/EU

Battery in the product complies with the European Battery Directive 2013/56/EU. For proper recycling, return the battery to your supplier or to a designated collection point.