NAS Management System User Manual

Manual Version: V1.00

Software Version: DX-B1101

Contents

1 System Introduction
1.1 System Login
1.2 Home Page2
1.3 Quick Guide
2 Personalization ·······3
3 Control Panel
3.1 Account Management
3.1.1 Group Management ······ 5
3.1.2 User Management
3.2 System Configuration 10
3.2.1 Network Configuration 10
3.2.2 Interface Bonding ······ 13
3.2.3 NTP Configuration ······· 14
3.2.4 Hardware and Power Supply 15
3.3 Task Management 18
3.3.1 S.M.A.R.T. Test Task 18
3.3.2 Rsync Task 19
3.3.3 Data Scrubbing Task······ 21
3.3.4 Schedule Snapshot Task ····· 22
3.4 Security Management 23
3.4.1 Service Management ····· 23
3.4.2 Firewall Setting 25
3.4.3 Certificate Management 26
4 Storage Management 27
4.1 Storage Management······ 27
4.1.1 Storage Pool Information 28
4.1.2 Create Storage Pool 28
4.1.3 Manage Storage Pool 29
4.1.4 Rename Storage Pool ······ 30
4.1.5 Delete Storage Pool ······ 31
4.2 Cache Configuration

4.3 HDD 31
5 Sharing Management 33
5.1 Shared Folder ······ 33
5.1.1 Add Shared Folder ······ 33
5.1.2 Properties Management 35
5.1.3 Snapshot
5.1.4 Share with Linux ······ 40
5.1.5 Lock/Unlock 41
5.1.6 Delete Shared Folder 41
5.2 Sharing Configuration 42
5.2.1 Share with Windows 42
5.2.2 Share with Linux ······ 44
5.2.3 Share with Mac ······ 45
5.2.4 Share by WebDAV 45
5.2.5 Share by FTP
6 Block Sharing 47
6.1 Resource Overview 47
6.2 Host 47
6.2.1 Add Host ······ 48
6.2.2 Edit Host 49
6.2.3 View Initiator ······ 49
6.2.4 Delete Host ······ 50
6.3 LUN Resources ······ 50
6.3.1 Add LUN 50
6.3.2 Edit LUN 51
6.3.3 Snapshot 51
6.3.4 Delete LUN 51
6.4 Target
6.4.1 Add Target······ 52
6.4.2 Edit Target 54
6.4.3 Delete LUN Mapping ······ 54
6.4.4 Delete Link
6.4.5 Delete Target ······ 54
6.5 Use NAS Resource on the Host ····· 55
6.5.1 Windows Host 55

6.5.2 VMware ESXi Host ······ 56
6.5.3 Linux Host 57
7 File Manager
7.1 File Manager ····· 58
7.1.1 New Folder 58
7.1.2 Upload Files 58
7.1.3 Share Files 59
7.1.4 Download File 60
7.1.5 File Management Actions 60
7.2 Share Links ····· 60
7.3 Recycle Bin
8 System Maintenance61
8.1 System Update and Restore 61
8.1.1 System Update ······ 61
8.1.2 System Configuration Backup and Restore 62
8.2 Log Center 63
8.2.1 Alarm Logs 63
8.2.2 Operation Logs 63
9 Acronym and Abbreviations
Disclaimer and Safety Warnings

1 System Introduction

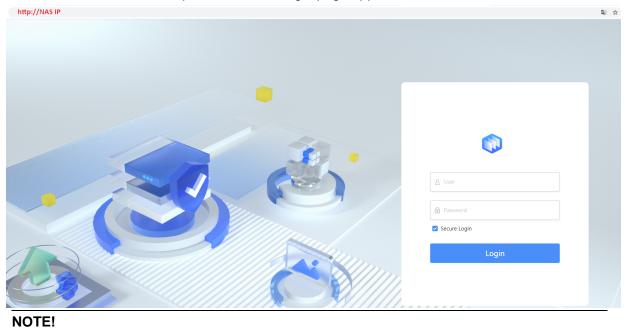
The desktop Network Attached Storage (NAS) is a powerful storage device with high-capacity file storage and data protection.

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.





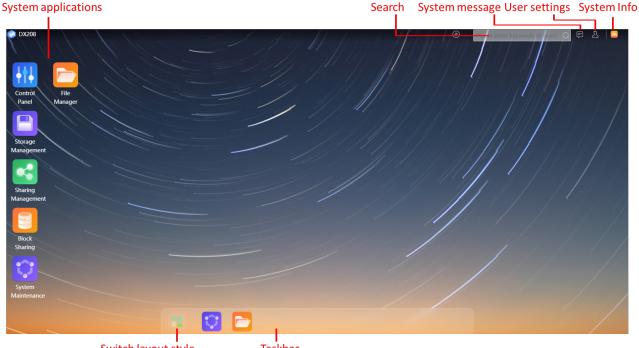
3. Enter the username and password, and then click Login.



NOTE!

- The default username/password: nas/nas
- For data safety, 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 (<u>http://192.168.0.1</u>) to access the NAS management system.
 - (3) Go to **Control Panel** > **System Configuration** > **Network Configuration**, change the IP address. See Network Configuration.
 - (4) Connect the NAS device to the networking device (switch, router) using a network cable.

1.2 Home Page



Switch layout style

Taskbar

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 \bigcirc to search for a function, and then click to open the application page.
System message	Click 투 to see system errors, warnings, and alerts.
User settings	Click $\stackrel{2}{\frown}$ to view user information, to personalize, restart, turn off, or log out of the NAS device.

System In	fo
-----------	----

1.3 Quick Guide

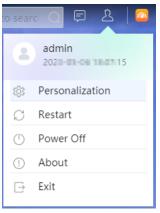
For first-time use, follow the steps to configure the NAS device before using it to store your files.

- 1. <u>Create storage pool and cache</u>: Add hard disks to a storage pool to create storage space; use SSD to create cache space.
- 2. <u>Configure shared folder and service</u>: Create shared folders to store files and manage subfolders; configure sharing service to allow data access from other clients.
- 3. <u>Create groups/users</u>: Create accounts for family or enterprise members, set permissions, and assign storage space.
- 4. <u>Use NAS to store files</u>: Upload files to the NAS device, view, download, and share files on the NAS device.
- 5. <u>Use NAS as local disk</u>: 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 \underline{A} in the upper right corner.



2. Click Personalization.

3. View or edit settings as described below.

ltem	Description
Basic Information	Basic information

	Personalization	X
	Basic Information	
	Personalization	Username: admin
		Description: System default user
		Email: Please enter
		Password: Last Time Modified:2023-05-06 16:58:30
		Change Password
		OK Cancel
		n: Type a personal description.
		out your personal email address to receive system messages and retrieve
	•	in case you forget it.
		: Click Change Password to set a new password. After changing the
	-	, you need to log in with the new password.
		vileged user can allow or forbid other users to change password (Control
	Panel > U	Jser Management, see User Management).
Personalization	Personalize t	he system according to your preferences.
	Personalization	×
	Basic Information	Date and Time
	Personalization	
		Date Format : YYYY-MM-DD(System Setting) V
		Time Format : 24H Time(System Setting)
		Language
		System Language : English \lor
		Desktop Background
		Select Image
		Image Position: Fill V
		OK Cancel
		Cancer
	 Date and 	Time: Choose the date and time format.
		E Choose the system language.
		Background: Click Select Image , and choose an image from your computer,
		from default images in the system.
		sition: Set how the image will be displayed (fill or tile).

Select Image X
My Images System Default
Select:
+ Upload Image
Recent Images:
OK Cancel

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

3 Control Panel

Use the control panel to navigate system settings.

3.1 Account Management

3.1.1 Group Management

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 Management > Group Management.

		- • ×
User Group List (2) Add Delete		Please enter Q
User Group Name	Description	Action
administrators	System default admin group	2
everyone	System default group	2 1
	User Group Name administrators	User Group Name Description administrators System default admin group

NOTE!

=(/

The system includes two default user groups:

- administrators: including nas and admin.
- everyone: including common users.

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.

ltem	Description						
Basic	Input the group name and description.						
Information	Add Group				×		
	1 Basic Infor	rmation Sel	ect Members	3 Shared Folder			
				Permission			
	* User Group Name :						
	Description :						
		Next	Cancel				
	 User Group Na letters, digits, a 	me: Input the grou	o name. The nar	ne contains 4-16 char	acters and allows		
		out a description of	the group for dif	ferentiation.			
Select Members	Add users to the g	roup. (To add user	s, see User Man	agement).			
Members	-	ou want to add to th	•	step and add later.			
	Add Group				×		
	(✓ ———	2	3			
	Basic I	nformation	Select Members	Shared Folder Permission			
	Username	User Description		Add To			
	admin	System default user					
	guest	Guest					
	nas	System default user					
		Back	Next C	ancel			
Access to Shared Folder	Set permission for						
		d/Write and group p	ermission is Der	Vrite > Read Only. Fo ny, then the final perm			

Add Group					
	\bigcirc ——		3		
	Basic Information	Select Members	Shared Folder Permission		
	nission from high to low: Deny > Read final permission of the member is Deny		s permission is Read/Write and the group's permissi		
Shared Folder	Deny	Read/Write	Read Only		
AutoCar		~			
AutoCar					

3. Click Finish to save the settings.

Edit a Group

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



NOTE!

Default system groups cannot be deleted.

3.1.2 User Management

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 Management > User Management.

, v	^ Us	ser List (3) Add	Delete			Please enter	
Group Management User Management		Username	Email	Description	Status	Action	
System Configuration	~	admin		System default user	Normal	2 🔟	
	~	guest		Guest	Normal	2	
	~	nas		System default user	Normal	2 🗉	
, ,							



NOTE!

The system has three 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 Management). 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	Enter the username, password, etc.						
Information	Add User X						
	Basic Information Add to User Shared Folder Application Group Permission Program Permission						
	* Username :						
	Description :						
	Email:						
	* Password:						
	* Confirm Password :						
	Forbid the User to Change Password						
	 Next Cancel 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	Add the user to a user group (see Group Management).						
Group	 If the user group already exists, choose it to add the user. Or skip this step and add later. 						

	Add User					×
		Ø		(3)	4)
		Basic Information	Add to User Group	Shared Folder Permission	Applic	
			Group	1 (11115510)1	Permis	
	User Group Name		Description		Add To	
	administrators		System default admin grou	p		
	everyone		System default group		\checkmark	
	Mygroup				~	
			Back	Next Cancel		
Shared Folder	Set permissio	on for the user	to access share	ed folders.		
Permission	Priority of per	mission from h	high to low: Den	y > Read/Write >		For example, if user
		Read/Write ar Deny overrides		ssion is Deny, the	n the final pe	rmission of the user
	Add User					X
		—	(\vee\	3	4)
		Basic Information	Add to User Group	Shared Folder Permission	Applica Progr Permis	am
	Priority of permission from high to low: Deny > Read/Write > Read Only. For example, if the member's permission is Read/Write and the group's permission is Deny, then the final permission of the member is Deny (as Deny overrides Read/Write).					
	Shared Folder	Final Permission	Group Final Permission	Deny	Read/Write	Read Only
	DOC_File	Read/Write	-			
			Back	Next Cancel		
Application	Set permission	on for the user	to access appli	cation programs.		
Program Permission						permission is Allow (as Deny overrides

Basic Information Add to User Group Shared Folder Permission Application Program Permission Application Program Final Permission Allow Deny Storage Management Allow Image: Compare to the storage of the st	Add User	(v) ———		(\alpha)	4
Storage Management Allow Image: Comparison of the state of th		Basic Information		Shared Folder Permission	Application Program Permission
Sharing Management Allow Image: Comparison of the state of the sta	Application Program	Final Permiss	sion	Allow	Deny
Block Sharing Allow Image: Constraint of the state of	Storage Management	Allow			
System Maintenance Allow	Sharing Management	Allow			
	Block Sharing	Allow			
File Manager Deny	System Maintenance	Allow			
	File Manager	Deny			
			Back Comp	lete Cancel	

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

Edit a User

In the user list, click \sim 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 $\overline{\square}$ for the user you want to delete and then confirm the deletion.



NOTE!

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

3.2 System Configuration

3.2.1 Network Configuration

Configure the IP, route, and DNS server information so the NAS device can connect to network. Go to **Control Panel > System Configuration > Network Configuration**.

Control Panel							- 🗆 X
🚖 Account Management ,	Network Con	figuration Interface	Bonding				
Group Management	Network In	terface Information Route	Management				
User Management	Interface	IP Assignment Mode	Network Protocol Type	IP Address	Netmask	MTU	Speed
System Configuration ~	eth1	Auto	IPv4	10.222.57.234	255.255.252.0	1500	1000
NTP Configuration	eth0	Manual	IPv4	208.208.5.222	255.255.255.0	1500	100
Hardware and Power							
Task Management ~	DNS Inform	nation 🕘 Delete					
Security Management 🗸		DNS Address	Action				
		10.220.3.54	2				
		10.220.5.55	2 1				

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 \swarrow for the network interface.

Network Protocol Type		×
Interface :	eth0	
IP Assignment Mode :	Assign Manually 🗸	
IP Address :	308.308.3.222	
Netmask :	255.255.255.0	
MTU:	1500	
	OK Cancel	

- 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.

Route Management

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

1. Click Route Management.

Route Management					×
Route Configuration Add Delete	Refresh				
Network Destination	Netmask	Gateway	Interface	Action	
207.207.0.0	255.255.255.0	208,208,3.1	eth0		
Default Gateway		Interface:	eth0		~
	OK	Cancel			

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

Add Route		>
Network Protocol Type:		V
Network Destination :	Please enter the destination network address	
Netmask :	Please enter the netmask.	
Gateway :	Please enter the gateway address	
Interface :		~

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.

Add DNS			×
DNS Address:	10.220.3.53		
	ОК	Cancel	

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 Configuration > Network Configuration > Interface Bonding.

Control Panel					- • ×
💼 Account Management 🕠	Network Configuration Interface Bonding				
Group Management User Management	Interface Bonding Cancel Bonding				
System Configuration	Interface Network Protocol Type IP Address Netmask	Bonding Mode	MTU	Members	Action
Network Configuration	☑ bond0 IPv4	active-backup	1500		6 -
NTP Configuration	bond1 IPv4	active-backup	1500		G _
🔁 Task Management 🗸					
Security Management 🗸 🗸					

Set Bonding

1. Click **Set Bonding**. A page as shown below appears.

Set Bonding					
* Interface :	bond1				
Network Protocol Type:	IPv4				
* IP Address :	Please enter the IP address				
* Netmask :	Please enter the netmask.				
* Select Bonding Mode:	active-backup \lor				
Interface	IP Address				
eth1	10.122.57.234				
eth0	201.201.3.222				

OK Cancel

2. Complete the required information, and choose member interfaces.

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

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.

Interface bonding modes are described in the table below:

Cancel Bonding

Select the member interfaces, click **Cancel Bonding** and then confirm.

3.2.3 NTP Configuration

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

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

Control Panel					_	
Croup Management Account Management User Management	Time Zone : Time :	(GMT+08:00) Beijing, Chongqing, Hor 2023-05-08 10:19:18	ng Kong, Urumqi 🗸			
System Configuration Network Configuration	NTP Server: NTP Sync Interval:	Please enter the NTP server addr 10				
NTP Configuration Hardware and Power	Save	Minute(1-10080) Reset				
 Task Management ~ Security Management ~ 						

Set Time Manually

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

Sync Time with an NFT Server

- 1. Set the NTP server IP and a time synchronization interval.
- 2. Click **Save** to save the settings.

3.2.4 Hardware and Power Supply

Go to Control Panel > System Configuration > Hardware and Power Supply.

1. Fan

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

Fan	LED	HDD	Power	Power On/Off	
	Please select a n	node			
		0		e	O
		II-speed mode at full speed. It system but ma loud noises	can quickly	Low-temperature mode The fan works at a high speed to keep the system cool	Silent mode The fan works at a slow speed to decrease noises
	Note: If the syste	em temperature	e rises, the syste	m will still raise fan speed automatically even in lo	ow-temperature or silent mode.

Reset

2. **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.

Fan		LED		HD	D		Po	ower		Power C	n/Off					
	2							-								
	Drag	the slide	er to a	djusi	t LEL) bri	ghtn	iess. I	he cur	rent brigh	tness leve	IS /				
	٠Ö٠	 _		•	•	-0-	-0-	-0	-;ó(-							
		0 1	2	3	4	5	6	7								
												Sa	ve	Rese	1	
												30	ve-	i/csc		

3. **HDD**

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.

Fan	LED	HDD	Power	Power On/Off	
	Internal HDDs will	enter sleep mo	ode after being	idle for a certain length of time	Never ∨
				Save	Reset

4. 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.

Fan	LED	HDD	Power	Power On/Off		
	Using UPS can pre Enable UPS	event losing da	ata in case of po	wer outage		
	UPS Type:	At	USB UPS usiliary power supply to nected to the USB port	hat is		
		con	NAS device	on the	Save	Reset

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

5. Power On and Power 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.

Fan	LED	HDD	Power	Power On/Off		
	Add	Delete Scheo	dule Overview			
		Trigger Time	Туре	Enable/[Disable A	Action
		Monday 08:30:00	Powe	er On		
				l	Save Reset	

- Add a power-on/off schedule
- 1. Click Add.
- 2. Set a schedule.

Add		×
Type :	● Power On ○ Power Off	
Date :	● Every Day ○ Every Week ○ Specified Date	
Time :	Select time (S	
	OK Cancel	

- > 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 Z 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 Management

3.3.1 S.M.A.R.T. Test Task

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.

🚻 Control Panel o × c Account Management S.M.A.R.T. Test Task Add Delete Group Management HDD Description Schedule Enable/Disable Action Туре User Management 之前 1 Short Test Run at 00:00 every day System Configuration Network Configuration 之前 2 Long Test Run every 1 hours start... NTP Configuration Hardware and Power 🔋 Task Management Rsync Task Add a Task 1. Click Add.

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

Add Task		>
* HDD:		
* Type:	Short Test	\vee
Description:		
Schedule		
* Task Schedule:	● Every Day ○ Every Week ○ Specified Date	
* First Running Time:	00:00	
* Task Frequency:	Every Day	~
* Last Running Time:	00:00	~



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

Paramet	er	Description
HDD		Choose the HDD you want to test.
Туре		 Short: The test only tests key items and takes a short time. Long: 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 Task

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 Management** > **Service Management** first. See Service Management.

Go to Control Panel > Task Management > Rsync Task.

🚻 Control Panel										-	o x
Croup Management	Rsync Tas	sk Add De	lete						Please en		Q
User Management		Shared Folder	Remote Host	Remote Module Name	Username	Direction	Description	Schedule	Enable/Disable	Action	
🤹 System Configuration 🔦		DOC_File	207.207.90.2	FileModule	admin	Push		Run at 00:0		2	
Network Configuration											
NTP Configuration											
Hardware and Power											
뉯 Task Management 🔷 🔨											
S.M.A.R.T. Test Task											
Rsync Task											

Add a Task

1. Click Add.

dd Task			X
Source			
* Shared Folder:		~	
* User:		~	?
Direction:	● Push ◯ Pull		
Description:			
Remote			
* Remote Host:			?
* Rsync Mode:	Module	~	
* Remote Module Name:			?
* Password:		Ø	
Schedule			
* Task Schedule:	● Every Day ○ Every Week ○ Specified Date		
* First Running Time:	00:00		
* Task Frequency:	Every Day	~	
* Last Running Time:	00:00	~	

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

Paramet	er	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.

Cancel

	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 Task

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 Management > Data Scrubbing Task.

Account Management	Data Scru	Ibbing Task Add	Delete			Plea	se enter	
Group Management User Management		Storage Pool	Threshold Days	Description	Schedule	Enable/Disable	Action	
System Configuration		pools	36		Run at 00:00 ev		2	
Network Configuration								
NTP Configuration								
Hardware and Power								
Task Management								
S.M.A.R.T. Test Task								
Rsync Task								
Data Scrubbing Task								
Scheduled Snapshot Task								

Add a Task

1. Click Add.

Add Task			×
t Charren Dault			
* Storage Pool:			
* Threshold Days:	36		?
Description:			
Schedule			
* Task Schedule:	Every Day Every Week Specified Date		
* First Running Time:	00:00 (5)		
* Task Frequency:	Every Day	\sim	
Test Denning Times			
* Last Running Time:	00:00	×	
	OK Cancel		

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 Schedule Snapshot Task

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 Management > Schedule Snapshot Task.

Add a Task

1. Click Add.

dd Task		
* Snapshot Task Name:		
-	Please enter 1-63 characters, which may include digits, uppercase and lowercase letters, and special characters	
Snapshot Target Type:	● LUN ○ Shared Folder	
* Snapshot Target:	v	
Schedule		
* Task Schedule:	● Every Day ○ Every Week ○ Specified Date	
* First Running Time:	00:00 (3)	
* Task Frequency:	Every Day 🗸	
* Last Running Time:	00:00 ~	

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".

Cancel

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

3.4 Security Management

3.4.1 Service Management

You can enable or disable services and automatic service startup.

Go to Control Panel > Security Management > Service Management.

Control Panel			- 0
System Configuration	Service List	Port: 22	
Network Configuration NTP Configuration Hardware and Power	ssh Run Service 🚺 Auto Start	Save Reset	
Task Management ^	iSCSi Run Service 🚺 Auto Start		
Rsync Task Data Scrubbing Task Scheduled Snapshot Task	rsync Run Service Auto Start		
Security Management	docker Run Service Auto Start		
Firewall Setting Certificate Management			

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.

Service List	Please choose the root path for Docker:
ssh Run Service Auto Start	pools \lor Please set the mirrored repository address for Docker:
iscsi Run Service Auto Start	https://hub.daocloud.io
rsync Run Service Auto Start	Start Portainer as the visual management tool for Docker Please click 10.222.97.234:9000 to visit this website
docker Run Service Auto Start	Save

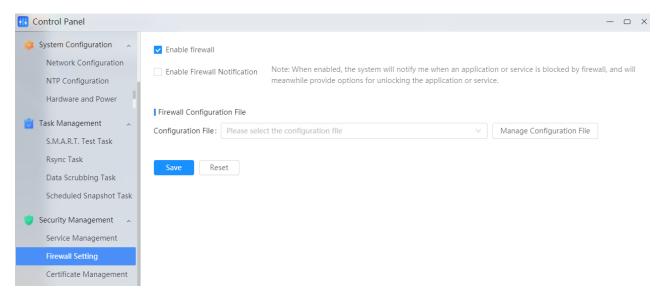
2. To enable a service to restart automatically after the NAS device restarts, turn on **Auto Start** for the service.

3. Click Save to save the settings.

3.4.2 Firewall Setting

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 Management > Firewall Setting.



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 applica and provide unlock options.	ation or service is blocked by firewall
Firewall Configuration File	ewall You can set different configuration files to quickly apply different firewall rules a	
	 2. Click Add. On the page as shown below, input the from the list. 	file name, and choose a firewall rule

Add Configuration File					\times
Configuration File Name:					
Firewall Rules					
All Interfaces \lor	Add Delete				
Port	Communi cation Protocol	Source IP	Action Enabl ab	Action	
5060(Source Port)	ICMP	All	Allow		
Comparison of rules will be m					
You can drag to change the or	der of rules. The higher the o	order, the higher the priority			
		ОК Са	ncel		
If the firewall rule is	not propted				
	not created,		eale II.	~	
Add Firewall Rules				×	
Port					
FOIL					
All			∨ Selec	zt	
-			∨ Selec	rt	
A11			 ✓ Select ✓ Select 		
All Source IP					
All Source IP All					
All Source IP All					
All Source IP All Action					
All Source IP All Action			✓ Selec		
All Source IP All Action	Add	Cancel	✓ Selec		
All Source IP All Action			✓ Selec	:t	
All Source IP All Action Allow O Deny Port: All (default	t), Custom (yo (default), Spe	ou need to spe	Selection Selection <t< th=""><th>:t</th><th>r an</th></t<>	:t	r an
All Source IP All All Action Allow Deny Port: All (default Source IP: All Address range).	t), Custom (yo (default), Spe illow access f	ou need to spe cified IP (you	 Selection Selection	port range).	

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

3.4.3 Certificate Management

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 Management > Certificate Management**.

Uniview/Default Certificate	
Issuer: UNV Systems,Inc.	
Entity Alias:	
Certificate Expi 2032-04-03	
Import Certificate	
Export Certificate	

Import a Certificate

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

Import Certificate	×
After the new certificate is imported, it will replace the current certificate; you certificate.	a may also restore the default
* Certificate:	Select
* Private Key :	Select
Intermediate Certificate :	Select
OK Cancel	

- 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 Management

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

4.1 Storage Management

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 Management > Storage Management.

4.1.1 Storage Pool Information

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

Storage Management							— 🗆 X	
Storage Management	Storage Pool(1)	Create				Please enter	Q	
Cache Configuration	✓ pools Norm	✓ pools Normal 7.85MB/434.13GB 0%						
🦲 HDD	Basic Inform	ation	15	Space Usage				
	RAID Level: RAID0	RAID status: Norma	I		0%			
	Data Scrubbing					Shared Folder 432	2KB	
	Status: Completion Time:					 LUN 1.53MB Others 0B 		
	Scrubbing complete	2023-04-28 10:17:20)		100%	Free Space 434.12	2GB	
	HDD Informa							
	HDD ID	Туре	Capacity	Status	Vendor	Model		
	1	HDD	465.76GB	 Normal 	SEAGATE	ST500DM009-2F110A		

4.1.2 Create Storage Pool

Follow the steps to create a storage pool:

Create								×
* Storage	Pool Na	Plea				nd may include	digits, uppercase and lowercase	
* RAID Lev	rel:	RAID0	ers. Do not ente	er space or symbo	ols such as / @			
Please se	lect HE	DD:	Selected	11				
	HDD	DID	Туре	Capacity	Status	Vendor	Model	
	1		HDD	3.64TB	 Normal 	WD	WDC WD4000FYYZ-01UL1B2	

OK Cancel	ОК
-----------	----

- 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.

\mathbf{i}

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.

4.1.3 Manage Storage Pool

Rebuild, expand, and scrub a storage pool.

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

Ν	Manage									
	Rebuild Expand Scrubbing									
	Groupl ∨									
	HDD ID	Туре	Capacity	Status	Vendor	Model				
	1	HDD	465.76GB	• Normal	SEAGATE	ST500DM009-2F110A				

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.

4.1.4 Rename Storage Pool

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

4.1.5 Delete Storage Pool



CAUTION!

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

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

4.2 Cache Configuration

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 Management > Cache Configuration.

Add Cache Device

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

0	Create Cach	e						>
		1	select SDD			2 Configure Cad	the Storage	
	Only :	SSD can be used to	o create cache.					
	Select SSD	Selecte	d0 ,estimated capacity:0					
		HDD ID	Туре	Capacity	Status	Vendor	Model	

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

4.3 HDD

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 Management > HDD**.

Storage Management	HDD Management	t (8)						
Cache Configuration	HDD ID	Туре	Capacity	Status	Home Storage Pool	Purpose	Set as Ho	Action
HDD	1	HDD	465.76GB	 Normal 	pools	Data Disk	C	民龄
	2	HDD	OB	No HDD	-	Idle	C	E ¢
	3	HDD	OB	No HDD	-	Idle	C	E ŵ
	4	HDD	OB	No HDD	-	Idle	C	E ©
	5	HDD	OB	No HDD	-	Idle	C	图 ‡
	6	HDD	OB	No HDD	-	Idle	C	E ŵ
	7	HDD	OB	No HDD	-	Idle	C	民命

• 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.		
HDD 2Information		×
Basic Information		
HDD ID	2	
Storage Pool	-	
Health Status	Normal	
Purpose	Idle	
Temperature	0°C	
Serial No.	-	
Firmware Version	-	
S.M.A.R.T. Test Task : 💿 S	Short Test 🔵 Long Test	
Sta	art	
S.M.A.R.T. Attributes : Vie	ew Details	

• Configure a S.M.A.R.T. test task:

Click ⁽²⁾ to configure a S.M.A.R.T. test task for an HDD. See S.M.A.R.T. Test Task for more information.

* Detection Type:		~
* Task Schedule:	● Every Day ○ Every Week ○ Specified Date	
* First Running Time:	00:00	
* Task Frequency:	Every Day	~
* Last Running Time:	00:00	~
	OK Cancel	

5 Sharing Management

Sharing management 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 Management** > **Shared Folder** to view shared folders, including folder information and space usage.

🕄 Sharing Management		
bared Folder	Shared Folder (2) Add	Q
Sharing Configuration	➤ ➢ AutoCar123 Ready 0.25MB/20GB 0% Properties Management Snapshot ∨ 1	More 🗸
	✓ ∞ DOC Ready 100KB/0.42TB 0% Properties Management Snapshot ∨ 1	More 💛
	Basic Information Home Storage Pool: pools	
	Description : Enable Recycle Bin: No Enable Encryption: No Enable Quota: No Enable File Compression: No Enable File Deduplicati	ion: No
	< 1 > 2/page -	

5.1.1 Add Shared Folder

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

Add Shared Folder				×
1 Basi	ic Configuration	(2	Permission Configuration	
* Folder Name:				
* Home Storage Pool:				~
Description:				0/64
Others:	✓ Enable Recycle Bin			
	Only Accessible	to Admin		
	✓ Encrypt This Shared F	older		
	* Encryption Key :		Ø	
	* Confirm Key :		Ø	
	✓ Enable Quota for Shar	ed Folder		
	Enter Quota :		GB V	
	✓ Compress			
	Deduplicate(requires a	minimum of 16GB memory, cur	rent memory: 4GB)	

Next Cancel

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.

✓ Bas	ic Configuration		– 2 Perr	nission Configurati	on
User Permission	Group Permission				
Username	Final Permission	Group Permission	Deny	Read/Write	Read Only
admin	Read/Write	-		~	
guest	Read/Write	-		~	
nas	Deny	-	~		
chain	Read Only	-			~
Bob	Read/Write	-		~	
		omplete Car	ncel		

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

5.1.2 Properties Management

Edit a shared folder.

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

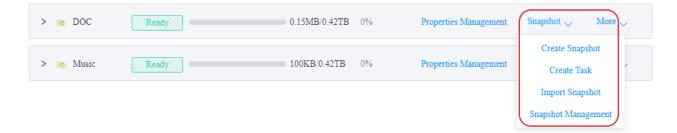
Properties Management		×
Basic Configuration	Permission Setup	
* Folder Name:	DOC	۲
* Home Storage Pool:	pools	\sim
Description:		0/64
Others:	 Enable Recycle Bin Encrypt This Shared Folder Edit Key Enable Quota for Shared Folder Compress Deduplicate(requires a minimum of 16GB memory, current memory: 4GB) 	
	OK Cancel	

- 2. Edit the properties and access permission. For parameter descriptions, see Add Shared Folder.
- 3. Click **OK** to save the settings.

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.

Create Snapshot		\times
* Snapshot Name :	GMT08_2023-05-08_150718	7
	Please enter 1-63 characters, which may include digits, uppercase and lowercase letters, and special characters	
	OK Cancel	

2. Create Task

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

Create Snapshot Task		
* Snapshot Task Name :		
	Please enter 1-63 characters, which may include digits, uppercase and lowercase letters, and special characters	
* Task Schedule:	● Every Day ○ Every Week ○ Specified Date	
* First Running Time :	00:00	
* Task Frequency :	Every Day \lor	
* Last Running Time :	00:00 ~	
	OK Cancel	

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 Management

View the snapshots created for the shared folder.

Snapshot Management			
Delete			
Snapshot Name	Space Used by Snapshots	Creation Time	Action
GMT08_2023-05-12_192120	OB	2023-05-12 19:20:14	@ 5 ⊥ ΰ
GMT08_2023-05-12_192125	OB	2023-05-12 19:20:19	í ± ⊂ ∃

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.

Please sel	ect the destination	n storage pool.		~
Please en	ter a name for the	e copy of the si	hared folder	
Please en	ter a name for the	e copy of the s	hared 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.

PRollback: 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.

Message		×
	After rollback, the data at the time of the snapshot will be restored, but data from the time of the snapshot to the current time will be lost. Are you sure you want to continue?	
	OK Cancel	
Export Dick	: Export the snapshot to the shared folder	
Snapshot e	xported	
* Please sel	ect the destination folder	
Please sel	ect the destination folder	
	OK Cancel	

- (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.

Message		×
•	The snapshot cannot be recovered after being deleted. Continue?	

4. Import Snapshot

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

Cancel

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

• Import a snapshot to the current device

Snapshot of Shared	Export Any Shared Folder	nport	Copy of Shared
Folder A	Ally Shared Folder		Folder A

Import a snapshot to other devices

D	evice A	Device B
Snapshot of Shared Folder A	Any Shared Folder	Any Shared Folder Folder Folder A
	Download	Upload
	Loca	l Storage

Follows the steps to import the snapshot:

1. Click Import Snapshot.

Import Snapshot	×
* Please select the destination shared folder	
Please select the destination shared folder	~
* Please select the image file.	
Please select the image file.	\sim
* Please select the destination storage pool.	
Please select the destination storage pool.	\sim
* Please enter the name of the folder created after the import	
Please enter the name of the folder created after the import	
OK Cancel	

- 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 Share with Linux

NOTE!

Configure sharing so users can access data on the NAS device from a Linux client.

÷.
2
í

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

1. On the **Sharing Management** page, click **More** for the folder you want to share, choose **Linux**.

	>	📚 AutoCar123	Ready	0.25MB/20GH	B 0%	Properties Management	Snapshot 💛	More 🗸
	~	s DOC	Ready	0.15MB/0.427	IB 0%	Properties Management	Snapshot 🧹	Linux Delete
	I	Basic Information						Lock
Lir	านx							×
	Ad	d Delete]					
		Client	Access Permission	on Squash	Asynchronou	us Non-Privile	ged Port Ac	tion
		208.208.90	2 Read Only	Do Not Map Roo	ot Not Allow	Not Allow	Ô.	

2. Click Add.

Add Sharing		×	C
* Server Name or IP :			
Permission:	Read Only	\vee	
Squash:	Do Not Map Root	\sim	
Security :	AUTH_SYS	\sim	
	Enable Asynchronous		
	Allow Connections from Non-privileged Ports (ports greater than 1024)		
	OK Cancel		

- 3. Input the Linux server name or IP address.
- 4. Click **OK** to save the settings.

5.1.5 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**.

> 😒 Picture	Ready	0.21MB/0.42TB 0%	Properties Management	Snapshot 🗸	More 🗸
					Linux
					Delete
					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**.

> 😋 Picture	Locked	0.27MB/0.42TB	0%	Properties Management	Snapshot 🗸	More 🗸
						Delete
						Unlock

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

essage		×
* Please enter the key :		
Please enter		
ОК	Cancel	

5.1.6 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 Management** > **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.

🚭 Sharing Management									×
늘 Shared Folder	Windows	Linux	Mac	WebDAV	FTP				
Sharing Configuration	☑ Enable SMB S	Service(to all	ow access fron	n Windows client)					
	Service Descrip	tion: n	as						
	Workgroup:	W	vorkgroup						
	 Stand-alone 	e Server(USR	Mode)						
	Active Direction	ctory Service	(AD Domain)	ැබූ To enable this	option, please	configure firs	t		
	🔵 LDAP 🔞 T	o enable this	option, please	e configure first					

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.
LDAP	LDAP users can access the NAS device when LDAP domain is enabled.

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 When enabled, the NAS device can be used as the local master browser Browser master browser is responsible for maintaining the device list in 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	This option is available when AD Domain is enabled.			
Update	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	This mode can improve SMB performance through asynchronous I/O.			
Mode	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	Choose the highest and lowest SMB protocol versions used on your network.			
Lowest SMB Version	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	Choose whether identity verification is required when anonymous user wants to access the shared folder via SMB.			
Folder	• 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.			
	✓ Please enter file hiding criteria			
	File Hiding Criteria:			

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.

💣 🕑 📙 🖛 207.129.130.45		
File Network View		
← → × ↑ 💣 > Network > 207.12 NA	1.750.45 → \S IP	
🗸 🛄 This PC	vedio	Document
> 📃 Desktop		 bocament
> 🗄 Documents		
> 🕂 Downloads		
N Music		

 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.

Pin to Quick access Manage Pin to Start TortoiseSVN	What network folder would you like to map? Specify the drive letter for the connection and the folder that you want to connect to:	File Computer View ← → ↑ ▲ > This PC >	
Map network drive Disconnect network drive Create shortcut Delete Rename Properties	Drive: Z: Folder: Kample: \\serve:\share Cample: \\serve:\share Connect using different credentials Connect to a Web site that you can use to store your documents and pictures.	✓ This PC ✓ This PC ✓ This PC ✓ Desktop ✓ Ocuments ✓ Downloads ✓ Music	 > Folders (7) > Devices and drives (5) > Network (1) test001 (\\sub_12,134.43) (Z) 45GB free of 45GB

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.

Sharing Management							
늘 Shared Folder	Windows	Linux	Mac	WebDAV	FTP		
Sharing Configuration	✓ Enable NFS Services						

2. Configure Linux Client

Configure the Linux client that is allowed to access the shared folder. See Share with Linux.

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.

< Sharing Management							— (
늘 Shared Folder	Windows	Linux	Mac	WebDAV	FTP			
Sharing Configuration	🔽 Enable AFF	o (to allow acce	ss from Mac c	lient)				

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.

💽 Sharing Management					
늘 Shared Folder	Windows	Linux	Mac	WebDAV	FTP
Sharing Configuration	Enable HTTP				
	HTTP Port:	8080			
	Enable HTTPS	5			
	HTTPS Port:	8081			
	Save Res	et			

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

Allow Anonymous

Access

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

💽 Sharing Management	:						
늘 Shared Folder	Windows Linux Mac	WebDAV F1	ГР				
Sharing Configuration	Enable FTP						
	Protocol Type:	 FTP (standard) 	FTP (external SSL/TSL)				
	Port:	21					
	Unicode Supported:	• Yes O No (choose this option if FTP does not support Unico					
	Allow Anonymous Access:	🔿 Yes 💿 No					
	Connection Settings						
	Max Total FTP Connections:	30					
	Max FTP Connections per Account:	21					
	Max. Upload Speed	0	KB/S				
	Max. Download Speed	0	V'R /C				
Item	Description						
Enable FTP	Select the checkbox to enable the F	TP service.					
Protocol Type	Choose an FTP protocol type.						
	 provide encryption for session in consumes less system resource FTP (external): An extension of option provides session information 	 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 defa	ault is 21.					
Unicode Supported	Set whether Unicode is supported characters in files.	. This setting helps	the FTP client correctly display				
	 The default is Yes. Chapped No if the ETD eligent data 	o not ounnort l laise	do				
	 Choose No if the FTP client does not support Unicode. 						

Set whether to allow anonymous users to access the NAS device.

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.

6.1 **Resource Overview**

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

Block Sharing	×
🔮 Overview	
Target	Block share is normal.
EUN resources	
🧧 Host	Mapped LUN 0 Unmapped UN 1 UN 0 Unlinked Target 1

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).

Block Sharing			- 0
🔵 Overview	Host (2) Add		Please enter Q
 Target LUN resources 	host01 VMware ESX Description:	host02 VMware ESXI Description:	
🗧 Host	Initiators: 1个	Initiators: 0个	
	Edit View Initiators Delete	Edit View Initiators Delete	

6.2.1 Add Host

1. Click Add.

		>
Please ente	r the name.	
VMware E	SXi	~
		li
Add		
	Initiator(IQN/WWPN)	Action
	Example:iqn.2022-08.com.test	✓ ×
	VMware E	Initiator(IQN/WWPN)



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. iSCSI Initiator Desktop app		
	(2) On the iSCSI Properties page, find the initiator name on the Configuration tab.		

		~
	iSCSI Initiator Properties	×
	Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration	1
	Configuration settings here are global and will affect any future connections made with the initiator.	
	Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.	
	When connecting to a target, advanced connection features allow specific control of a particular connection.	
	Initiator Name:	ר ר
	iqn. 1991-05.com.microsoft	
	To modify the initiator name, click Change. Change	
	VMware ESXi	
	 Open a web browser, type the VMware ESXi host IP in the address batthe VMware ESXi management portal. Go to Storage > Adapter, choose the iSCSI adapter, click Configuration find the initiator name next to iSCSI name and Alias. 	
	vmware esxi	
	Navigator	
	Host Data Storage Adapter Device Permanent Memory No Virtual machine 1	
	📱 Storage 🛛 🖉 Configure ISCS 🖾 Software ISCSI 🖉 Rescan	
	> □ naa.60014052a808671b Name ∨ Type > □ vmhba64 □ Image: Course of the state of the s	Controller
	More Viscus Software Adapter	
	Configure (SCS) - vmhba64	
	ISCSI Enabled Obsable Enable	•
	Name and Alles ign 1998-01.com.vmvare.63a1f1b3-6357-7e0F4ae6-48ea634b5d31-2120761d	4
•	Linux	
	(1) Use an SSH tool to log in to the management portal of the Linux hos	st.
	(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.

host01	VM	ware ESXi
Description	:	
Initiators: 1	个	
Edit	View Initiators	Delete

- 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 Resources

An iSCSI LUN is a logical unit of storage.

📋 Block Sharing				
🕚 Overview	LUN (3) Add			
📑 Target	LUN01	Normal	LUN02	Normal
E LUN resources	Locationpools		Locationpools	
Host	Total Capacity 2GB / Block Size 128KB		Total Capacity 10GB / Block Size 128KB	
	Edit Snapshot v	Delete	Edit Snapshot v	Delete

6.3.1 Add LUN

1. Click Add.

Add LUN		>
* LUN Name :	Please enter the name.	
* Home Storage Pool:		\sim
Provision Type :	Thin Provision Thick Provision ?	
Total Capacity :	GB V Max: 1PB	
Block Size:	128KB	~
Description :		

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.	

Cancel

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.

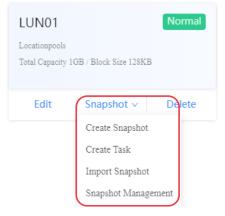
LUN01	Normal
Locationpools Total Capacity 1GB / Block Size 128KB	
Edit Snapshot v	Delete

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 <u>Snapshot</u> 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.

Block Sharing					×
🕑 Overview	Target(1) Add			Please enter	Q
📇 Target	v iqn.2022-08.qq.ca Connec	ted Initial LUN No: 1 IP: 208.208.	3.222 (+2)	Edit	Delete
EUN resources	LUN resources Host	Add mapping Delete mapping			
🚽 Host	LUN Name	Home Storage Pool	Total Capacity	Action	
	LUN02	pools	10GB		

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.

Add Target				×
1	Basic Information	2 Map LUN —	3 Link Host	
* Target Name :	Example:iqn.2022-08.com.t	est		
Initial LUN No:	1			V
IP:	Selected0/2			
	200.300.3.222 10.122.57.234			
		Next Cancel		

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

Ado	l Target				×
		Basic Information	2 Map LUN	J Link Host	
	LUN Name	Add			
		LUN Name	Home Storage Pool	Total Capacity	
		asdadasd	pools	2GB	
		LUN01	pools	1GB	



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

Add	Add Target						
Basic Information — Map LUN Ink Host							
	Host Name	Add					
		Host Name	Operating System	Number of Initiators	Permission		
		host01	VMware ESXi	1	Read Only 🗸 🗸		
		host02	VMware ESXi	0	Read/Write v		

Back Cancel	Back	Complete
-------------	------	----------



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.

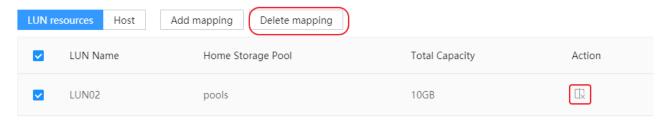


2. After you complete the modification, click OK.

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 \square 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.

LUN re	esources Host	Add Link Delete Link			
	Host Name	Operating System	Number of Initiators	Permission	Action
	host02	VMware ESXi	0	Read Only	X

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.



 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.

iSCSI Initi	iator Proper	ties				×				
Targets	Discovery	Favorite Targets	Volumes and Device	s RADIUS	Configuration					
To disc	Quick Connect To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.									
Target	: 183	12.000.12		Q	uick Connect					
Discove	ered targets				Refresh					
Name				Status		1				
i gn. 1	992-05. com	.microsoft:(). oa. en univ	connecte	d 2					

- 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.

	Computer	r Manage	ment				
File	Action	View	Help				
(2 🖈	?	F	🗙 🛃 📑 📴 🗵	3		
	System • • • Tas • • • • • • • • • • • • • • • • • • •	n Tools k Schedu ent Viewe	r	Volume (C:)	Layout Simple		Status Healthy (System, Boot, Page File, Active, Crash Dump, Primary F
	> 🌆 Loc > 🔊 Per 者 Dev	formance /ice Mana	and Groups e				
~ [Storage 🖶 📑	e k Manag	ement				
>	Service	s and Ap	plications				
				<			>
				Disk 0 Basic 465.76 GB Online		GB NTI y (Syste	
				Disk 1 Unknow 122.00GB Not initialized	122.00 Unalk		

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.

vmware' esxi"			
Navigator	Iccalhost.localdomain - Storage		
▶ 🖥 Host	Data Storage Adapter Device Permanent Memory		
▶ 🔂 Virtual machine 1			
🐨 🗐 Storage 📃 2	🔯 Configure iSCSI 💆 Software iSCSI 💻 Rescan 🧧 🕻 Refresh 🛛 🏠 Operation		
🕨 📃 naa.60014052a808e71b	Name	~	Туре
🖻 📠 vmhba64 👔 🚺	🐖 vmhba0		Cougar Point 6 port SATA AHCI Controller
More	whba64		iSCSI Software Adapter 🛛 🕗
Network 1			

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

Configure iSCSI - vmhba64					
CHAP Authentication	Without using CHAP	~			
Bidirectional CHAP authentication	Without using CHAP	~			
Advanced Settings	Click to expand				
	触 Add port binding 🛒 Delete port binding				
Network Port Binding	VMkernel NIC ~ Po	ort Group	~	IPv4 Address	~
		No Data			
•	🔯 Add static target 🖉 Delete static target 🥒 Edi	t	Q Search	Q Search	
Static Target	Target	~	Address	✓ Port	~
	iqn.2023-01.com.test:tar001		207.207.00.213	3260	
Ø	iqn.2023-01.com.test:tar9080		207	3260	
	iqn.2023-01.com.test:tar002		207.121.130.45	3260	
	iqn.2023-01.com.test:tar001		207.201.91.30	3260	
	🔯 Add dynamic target 🧾 Delete dynamic targey? Edit		Q Search	Q Search	
Dynamic Target	Address	~	Port		~
	207.007.00.213		3260		
	207.301-80.80		3260		
	207.121.130.45		3260		
				3 Save	Cancel

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

vmware" esxi"											
🖫 Navigator 🗆	localhost.localdomain - Storage										
▶ 🖥 Host	Data Storage Adapter Device Permanent Memory	Storage Adapter Device Permanent Memory									
▶ ⊕ Virtual machine 1 > ≡ Storage 2	😫 Add Data Storage 🔹 Add Capacity 📃 Rescan 🔰 🥐 Refresh 🛛 🧔 Operation										
Network 1	Name 🗸 🗸	Status 🗸	Type 🗸	Capacity							
	Local ATA Disk (t10.ATAST2000NM00552D1V4104	📀 ,Normal	HDD	1.82 TB							
	LIO-ORG iSCSI Disk (naa.6001405e97fb85d59b9446698dcc3160)	🔥 Normal, downgraded	SSD	10 GB							
	LIO-ORG iSCSI Disk (naa.600140504e377761dd14a068b7857794)	🔥 Normal, downgraded	SSD	1,024 GB							
	LIO-ORG iSCSI Disk (naa.6001405104e4b28750b4f669a776eecc)	🔥 Normal, downgraded	SSD	1 GB							
	LIO-ORG iSCSI Disk (naa.6001405d3630b8f5a89448c91c76b851)	🔥 Normal, downgraded	SSD	1 GB							

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 -- I // 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.

🔁 File Manager		-	o x
늘 File Manager	< > C DOC	Please enter	Q
AutoCar123123	New Folder Upload-Ignore Upload-Overwrite Share Download Copy Move Delete		
> 🗟 DOC	Name Size Type	Date Modified	
Picture	BOOK 🗠 🖞 🗄 🚥 - Folder	5/8/2023, 3:22:40 PM	
	- Folder	5/8/2023, 3:23:06 PM	
			<
Share Links			
👕 Recycle Bin			

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**.

New Folder			Х
Folder Name :	Please enter the folder name		
		ОК	Cancel

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.

Sharing Type :	Public			\sim				
Number of Acces	sses Allowed	Please enter						
Validity Period	Last 1 Day	Last 3 Day	Last 7 Day	Custom	Start Time	🛁 End Tin	ne	
				Create Lin	k			
ck Create Link	to gene	rate a lin						
	-	rate a lin						
Ck Create Link ile(Folder): Total 1 File	-	rate a lin						
	-	rate a lin						



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

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

7.1.4 Download File

NOTE!

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
Сору	Copy a file to a different folder for backup.	 On the file list, select the file/folder and then click Copy. Choose the destination folder, and then click OK.
Move	Move a file to a different folder.	 On the file list, select the file/folder and then click Move. Choose the destination folder, and then click OK.
Delete	Delete a file from the NAS device.	 On the file list, select the file/folder and then click Delete. 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 open 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.

🔁 File Manager											_	
늘 File Manager	Delete	Invalid Links	Cancel S							Please enter		Q
🜏 Share Links		Name	Å	Path	÷	Time of Sharing	≑ Status	÷	View Count	5 🙏	Action	n
i Recycle Bin		BOOK		/DOC		5/8/2023, 3:24:48 PM	Valid		No limit		j c	°×

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.	 Click I. 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.	 On the shared file list, select the file. Click Cancel Sharing. 		

Delete Links	Invalid	Delete millo of expired sharing.		On the shared file list, select the file. 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.

						- 🗆 ×
Empty Recycle Bin Res	tore Delete				Please enter	Q
- N			Date		Remaining	A
Name	Previous Path	⇒ Size	Deleted	Ŧ	Days	Action
		NO GALA				
	Total 0 <	1 > 10 / pa	ige 👻			
	Empty Recycle Bin Res	Name	Name	Name \$ Previous Path \$ Size \$ Date Deleted No data	Name \$ Previous Path \$ Size \$ Date Deleted \$	Name Previous Path Size Date Deleted Remaining Days Image: Name Image: Nam Image:

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

WARNING!

(i)

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 $\overline{\square}$ to delete a file.

8 System Maintenance

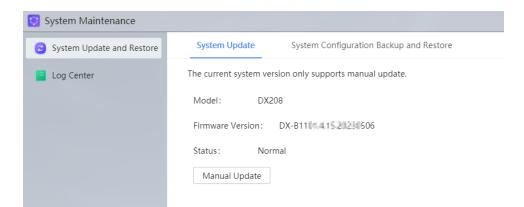
8.1 System Update and Restore

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

8.1.1 System Update

The system supports automatic version update.

Go to System Maintenance > System 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.

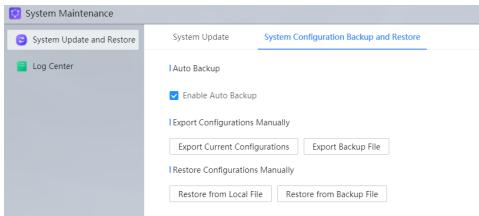
Manual Updat	e	×
Please select version.	a local update file. Make sure the selected version is higher than the current	
* File Path:	Please select the file path Browse	
	OK Cancel	

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

8.1.2 System Configuration 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 > System Update and Restore > System Configuration 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.

8.2 Log Center

View system alarm logs and operation logs.

8.2.1 Alarm Logs

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

😲 System Maintenance				— — ×
System Update and Restore	Alarm Log	Operation Logs		
E Log Center	Time: Last D	ay Last 3 Day Las	t 7 Day Custom	Start Time 🖌 🗧 📾
	Module: All	V Level:	All	Search Reset Export
	Level	Module	Time	Event
	Error	Sharing Management - AFP Management Module	2023-05-12 09:20:06	Failed to enable UPS service. Failed to enable UPS service, command: systemctl start apcupsd, result: 256
	Warning	O&M Module - Operation and Maintenance	2023-05-12 09:13:14	The system CPU usage exceeds the preset threshold 80%! Current usage is 90%
	Error	O&M Module - Operation and Maintenance	2023-05-12 09:02:37	The system CPU usage exceeds the preset threshold 90%! Current usage is 98%
			Total 3 <	1 > 10 / page 👻

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.

8.2.2 **Operation Logs**

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

System Maintenance				- 0
System Update and Restore	Alarm Logs	Operation Logs		
E Log Center	Time : Last Day	/ Last 3 Day Last 7 Da	ay Custom Start 7	Time ~ End Time
	Usemame : All	∨ Module :	All v	Search Reset Export
	Username	Module	Time	Operation Details
	admin	Sharing Management - Sharing Management Module	2023-05-08 15:40:06	Rename shared folder, old share name:AutoCarT, new share name:AutoCarTca, shared pool:pools, result:0
	admin	Sharing Management - Sharing Management Module	2023-05-08 15:40:06	Edit shared folder, pool name:pools, folder name:AutoCarT, Quota:Enable, result:1
	admin	Sharing Management - Sharing Management	2023-05-08 15:40:05	Edit shared folder description, share name:AutoCarTca, description:ZZZZZZZZZ, result:0
		Total 0 < 1	2 3 4 5	24 > 10 / page - Go to Page

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.

9 Acronym and Abbreviations

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.
LADP	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.
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.

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

Acronym	Full Name	Description
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

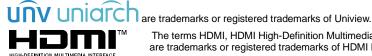
Copyright Statement

©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



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 das ≻
 - 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.