

# Pac Storage GUI User Interface Manual



# Table of Contents

Table of Contents .....	2
-------------------------	---

## Introduction

<b>Connecting PAC Storage User Interface Firmware to Storage Subsystems .....</b>	<b>7</b>
Elements of a Storage Subsystem Network.....	8
Computer Requirements.....	8

## Installation

Enabling Access Ports .....	8
Initiating PAC Storage User Interface Firmware Installation.....	9
Installing PAC Storage User Interface Firmware.....	9
Uninstalling/Upgrading PAC Storage User Interface Firmware .....	9

## Accessing the Firmware

<b>Firmware Interface .....</b>	<b>10</b>
List of Available Configurations .....	10
<b>Establishing LAN Connection.....</b>	<b>11</b>
Checking IP Address of Management Port via Terminal .....	11

## Initial Setup Wizard

Step 1 - Firmware Update .....	13
Step 2 – Event Notice .....	14
Step 3 - System Settings .....	14
Step 4 - Storage.....	15
Step 5 - Channel .....	16
Step 6 - Network Services .....	16
Step 7 - AD/LDAP .....	17
Step 8 - Summary .....	17

## Navigating User Interface

<b>Overview .....</b>	<b>19</b>
Logging into/Logging out of PAC Storage User Interface Firmware UI .....	19
Changing PAC Storage User Interface Firmware Login Password via PAC Storage User Interface Firmware .....	21
Changing PAC Storage User Interface Firmware Login Password via Default Button ..	22
Changing Display Language.....	23
Administrator Privilege .....	24
User Interface .....	27
Adding/Logging into/Removing a Device .....	31
Calibrating System Settings.....	34
<b>Monitoring .....</b>	<b>35</b>
Storage Resource Management (SRM).....	36
Monitoring Storage Performance .....	39
Monitoring Storage Capacity.....	43
Monitoring GPU Status .....	44
Monitoring client connections.....	45
<b>Workflow .....</b>	<b>46</b>

Creating SSD Cache, Pool, Volume and LUN Mapping .....	47
Creating Pool, Volume and LUN Mapping .....	51
Creating Folder and Share.....	55
Creating Volume and LUN Mapping.....	58
Scheduling a Volume Replication.....	59
Scheduling a Folder Rsync .....	62
<b>Event Log .....</b>	<b>72</b>
Types of Events .....	72
System Log.....	<b>73</b>
Action Log.....	75
Data Access Log .....	78

## Service Manager

<b>Configure Service Manager.....</b>	<b>80</b>
<b>Service Manager Status .....</b>	<b>83</b>
<b>Service Request.....</b>	<b>85</b>
<b>Ticket History &amp; Tracking.....</b>	<b>87</b>

## Certification

<b>Configure Web Certification.....</b>	<b>89</b>
---	-----------

## System

<b>General .....</b>	<b>93</b>
<b>Time Settings .....</b>	<b>97</b>
<b>Notification .....</b>	<b>98</b>
SNMP Settings.....	<b>99</b>
<b>Service Manager Settings .....</b>	<b>100</b>
<b>License Management.....</b>	<b>103</b>
Generating a License Application File.....	104
Generating an Advanced License .....	104
Upgrading Standard License to Advanced License.....	106
Renewing License.....	107
Downloading Trial License .....	<b>108</b>
<b>System Information .....</b>	<b>109</b>
<b>SED Key Management.....</b>	<b>111</b>
<b>Maintenance .....</b>	<b>113</b>
Exporting/Import System Configuration .....	113
Diagnostic information .....	115
<b>Power .....</b>	<b>116</b>
UPS .....	116
Power Schedule.....	118
Wake on LAN.....	121
<b>Enclosure View .....</b>	<b>122</b>

## Access

<b>Channel and Network .....</b>	<b>124</b>
----------------------------------	------------

Host Channel Parameters.....	126
Configuring IP Address (IPv4) of Management Port.....	131
Configuring IP Address (IPv6) of Management Port.....	133
Enabling Jumbo Frames.....	134
Trunking Host Interfaces to Increase Bandwidth.....	135
Changing Channel Type for Converged Host Board.....	138
Routing.....	140
<b>Initiators.....</b>	<b>142</b>
Configuring Alias for iSCSI Initiators.....	143
Configuring iSNS Server in Storage Subsystems.....	147
Configuring iSNS Server in Windows OS.....	149
<b>Network Services.....</b>	<b>150</b>
Configuring CIFS/SMB Service.....	151
Configuring FTP/SFTP Service.....	152
Configuring NFS Service.....	154
Configuring WebDAV Service.....	155
Configuring AFP Service.....	156
Configuring Rsync Target Service.....	157
Configuring DNS Service.....	158
Configuring NIS Service.....	159
Configuring Object Service.....	160
<b>Virtual Local Area Network (VLAN).....</b>	<b>161</b>
Create VLAN.....	161

## Privilege

<b>Users.....</b>	<b>164</b>
Adding a User Account.....	165
Importing User Accounts in Batch.....	166
Setting Password Policies.....	168
Deleting a User Account.....	170
Editing a User Account.....	171
Quota Management.....	172
Object Access Keys.....	173
Access Object Storage.....	175
<b>User Group.....</b>	<b>177</b>
Adding a User Group.....	177
Deleting a User Group.....	178
Combining User Accounts into a Group (Editing a User Group).....	178
<b>Shared Folders.....</b>	<b>180</b>
Creating/Editing a Folder.....	181
Deleting a Folder.....	189
Accessing a Folder.....	190
Encrypting a Folder.....	191
Quota Management for a Folder.....	194
Recycle Bin Schedule.....	195
<b>AD/LDAP Settings.....</b>	<b>197</b>
Windows Active Directory Settings.....	197
Lightweight Directory Access Protocol Settings.....	199

## Storage

<b>Volume.....</b>	<b>201</b>
Advanced Search.....	203
Volume advanced options.....	204
Adding a Volume.....	206
Creating a WORM Volume.....	210
About Thin Provisioning and Host Reclaim.....	214
Setting a Volume Threshold.....	217

Deleting a Volume .....	219
Expanding a Volume .....	220
Deduplicating Volume Data (Beta) .....	221
Defragmenting a Volume .....	223
Reflecting the Expanded Volume Status in Windows Server (Windows Server 2012 R2 for example) .....	224
Mapping a Volume to a LUN .....	226
Extended LUN Mapping (Fibre Channel) .....	228
Extended LUN Mapping (iSCSI Channel) .....	233
Deleting a LUN Mapping .....	236
About In-Band, Out-of-Band Flush .....	237
Configuring Out-of-Band Flush .....	238
<b>Pool .....</b>	<b>240</b>
Adding a Pool .....	241
Deleting a Pool .....	248
Configuring a Pool .....	249
Expanding a Pool .....	251
Pool Capacity Threshold .....	252
Storage Tiering .....	254
Pool Advanced Options .....	255
<b>Logical Drive .....</b>	<b>259</b>
Configuring Logical Drive Parameters .....	262
Migrating a Logical Drive to another RAID Level .....	263
Configuring Power Saving Mode .....	266
Expanding a Logical Drive .....	267
Adding Drives to a Logical Drive .....	267
Expanding the Size of a Logical Drive .....	268
Scanning a Logical Drive Manually .....	270
Rebuild a Logical Drive .....	271
Regenerating Parity .....	271
Restarting a Logical Drive .....	272
Optimizing Logical Drive Access .....	272
Optimizing Stripe Size .....	273
Calculating Logical Drive Performance .....	274
Protecting a Logical Drive with Self-encrypting Drives (SED) .....	276
<b>Drive .....</b>	<b>278</b>
Advanced Search .....	283
Drive advanced options .....	284
Spare Drive Types .....	286
Adding/Deleting a Spare Drive .....	288
Scanning a Spare Drive .....	289
Running Read/Write Test .....	289
Removing a Drive Reserved Space .....	291
Identifying a Drive .....	292
Preventing/Recovering a Failing Drive .....	293
Cloning a Drive .....	293
Copying & Replacing a Drive .....	294
Erasing SED drive .....	296
<b>SSD Cache .....</b>	<b>297</b>
Enabling/Disabling SSD Cache Function .....	299
<b>Storage Maintenance .....</b>	<b>301</b>

## Scheduling & Backup

<b>Task Scheduler .....</b>	<b>303</b>
Creating Schedules: General Rules .....	304
Creating a Folder Rsync Schedule .....	305
Creating a Disk Scan Schedule .....	308
Creating a Snapshot-taking Schedule .....	311
Creating a Volume Replication Schedule .....	313
Creating a Tiered Data Migration Schedule .....	315

Creating a Volume Defragmentation Schedule .....	317
Set Email Notification .....	319
<b>Replication.....</b>	<b>320</b>
Creating a Volume Replication Pair .....	320
Replication Pair Actions .....	326
Creating a Folder Replication Pair .....	329
Creating a Replication Schedule .....	332
<b>Snapshot .....</b>	<b>337</b>
Number of Snapshots .....	337
Creating/Editing/Deleting a Snapshot .....	339
Recovering Source Volume from a Snapshot (Rollback) .....	344
Mapping/Unmapping a Snapshot Image to a Host.....	346
Mounting/Unmounting a Snapshot Image .....	348
Backing up Snapshot Images .....	348
Creating a Volume Copy from a Snapshot Image .....	351
Backup to cloud .....	353
Snapshot Schedule.....	353

## Application

<b>Anti-Virus.....</b>	<b>358</b>
<b>File Explorer .....</b>	<b>365</b>
<b>LDAP Server .....</b>	<b>382</b>
<b>Proxy Server.....</b>	<b>387</b>
<b>Syslog Server .....</b>	<b>391</b>
<b>VPN Server .....</b>	<b>393</b>
<b>Docker.....</b>	<b>395</b>

## Update & Security

<b>Security.....</b>	<b>408</b>
<b>Firmware Update.....</b>	<b>412</b>
<b>Factory Reset .....</b>	<b>414</b>

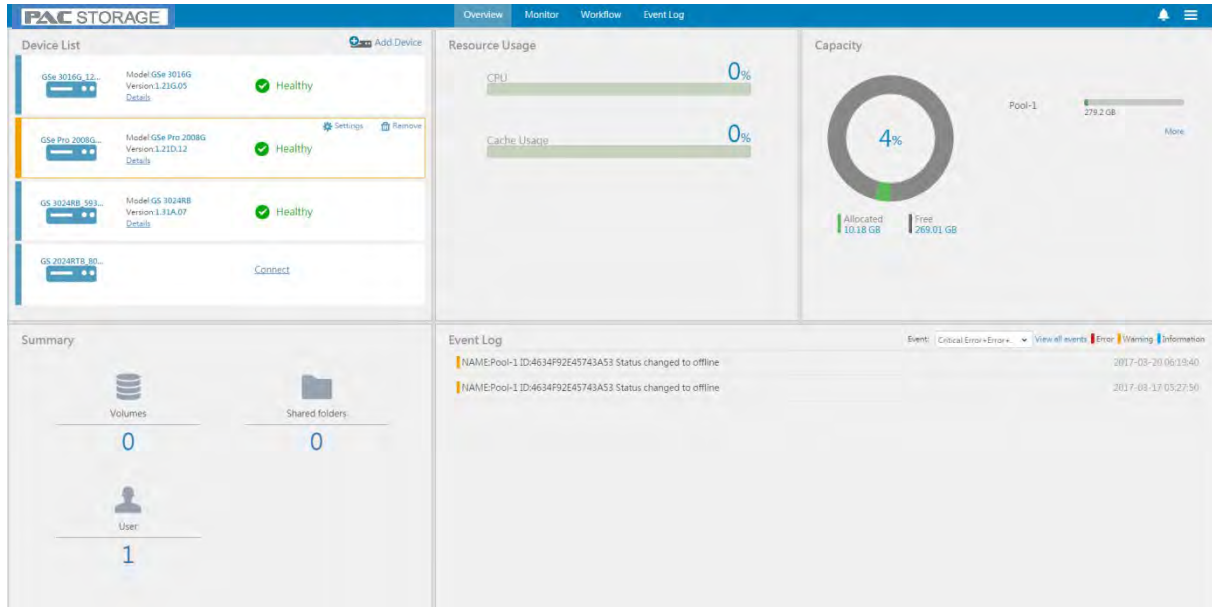
## Cloud Gateway

<b>Quick Setup.....</b>	<b>416</b>
Cloud File Cache .....	417
Cloud File Sync.....	419
Cloud Volume Replication.....	420
Cloud Archiving Storage .....	421
Cloud Tiering.....	422
<b>Cloud-connected Folder.....</b>	<b>423</b>
<b>Cloud-connected Volume .....</b>	<b>428</b>
<b>Cloud Storage .....</b>	<b>431</b>
Access Control Management .....	433
Connection History.....	435
Status Management.....	435
<b>Database.....</b>	<b>436</b>
Database .....	436
SyncCloud and Cloud Gateway .....	436





# Introduction



PAC Storage User Interface Firmware is the proprietary software suite for managing single or multiple PAC Storage PS storage systems. PAC Storage User Interface Firmware is accessible through a web browser if both the computer running PAC Storage User Interface Firmware and the subsystems are online. It is no longer required to install complex desktop applications on the local computer. Everything is always available over the network.

Each PAC Storage PS/PSV storage system has an embedded copy of PAC Storage User Interface Firmware pre-installed in the firmware for management of the individual device. The PAC Storage User Interface Firmware software suite (Central PAC Storage User Interface Firmware) being referred to in this manual can be installed on different servers to manage multiple PAC Storage PS/PSV storage systems. The graphic user interfaces are similar with only slight differences.



## Connecting PAC Storage User Interface Firmware to Storage Subsystems

PAC Storage User Interface Firmware, the storage subsystems and the host computers can be connected either in-band (connection through host links) or out-of-band (connection through LAN management port). PAC Storage User Interface Firmware is web-based and therefore is accessible from anywhere on the network. The flexible connection schemes allow the user to manage PAC Storage User Interface Firmware based on needs and system configurations, notably with considerations on the following two factors:

- Local management vs. remote management
- Full configuration vs. monitoring & notification

### Elements of a Storage Subsystem Network

<b>Storage Subsystems</b>	A storage subsystem refers to a hard drive array (storage subsystems + expansion enclosures).
<b>Host Computer</b>	The host computer refers to the computer to which the storage subsystem's host links are connected.
<b>Remote Computer</b>	The remote computer refers to a computer on the network to which the host computer is connected via LAN.
<b>In-Band Connection</b>	In-band connection refers to the scenario where the host computer and the storage subsystems are connected through host links: Fibre, SAS, or iSCSI host connectors on the storage subsystem controller module.
<b>Out-of-Band Connection</b>	Out-of-band connection refers to the scenario where the host computer and the storage subsystems are connected through Ethernet: Management LAN connector on the storage subsystem controller module.

# Accessing the Firmware

In this manual, the term “firmware” refers to the tool that enables access to functionalities of the PAC Storage PS/PSV without having to install software in a computer.

## Firmware Interface

Tool	Description	Interface
<b>PAC Storage User Interface Firmware</b>	You will access the firmware online with a GUI interface similar to that of the Central PAC Storage User Interface Firmware.	LAN

## List of Available Configurations

In addition to the firmware tool, you can configure your subsystem through the GUI-based PAC Storage User Interface Firmware.

Tool	System Configuration	Drive Configuration	Event Notification	Data Replication*	Centralized Management
PAC Storage User Interface Firmware	Yes	Yes	Yes	Yes	No
Central PAC Storage User Interface Firmware	Yes	Yes	Yes	Yes	Yes

\*Data replication refers to snapshot, volume copy/mirror, and local/remote replication.

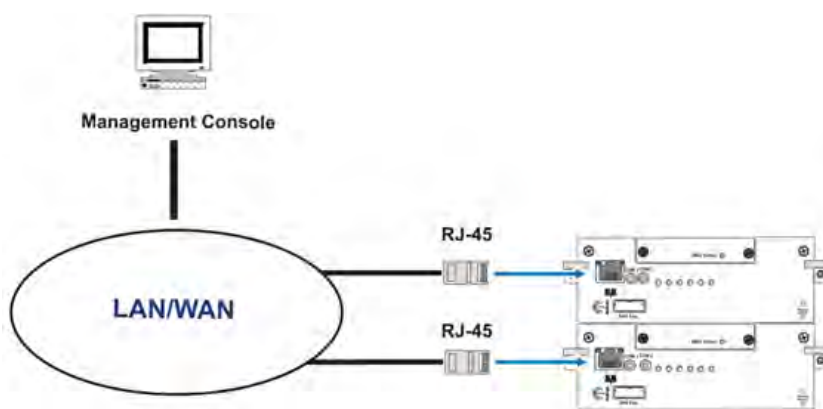
\*Remote replication and disk roaming cannot be executed between PAC Storage DS and PAC Storage PS.

## Establishing LAN Connection

### Cabling

Before using the PAC Storage User Interface Firmware (or using the terminal interface via LAN), make sure the subsystem is connected to the Internet through a LAN cable.

Note that the default IP of the PAC Storage PS/PSV system is **10.10.1.1**, please connect your storage system via direct attached storage (DAS) topology and set your host server under the same subnet (10.10.1.x) to ensure your PAC Storage PS/PSV can be found by the host server.



### Dual-Controllers

For dual-controller subsystems, connect Ethernet cables to both controllers. The Ethernet port on the secondary controller stays idle and becomes active in the event of a primary controller failure. The Ethernet port IP on the primary controller's Ethernet port will be inherited by the secondary controller during the controller failover process.

## Checking IP Address of Management Port via Terminal

The firmware can be configured with a text user interface and can be accessed through a terminal emulator application such as PuTTY.

**Baud Rate** 38400

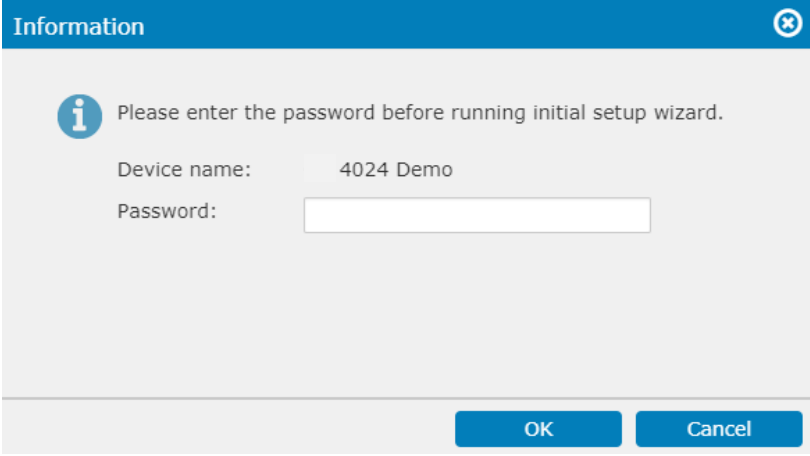
**Checking IP address of management port via Terminal**

Main Menu > view and edit Configuration parameters > Communication Parameters > Internet Protocol (TCP/IP) > lan0 [ ]

# Initial Setup Wizard

After the PAC Storage User Interface Firmware installation, during the first-time login, PAC Storage User Interface Firmware will automatically start the Initial Setup Wizard. It guides you through the process of configuring an PAC Storage PS/PSV storage system. You should be able to work with the storage spaces after the setup is completed. New users and those who are unfamiliar with PAC Storage User Interface Firmware software and PAC Storage storage systems are strongly recommended to make use of the setup wizard.

When you select **Initial Setup Wizard** from the Settings menu, a message pops up and asks you to enter the password before running the wizard.



The image shows a software dialog box titled "Information" with a blue header bar. Inside the dialog, there is an information icon (a lowercase 'i' in a blue circle) followed by the text "Please enter the password before running initial setup wizard." Below this text, there are two labels: "Device name:" and "Password:". The "Device name:" label is followed by the text "4024 Demo". The "Password:" label is followed by an empty rectangular text input field. At the bottom right of the dialog, there are two buttons: "OK" and "Cancel", both with blue backgrounds and white text.

If you do not wish to run the Initial Setup Wizard at this moment, click **Exit initial setup wizard**. Otherwise, click **Next** to begin.

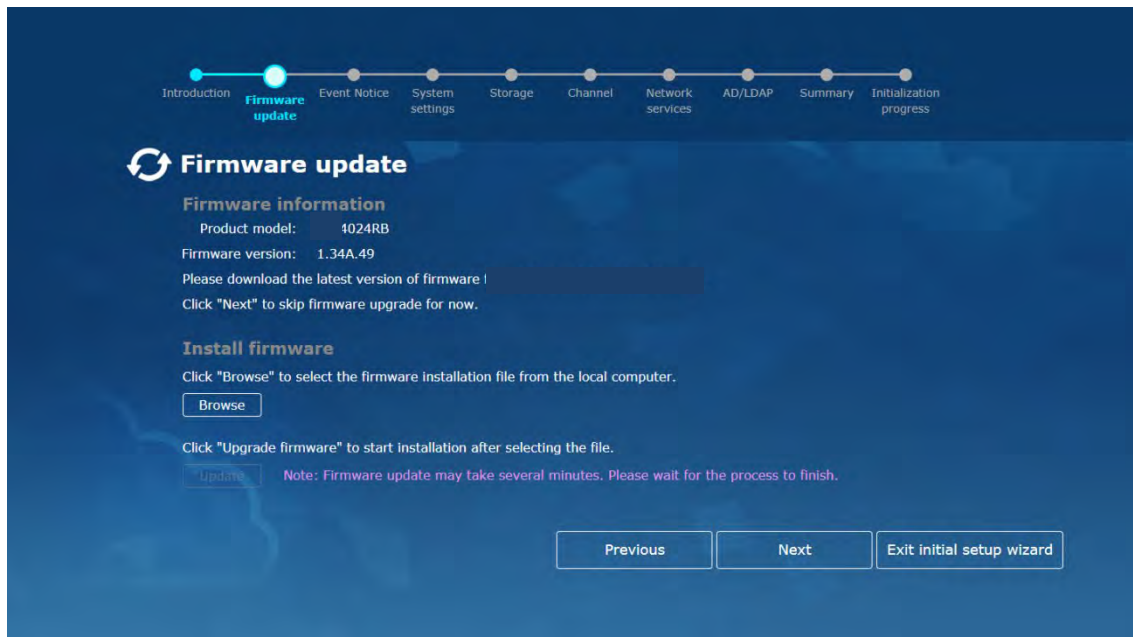


## Step 1 - Firmware Update

To check or obtain the latest version of firmware, please go to [PAC Storage Documents Center](#).

To skip firmware update for now, click **Next**. You can also go to Settings > Update & Security > Firmware Update to upgrade firmware at a later time.

To go on with firmware update, select the firmware installation file by clicking the **Browse** button. Then, click **Update firmware**. The process may take several minutes. Please wait for it to finish and click **Next** to proceed.



## Step 2 – Event Notice

After completing firmware upgrade, you will be directed to set “Notification Settings” and “Service Manager Settings”

- Click the Notification Settings button, you will be prompted to Notification setting webpage (see Notification Settings and SNMP Settings for details)
- Click the Service Manager Settings button, you will be prompted to Service Manager webpage (see Service Manager for details)

Note: Please make sure that you have completed the SMTP Settings and the email notification has been activated properly before you enable the Service Manager.

## Step 3 - System Settings

Set the system name, password for administrator, time and time zone for the device and configure DNS server(s). Click **Next** to save the Settings and proceed to the next step.

Introduction Firmware update Event Notice **System settings** Storage Channel Network services AD/LDAP Summary Initialization progress

## System settings

**Device name & Password**

Device name: i024 Demo

Device login password(admin):

Confirm password:

File server name:

ControllerA: NAS\_9812040

ControllerB: NAS\_9812040

**Time & Timezone**

Time: 2018-06-11 03:41:45  
Change

Timezone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Previous Next Exit initial setup wizard

## Step 4 - Storage

This step helps you configure the drives for storage spaces. The system will combine all selected drives into a single storage unit called a Logical Drive. One or more Logical Drives can be combined into a Pool. Volumes then can be created on top of Pools. Users are able to access a volume either by LUN mapping it to a server (block-level) or using it to create share folders and mount the folders onto file service protocols (file-level).

Introduction Firmware update Event Notice System settings **Storage** Channel Network services AD/LDAP Summary Initialization progress

## Storage

☐ Create storage spaces later

**Create a pool**

The following settings are recommended by the system to help you create a pool.

Pool mode: Asymmetric active/active mode ⓘ

Note: For a pool created in asymmetric active/active mode, a volume created on top of the pool can only be accessed by its assigned controller. If the assigned controller fails, the volume will be reassigned to the redundant controller to ensure uninterrupted system operation.

**Controller A**

Pool name: Pool-3

Pool capacity: 0 Byte(Selected drive(s):0, ,30% Capacity reserved)  
Change

**Controller B**

Previous Next Exit initial setup wizard



## Step 5 - Channel

PAC Storage User Interface Firmware currently manages PAC Storage PS/PSV systems via management ports. You should configure the data ports in the storage system in order to access the volumes. Since PAC Storage PS/PSV are unified storage systems built with both block and file engines, you can easily configure drives as either block-level or file-level volumes. Block-level volumes can be mounted through interfaces such as iSCSI, Fiber Channel (FC) or SAS. File-level volumes can be shared as folders via internet file-systems such as CIFS, NFS, FTP, etc.

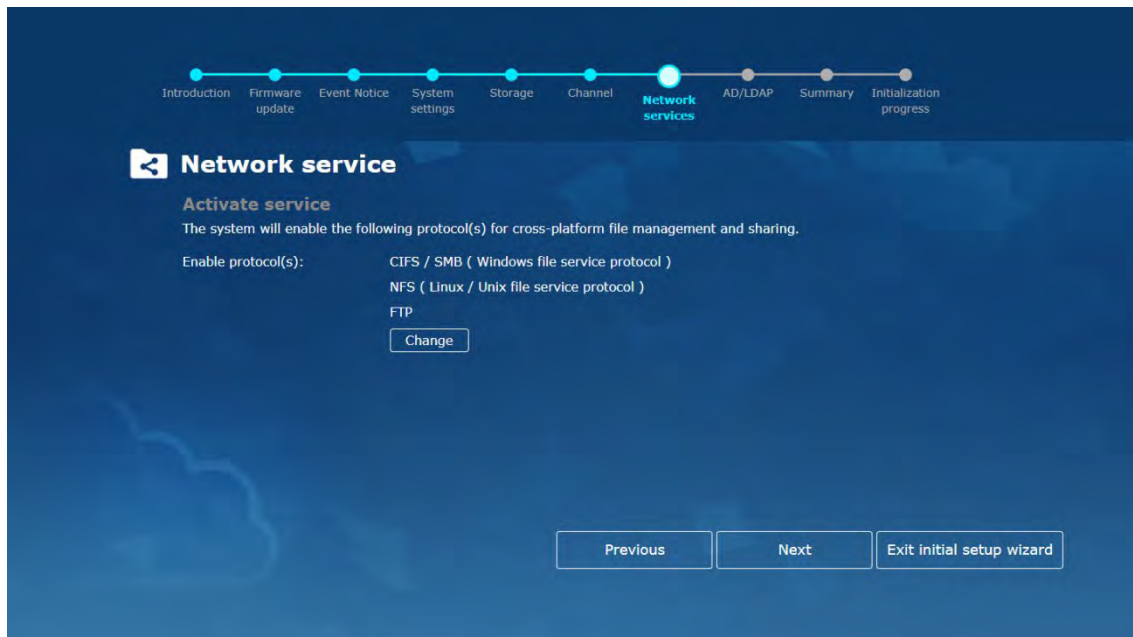
By default, the system automatically sets all on-board data ports for file-level access. Here, you can change the channel type to block-level service manually.

Please note that application services available on PAC Storage User Interface Firmware, such as file explorer, proxy server, syslog server and VPN server (Settings > Application), are accessible only through the data ports, not the management ports.



## Step 6 - Network Services

The system will list the enabled protocols. Click **Change** if you wish to configure the Settings.



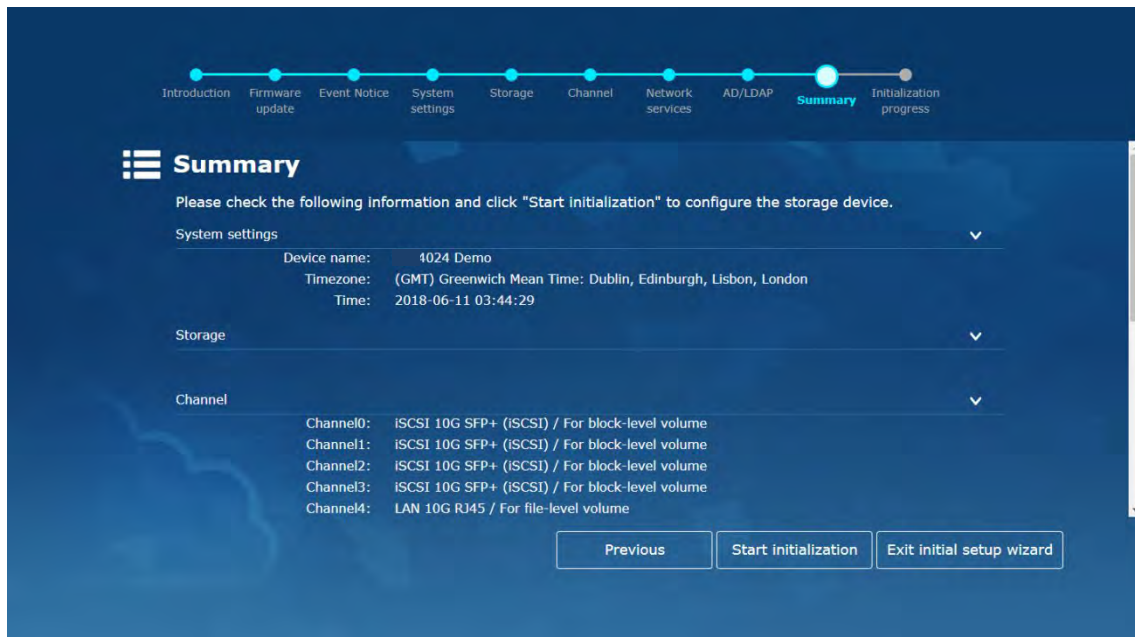
## Step 7 - AD/LDAP

Select whether you need to join the device to an AD (Active Directory) server or a LDAP (Lightweight Directory Access Protocol) server. For further explanation, please refer to AD/LDAP Settings.

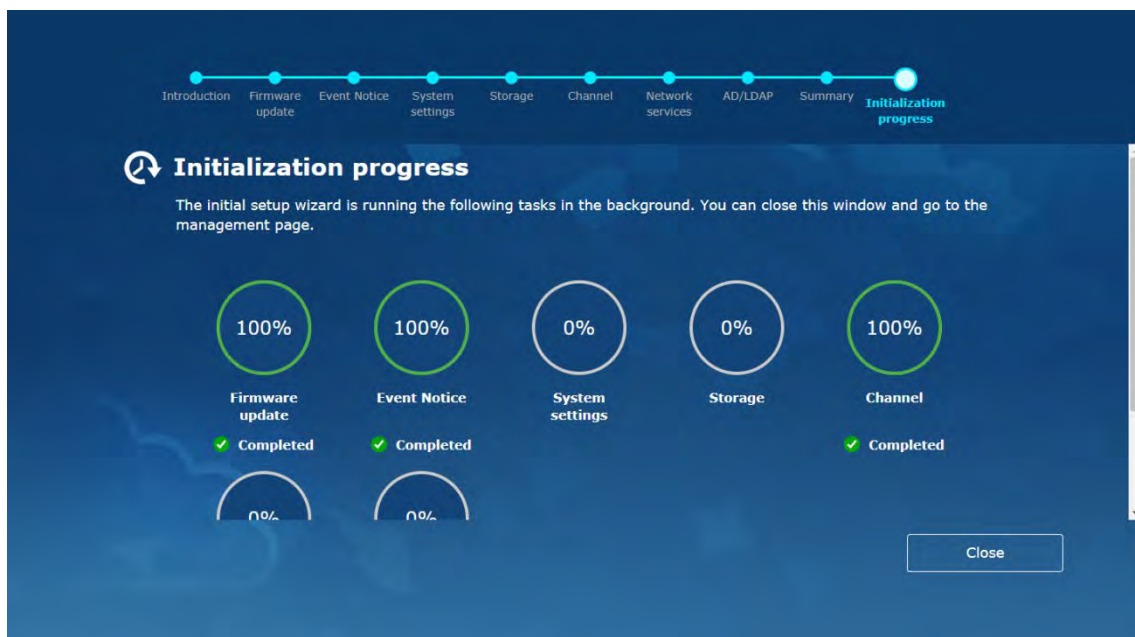
If you don't want to configure the AD domain at this moment, select **Don't join any domain** and click **Next** to proceed.

## Step 8 - Summary

All the Settings will be displayed for you to check if there is any mistake. After you click **Start initialization**, the system will start to execute the initialization process in the background.



The progress of each task is displayed. You can close the window and continue to configure another PAC Storage PS/PSV device or go to the PAC Storage User Interface Firmware management page.



# Navigating User Interface

## Overview

In this section, you can learn about the basic GUI elements of the PAC Storage User Interface Firmware management suite.

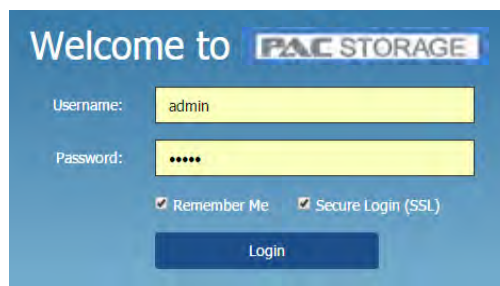
## Logging into/Logging out of PAC Storage User Interface Firmware UI

To open the PAC Storage User Interface Firmware software in the browser, double click the PAC Storage User Interface Firmware software icon.

---

### Login

The login screen will appear. Type in the username and password ( the default username and password are both “**admin**” ) and click Login. (You may check Remember Password if you prefer automatically logging into the interface in the future.)

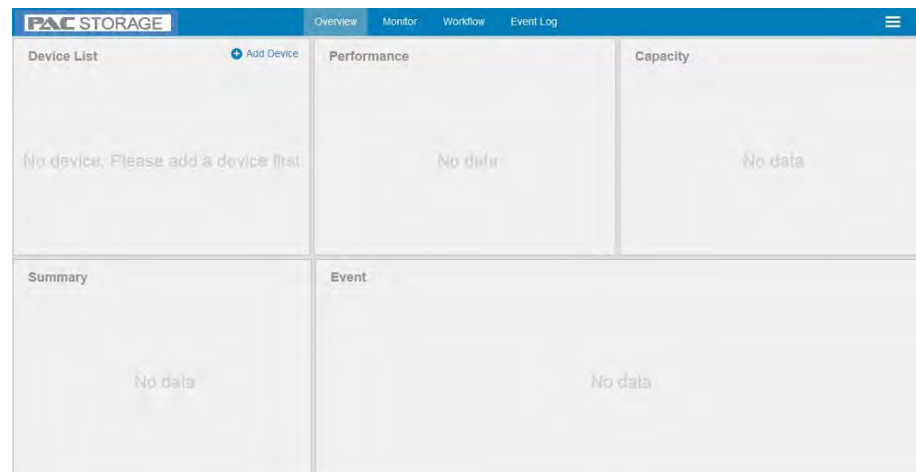


At the first-time login to the system, the Initial Setup Wizard will guide you through the system configuration.

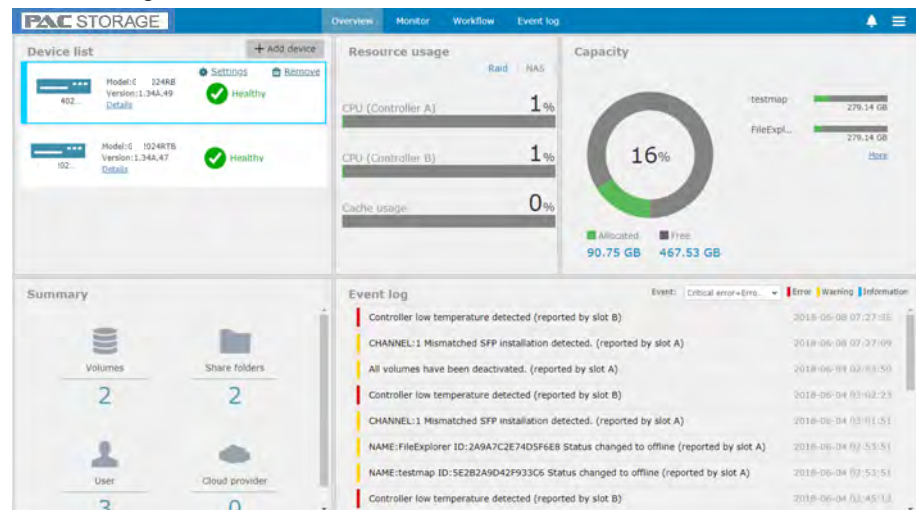


If you abort the Initial Setup Wizard without adding any devices, you will see a

blank user interface.

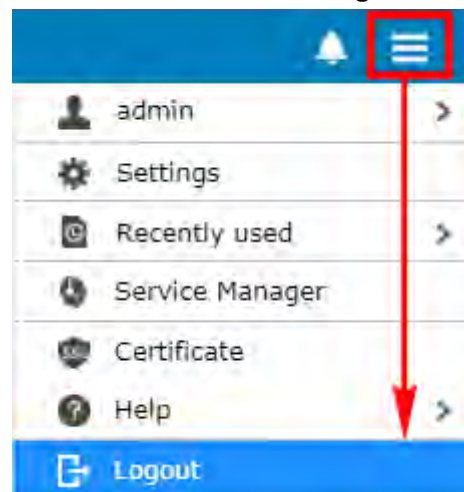


After adding a device, the user interface will show its renewed status.



## Logout

Click on the **Menu Icon > Logout**. You will be redirected to the login page.

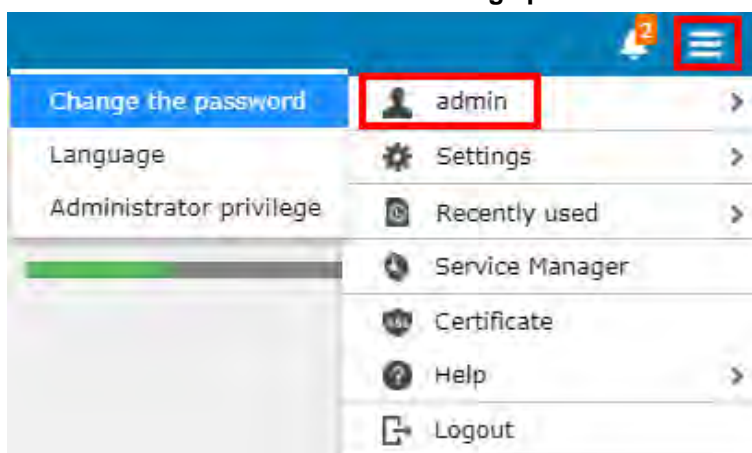


## Changing PAC Storage User Interface Firmware Login Password via PAC Storage User Interface Firmware

You can change the PAC Storage User Interface Firmware login password or set a new password for storage subsystems.

### Go to

Click on the **Menu Icon > Admin> Change password**



### Changing PAC Storage User Interface Firmware Login Password

Enter the old password and new password (twice for confirmation) in the pop-up window. The default login password is **"admin"**.

For an embedded system, the login password and the system's storage device password (in **Settings > System > General > Storage device password**) share the same value.

**Personal settings**

[Change the password](#) | [Language](#) | [Administrator privilege](#)

You can change the password for logging in the central management system.

\* Old password

\* New password

\* Confirm the new password



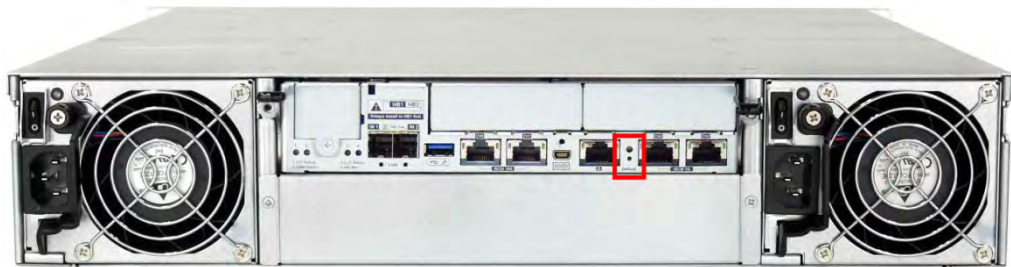
## Changing PAC Storage User Interface Firmware Login Password via Default Button

You can change the PAC Storage User Interface Firmware login password for storage subsystems.

---

**Go to**

Press and hold the default button on the *primary* controller of the storage system until the default LED is off (around 5 seconds) and the system will beep to inform you that the password has been reset.



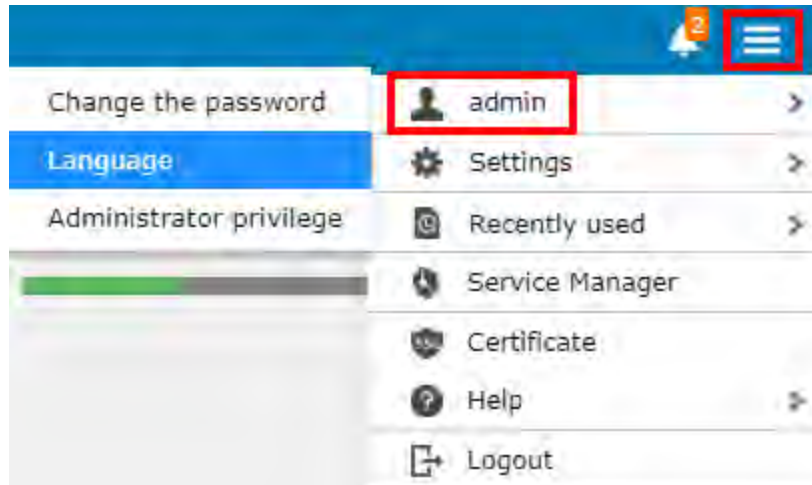
**Changing  
PAC Storage  
User  
Interface  
Firmware  
Login  
Password**

The PAC Storage User Interface Firmware and the terminal login password will be reset. Their default login passwords are both **"admin"**.

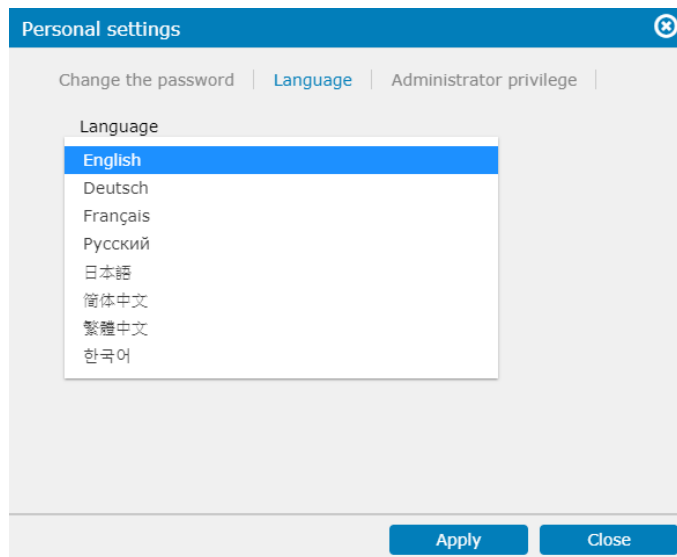


## Changing Display Language

Go to **Menu Icon > Admin > Language**



Choose the display language you prefer.



## Administrator Privilege

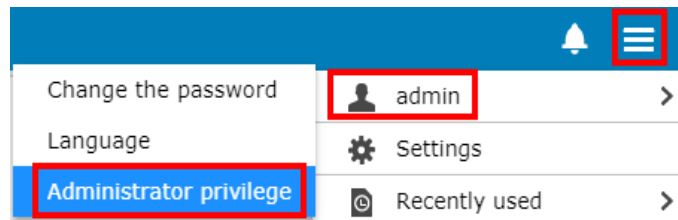
Three types of administrator accounts with different privileges are available, including super administrator, power administrator, and general administrator. Refer to the following table for their limit numbers and authorized actions.

Admin type	Max. Number	Manage admin acct	Configure device	Monitor device
Super administrator	1	Yes	Yes	Yes
Power administrator	5	No	Yes	Yes
General administrator	5	No	No	Yes

Note: Administrator privilege management is only available on **Central PAC Storage User Interface Firmware**.

Go to

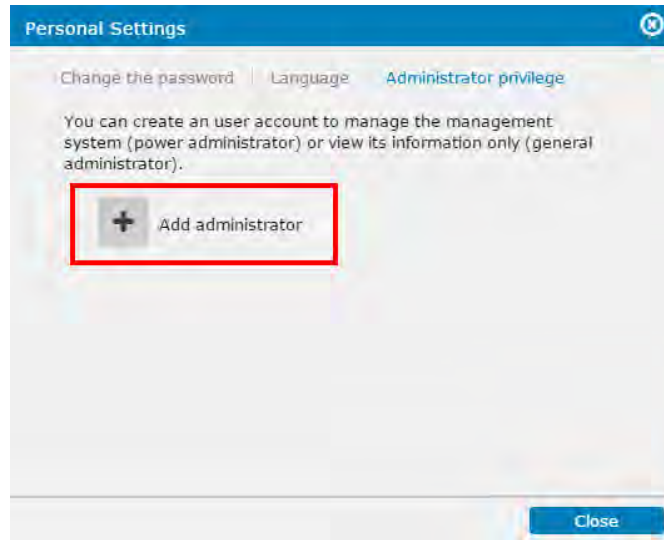
Menu Icon > Admin > Administrator privilege



Only the super administrator will see the administrator privilege menu item.

**Add an administrator**

After clicking **Administrator privilege**, you will see the following window. Click **Add administrator** to add an administrator account on PAC Storage User Interface Firmware.



Then, you will see the following window.

 The screenshot shows a window titled 'Add administrator' with a blue header bar. The main content area contains three input fields: 'Name' (a text box), 'Administrator type' (a dropdown menu with 'Power Administrator' selected), and 'Verify password' (a text box). Below these fields, there are two buttons: 'Add' and 'Cancel'.

**Name:** Enter the administrator name. The administrator name shall not exceed 32 characters in length and can include all alphanumeric characters and the symbols “\_”(underscore), “-”(hyphen), “.”(period) and “@”(at sign).

**Administrator type:** Select an administrator type (power or general) from the drop-down menu.

**Password:** Enter a password for the account. The password must be between 8 to 16 characters in length and can include all alphanumeric characters and all the symbols on the keyboard. However, we do not recommend using the space character.

**Verify password:** Re-enter the password to verify it.

Click **Add** to save and apply the Settings.

Note:

1. A power administrator cannot add/edit/delete any administrator account but can perform all other operations, i.e. configuring and monitoring all functions on the PAC Storage User Interface Firmware.
2. A general administrator only has permission to view the Settings on the PAC Storage User Interface Firmware but cannot change any Settings. He/she also has no permission to view action logs.
3. All administrators can change his/her own password at **Menu Icon > Admin > Change the password**. The super administrator can change the passwords of other administrators through the edit administrator function.

---

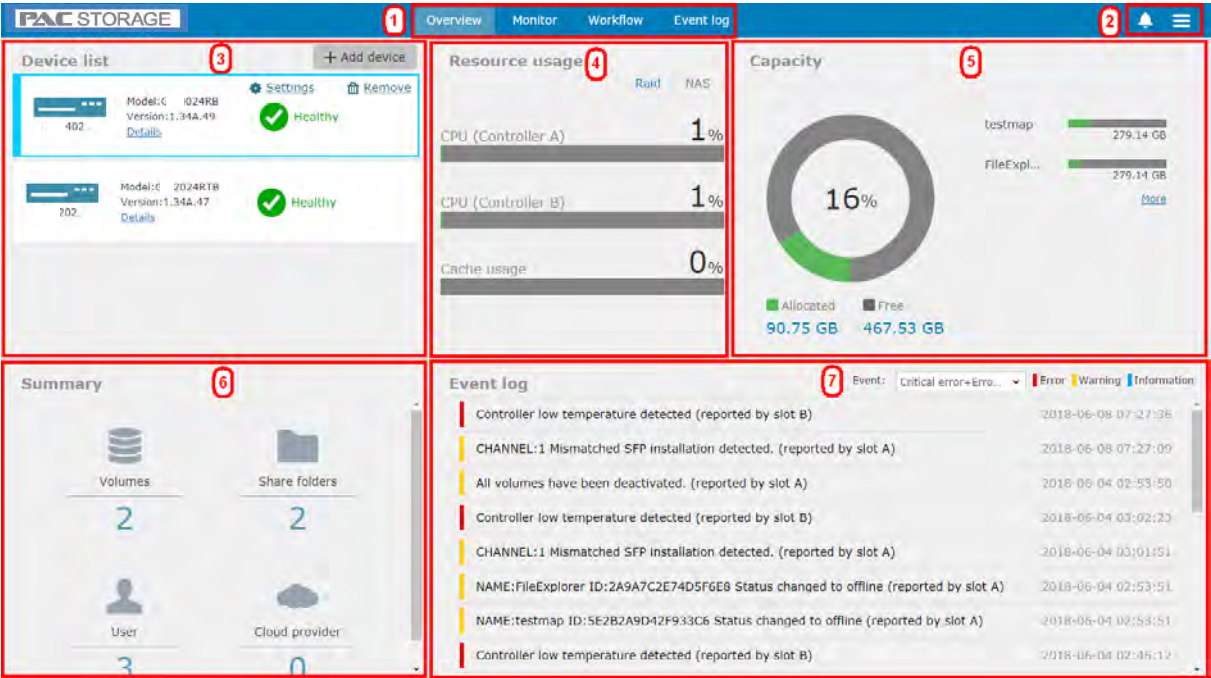
**Edit/delete an administrator**

After clicking **Administrator privilege**, you will see a list of current administrators.








Click on an administrator and then click the **Edit** button to change the account Settings or click the **Delete** button to remove the administrator.



## User Interface



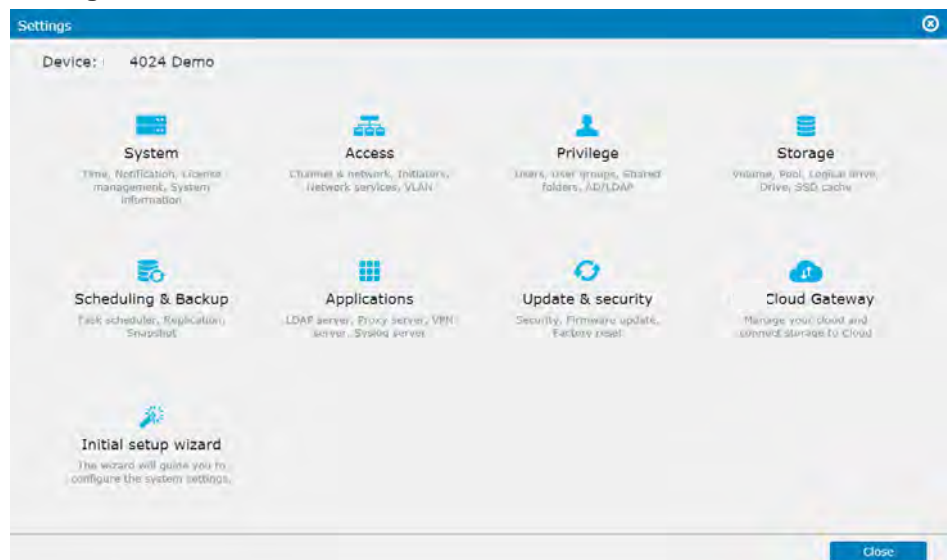
Display Elements	Description
<b>1: Top Menu Bar (Navigation Buttons)</b>	You can switch between the pages (Overview, Monitor, Workflow and Event Log) by using the navigation buttons on the top menu bar.
<b>2: Top Menu Bar (System Setting Buttons)</b>	Click on the Menu button. <div data-bbox="483 1657 616 1769" data-label="Image"> </div> The system setting buttons will appear.

	admin	>
	Settings	>
	Recently used	>
	Service Manager	
	Certificate	
	Help	>
	Logout	

### Admin

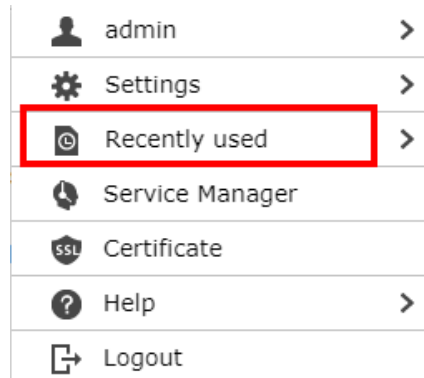
Select the administrator setting button to change the display language and the PAC Storage User Interface Firmware login password.

### Settings



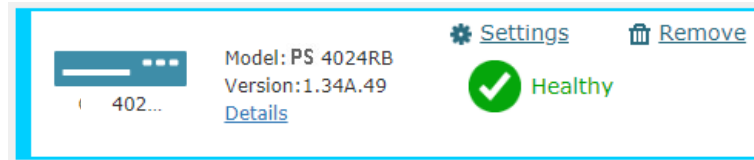
The device setting button contains links that enable users to set detailed configurations for PAC Storage PS/PSV devices, including System Settings, Data Access Configurations, Account Privilege Settings, Storage Provisioning, Scheduling & Backup, Applications, Update & Security, Cloud Gateway, Initial Setup Wizard.

### Recently Used



The **Recently used** option below the **Settings** button shows the most recently modified configurations of every PAC Storage PS/PSV devices. The button allows users to skip to the configuration page for other devices via a single click. For example, if we have modified the general Settings of PAC Storage PSV 3016, the **General** option allows the user to open the general Settings page for other PAC Storage PS/PSV devices connected with the PAC Storage User Interface Firmware software.

Note: Users can also enter the Settings page by clicking the **Settings** button in **Overview > Device List**



### Notification

The notification setting button allows users to set their notification rule and information.

### Service Manager

The Service Manager button allows users to configure Settings related to the Service Manager functions.

### Certificate

The Certificate button allows users to configure Settings related to the Certification functions.

### Help

Users can access Online Help, Online Support and About (information about PAC Storage User Interface Firmware software) via the Help button.

### Logout

Log out of the PAC Storage User Interface Firmware software and go back to the login page.



### 3: Device List

Device List shows the PAC Storage PS/PSVs that currently have connection with the PAC Storage User Interface Firmware. You can add a new PAC Storage PS/PSV by clicking **Add Device**, or you can configure the device setting for already added PAC Storage PS/PSV.

The **Add Device** button is only available on Central PAC Storage User Interface Firmware.

---

### 4: Performance Quick Monitor

Performance Quick Monitor shows the usage of CPU, memory and SSD cache for a connected PAC Storage PS/PSV.

---

### 5: Capacity Usage Quick Monitor

Capacity Usage Quick Monitor shows a brief summary of capacity usage rate of a connected PAC Storage PS/PSV.

---

### 6: Storage Summary

Storage Summary shows a brief summary of configured volumes, shared folders, and cloud spaces.

---

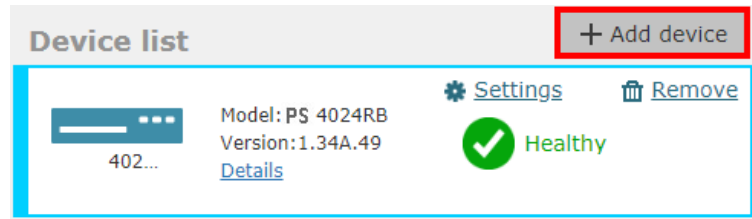
### 7: Events Quick View

Events Quick View shows the current warnings, errors, and information of a connected device.

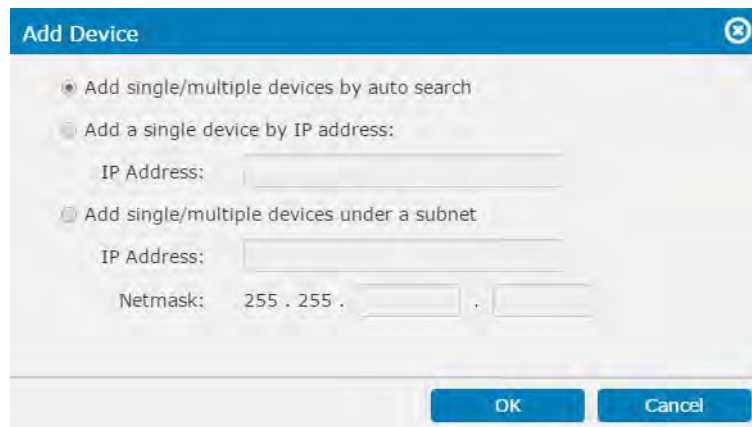
## Adding/Logging into/Removing a Device

Go to

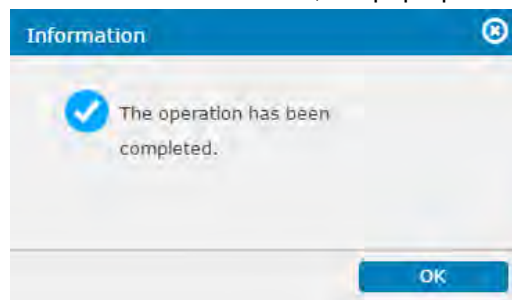
Device List > Add Device



Add a device



1. Choose a method to connect to a PAC Storage PS/PSV
  - a) Add single/multiple devices by auto search – the system will automatically search for connected device(s).
  - b) Add a single device by IP address – enter the IP address of the PAC Storage PS/PSV.
  - c) Add single/multiple devices under a subnet – enter the starting IP address and Netmask to automatically connect all PAC Storage PS/PSVs within a subnet.
2. Click **OK**.
3. If all information is correct, the pop-up message below will be displayed.

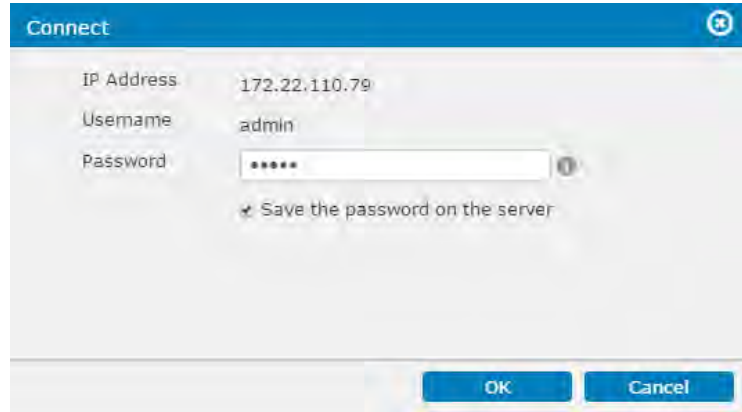


- Connect to a device** 1. The device will appear on the device list. Click **Connect**.

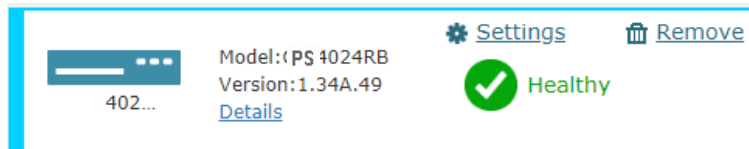


2. Type in the password in the login pop-up window.

Note: The login name and password are both “admin” by default.



2. The device status will appear, including the model name, firmware version and the working status.



3. For more information of the device, click **Details**.

Detail information

View parameters of the selected device.

Device name:

4016R

Model:

4016R

IP address:

172.27.113.238

Service ID:

8817400

Controller ID:

428792 (0x68AF8)

Firmware version:

1.32N.01


Host board:

Slot A #1: FC 8G(SN: 0)  
Slot B #1: FC 8G(SN: 8672130)  
Slot A #2: iSCSI 10G RJ45(SN: 0)  
Slot B #2: iSCSI 10G RJ45(SN: 0)

EonOne Version:


2.4.n.01

Status:

 Healthy

## Remove a device


1. To disconnect a device, click the trash can icon on the upper-right corner of the device status window.





Model: PS 4024RB

Version: 1.34A.49

[Details](#)

 [Settings](#)

 [Remove](#)

 Healthy

2. A warning message will appear. The device will be disconnected after you click **OK**.

Warning



Are you sure you want to remove this device?

OK

Cancel

## Calibrating System Settings

When some Settings are not compatible with current firmware due to firmware update, the system automatically prompts and guides through calibrating the Settings.

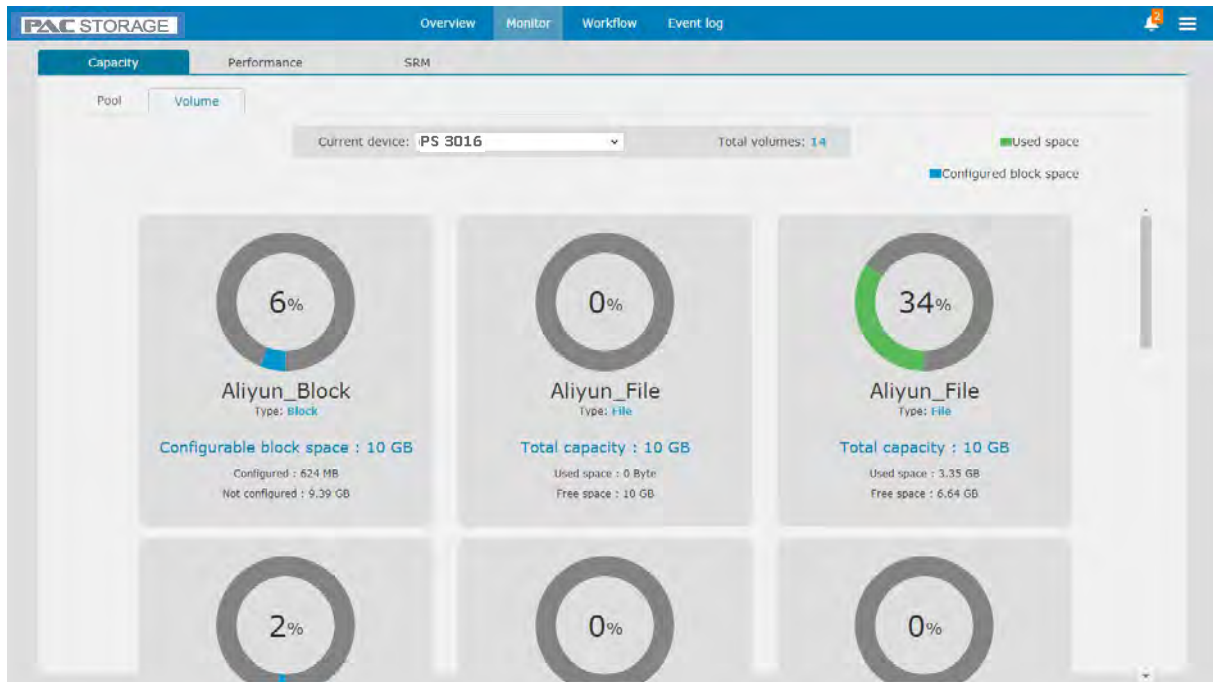
---

### Steps

1. Go to the **Overview** page.
2. When the system has a default route setting to calibrate due to firmware update, a pop-up appears and prompts you to calibrate the setting.  
  
The default route is responsible for communicating data with external systems.
3. Go to the channel menu.
4. Select a network channel as the default route. To edit the channel Settings, click **Edit** and proceed.
5. Click **Refresh** to update the default route setting.

## Monitoring

This section introduces Storage Resource Management (SRM) and how to monitor the capacity usage and performance of your PAC Storage PS/PSV devices.





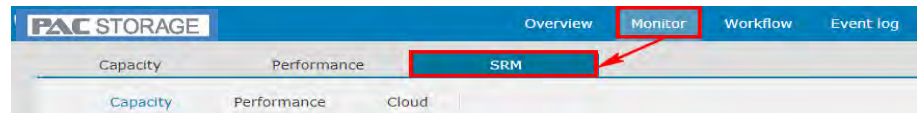
## **Storage Resource Management (SRM)**

The main purpose of SRM is to allow users to monitor the usage of PAC Storage disk array systems. SRM collects the usage logs from disk array systems and displays them in trend charts for users to easily plan storage usage ahead, make decisions and even discover abnormality. The SRM function is only available on the Central PAC Storage User Interface Firmware.



Go to

Monitor > SRM



Add an SRM  
diagram

1. Click the **Add Contents** button in the pop-up window.



2. Choose the item you want to monitor and click **Next**. Available items include device, pool, volume and channel.

Step 1: Select what contents you would like to monitor

☒ Device

Target Device:

\* Content title:

☐ Pool

Target Device:

Pool:

\* Content title:

☐ Volume

Target Device:

Pool:

Volume:

\* Content title:

☐ Channel

Target Device:

Channel:

\* Content title:


☐ Cloud

Target device:

☒ Local volume


☐ Local folder


\* Content title:


3. Select the type of content you want to see and click **OK**. in this case the below selections are for block-level volumes, (for file-level volumes, only one selection is available which is the **Cloud data performance**)


Add contents

Step 2: Select what contents you would like to see


☒ Cloud data performance (Cloud data transfer)


☐ Cloud data performance (Read cache hit rate)



☐ Cloud data performance (Read/write throughput)

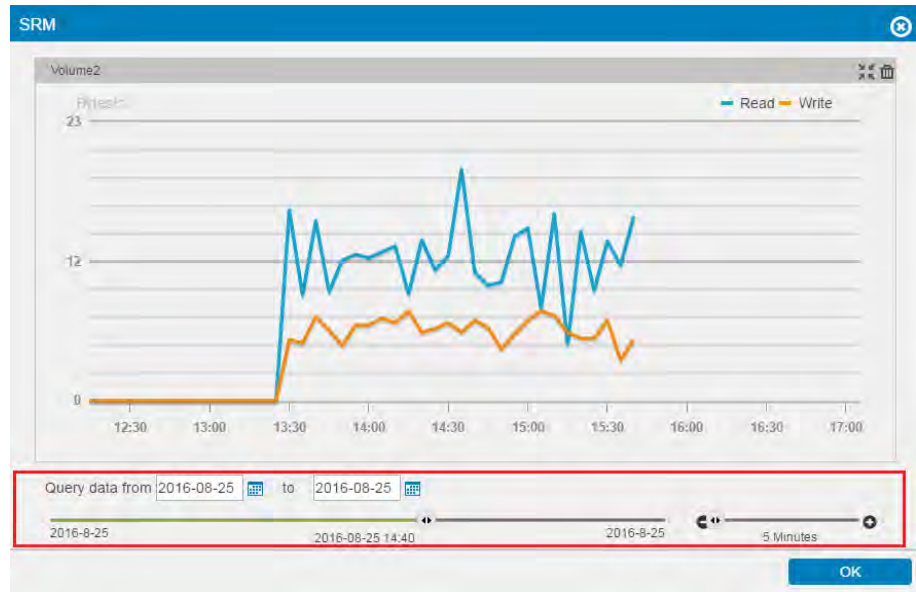

☐ Cloud data performance (Cache usage)

4. You will see the contents of the selected item displayed in graphs.




## Configure an SRM diagram

Click the icon  at the upper right corner of each chart for a closer view of the chart at a time interval of your choice.

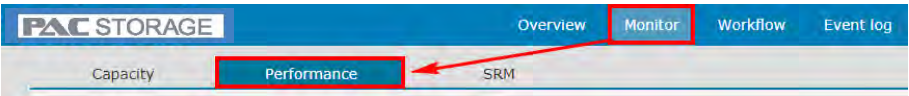


## Export SRM records

Click the **Export** button  and select the records to export. The SRM data is recorded in .csv files and compressed into a .zip file for users to download.

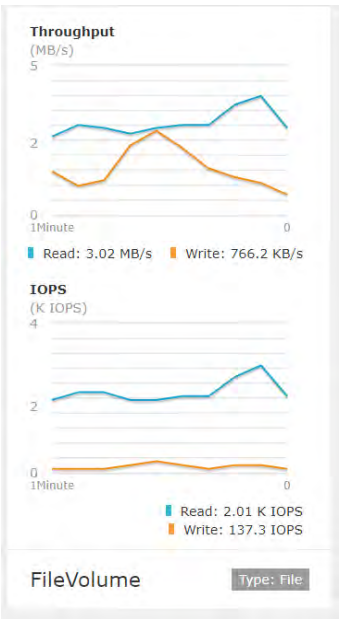
The figure shows an 'Export' dialog box. It contains the instruction 'Please select the item(s) that you want to export and click the Export button.' Below this, there are two rows of items to select, each with a checkbox and a label. The first row has a checked checkbox and the label 'Target' with 'Contents' to its right. The second row has a checked checkbox and the label 'Data performance (R/W IOPS)' with 'SRM' to its right. An 'Export' button is located at the bottom right of the dialog.

Go to **Monitor > Performance**



**Monitor storage performance (Volume)**

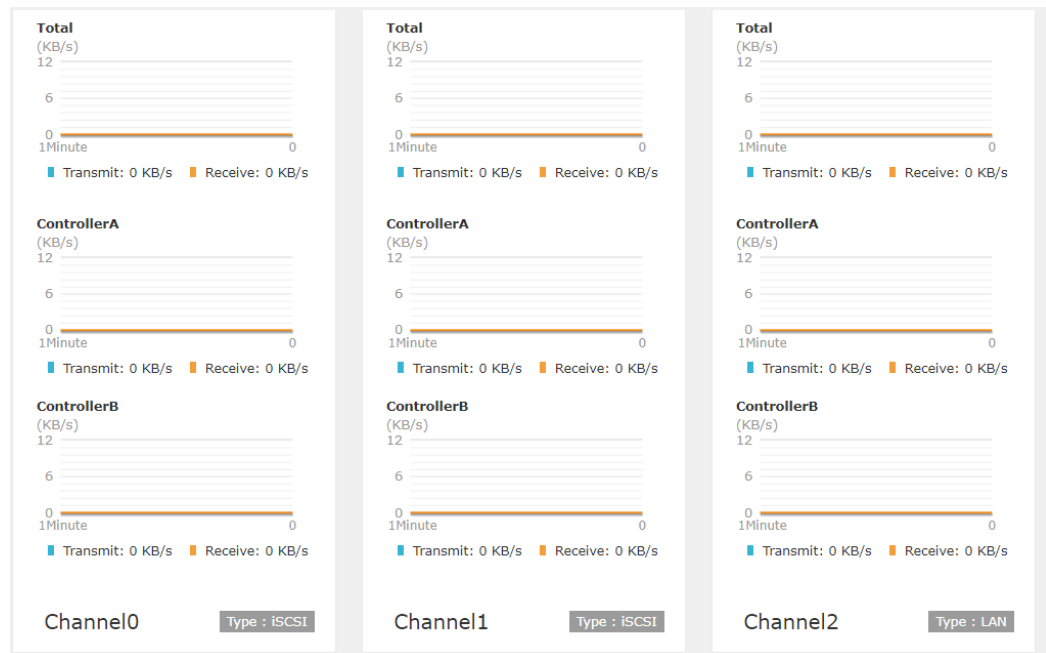
Click the **Volume** tab and select the volume. The read/write Throughput and IOPS will be displayed instantly in charts for each volume.



**Monitor storage performance (Channel)**

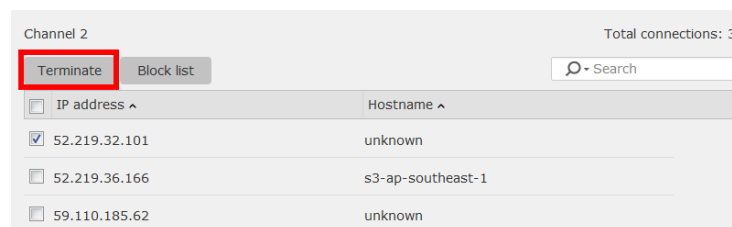
Click the **Channel** tab and select the device. Each channel's data transfer status is displayed in charts.

Note: The data related to cloud is excluded.

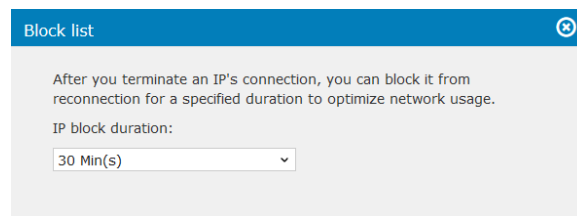


For a LAN type channel, you can terminate and block its IP connections:

1. Click on **Details** to view current IP connections.
2. To end an unwanted IP connection, select one in the list and click **Terminate**.



3. On the pop-up, you can set **IP block duration** to keep the selected IP disconnected for a while. Click **OK** to save the setting.



4. You can find the blocked IP by clicking on **Block list**.

### Monitor storage performance (Cloud)

Click the **Cloud** tab and select the cloud cache volume which you want to monitor its status. The system will display the read cache hit rate, cache usage, cloud data transfer and volume throughput.

Cache)

Capacity

Performance

SRM

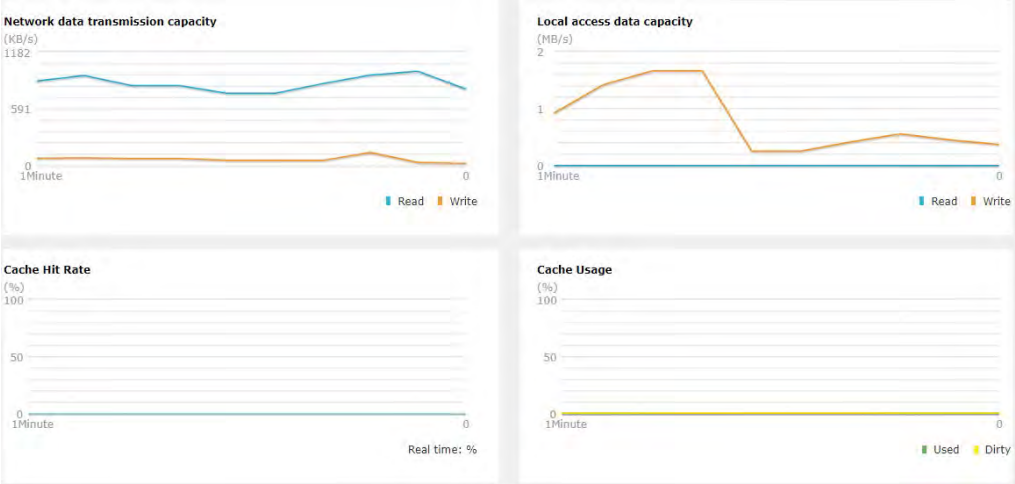
Capacity

Performance

Cloud

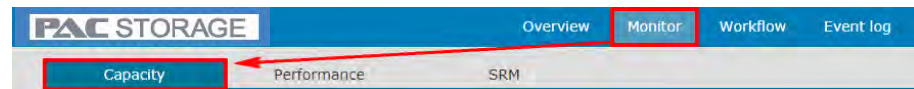
Export

Add contents



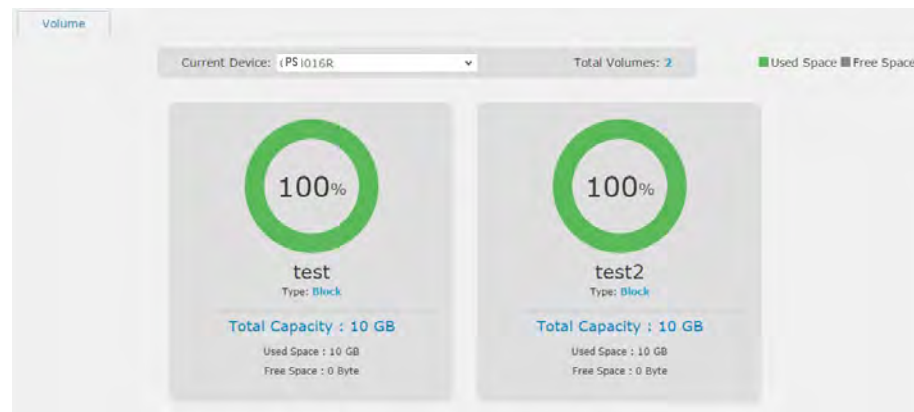
Go to

Monitor > Capacity



**Monitor storage capacity**

Volumes in your PAC Storage PS/PSV devices will be listed with their usage of capacity and type of volume shared.

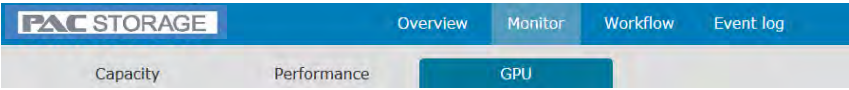


## Monitoring Storage Capacity



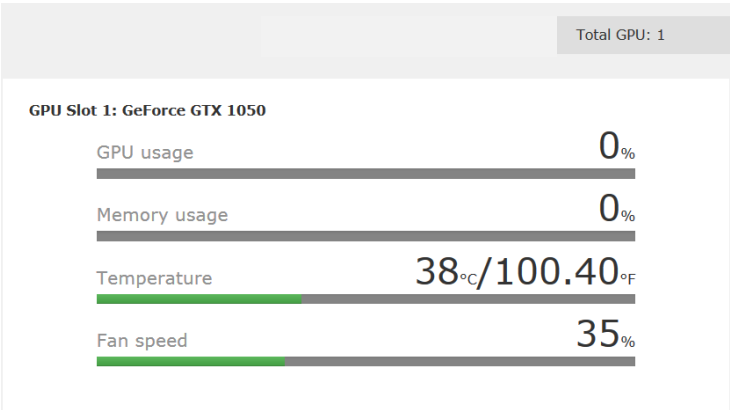
Go to

Monitor > GPU



**Monitor GPU  
Status**

Check the number of GPUs installed on your PS device and their status.



**Monitoring GPU Status**

## Monitoring client connections

**Go to**

**Monitor > Connection**

---

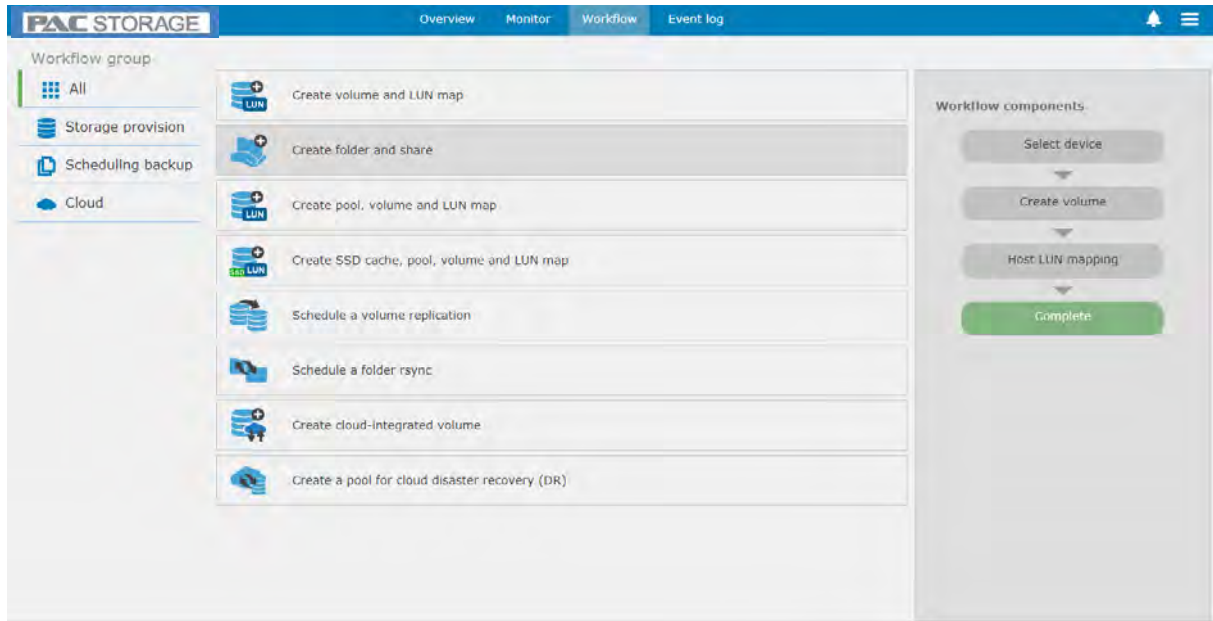
**Steps**

1. Go to **Current device**.
2. Select a storage system to monitor its client connections over the enabled protocols.
3. Check **Total current connections** to find the total number of active connections to the selected system.
4. For more information, you can check the number of connections by protocol.

When the system enables the CIFS/SMB, FTP, or SFTP protocols, you can monitor the number of client connections using these protocols.

## Workflow

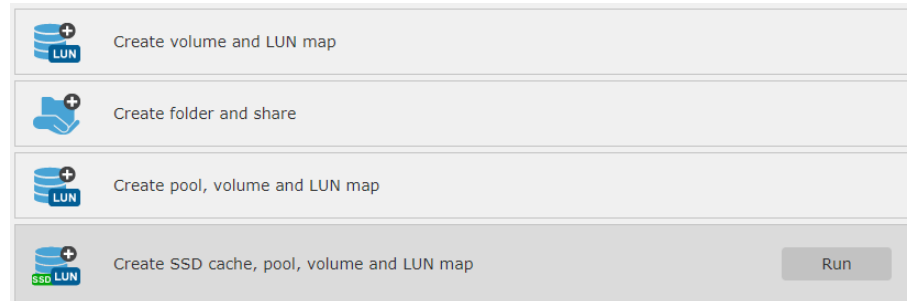
The workflow process is created to allow users to combine multiple steps into one workflow which simplifies tasks and saves time.



## Creating SSD Cache, Pool, Volume and LUN Mapping

### Go To

Workflow > Create SSD cache, pool, volume and LUN map > Run

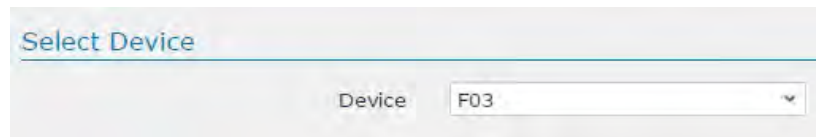


The workflow consists of four steps:

- Create volume and LUN map
- Create folder and share
- Create pool, volume and LUN map
- Create SSD cache, pool, volume and LUN map (highlighted in grey with a 'Run' button)

### Select device

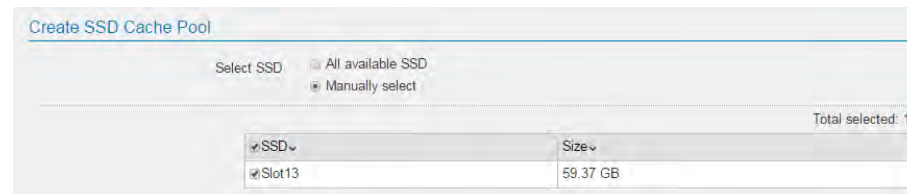
Select a connected device from the drop down list.



The 'Select Device' dialog shows a dropdown menu for 'Device' with 'F03' selected.

### Create SSD cache pool

Select the SSD drives for creating SSD cache pool.

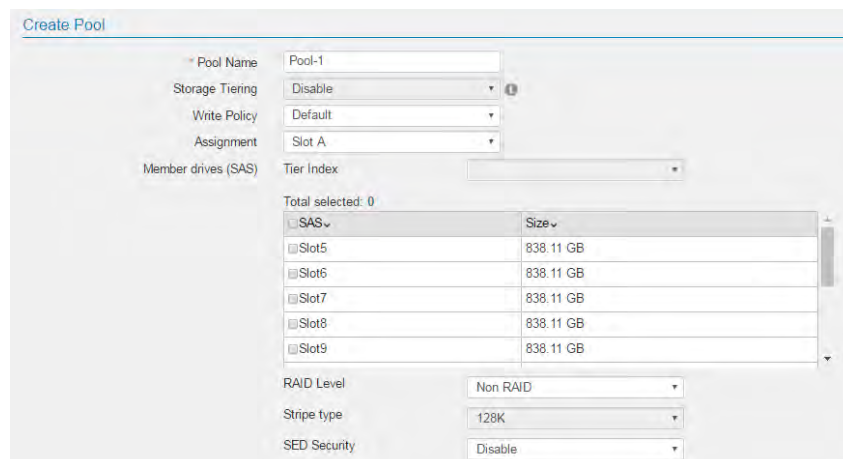


The 'Create SSD Cache Pool' dialog shows the 'Select SSD' section with 'All available SSD' selected. A table lists the selected SSDs:

SSD	Size
Slot13	59.37 GB

Total selected: 1

### Create pool



The 'Create Pool' dialog shows the following settings:

- Pool Name: Pool-1
- Storage Tiering: Disable
- Write Policy: Default
- Assignment: Slot A
- Member drives (SAS): Tier Index
- Total selected: 0
- Table of member drives (SAS):

SAS	Size
Slot5	838.11 GB
Slot6	838.11 GB
Slot7	838.11 GB
Slot8	838.11 GB
Slot9	838.11 GB

- RAID Level: Non RAID
- Stripe type: 128K
- SED Security: Disable

### Parameters

**Pool name** The default pool name is “pool” followed by index numbers, e.g. pool-1 and pool-2. You can modify it to your preference.

**Storage Tiering / Tier Index** Disable or Enable.  
For more information about storage tiering, click [here](#).

**Write Policy** Specifies the write policy: Default, Write-Back, or Write-Through. Selecting Write-Through increases security but decreases performance.

- Default: Writing policy is determined by the controller’s caching mode and event trigger mechanism
- Write Back: Writing is considered completed when cache data is overwritten
- Write Through: Writing is considered completed only after the disk data is overwritten

**Assignment** Specifies which controller slot the new pool will be assigned to.

This option is available for R-models only.

**Member Drives** Select the drives you wish to have in the pool.

**RAID Level** Select the RAID level to protect your data.

The available RAID level depends on the number of disk drives.

RAID level	Minimum number of drives
RAID 0	1
RAID 1	2
RAID 3	3 (4 if you want to add a spare drive)
RAID 5	3 (4 if you want to add a spare drive)

RAID 6      4 (5 if you want to add a spare drive)

**Stripe Size**      Specifies the array stripe size. Do not change this value unless you are sure the modified value leads to increased performance.

**SED Security**      Specifies whether you want to protect the member drives with SED (Self Encrypting Drives) security.

Before enabling this option, the following requirements should be met:

- A SED authentication key is created
- All member drives support SED.

## Create volume

Create Volume

\* Pool: Pool-2 (0FAA929D29357A1...)

Quantity: 1

Volume Name: Volume+index

☐ Enable Thin Provisioning

\* Volume Size: 314.95 GB      Maximum: 807.58 GB

Minimum reserved space: 0 GB

☒ Initialize Volume After Creation

☐ Enable File System

Modify the configurations accordingly.

**Pool:** Specify the pool where the new volume(s) can claim space.

**Quantity:** You can decide how many volumes you want to create at a time within the specified pool.

**Enable Thin Provisioning & Initialize Volume After Creation:** Choose to enable thin provisioning or initialize volume after creation. They are two mutually exclusive options. For more information, refer to About Thin-Provisioning.

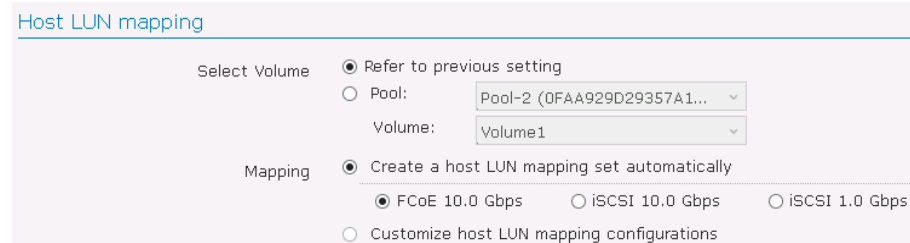
**Volume Size:** Specify the volume size for a new volume.

**Minimum reserved space:** You can only select minimum reserved space if thin provisioning is enabled.

**Enable File System:** If the volume(s) is created for folder sharing, check the **Enable File System** option, and there is no need to configure Settings in "Host

LUN Mapping” afterward.

## Host LUN mapping



The screenshot shows the 'Host LUN mapping' configuration window. It has two main sections: 'Select Volume' and 'Mapping'. In the 'Select Volume' section, the 'Refer to previous setting' radio button is selected. Below it, there are dropdown menus for 'Pool' (showing 'Pool-2 (0FAA929D29357A1...') and 'Volume' (showing 'Volume1'). In the 'Mapping' section, the 'Create a host LUN mapping set automatically' radio button is selected. Below this, there are three radio buttons for the protocol: 'FCoE 10.0 Gbps' (selected), 'iSCSI 10.0 Gbps', and 'iSCSI 1.0 Gbps'. At the bottom, there is an unselected radio button for 'Customize host LUN mapping configurations'.

**Select Volume:** “Refer to previous setting” means to map the volume(s) that you just created. You can also choose to map volumes other than the ones just created according to your needs.

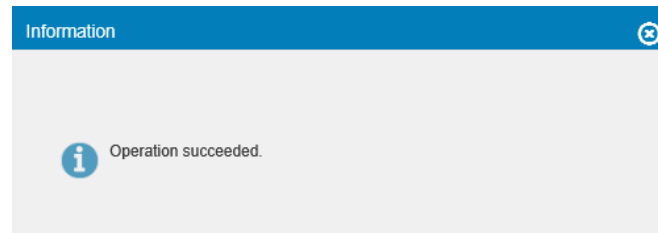
**Mapping:** PAC Storage PS/PSV device has hybrid host connectivity. Choose the suitable one for your environment.

## Finishing

Click the **Execute** button.



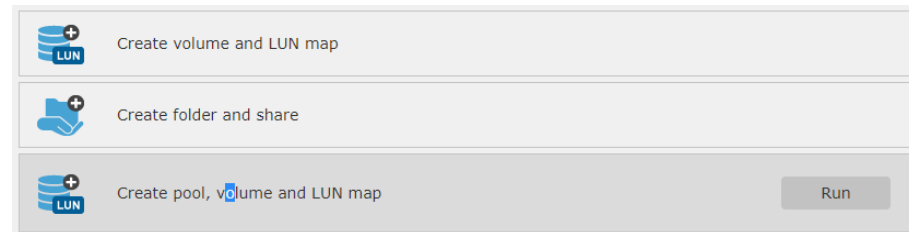
The below pop-up message will be displayed if the tasks are successful.



## Creating Pool, Volume and LUN Mapping

### Go To

Workflow > Create Pool, volume and LUN map > Run

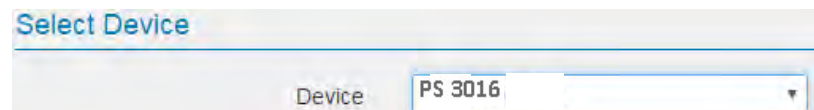


The workflow consists of three steps:

- Create volume and LUN map
- Create folder and share
- Create pool, volume and LUN map (highlighted with a 'Run' button)

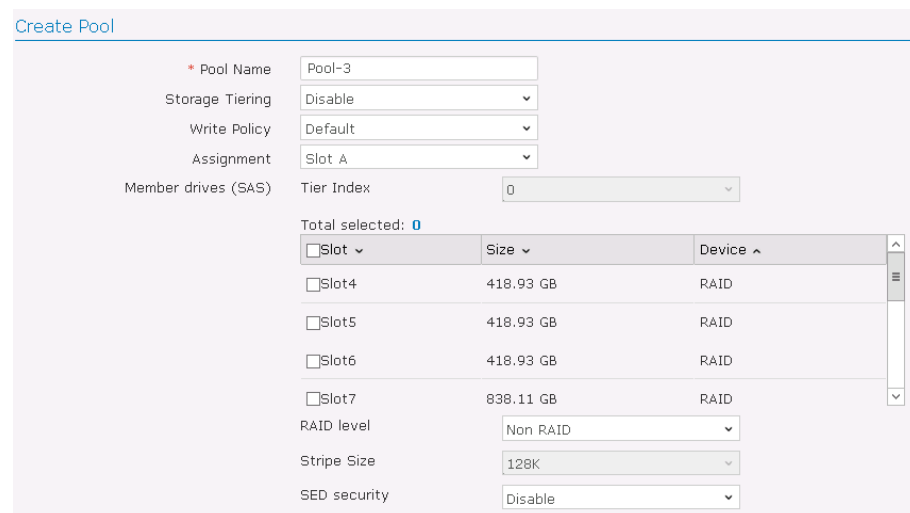
### Select device

Select a connected device from the drop down list.



The 'Select Device' dropdown menu shows 'PS 3016' as the selected device.

### Create pool



The 'Create Pool' form includes the following fields:

- Pool Name: Pool-3
- Storage Tiering: Disable
- Write Policy: Default
- Assignment: Slot A
- Member drives (SAS): Tier Index: 0
- Total selected: 0
- Table of available slots:

Slot	Size	Device
Slot4	418.93 GB	RAID
Slot5	418.93 GB	RAID
Slot6	418.93 GB	RAID
Slot7	838.11 GB	RAID

- RAID level: Non RAID
- Stripe Size: 128K
- SED security: Disable

### Parameters

**Pool name** The default pool name is pool followed by index numbers, such as pool-1, pool-2, etc.

**Storage Tiering / Tier Index** Disable or Enable.  
For more information about storage tiering, click [here](#).

**Write Policy** Specifies the writing policy: default, write-back, or write-through. Selecting write-through increases security but



decreases performance.

- Default: Writing policy is determined by the controller's caching mode and event trigger mechanism.
- Write-back: Writing is considered completed when cache data is overwritten.
- Write-through: Writing is considered completed only after when the disk data is overwritten.

---

**Assignment** Specifies which controller slot the new pool will be assigned to.

This option is available for R-models only.

---

**Member Drives** Select the drives you wish to have in the pool.

---

**RAID Level** Select the RAID level to protect your data.

The available RAID level depends on the number of disk drives.

---

RAID level	Minimum number of drives
RAID 0	1
RAID 1	2
RAID 3	3 (4 if you want to add a spare drive)
RAID 5	3 (4 if you want to add a spare drive)
RAID 6	4 (5 if you want to add a spare drive)

---

**Stripe Size** Specifies the array stripe size. Do not change this value unless you are sure the modified value leads to enhanced performance.

---

**SED Security** Specifies whether you want to protect the member drives with SED (Self Encrypting Drives) security.

Before enabling this option, the following requirements

should be met:

- A SED authentication key is created.
- All member drives support SED.

## Create volume

Create Volume

\* Pool: Pool-2 (0FAA929D29357A1...)

Quantity: 1

Volume Name: Volume+index

☐ Enable Thin Provisioning

\* Volume Size: 452.8 GB Maximum: 808.58 GB

Minimum reserved space: 0 GB

☒ Initialize Volume After Creation

☐ Enable File System

Modify the configurations accordingly.

**Pool:** Specify the pool where the new volume(s) can claim space.

**Quantity:** You can decide how many volumes you want to create at a time within the specified pool.

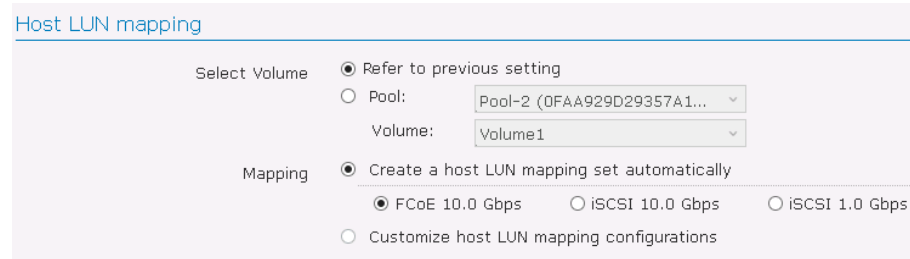
**Enable Thin Provisioning & Initialize Volume After Creation:** Choose to enable thin provisioning or initialize volume after creation. They are two mutually exclusive options. For more information, refer to About Thin-Provisioning.

**Volume Size:** Specify the volume size for a new volume

**Minimum reserved space:** You can only select minimum reserved space if thin provisioning is enabled.

**Enable File System:** If the volume(s) is created for folder sharing, check the **Enable File System** option, and there is no need to configure Settings in “Host LUN Mapping” afterward.

## Host LUN mapping



Host LUN mapping

Select Volume

- ☒ Refer to previous setting
- ☐ Pool: 
  - Volume:

Mapping

- ☒ Create a host LUN mapping set automatically
  - ☒ FCoE 10.0 Gbps
  - ☐ iSCSI 10.0 Gbps
  - ☐ iSCSI 1.0 Gbps
- ☐ Customize host LUN mapping configurations

**Select Volume:** “Refer to previous setting” means to map the volume(s) that you just created. You can also choose to map volumes other than the ones just created according to your needs.

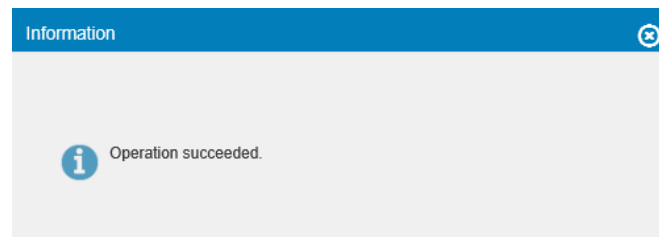
**Mapping:** PAC Storage PS/PSV device has hybrid host connectivity. Choose the suitable one for your environment.

## Finishing

Click the **Execute** button.



The below pop-up message will be displayed if the tasks are successful.



## Creating Folder and Share

To create a folder for sharing, you need a volume that has the **Enable File System** option checked during the creation process. For more information please refer to the section “Create Pool, Volume and LUN Mapping”.

**Go to**

**Workflow > Create folder and share > Run**



The workflow consists of three steps:

- 1. Create volume and LUN map (represented by a LUN icon)
- 2. Create folder and share (represented by a folder icon with a plus sign). A "Run" button is visible to the right of this step.
- 3. Create pool, volume and LUN map (represented by a LUN icon)

**Select device**

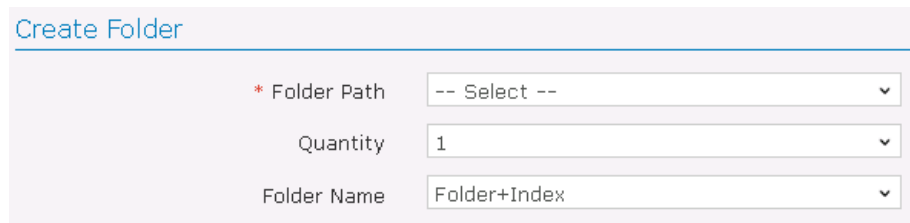
Select a connected device from the drop down list.



The "Select Device" dropdown menu shows "PS 3016" as the selected device.

**Create folder**

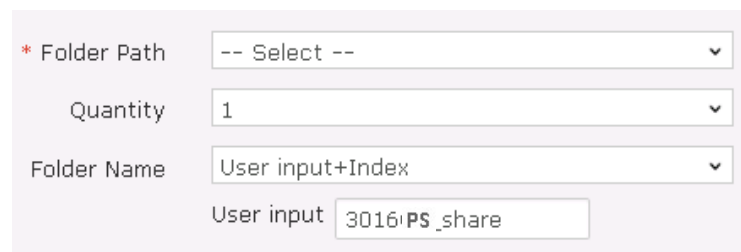
Create a folder which claims space from a file system enabled volume. Specify the quantity and folder name. The default folder name is folder followed by index: "Folder+Index."



The "Create Folder" form has the following default settings:

- \* Folder Path: -- Select --
- Quantity: 1
- Folder Name: Folder+Index

You can also choose to enter a unique name for the folder. Change the option of folder name to "User input+index" and then type in a name.



The "Create Folder" form is configured with custom settings:

- \* Folder Path: -- Select --
- Quantity: 1
- Folder Name: User input+Index
- User input: 3016PS\_share

**Permission setting**

Enter a share name for the folder and select the type of protocols you want to go through. You can customize the sharing Settings for CIFS and NFS protocols by checking the **Settings** option. When creating multiple shared folders, an index

number will be added after the share name.

Permission Setting

Folder Path

Share Name

Select Protocols

- ☐ CIFS ☐ Settings
- ☐ NFS ☐ Settings
- ☐ AFP
- ☐ FTP
- ☐ SFTP
- ☐ WebDAV
- ☐ Object

Share name will add index number after the share name when creating multiple share folders.

Add or edit permissions for an existing user or group.

**Full Control:** Full read/write access to the selected users or groups.

**Read-Only:** Selected users or groups can only read the files in the shared folder.

**Access denied:** Selected users or groups will be denied from accessing the folder.

Access Rights Add Delete

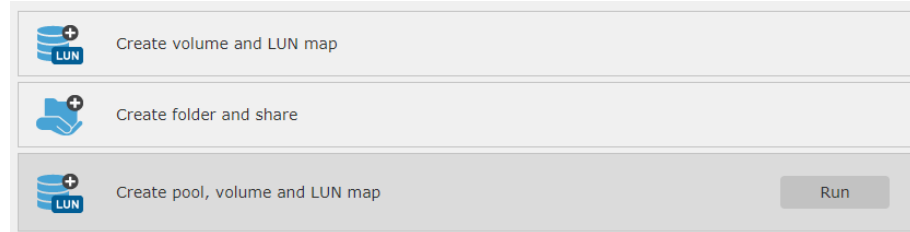
<input type="checkbox"/> Name ^	Full Control	Read-Only	Access denied
Other	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

☐ Propagate access control list setting to subfolders

## Creating Volume and LUN Mapping

### Go To

Workflow > Create volume and LUN map > Run



The workflow consists of three steps:

- 1. Create volume and LUN map (indicated by a blue LUN icon and a plus sign)
- 2. Create folder and share (indicated by a blue folder icon and a plus sign)
- 3. Create pool, volume and LUN map (indicated by a blue LUN icon and a plus sign)

A "Run" button is located at the bottom right of the third step.

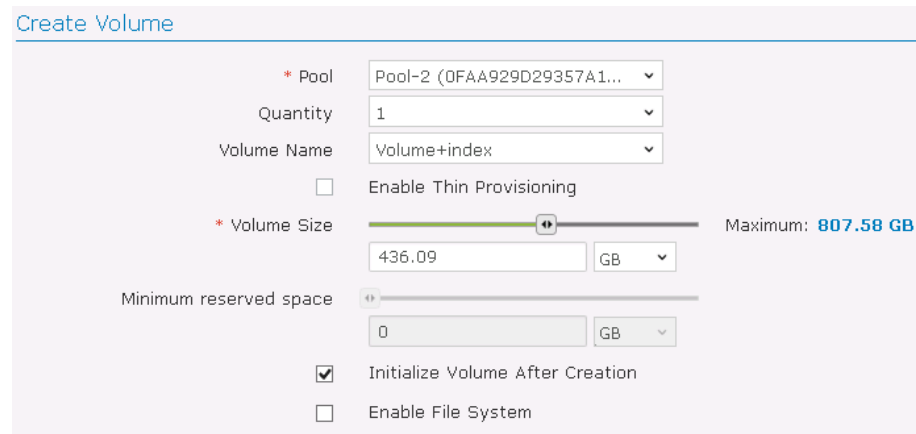
### Select device

Select a connected device from the drop down list.



The "Select Device" dropdown menu shows "PS 3016" as the selected device.

### Create volume



The "Create Volume" form includes the following fields and options:

- \* Pool:** Pool-2 (0FAA929D29357A1...)
- Quantity:** 1
- Volume Name:** Volume+index
- ☐ Enable Thin Provisioning
- \* Volume Size:** 436.09 GB (Maximum: 807.58 GB)
- Minimum reserved space:** 0 GB
- ☒ Initialize Volume After Creation
- ☐ Enable File System

Modify the configurations accordingly.

**Pool:** Specify the pool where the new volume(s) can claim space.

**Quantity:** You can decide how many volumes you want to create at a time within the specified pool.

**Enable Thin Provisioning / Initialize Volume After Creation:** Choose to enable thin provisioning or initialize volume after creation. These are mutually exclusive options. For more information, refer to About Thin-Provisioning.

**Volume Size:** Specify the volume size for a new volume.

**Minimum reserved space:** You can only select minimum reserved space if thin provisioning is enabled.

**Enable File System:** If the volume(s) is created for folder sharing, check the

**Enable File System** option, and there is no need to configure Settings in “Host LUN Mapping” afterward.

**Volume name** The default volume name is volume followed by index numbers, such as volume-1, volume-2, etc.

Volume Name

You can also choose to enter a unique name for the volume. Change the “Volume Name” option to “user input+index” and then type in a name.

Volume Name   
\* User input

## Host LUN mapping

Host LUN mapping

Select Volume ☒ Refer to previous setting  
☐ Pool:   
 Volume:

Mapping ☒ Create a host LUN mapping set automatically  
☒ FCoE 10.0 Gbps ☐ iSCSI 10.0 Gbps ☐ iSCSI 1.0 Gbps  
☐ Customize host LUN mapping configurations


**Select Volume:** “Refer to previous setting” means to map the volume(s) you just created. You can also choose to map volumes other than the ones just created according to your needs.

**Mapping:** PAC Storage PS/PSV device has hybrid host connectivity. Choose the suitable one for your environment.

## Finishing

Click the **Execute** button.

The below pop-up message will be displayed if the tasks are successful.




 Operation succeeded.

## Scheduling a Volume Replication



Go to

**Workflow > Schedule a volume replication > Run**

	Create pool, volume and LUN map
	Create SSD cache, pool, volume and LUN map
	Schedule a volume replication

**Select device**

Select a connected device from the drop down list.

Select Device

Device

F03

#### Configure Volume Replication

* Replication Pair Name	Replication_20170619_110403
Type	Asynchronous Mirror
	<input type="checkbox"/> Configure the sync point inside the target volume (target snapshot) <input type="checkbox"/> Support Incremental Recovery <input type="checkbox"/> Compress Data before Transmission
Remote Timeout Threshold	30 Seconds
Source Pool	Pool-1
Source Volume	Volume_1
Target Device	LUN_3024RUB
Target Pool	Pool-1
* Target Volume	RRtarget
Priority	Normal

#### Parameters

**Replication Pair Name**

Name this replication task

**Type**

**Synchronous / Asynchronous / Volume Copy**

When synchronous mode is enabled, the host will write data to both the source and target at the same time. In asynchronous mode, the host I/O will be allocated to the source volume only, thus allowing higher bandwidth and optimized performance. New data will be written later into the target in batch to reduce I/O traffic. If Volume Copy is chosen, the source volume will be copied to the target volume once, and any changes to the source volume later will not be applied to the target volume.

**Incremental Recovery**

Allows tracing data back from the target volume to the source volume. The new data accumulated in the target volume during

	downtime will be gradually copied to the source volume.
<b>Compress Data</b>	<p>If the bandwidth is not enough for asynchronous mirroring, compressing data will reduce the amount of I/O.</p> <div> <p>This option impacts the subsystem performance by taking up extra computing power.</p> </div>
<b>Remote Timeout Threshold</b>	<p>The remote timeout threshold option allows you to avoid breaking a remote replication pair when the network connection between the source and the target becomes unstable or too slow. You may choose how long the controller will wait (timeout). The replication pair will receive better protection if the timeout period is long, but fewer interruptions impact the host performance. The reverse is also true: shorter timeout &gt; less impact &gt; more risk of breaking the pair.</p> <p><b>Enabled:</b></p> <p>Depending on the situation, the controller either splits or halts the volume mirror when there is no network activity for the length of the timeout period.</p> <p><b>Disabled:</b></p> <p>Host I/O may be seriously impacted when the network connection becomes unstable.</p> <div> <p>This option is for remote replication pairs only. If you create a local replication pair, this option will be disabled.</p> </div>
<b>Source Pool</b>	Specify the pool where the source volume will be located.
<b>Source Volume</b>	Specify the source volume which you want to replicate data.
<b>Target Device</b>	Specify the device where the replicated data will be restored.
<b>Target Pool</b>	Specify the pool where the replicated data will be restored.
<b>Target Volume</b>	Create a new volume to restore the replicated data.
<b>Priority</b>	Choose the processing priority for the replication task.
<b>Scheduling (only for synchronous mirror and volume copy)</b>	The scheduling options will appear if users select <b>Asynchronous Mirror</b> or <b>Volume Copy</b> for the replication job.

Configure Volume Replication

* Replication Pair Name	
Type	<div> -- Select --  Synchronous Mirror  <b>Asynchronous Mirror</b>  Volume Copy </div>

**Asynchronous Mirror:** Specify the start time and frequency for the system to perform asynchronous mirror tasks.

Schedule

* Name	New_Schedule_201706		
Start Date	2017-06-19		
Start Time	11	:	07
End Date	2017-06-19		
End Time	23	:	59
Frequency	<input checked="" type="radio"/> Once <input type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly <input type="radio"/> Backup every 10 minutes		

**Volume Copy:** Specify the time for the system to perform volume copy tasks.


Schedule

* Name	New_Schedule_201706		
Start Date	2017-06-19		
Start Time	11	:	07

## Scheduling a Folder Rsync

Go to

**Workflow > Schedule a folder rsync > Run**

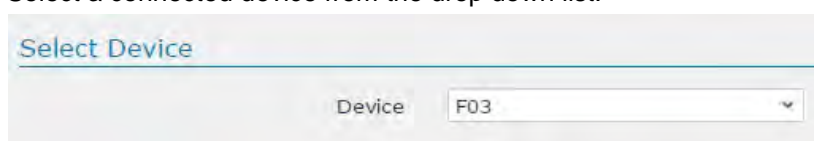


The workflow consists of four steps:

- Schedule a volume replication
- Schedule a folder rsync (highlighted with a 'Run' button)
- Create cloud-integrated volume
- Create a pool for cloud disaster recovery (DR)

**Select device**

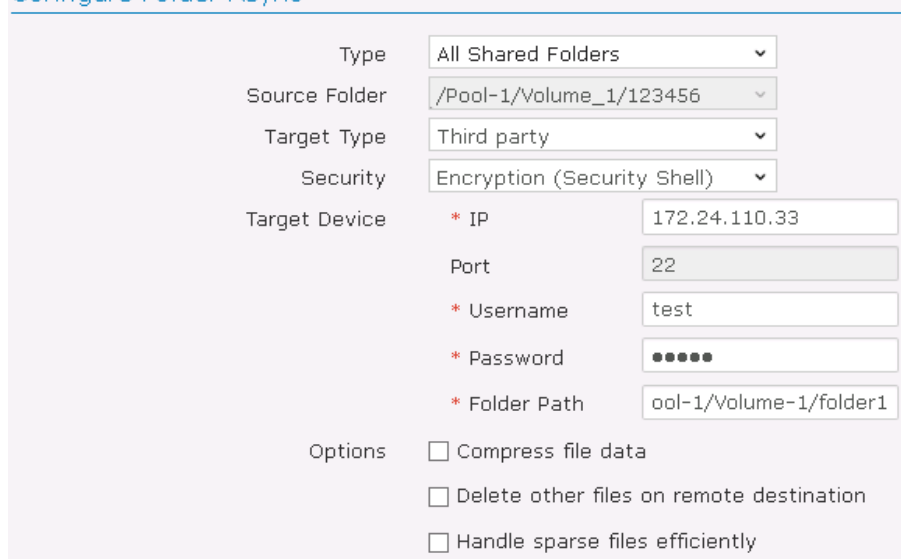
Select a connected device from the drop down list.



The 'Select Device' dropdown menu shows 'F03' as the selected device.

**Configure folder rsync**

Configure Folder Rsync



The configuration form includes the following fields:

- Type: All Shared Folders
- Source Folder: /Pool-1/Volume\_1/123456
- Target Type: Third party
- Security: Encryption (Security Shell)
- Target Device:
  - \* IP: 172.24.110.33
  - Port: 22
  - \* Username: test
  - \* Password: [masked]
  - \* Folder Path: ool-1/Volume-1/folder1
- Options:
  - ☐ Compress file data
  - ☐ Delete other files on remote destination
  - ☐ Handle sparse files efficiently

## Parameters

**Source folder**

Select the source folder for which you want to perform folder rsync.

**Target Type**

Choose the type of the target, whether it's an PAC Storage NAS system or a third party device.

**Security**

Choose whether you want to encrypt your data in the folder rsync progress. The port of the target device will vary due to different security Settings. (This option is only for "Third party" Target Type.)

---

**Target Device**

Specify the file service IP and the target rsync user Settings. Please note:

- The username and password here are not the same as those for the user account.
- Target rsync information will be different depending on Target Type and Security.

---

Target Type	Security	Rsync Information
Third Party	None	Share Name
	Encryption	Folder Path
NAS	Encryption	Directory (Absolute path)

---

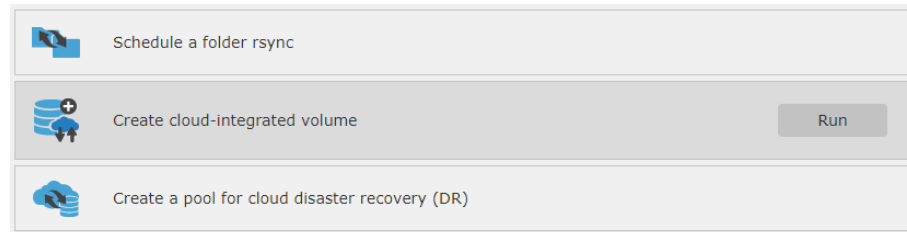
**Schedule**

Configure the schedule for the folder rsync operations.

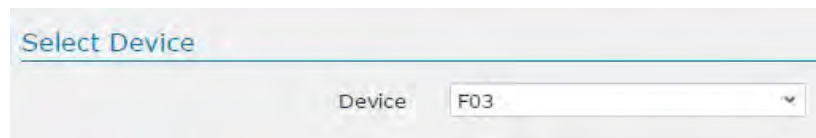
---

## Creating a Cloud-integrated Volume

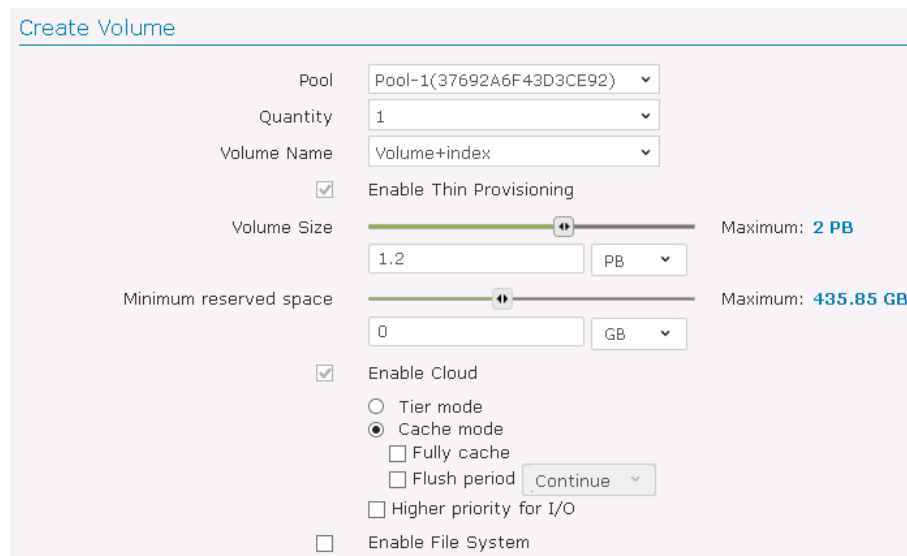
**Go To**      **Workflow > Create cloud integrated volume > Run**



**Select device**      Select a connected device from the drop down list.



**Create Volume**



### Parameters

#### Pool



Select an existing pool that will be mapped with a cloud bucket. Note that the selected pool cannot be connected with any cloud providers.

To create cloud enabled volumes within a pool that are connected with a cloud provider, please refer to Cloud Gateway.

<b>Volume Name</b>	Enter the name of the volume.
<b>Volume Size</b>	<p>Specifies the size and unit of the volume. If Thin Provisioning is enabled, the total size of volumes can exceed the size of the pool.</p> <div>The minimum size of a volume is 10GB.</div>
<b>Enable Cloud-Tier mode</b>	<p>If users set the cloud-integrated volume to “Tier mode,” the cloud bucket will be seen as the lowest storage tier. The less frequently accessed data (normally called cold data), will be moved to the cloud when the cloud-integrated volume has reached its capacity threshold.</p>
<b>Enable Cloud-Cache mode</b>	<p>If users set the cloud-integrated volume to “Cache mode,” all data stored in the volume will be flushed to the cloud according to schedule.</p> <p>If fully cache is enabled, all data will be stored on both the cloud bucket and the local cloud-integrated volume after the flush operation. If fully cache is disabled, all data will be stored on the cloud bucket after the flush operation, but only frequently accessed read data will be available on the local cloud-integrated volume. Regardless of whether fully cache is enabled, all data will be stored on cloud after the last flush operation and users can recover data based on the last snapshot if necessary.</p> <p>Users can set the data flush schedule by configuring the “Flush Period.”</p>
<b>Thin Provisioning &amp; Minimum Reserved Space</b>	<p>In order to expand storage capacity to the cloud buckets, thin-provisioning must be enabled in cloud-integrated volumes.</p> <p>Move the Minimum Reserved Space slide bar to set the percentage of the volume capacity that will be physically allocated as a safe reserve. For more information, refer to About Thin Provisioning.</p>
<b>Enable File System</b>	Users have to enable this option before creating a folder on the volume. The volume will be mounted to file

system.

The icons will be shown in the Volume List.

Volume with file system enabled	Volume without file system enabled
	

### Create Cloud Provider

To create a volume for cloud cache and cloud tiering, users need to provide cloud credential information for PAC Storage User Interface Firmware. The credential is used to create new buckets and mapping relationship with the volume(s).

The pool you have selected for creating the volume will be mapped with a new cloud bucket. Enter the credential information. The credential requirements may vary with different cloud providers. For example, to verify the user's identity, Amazon S3 needs a paired access key and secret key, while Microsoft Azure needs endpoint and share key information.

#### Create Cloud Provider

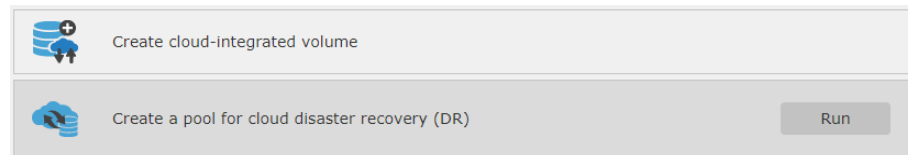
Pool	Pool-1 (37692A6F43D3CE9... ▼)
Cloud vendor	Aliyun Object Storage Ser... ▼
Access key ID	<input type="text"/>
Secret	<input type="text"/>
Region	China East 2 (Shanghai) ▼
Node Name	oss-cn-shanghai.aliyuncs.com
Bucket	Create a new bucket
	<input type="checkbox"/> Encryption
	<input type="checkbox"/> Compression
	<input checked="" type="checkbox"/> Use SSL



## Creating a Pool for Cloud Disaster Recovery (DR)

### Go To

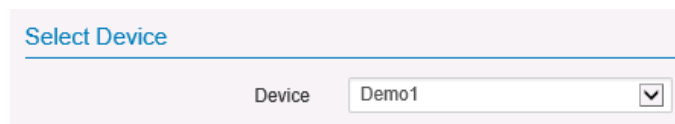
**Workflow > Create a pool for disaster recovery (DR) > Run**



The screenshot shows a workflow interface with two steps. The first step is 'Create cloud-integrated volume'. The second step is 'Create a pool for cloud disaster recovery (DR)', which is highlighted in grey and has a 'Run' button to its right.

### Select device

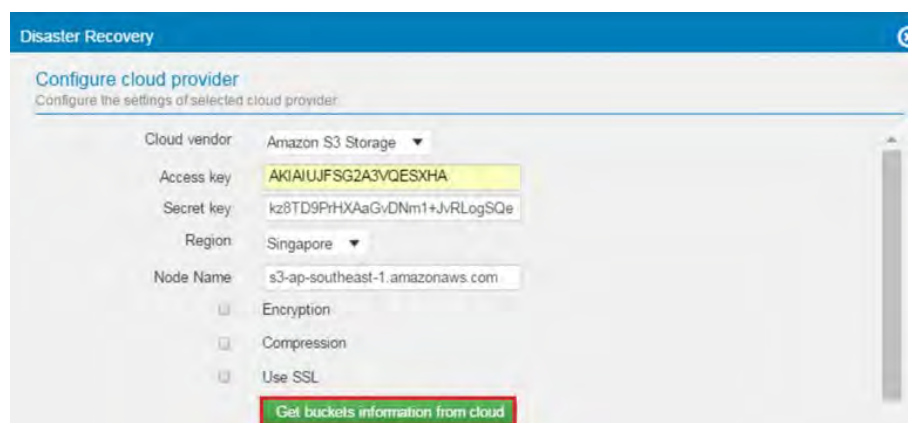
Select a connected device from the drop down list.



The screenshot shows a 'Select Device' section with a dropdown menu. The dropdown is open, showing 'Demo1' as the selected device.

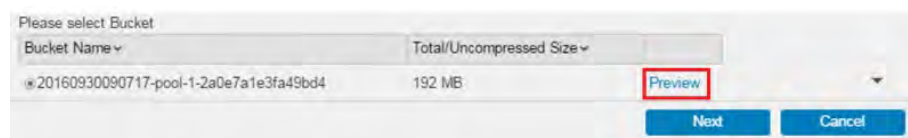
### Add a Cloud Provider

To retrieve the bucket information, the system needs your cloud provider access privilege. Select your cloud provider. Enter the credentials and click the **Get buckets information from cloud** button.



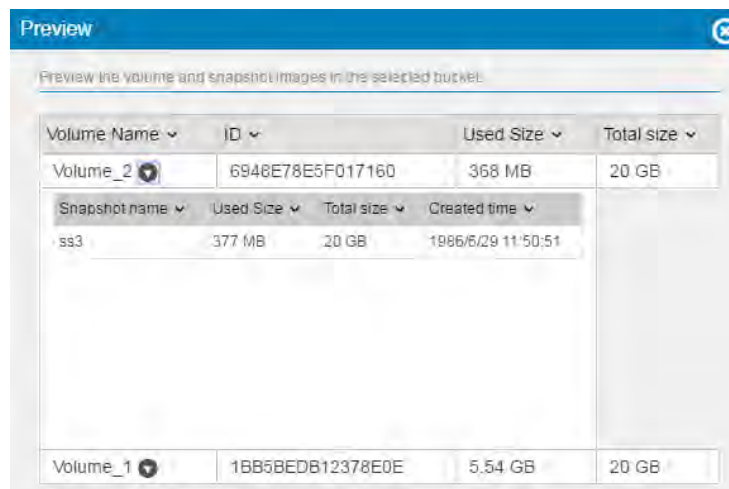
The screenshot shows the 'Configure cloud provider' form. It includes fields for 'Cloud vendor' (Amazon S3 Storage), 'Access key' (AKIAIUJFSG2A3VQESXHA), 'Secret key' (kz8TD9PHXAAGvDNm1+JvRLogSQe), 'Region' (Singapore), and 'Node Name' (s3-ap-southeast-1.amazonaws.com). There are checkboxes for 'Encryption', 'Compression', and 'Use SSL'. A green button labeled 'Get buckets information from cloud' is highlighted with a red box.

The bucket information will be listed. Users can see the detailed information of the buckets by clicking the **Preview** button.



The screenshot shows a table titled 'Please select Bucket'. It has two columns: 'Bucket Name' and 'Total/Uncompressed Size'. The first row shows a bucket name '20160930090717-pool-1-2a0e7a1e3fa49bd4' and a size of '192 MB'. A 'Preview' button is highlighted with a red box next to the bucket name.

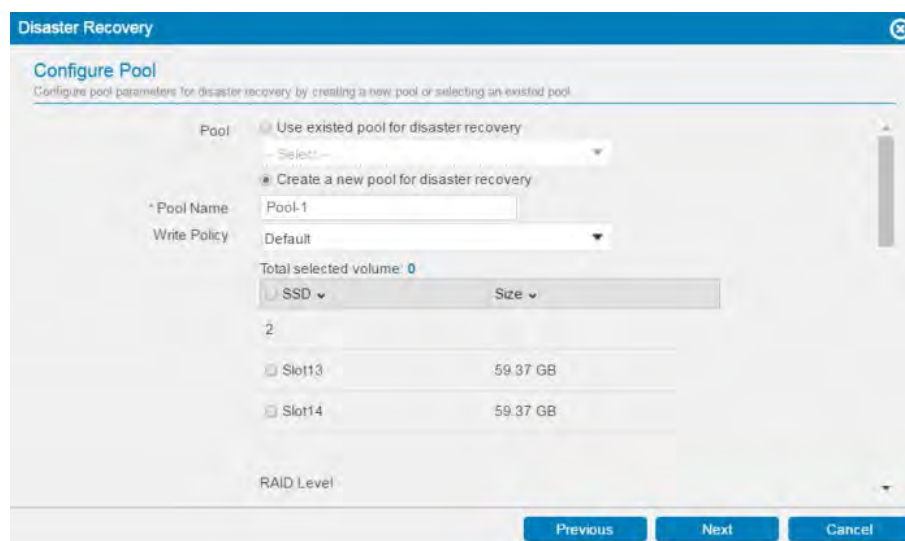
The bucket preview page shows information of volumes in the bucket. You can click on the arrow image to see the snapshots in the volumes.



Select the bucket that has the snapshot images you want to roll back and click **Next**.

### Configure Pool

Select an existing pool or create a new one. The disaster recovery process will create a new volume that claims capacity from the pool and then import the snapshot image to the new volume.



### Parameters

#### Pool Name

Enter a unique name for the volume.

#### Storage Tiering & Tier Index

Disable or Enable.

For more information about storage tiering, click a pool in the Device sidebar. Click the Help icon at the top-right corner, and look for **Storage Tiering**.

---

<b>RAID Level</b>	<p><b>RAID 0:</b> at least 2 drives (best performance but no data protection).</p> <p><b>RAID 1:</b> at least 2 drives (average performance with excellent data protection).</p> <p><b>RAID 5:</b> at least 3 drives (improved performance with improved data protection).</p> <p><b>RAID 6:</b> at least 4 drives (improved performance with excellent data protection).</p>
-------------------	---

---

<b>Write Policy</b>	<p>Set the write cache policy for this pool.</p> <ul style="list-style-type: none"> <li>● Default: The write cache policy follows system setting.</li> <li>● Write-Back: Write data will be stored into the cache memory first and will be written into the disk drive later.</li> <li>● Write-Through: Write data will be stored into the disk drive directly.</li> </ul> <p>The Write-Back and Write-Through setting overrides the write cache policy for the system.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>When a critical event occurs, the write policy may automatically switch to the more conservative Write-Through.</p> </div>
---------------------	--

---

<b>Assignment</b>	Specifies which controller (Slot A or Slot B) this pool will be assigned to. (This option is only available with PAC Storage PS/PSV devices)
-------------------	--

---

<b>Stripe Size</b>	Specifies the stripe size of the array.
--------------------	---

---

<b>SED Security</b>	Specifies whether you want to protect the member drives with SED (Self Encrypting Drives) security.
---------------------	---

- Before enabling this option, the following requirements should be met:

  - A SED authentication key is created
  - All member drives support SED.
-

## Configure Volume

Users can choose to restore all data in the selected bucket or choose to restore specific volumes.

**Disaster Recovery**

**Configure Volume**  
You can restore all data or select some volumes from cloud for disaster recovery.

☐ Restore all data from cloud directly.   
☒ Select the specific volume(s) for directly fully restored. Restore all others later using cloud gateway policy.

Total selected: 0

Volume Name	Volume Size	Total/Uncompressed Size
Volume_1	10 GB	0 Byte

Snapshot name	Used Size	Size	Created time
<input checked="" type="checkbox"/> Snapshot_20160930_174240	0 Byte	10 GB	2016/9/30 9:43:14

Previous Next Cancel

## Event Log

The PAC Storage User Interface Firmware provides a history of system events (**System log**), user actions (**Action log**), and file access (**Data access log**). You can choose to display the history information, or export it to the local computer by going to **Settings > System> System Information> System logs**.

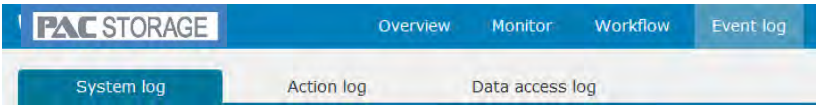
### Types of Events

Events can be categorized by (1) their scope and (2) their severity. For the detailed list of events and their descriptions, see the Troubleshooting Guide. Contact Support to obtain the guide.

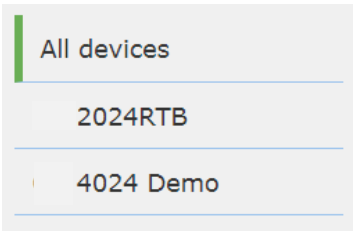
Scope of Events	Event Type	Scope
	Controller Event	the events related to the storage system controllers
	Drive Event	the events related to the physical disk drives
	Host Event	the events related to the host computer and host ports
	Logical Drive Event	the events related to logical drives and logical volumes
	System Event	the events related to the overall storage subsystem
	Schedule Event	the events related to the schedule tasks of storage system controllers
Severity of Events	Severity	Description
	Critical error	Users should pay immediate attention to the events and perform required actions.
	Error	Users should pay attention to the events and perform required actions.
	Warning	Users should pay attention to the events.
	Information	Users are notified of non-critical changes in system status.



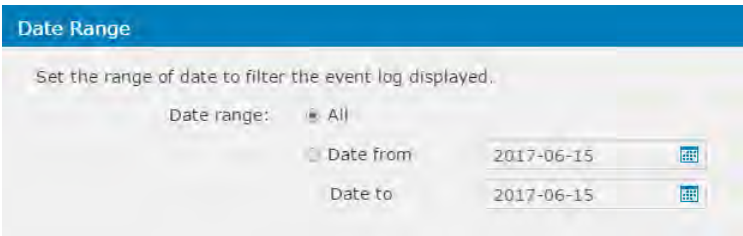
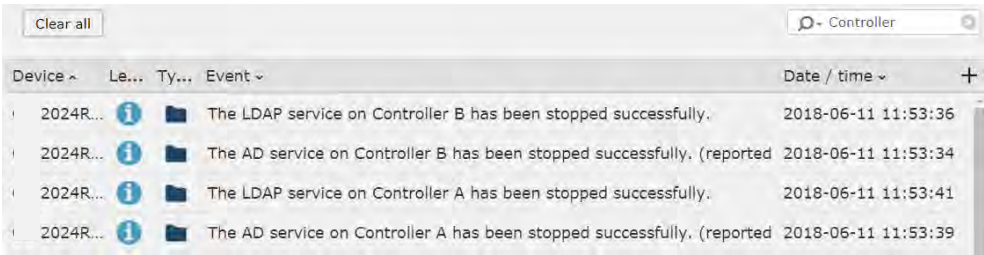
Go to **Top menu bar > Event Log > System Log**



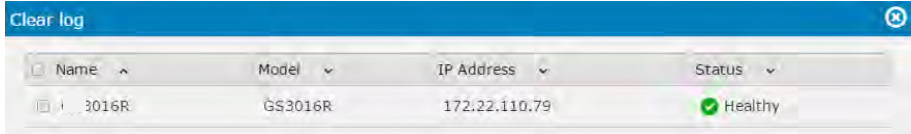
**System log** 1. Select a specific device or all devices by default.



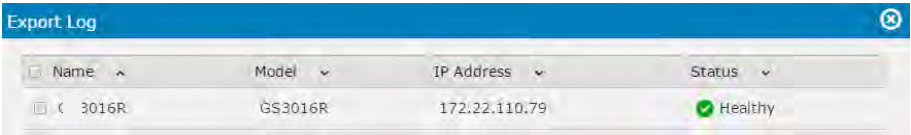
2. You can use the search bar to display certain events.



**Clear system log** Click the **Clear all** button, select the device(s), and click **OK**. The system log of the device(s) will be cleared.



**Download system log** Click the **Download** button, select a device and click **OK**. The PAC Storage User Interface Firmware will start downloading the system log of the device as a .zip file.



## Event Login Log

When user log into PAC Storage User Interface Firmware, the Event log will show the history of the user login:

Event log		Event: All events
	User admin logged in from 172.28.10.91	(reported by slot A)
	User admin logged in from 172.22.10.25	(reported by slot A)

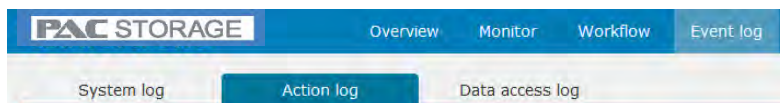
If failed to log in the following message will be displayed:

Event log		Event: All events	Error	Warning	Information
	User Jack failed to logged in from 172.27.12.120	(reported by slot A)			2018-06-25 11:08:08
	User yichun failed to logged in from 172.27.12.120	(reported by slot A)			2018-06-25 11:08:01

## Action Log

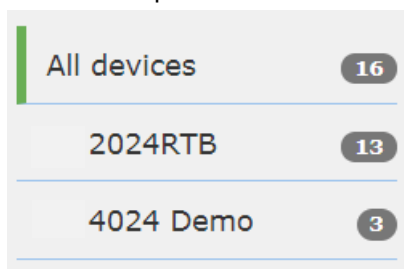


Go to **Top menu bar > Event Log > Action Log**

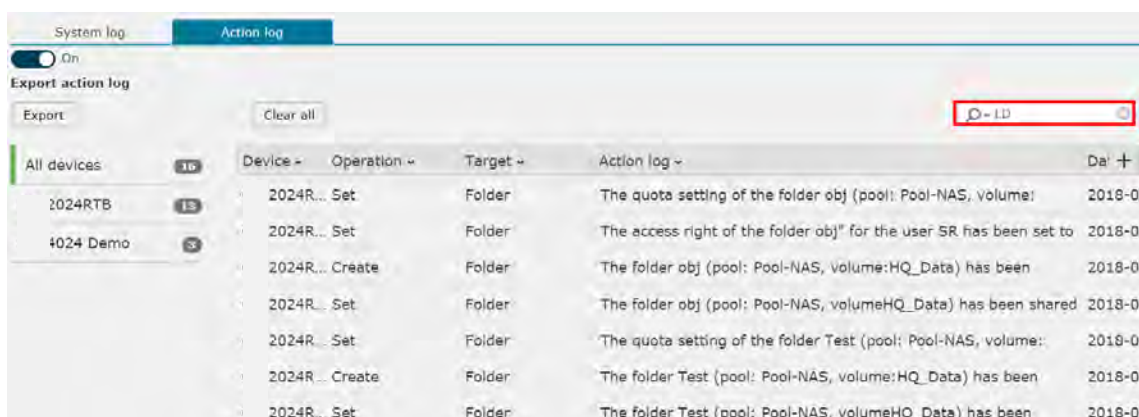


**Action log**

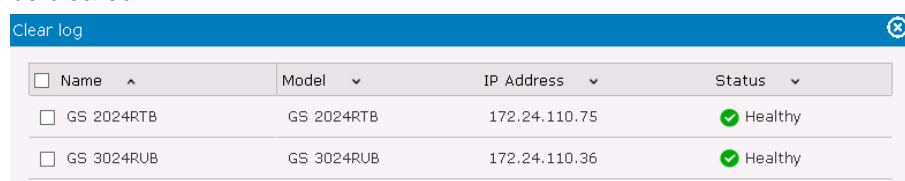
1. Turn on the switch on the upper left corner
2. Select a specific device or all devices by default.




3. You can use the search bar to display certain events.



**Clear action log** Click the **Clear all** button, select the device(s), and click **OK**. The action log of the device(s) will be cleared.



**Export action log** Click the **Export** button  , select a device and click **OK**. PAC Storage User Interface Firmware will start downloading the action log of the device as a .zip file.



## Data Access Log

Note:

**Go to**                      **Top menu bar > Event log > Data access log**

### Steps

1. Go to the left panel and click on a desired storage device. All file access to the storage device is listed.

Before checking data access logs, make sure you have finished the setup in **Settings > System > General > Data access log**.

2. From an access log record, you can check the following information:

<b>File protocol</b>	The file protocol used for accessing file data
<b>Time</b>	The time when the access event occurs
<b>IP address</b>	The accessing user's IP address
<b>Username</b>	The accessing user's PAC Storage User Interface Firmware username
<b>Action</b>	The file operation performed on file data
<b>File path</b>	The location of accessed file data

3. You can manage data access logs with the following buttons:

<b>Export</b>	Export all access logs into a .csv file.
<b>Clear all</b>	The system erases all access logs.
<b>Refresh</b>	The system updates access logs to the latest state.

- You can only view data access logs on Central PAC Storage User Interface Firmware.
- To properly display exported log contents, open the exported file in UTF-8.

# Service Manager

Service Manager provides proactive technical support for your storage system. It automatically creates a monitoring connection with PAC Storage Service Center so that the center can check system health in real time. When the connection is lost or a critical event occurs on PAC Storage PS/PSV, Service Manager can automatically send a service request to PAC Storage Service Center with related system information for diagnosis. PAC Storage Service Center will react to the reported issue and provide a resolution within a minimal time span.

A critical event can be a failure of a fan, BBU, PSU, controller or drive. Related information for diagnosis by PAC Storage Service Center may include contact information, product information, system logs and configurations, as well as core dumps.

You will need to configure Service Manager in the Initial Setup Wizard when you log in to PAC Storage User Interface Firmware for the first time.



## **Configure Service Manager**

**Go to**                      **Settings > System > Service Manager Settings**

(Service Manager Settings can also be accessed through **Initial Setup Wizard**)

**Configure  
Service  
Manager  
Settings**

1. Enable Service Manager with the toggle. Service Manager automatically connects with PAC Storage Service Center for a daily check on system health.

Click on the switch bar to turn on Service Manager



Fill in your contact information.

2. We recommend you enable the option **I agree to automatically notify PAC Storage when critical events occur**. The system will automatically create a support ticket to PAC Storage Service Center when any critical errors occur.
3. We also recommend you enable the option **I agree the requests from PAC Storage support engineers to transmit system information for troubleshooting**. Upon request, the system will send out relevant information (i.e., logs, system configurations, and core dumps) for diagnosis to PAC Storage and a notification to you. No private data on your storage will be accessed.
4. Press **Save** button at the bottom of the page to save the Settings. After that, you can also verify the Settings by pressing the **Send test ticket** button.

Note that before sending the test ticket, you have to configure the SMTP server and email notification in Notification Settings to ensure the notification can be successfully created by your PAC Storage PS/PSV storage system.

**Parameters**

<b>Name</b>	Fill in this field with the name of the person PAC Storage should contact.
<b>Company</b>	Enter the name of your company. This field is optional.
<b>Email</b>	Fill in this field with the email address to receive notifications. This field is required.
<b>Office / Mobile phone</b>	Fill in this field with the person's office or mobile phone number.
<b>Country</b>	Select your location. This field is required.

---

If a warning window pops up please contact support.

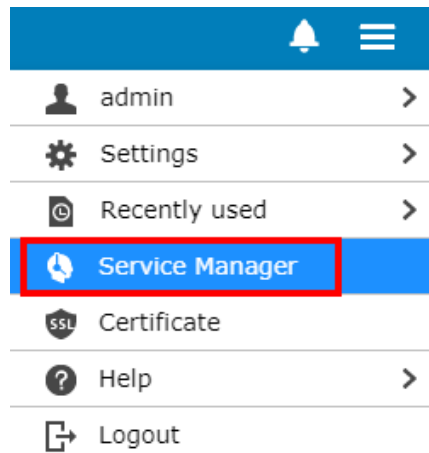
---

## Service Manager Status

After configuring Service Manager setting, you can access Service Manager from the PAC Storage User Interface Firmware main menu. From here you can send service request and track your ticket easily directly via Service Manager.

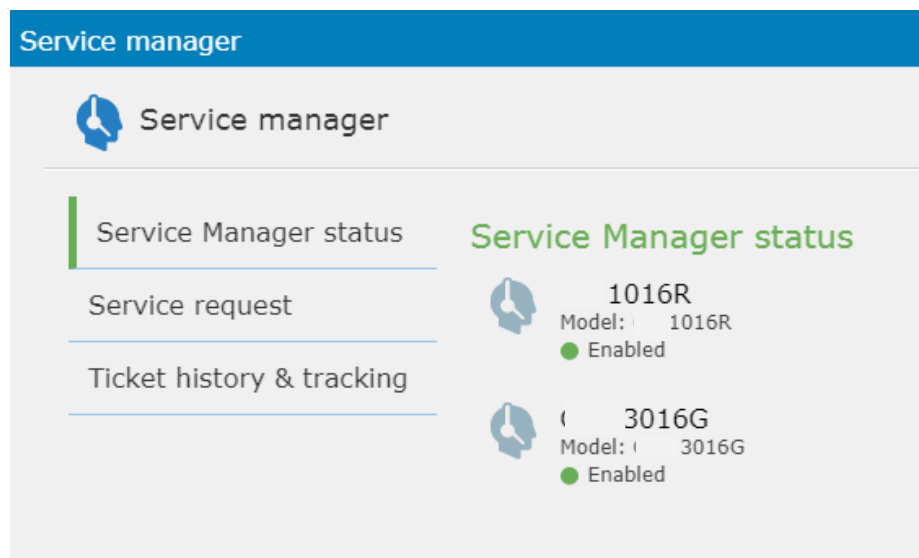
Go to

Main menu > Service Manager



### Service Manager Status Management

Once you have accessed to Service Manager, you may find the Service Manager status of your storage system. For the Embedded PAC Storage User Interface Firmware, you may only see the status of the storage model that you are using; for the Central PAC Storage User Interface Firmware, you may see the status of multiple devices.



You can select a model to examine the status of its service manager and



action to critical events. There are five statuses you can find on the PAC Storage User Interface Firmware.

<b>Service Manager Status</b>	<b>Status Color</b>	<b>Action to Critical Events</b>
Enabled	Green	If a critical event is encountered, you will be notified by the Service Manager, a ticket will be automatically sent to PAC Storage Service Center via internet, you can track the ticket information in the Ticket history & Tracking page.
Enabled, no Internet connection, but you can send emails to PAC Storage Service Center automatically	Yellow	If a critical event is encountered, you will be notified by the Service Manager, a ticket will be automatically sent to PAC Storage Service Center via email. Since there's no internet, you cannot track ticket information in the Ticket history & Tracking page.
Enabled, but not allowed to send emails to PAC Storage Service Center automatically	Orange	If a critical event is encountered, the Service Manager will send you an email with support ticket information, you can then send the email to PAC Storage Service Center for instant help from our technical support engineers. Since Service Manger will not notify PAC Storage automatically, therefore the Ticket history & Tracking function is unavailable.
Enabled, but no connection to PAC Storage Service Center	Red	Service Manager is unable to connect to PAC Storage Service Center, please check your SMTP server Settings.
Disabled	Grey	Enable Service Manager at Settings > System > Service Manager Settings

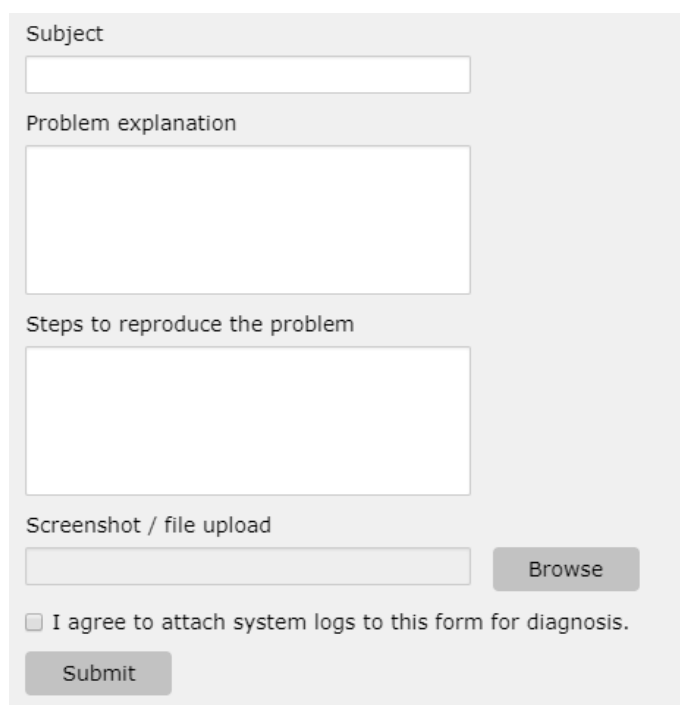
## Service Request

Here you can manually submit a service request or issue ticket to PAC Storage Service Center by filling in relevant information.

**Go to**                      **Main menu > Service Manager > Service request**

### State a Request or Issue

1. Select the device name from the drop-down list.
2. Please check the contact email address for the device. If you wish to modify your contact email address, please go to the Service Manager Settings page.
3. Fill in the information of your problem or request. You can also upload screenshots or other files to illustrate the problem.



The screenshot shows a web form for submitting a service request. It includes the following fields and elements:

- Subject:** A text input field.
- Problem explanation:** A large text area for describing the issue.
- Steps to reproduce the problem:** A text area for providing steps to reproduce the problem.
- Screenshot / file upload:** A text input field for a file path, accompanied by a **Browse** button.
- Agreement:** A checkbox labeled "I agree to attach system logs to this form for diagnosis."
- Submit:** A button at the bottom of the form.

4. Check the box **I agree to attach system logs to this form for diagnosis**. Click **Submit** to save and send the service request to PAC Storage Service Center.

Parameters	Model	Model name of the storage system. This information is retrieved automatically and is read-only.
	Serial number	This information is retrieved automatically and is read-only.
	Service ID	This information is retrieved automatically and is read-only.

	The ID is displayed in 7 decimal digits.
<b>Firmware version</b>	The current firmware version. This information is retrieved automatically and is read-only.
<b>Subject</b>	Fill in this field with the subject of your service request. This field is required.
<b>Problem explanation</b>	Describe the problem here. This field is required.
<b>Steps to reproduce the problem</b>	Describe the steps to reproduce the problem.
<b>Screenshot / File upload</b>	Upload a screenshot or other files illustrating the problem. Click <b>Browse</b> to select the files to upload.

## Ticket History & Tracking

You can see a list of the service tickets, check their status or close tickets. Note that the internet connection is required to show the ticket status.

### Go to

Main menu > Service Manager > Ticket history & tracking

### Display ticket(s)

You can click the drop-down menu above the Ticket No. column to choose to display all tickets, active tickets or closed tickets.

You can check all issued tickets and their status here. To show the status, internet connection is required.

<input type="checkbox"/> Ticket no. ^	Issue date v	Description v	Status v
<input type="checkbox"/> ALE-060463	2017/09/07 08:45:43	Controller B shutdown due t...	Closed
<input type="checkbox"/> BBX-508597	2017/09/07 07:19:17	LD:72FC51F0 Logical drive ...	Closed

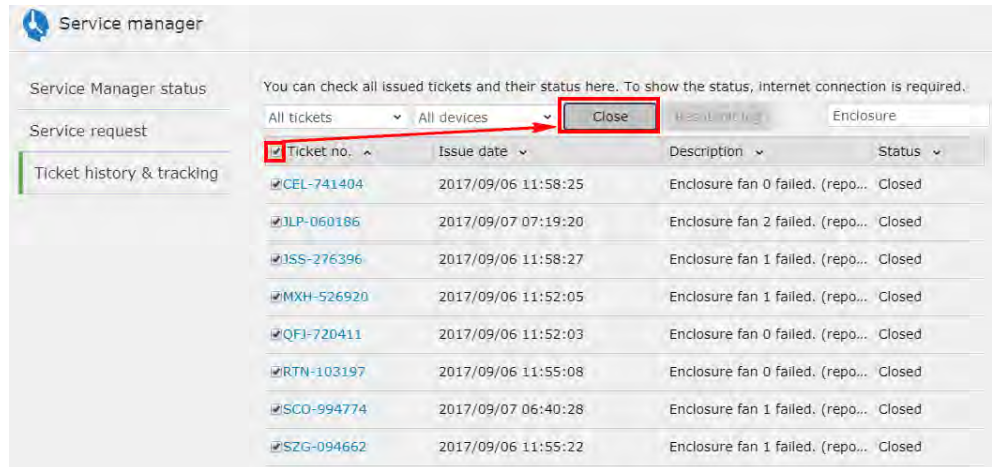
You can also enter a key word in the search ticket box to look up tickets. If the description contains the key word you entered, the ticket(s) will be listed in the table.

You can check all issued tickets and their status here. To show the status, internet connection is required.

<input type="checkbox"/> Ticket no. ^	Issue date v	Description v	Status v
<input type="checkbox"/> CEL-741404	2017/09/06 11:58:25	Enclosure fan 0 failed. (repo...	Closed
<input type="checkbox"/> JLP-060186	2017/09/07 07:19:20	Enclosure fan 2 failed. (repo...	Closed
<input type="checkbox"/> JSS-276396	2017/09/06 11:58:27	Enclosure fan 1 failed. (repo...	Closed

### Select & close ticket(s)

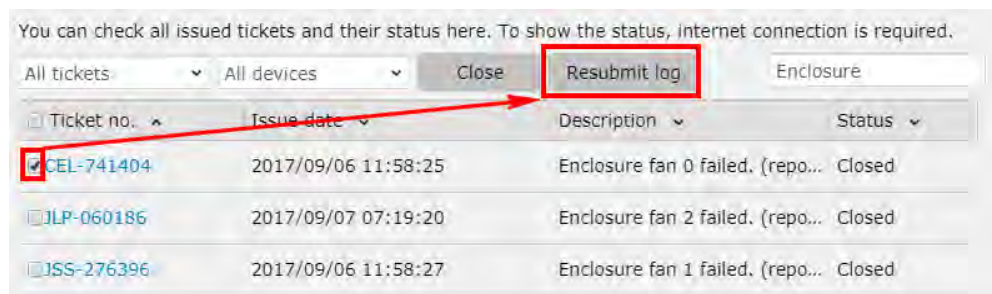
You can select one or more tickets by clicking the box next to the ticket number. You can select all tickets by clicking the check box next to the title Ticket No. Then, you can click **Close** to close the selected ticket(s).



Note: When the user closes a ticket, the status will be synchronized to PAC Storage Service Center if Internet connection is available. Otherwise, the system will retry the operation "update status to server" when Internet connection is up or until the ticket expires.

### Resubmit system logs

When needed, you can resubmit system logs to PAC Storage Service Center for a specified ticket. Select the ticket and click **Resubmit log**.



### Ticket Status

Each ticket can have one of the four statuses:

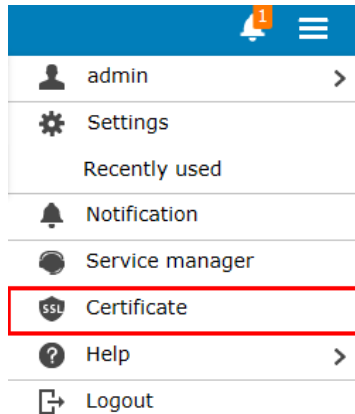
- **New:** PAC Storage Service Center has received the request.
- **Opened:** PAC Storage Service Center has accepted the request and is currently processing it.
- **Wait for customer:** The replacement unit is being sent to the customer. PAC Storage Service Center is waiting for the customer's confirmation.
- **Closed:** The issue has been resolved.

The status is available only if your system has Internet connection.

## Configure Web Certification

Go to

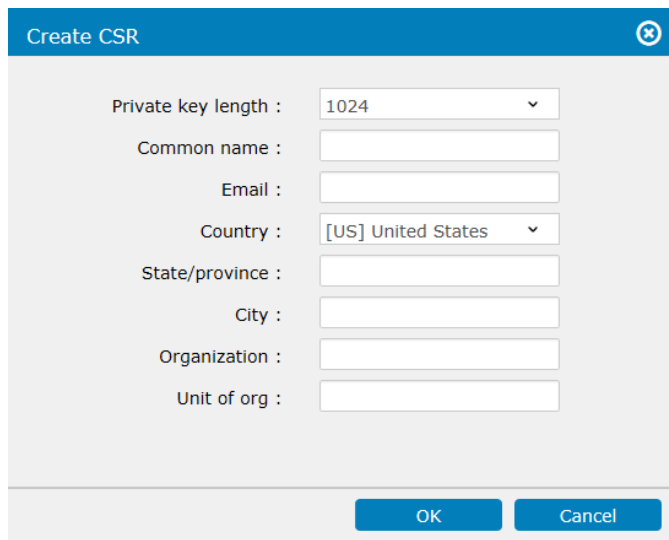
Main menu > Certificate



Click Certificate and you will be directed to see Create CSR, Import Certificate buttons and Server Certificate status.

### Create CSR

Click this button to display CSR page where users are required to fill in necessary information to request for a CSR authorization.



The 'Create CSR' dialog box contains the following fields:

- Private key length : 1024 (dropdown menu)
- Common name : (text input)
- Email : (text input)
- Country : [US] United States (dropdown menu)
- State/province : (text input)
- City : (text input)
- Organization : (text input)
- Unit of org : (text input)

At the bottom right, there are 'OK' and 'Cancel' buttons.

**Private key length:** Select the key length parameter from the scroll down list, available options are 1024,2048 and 4096. (factory default is 1024)

**Common name:** Enter the name for your CSR. (maximum words:64)

**Email:** Enter a valid and email address with correct format.

**Country:** Select your country from the scroll down list.

**State/province:** Select the correspondent state/province.

**City:** Select your city.

**Organization:** Enter the organization (maximum words: 64)

**Unit of org:** Enter Unit of Organization (maximum words: 64)

Press **OK** to submit CSR file. Note: if the entered information has an error, or column is left blank, the **OK** button will become unavailable, please ensure all information is filled.

Press **Cancel** to cancel all action and return to Certification Menu

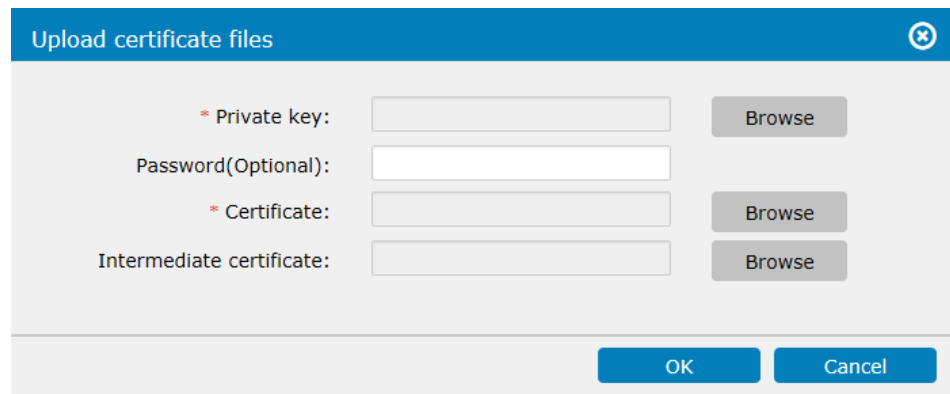
After submitting the CSR, you will see:

Press **Download** to start downloading csr.zip file (note that different browsers come with different way of downloading)

Press **Close** to return to Certification Menu (note that if proceed, data will not be saved, you must re-initialize the request again)

## Import Certificate

Select the Import Certificate button, you will be directed to Upload Certificate Files page, then fill in the credentials as below:



**Private key:** Click the Browse button, search for the file path of your Private key --  
\*this field is required

**Certificate:** Click the Browse button, search for the file path of your Certificate downloaded (.crt and .cer file format types are supported)--\*this field is required

**Intermediate certificate:** Browse the file path of your intermediate certificate.

**Upload:** press upload button to upload file (this function is unavailable if one of Private key and Certification is left blank)

**Cancel:** press cancel to remove all entered fields and return back to Certification Menu

**Back:** Click this button to return to Upload certificate files

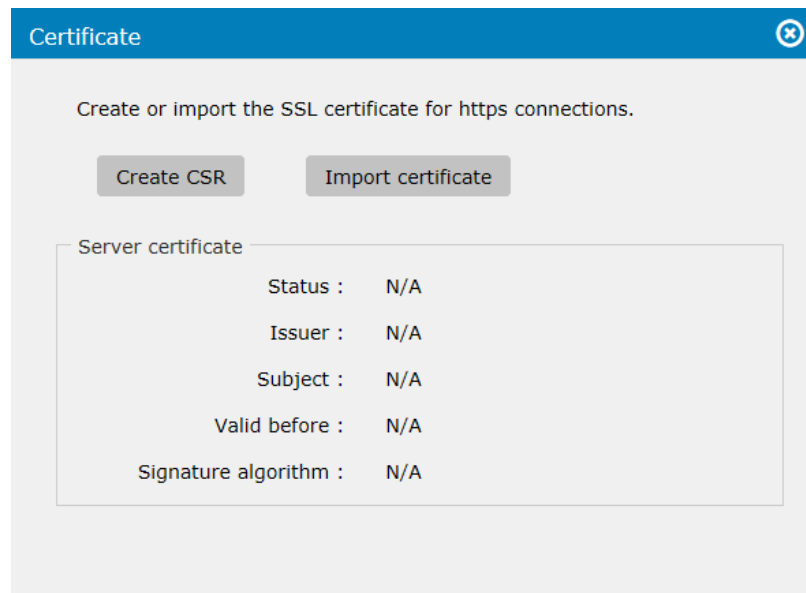
Once uploading the certificate onto your PS model, a window will be displayed with the information: **"The existing certificate will be replaced by the one below. Are you sure to import this certificate?"**

**OK:** Press OK to confirm, if an error occurs, a pop up window will appear showing "The certificate is invalid. Please check your certificate files"

**Cancel:** Click this button to cancel all action and return to Certification Menu

## Server Certificate

Once you have imported a certificate, the Server Certificate will display it's relevant information (Note that if no certificate is imported, Server Certificate will display all information with N/A.



Server certificate	
Status :	N/A
Issuer :	N/A
Subject :	N/A
Valid before :	N/A
Signature algorithm :	N/A



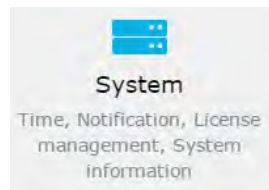
# System

The system setting menu contains the following sub-Settings.

1. General Settings
2. Time and Date Settings
3. Notification
4. Service Manager Settings
5. License Management
6. System Information
7. SED key management
8. Maintenance
9. Power
10. Enclosure View


**Go to**

**Settings > System**



---

## System Setting Menu

The System Setting menu for the chosen device will appear. Users can switch to the sub-setting pages or click  [Settings](#) to go back to the previous setting page.

## General

**Go to** Settings > System > General

- Steps**
1. Go to the **System administration** section.
  2. Click on a suitable button to manage the system:
    - **Restart system:** Click to restart the whole system.
    - **Shut down system:** Click to shut down the whole system.
  3. For dual-controller models, you can click **More** to manage each controller:
    - **Stop controller A:** Click to shut down controller A.
    - **Stop controller B:** Click to shut down controller B.
    - **Run both controllers:** Click to restart both controllers.

### Device Name

Users can modify the name of the storage device.



**Device name**  
Device name is for identification when configuring multiple devices.

3016R

Apply

**File server name**  
To access shared folders via CIFS/SMB, AFP, NFS, etc., please enter the file server name (e.g. NAS85\_A in PC Windows Explorer, and smb://NAS85\_A or afp://NAS85\_A in Mac Finder).

Controller A:  
NAS\_1123457\_A

Controller B:  
NAS\_1123457\_B

Apply

---

## Data Access Log

The system can record all access to stored file data for close monitoring.

1. Turn on the switch.
2. Select a local shared folder as a database to store all access logs.
3. Set a maximum number of retained access logs.
4. Select one or more file-level protocols to record their data access: **CIFS/SMB**, **FTP**, and **SFTP**.
5. Click **Save**. All data access logs are available in **Event log > Data access log**.

The screenshot shows the 'Data access log' configuration window. At the top, the title 'Data access log' is in green. Below it, a message says 'Enable this function to record all data access to this storage device.' followed by a toggle switch set to 'On'. There are three main sections: 'Database' with a dropdown menu showing '/pool1/FileVolume/Ifolder001'; 'Maximum retained logs' with a text input field containing '1000000'; and 'File protocol' with three checkboxes: 'CIFS/SMB' (checked), 'FTP' (checked), and 'SFTP' (unchecked). A 'Save' button is at the bottom.

---

## File Server Name

Users can modify the name the file server. For dual controller storage devices, the file server name will be displayed with -A and -B to differentiate between the two controllers.

To join the storage device to any Windows Active Directory (AD) domain, do not include any underline (\_) characters in the file server names.

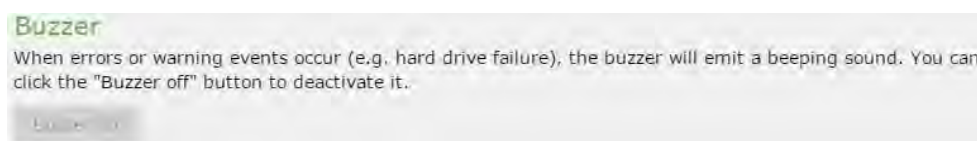
---

---

### Buzzer

Each storage system or expansion enclosure contains a hardware beep mechanism to notify users when system errors or hardware failures occur. You may directly mute the sound on the hardware (please refer to the hardware manual for details) or remotely through the user interface.

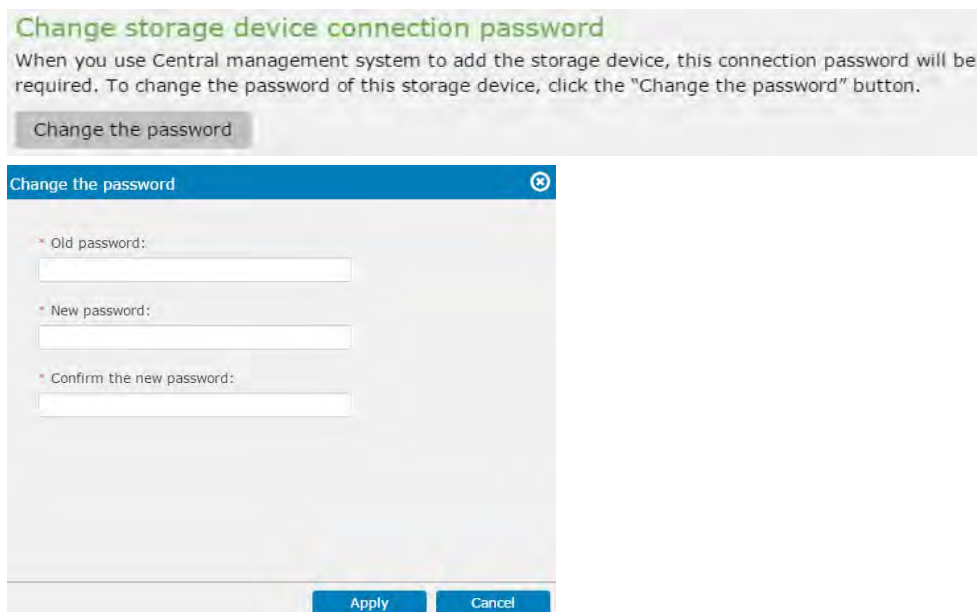
Note: You can only mute the currently beeping sound and cannot disable the buzzer setting from the user interface.



---

### Password Change

Click the **Change the Password** button and input the old and the new passwords to modify the login password for accessing the PAC Storage PS/PSV through the Central PAC Storage User Interface Firmware.



---

### Performance Optimization

Allocate more system resource to a specific data service to optimize its read and write access. Select either option: **Better performance for file access service** and **Better performance for block data access**.

---



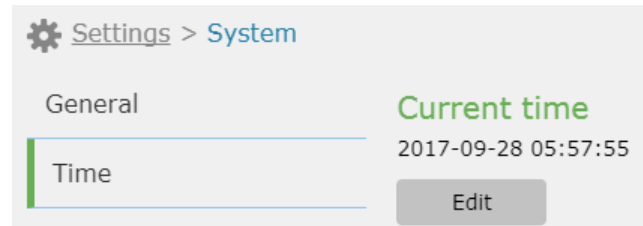
## Time Settings

Go to

Settings > System > Time

### Time Settings

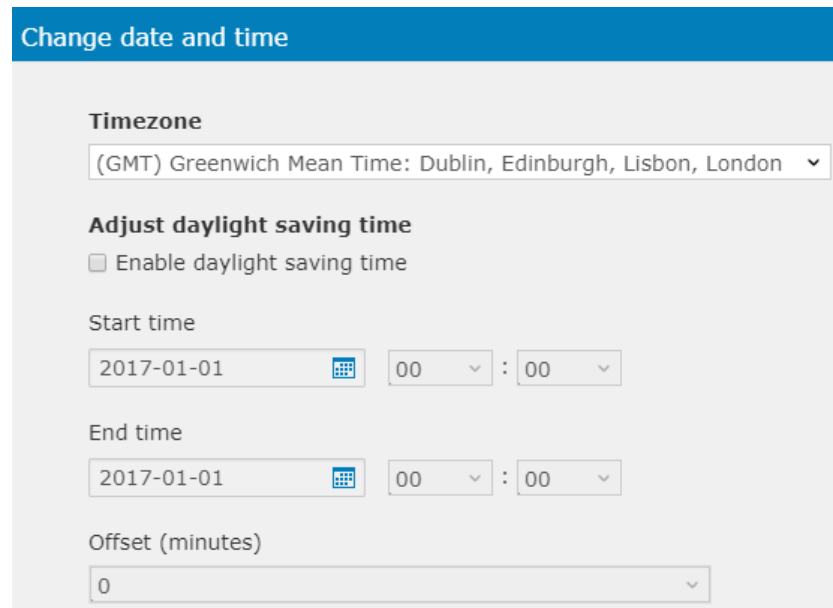
You can click the **Edit** button to set the device time by either changing the time zone or manually modifying the date.



### Change Date and Time

1. Select the time zone where your storage system is located.

You can also enable daylight saving time by checking the **Enable daylight saving time** below. Configure the start time, end time, and offset of the daylight saving



2. You can either manually set the time Settings or synchronize the time with the NTP server.

To manually set the system time, select **Manual Settings**. Then, specify the date and time in the fields.

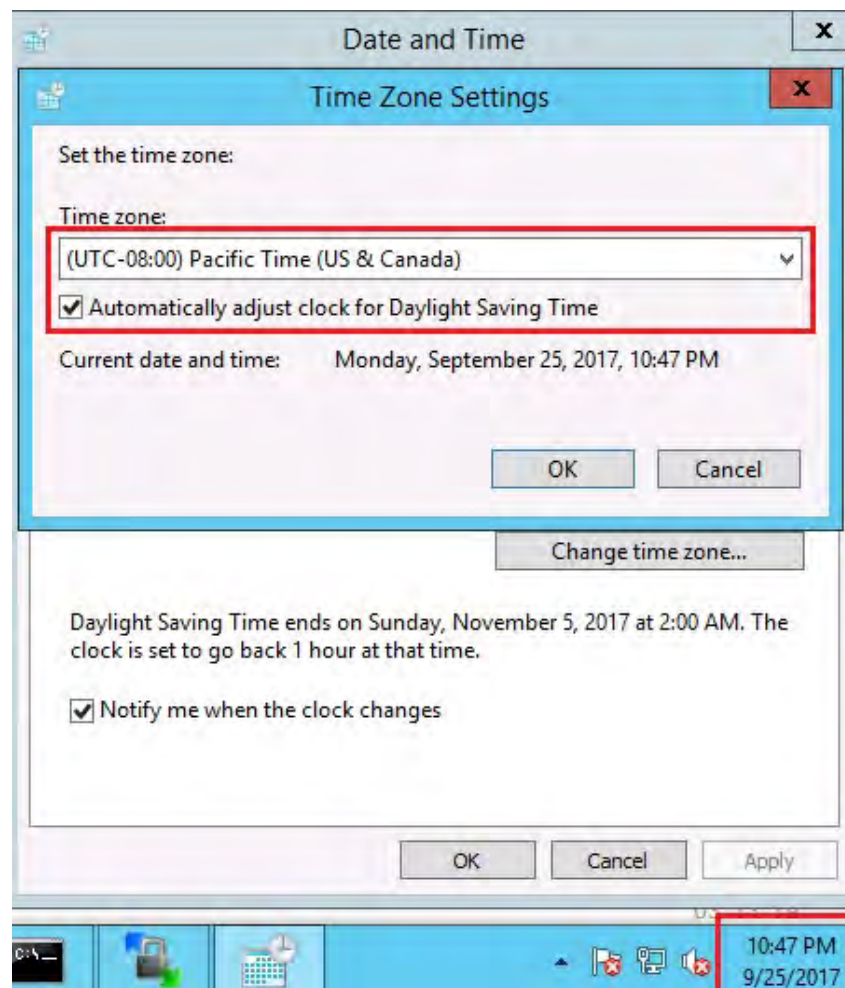
To synchronize system time with an NTP server, select **Synchronize with NTP server**. Go to the **Network time server** menu. Select an NTP server or **Customize** if you want to use a custom NTP server. Then, specify

**Polling period** to regularly calibrate system time with the NTP server.  
Then, click **Update now** to start time syncing.

3. Press **Apply** to save the Settings.

## Daylight Saving Time

To set the Daylight Saving Time on your system, you must first set your server time on your local computer. Go to **Windows**, at the right bottom of the bar click Date and Time, and then select **Change time zone** button. Remember to tick “Automatically adjust clock for Daylight Saving Time” box.



Now open your PAC Storage User Interface Firmware software and go to **Settings > System > Time** and press **Edit** button.

1. **Change date and time** -- Scroll down and go to **Change date and time**, then enable Manual Settings. Under manual Settings you should set your server time, not daylight saving time. For example: if your clock indicates 10:49PM, please set to 9:49PM.

**Change date and time**

☐ Manual settings

Date

2017-09-30

Time

17 : 07

2. **Adjust daylight saving time** -- Scroll up again, and locate **Adjust daylight saving time**, please enable Adjust daylight saving time switch button at this stage.

**Adjust daylight saving time**

☒ Enable daylight saving time

Start time

2017-01-01 00 : 00

End time

2017-01-01 00 : 00

3. **Offset** -- Enter **Offset value** (minutes) to 60, then press **Apply**.

Offset (minutes)

0

Apply Cancel

After a few seconds, the Current Time on your software will match the server time on your computer.

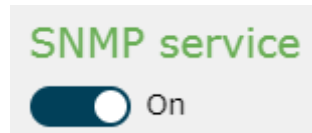


Go to

Menu > Settings > System > Notification > SNMP

### SNMP Notification

1. Enable SNMP notification by clicking the switch button. (You must first turn on SNMP service for any further SNMP Settings)



2. Enable one of the SNMP support version. You can also enable both SNMPv1 and SNMPv3 at the same time.

A screenshot of the SNMP configuration interface. At the top, there are tabs for 'Email' and 'SNMP'. The 'SNMP' tab is selected. Below the tabs, the title 'SNMP service' is in green. There is a toggle switch labeled 'On'. Below the toggle, there are two checked checkboxes: 'Enable SNMPv1 support' and 'Enable SNMPv3 support'. Under 'Enable SNMPv1 support', there is a field for 'Community' and a button with a plus sign labeled 'Add SNMPv1 trap receiver'. Under 'Enable SNMPv3 support', there is a field for 'Username', a dropdown menu for 'Authentication protocol' set to 'None', and a field for 'Authentication password'.

### Enable SNMPv1 support

1. Click the **Enable SNMPv1 support** check box to activate the SNMPv1.
2. Enter the **Community** information.
3. Click **Add SNMPv1 trap receiver** to add a trap server.
4. Enter the **Receiver IP address** and select the **severity** level to complete the Settings.

A screenshot of the 'Add receiver IP address' form. The title 'Add receiver IP address' is in a blue header. Below the header, there is a field for 'Receiver IP address' with a placeholder 'IP address'. To the right of this field is a dropdown menu for 'Severity' with the text 'Critical error + Error + Wa...'.

5. Press **Save** button at the bottom of the page to save the Settings. You can also verify the Settings by pressing the **Test SNMP trap** button.

<b>Parameters</b>	<b>Community</b>	<p>The password of the SNMP.</p> <p>Minimum / Maximum length of the community name: 1 / 31 digits.</p> <p>Note that the name must not contain any punctuation marks such as quotation mark, vertical bar and comma.</p>
<b>Enable SNMPv3 support</b>	<ol style="list-style-type: none"> <li>1. Click the <b>Enable SNMPv3 support</b> check box to activate the SNMPv3.</li> <li>2. Enter the <b>Username</b> of the SNMPv3 server.</li> <li>3. Select the authentication protocol of the SNMPv3 and the password.</li> <li>4. Select the privacy protocol of the authentication if needed.</li> <li>5. Click <b>Add SNMPv3 trap receiver</b> to add a trap server.</li> <li>6. Enter the <b>Receiver IP address</b> and select the <b>severity</b> level to complete the Settings.</li> </ol> <div data-bbox="478 1028 1161 1214" data-label="Form"> <p>Add receiver IP address</p> <p>* Receiver IP address: <input type="text" value="IP address"/></p> <p>Severity: <input type="text" value="Critical error + Error + Wa..."/></p> </div> <ol style="list-style-type: none"> <li>7. Press <b>Save</b> button at the bottom of the page to save the Settings. You can also verify the Settings by pressing the <b>Test SNMP trap</b> button.</li> </ol>	
<b>Parameters</b>	<b>Username</b>	The username for authentication. Maximum length: 31 digits.
	<b>Authentication Protocol</b>	Currently, the PAC Storage PS/PSV supports the <b>MD5</b> and <b>SHA-1</b> authentication. You can select the protocol in the drop-down list.
	<b>Authentication Password</b>	Enter the authentication password in the field. The minimum / maximum length is 8 / 16 digits.
	<b>Privacy Protocol &amp; Privacy Password</b>	<p>Select the privacy protocol in the drop-down list, which includes the <b>DES</b> and <b>AES-128</b>, and enter the privacy password.</p> <p>The privacy protocol field is enabled according to the <b>Authentication Protocol</b> and its</p>

---

minimum / maximum password length is 8 / 16  
digits.

---

## License Management

If you have any license-related issues (local and remote replication) with your subsystem, please contact your dealer.

**Go to** **Settings > System > License management**

### License Types

You will need to apply for or download a license key to use the following features in the PAC Storage PS/PSV series. A Standard License is provided for free for all users and is preloaded in your PAC Storage PS/PSV devices. An Advanced License may need to be additionally purchased.

Feature/Functionality	License Type
Standard Local Replication	Standard License
Expansion Enclosure Connection	Standard License
Thin Provisioning	Standard License
Advanced Local Replication	Advanced License
Remote Replication	Advanced License
Automated Storage Tiering	Advanced License
SSD cache pool	Advanced License
Cloud Gateway	Standard/Enterprise/Ultimate License

### Notes

- When your license expires, apply for a license renewal.
- When you have upgraded your features, apply for a license upgrade.
- If you want to try out the advanced license features for 30 days, apply for a Trial License.
- It is required to reset the system for the license to take effect after a license is installed.

## Generating a License Application File

The License Application File is needed when upgrading/renewing PAC Storage PS/PSV licenses. Users need to upload the License Application File to the license website, download the upgraded/renewed license and then reload the new license onto PAC Storage PS/PSV via PAC Storage User Interface Firmware.

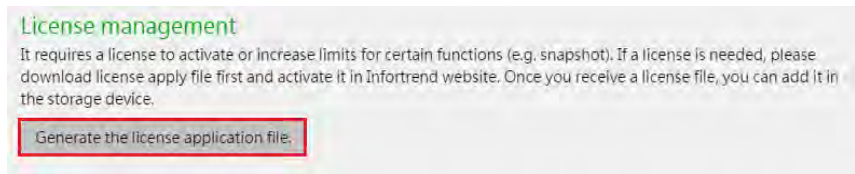
Before starting any PAC Storage PS/PSV license process, please make sure PAC Storage 's PAC Storage User Interface Firmware management suite shipped together with the PAC Storage PS/PSV storage system has been properly installed.

---

**Go to**                      **Settings > System > License management**

---

**Steps**                      In the License Key window, click **Generate License Application File**.



Download will start immediately and the file will be saved automatically in your computer.

## Generating an Advanced License

An advanced License is required to access the following features:

- Advanced local replication
- Remote replication
- Automated storage tiering
- SSD cache pool
- Cloud Gateway

You can try out these features for 30 days using the Trial License before making a purchase decision.

---

**Steps**                      1. Contact PAC Storage sales team.

2. At the **Product Family** drop-down menu located at the top right corner, select PAC Storage PS.

3. Then at the left column under **Licensing Service**, click **License Activation**.



4. Upload the License Application File you obtained through PAC Storage User Interface Firmware and click **Next**.

License Apply File	Choose File 55_LicenseApplyFile.bin
--------------------	-------------------------------------

**Next**

5. Fill in the License Serial Number you received and click Add. After adding the License Serial Number, click **Next**. You can generate multiple licenses in a single activation process. Simply fill in another License Serial Number and click **Add**. The added licenses will be listed in the **License** box.

License Serial Number	<input type="text"/> <input type="button" value="Add"/>
	<small>(Enter one license code at a time)</small> <small>Please insert Add-on License Code.</small>
Licenses to be added	<div style="border: 1px solid #ccc; height: 40px;"></div> <input type="button" value="Remove"/>
Activated Licenses	<div style="border: 1px solid #ccc; height: 40px;"></div>

6. Click **Download** to receive the License Key File.

Save the License Key File at a preferred location and upload it to PAC Storage User Interface Firmware.

Please note it is required to reset the system for the license to take effect after it is installed.

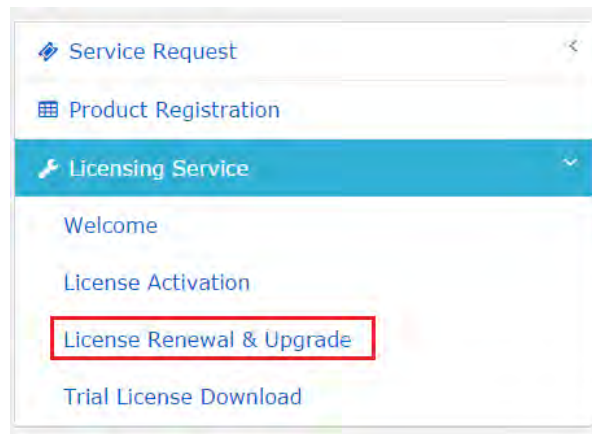
## Upgrading Standard License to Advanced License

The following introduces how to upgrade from a standard license to a new advanced license.

### Steps

1. Contact PAC Storage sales team
2. At the **Product Family** drop-down menu located at the top right corner, select PAC Storage PS.

1. If you have already purchased an advanced license, please click on **License Renewal & Upgrade** under **Licensing Service** at the left column.



4. Upload the License Application File generated through PAC Storage User Interface Firmware and click **Next**.

License Apply File

Choose File

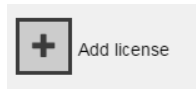
55\_LicenseApplyFile.bin

Next

5. Check whether the listed licenses are the ones you have purchased. If not, contact support.

6. Click **Download** to receive the License Key File and save the License Key File at a preferred location and upload it to PAC Storage User Interface Firmware.

- Click the Add License button in the License Management page and upload the License Key File.



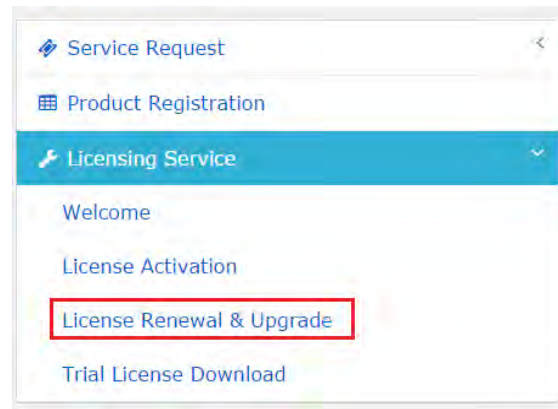
Please note it is required to reset the system for the license to take effect after it is installed.

## Renewing License

If you have lost a previously generated License Key File, you can regenerate it through contacting your sales team.

### Steps

- Visit PAC Storage's sales team for more information.
- At the **Product Family** drop-down menu located at the top right corner, select PAC Storage PS.
- Click on **License Renewal & Upgrade** under **Licensing Service** at the left column.



- Upload the License Application File generated through PAC Storage User Interface Firmware and click **Next**.

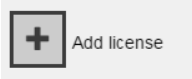
License Apply File
 
 55\_LicenseApplyFile.bin

Next

- Check whether the listed licenses are the ones you have purchased. If not, contact support.



6. Click **Download** to receive the License Key File and save the License Key File at a preferred location and upload it to PAC Storage User Interface Firmware.
7. Click the Add License button in the License Management page and upload the License Key File.



Please note it is required to reset the system for the license to take effect after it is installed.

## System Information

Go to

Settings > System > System Information

### System Information

This page shows the information of the PAC Storage PS/PSV, including device configuration, channel configuration, CPU and controller temperature, and cooling fan speed status. For more detailed information, pull the scrolling bar to the bottom and click **View detailed configuration list**.

#### System information

Model:	3016R
Device name:	3016R
File server name:	NAS_1123457_A
CPU:	Intel CPU
Memory:	16 GB
System time:	2017-06-15 17:56:20 (GMT Beijing, Chongqing, Hong Kong SAR, Urumqi)
System up time:	0 days 7 hours 4 minutes 38 seconds
Service ID:	1123457
Controller ID:	74881 (0x12481)
Firmware version:	1.32A.51
Serial No.:	Slot A: 8884624 (0x879190), Slot B: 8884603 (0x87917B)
Channel 0:	iSCSI 10G Block-level Data Service (iSCSI) ● Controller A: -- ● Controller B: --
Channel 1:	iSCSI 10G Block-level Data Service (iSCSI) ● Controller A: -- ● Controller B: --
Channel 2:	iSCSI 1G Block-level Data Service (iSCSI)

Channel 3:	iSCSI 1G Block-level Data Service (iSCSI) ● Controller A: -- ● Controller B: --
Channel 4:	SAS 12G JBOD ● Controller A ● Controller B
Channel 5:	SAS 12G JBOD ● Controller A ● Controller B
CPU Temperature:	33.0 C / Temperature within safe range
Controller Temperature(1):	39.5 C / Temperature within safe range
Controller Temperature(2):	47.0 C / Temperature within safe range
Controller Temperature(3):	43.5 C / Temperature within safe range
Controller Temperature(4):	42.0 C / Temperature within safe range
Backplane Temperature:	29.0 C / Temperature within safe range
Cooling fan(1):	Cooling fan is in the third lowest speed
Cooling fan(2):	Cooling fan is in the third lowest speed

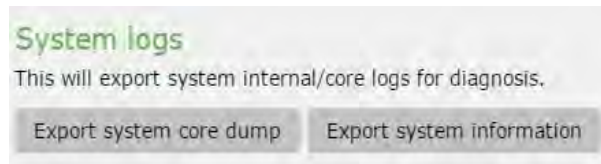
Cooling fan(3):	Cooling fan is in the third lowest speed
Cooling fan(4):	Cooling fan is in the third lowest speed

View detailed configuration list

---

**Export system  
information/coredump**

To export system information or the system coredump, click **Export system information** or **Export System Coredump**. Then, a zip file will be generated and it can be saved to the local host.



Within the system information file, you may find the various log files and a event service guide table document. Please refer to the event service guide to find the detailed information of the event logs.

Note: When a system error occurs, you may find the cause of the event via looking up the event ID from the "Event-Service\_Guide\_Table.docx" document.

---

## SED Key Management

You can create and manage a global encryption key to protect all logical drives on the storage device when they are made up of self-encrypting drives (SED).

Note:

- The system can only hold one global encryption key.
- Global encryption is unlocked after system reboot. To re-enable it, provide the global key file or enter the password again.
- If you disable encryption for a specific SED logical drive after setting up global encryption, previously-set global encryption turns ineffective.
- To encrypt a specific SED logical drive, refer to Protecting a Logical Drive with Self-encrypting Drives (SED).

Go to	Settings > System > SED key management	
Steps	1. Click on <b>Add an SED authentication key in the system.</b>	
	2. Select how to generate an SED authentication key:	
	<div> <b>Generate and download a key file from the system</b> </div>	<div> Click <b>Generate</b> to create a .key file that contains the SED authentication key.   Then, upload the key file for confirmation by clicking <b>Browse</b>.   You must keep this key in a secure place. This key cannot be recovered once lost. </div>
	<div> <b>Enter the key manually</b> </div>	<div> Enter a custom key and confirm it.   This key cannot be recovered once forgotten. </div>

Add an SED authentication key

### Add an SED authentication key

Name for this SED key :

3024RB(0)\_SED\_key

Select a way to create and store an SED authentication key in the system

☒ Generate and download a key file from the system (Type: File)

By clicking the "Generate" button below, a new "key" file will be downloaded. The system will require this key to delete/modify the SED key of this logical drive, or to unlock this logical drive when system reboots. This key file cannot be retrieve again, so it's highly recommend to download and keep this key file security.

Upload the key file you just download

☐ Enter the key manually (Type: String)

- Click **OK** to finish the setup.

### Delete the Global SED Authentication Key

- Click on the key in **Settings > System > SED key management**.
- Click **Delete > OK**.
- Provide the key for confirmation and click **OK** to delete the key.

## Maintenance

### Exporting/Import System Configuration

You may export system configuration information to preserve the current system status or import it to restore system configuration.

---

**When to export system configuration**

- After firmware upgrade
  - Before replacing both controllers
  - After mapping logical drives to host LUN or changing system configuration
- 

**When to import system configuration**

- The system has been unstable
  - Both controllers have been replaced
- Note: The firmware version of the system configuration to be imported must match the firmware version of the current system.
- 

**Go to****Settings > System > Maintenance**

The screenshot shows the 'Export/Import configuration' page. At the top, there are two tabs: 'Export/Import configuration' (active) and 'Diagnostic information'. Below the tabs, the title 'Export/Import configuration' is displayed in green. A paragraph states: 'This page is for users to export/import configuration on this system, exported file can only be imported to the same storage system.' Below this, a label 'Select whether to export or import configuration' is followed by a dropdown menu currently showing 'Exporting configuration'. There are two radio button options: 'Export system configuration' (selected) and 'Export operation schedule'. Under 'Export system configuration', it says 'A download request will be generated.' and there is an 'Export' button. Under 'Export operation schedule', it says 'A download request will be generated. Only snapshot, volume replication, and tier migration schedule will be exported.'

**Export/Import configuration**

Click the **Export/Import configuration** tab. Select whether to export or import configuration from the drop down list.

This is a close-up of the dropdown menu from the previous screenshot. It shows the text 'Select whether to export or import configuration' above a list with two items: 'Exporting configuration' (highlighted in blue) and 'Importing configuration'.

- Exporting configuration
1. Export system configuration

Click the **Export** button and a download request will be generated. You can download the system configuration file (.nvram file) to the host.

● Export system configuration

A download request will be generated.

**Export**

## 2. Export operation schedule

You can also export the schedule configuration from the system. Click the **Export** button and a download request will be generated.

● Export operation schedule

A download request will be generated. Only snapshot, volume replication, and tier migration schedule will be exported.

**Export**

[Note] Only snapshot, volume replication, and tier migration schedule can be exported.

## ● Importing configuration

### 1. Import system configuration

You can import a system configuration file by uploading a configuration file. Click **Browse** button to select a file and click Import button to start importing the configuration.

● Import system configuration

Select and import the system configuration file downloaded from this system.

5B848\_nvram **Browse**

**Import**

### 2. Import operation schedule

You can also import the schedule configuration file by uploading the file downloaded from the system. Click **Browse** button to select a file and click Import button to start importing the configuration.

[Note] Only snapshot, volume replication, and tier migration schedule can be imported.

☒ Import operation schedule  
Select and import the operation schedule file downloaded from this system. Only snapshot, volume replication, and tier migration schedule will be imported.

5B848\_nvram

## Diagnostic information

When your system experiences unrecoverable issues, you can export the system configuration and system log to our technical support team for further inspection.

---

**Go to** **Settings > System > Maintenance > Diagnostic information**

---

### Export information

You can export **Diagnostic log** and **System core dump** files by clicking the Export button in the corresponding fields.

**Diagnostic information**

When contacting with technical support engineers, diagnostic information will be required for further examination.

**Diagnostic log:**

**System core dump:**



## Power

### UPS

IT administrators connect important devices, such as storage systems, servers and routers, to UPS (Uninterruptible Power Supply) to prevent data loss resulted from power outage. The PAC Storage PS/PSV supports UPS with SNMP capability so the system can enter into a safe mode and continue to operate on UPS power to ensure data protection.

The administrator can establish a connection between the PAC Storage PS/PSV and SNMP UPS through the PAC Storage User Interface Firmware. When power supply is interrupted, the system can enter into a safe mode when the remaining power on the UPS has reached a certain threshold. The system will also keep a log on the events for tracking purposes.

Please consult PAC Storage website for the latest list of supported UPS systems.

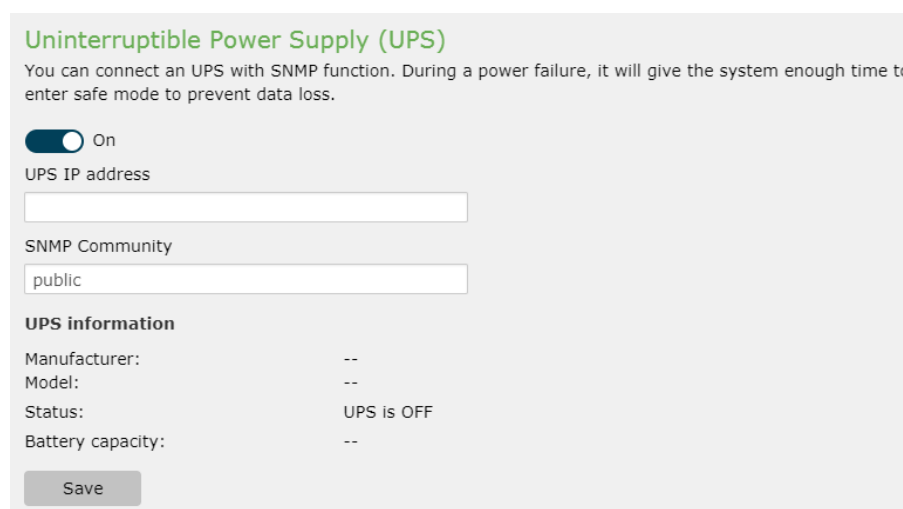
---

**Go to**                      **Settings > System > Power**

---

#### Enable UPS

1. Select the **UPS** tab and click the switch to **On** to enable UPS.  
This enables the UPS monitoring mechanism. When the user disables the service, the UPS IP address will be cleared.
2. Enter the Settings and click **Apply** to store the Settings.



**Uninterruptible Power Supply (UPS)**

You can connect an UPS with SNMP function. During a power failure, it will give the system enough time to enter safe mode to prevent data loss.

☒ On

UPS IP address

SNMP Community

public

**UPS information**

Manufacturer: --

Model: --

Status: UPS is OFF

Battery capacity: --

Save

---

#### Parameter

**UPS IP Address:** The destination for the PAC Storage PS/PSV to send SNMP requests.

**SNMP version:** Supports v1 and v2c. The default setting is v2c.



**SNMP Community:** The default setting is “public.”

Note: When in safe mode, the PAC Storage PS/PSV will unmount file-level volumes. For block-level volumes, the write policy will change from write-back to write-through to prevent data loss during power failure.

## Power Schedule

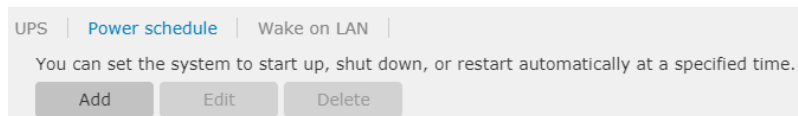
Users can make use of the power schedule function to start, shut down, and reset the system at a specified time. This function enables users to save energy consumption by scheduling automatic system shutdown and startup.

Note:

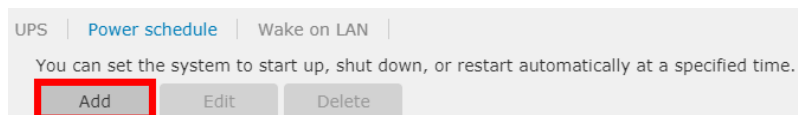
1. This function is available only on PSV Pro 100 and 200 series.
2. To prevent task failures and system failures, the system cannot perform a scheduled shutdown or reset task when it is still running any backup, restoration, or system update task.

**Go to** **Settings > System > Power**

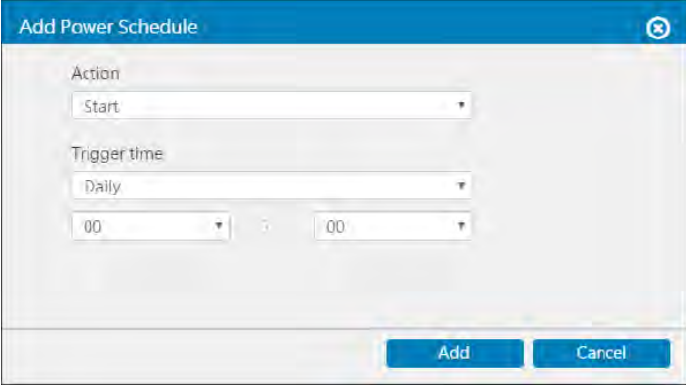
**Power Schedule** Select the **Power schedule** tab.



**Add a scheduled task** Click the **Add** button to create a scheduled task to shut down, reboot, or start the system at a specified time. The maximum number of scheduled tasks is 15. If the number reaches the maximum limit, this button will be grayed out.



After clicking **Add**, you can specify the action by making a selection from the drop-down menu. Available actions include Start, Shut down, and Reset/restart. Then, specify the time to trigger the action. Choose *Daily*, *Weekend*, *Weekday*, or one day in a week and select the time in the drop-down lists. Click **Add** to save and apply the Settings.



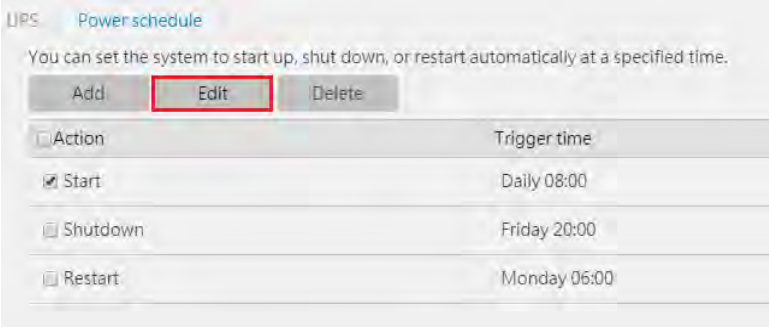
The 'Add Power Schedule' dialog box contains the following fields:

- Action:** A dropdown menu with 'Start' selected.
- Trigger time:** A dropdown menu with 'Daily' selected.
- Time:** Two time selection fields, both set to '00'.

At the bottom right, there are two buttons: 'Add' and 'Cancel'.

Note: The system will not automatically check time conflicts so please be careful when setting the scheduled tasks. In the case of schedule conflicts, the scheduled tasks will be carried out from the top to bottom as listed in the table.

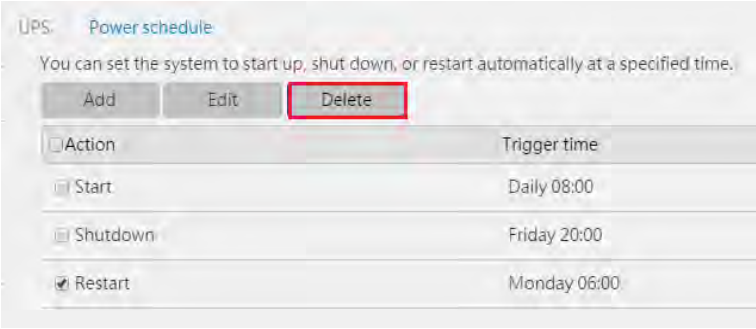
**Edit a scheduled task** Select a task and click **Edit** to modify the task. Only one entry can be edited at a time.



The 'Power schedule' interface shows a list of tasks. The 'Edit' button is highlighted with a red box.

Action	Trigger time
<input checked="" type="checkbox"/> Start	Daily 08:00
<input type="checkbox"/> Shutdown	Friday 20:00
<input type="checkbox"/> Restart	Monday 06:00

**Delete a scheduled task** Select one or more tasks in the list and click **Delete** to delete the task(s).



The 'Power schedule' interface shows a list of tasks. The 'Delete' button is highlighted with a red box.

Action	Trigger time
<input type="checkbox"/> Start	Daily 08:00
<input type="checkbox"/> Shutdown	Friday 20:00
<input checked="" type="checkbox"/> Restart	Monday 06:00



## Wake on LAN

Wake on LAN (WoL) allows users to remotely power on the storage system in the same local-area network, without having to start the system physically.

Note:

1. WoL is available only to PSV Pro 100 and 200 series.
2. Only the built-in 1Gb iSCSI ports (for both block & file level) support WoL.
3. Make sure WoL is supported and enabled on the host server connected to the storage system.

---

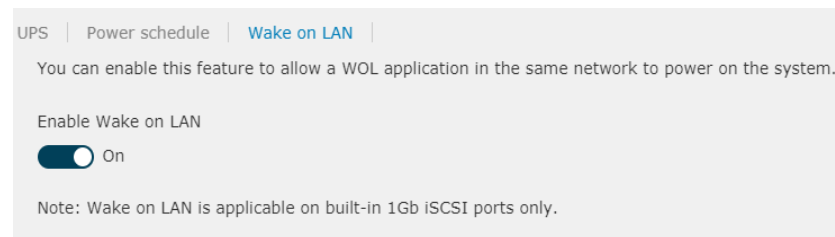
### Go to

**Settings > System > Power > Wake on LAN**

---

### Wake on LAN

Select the **Wake on LAN** tab.




---

### Enable/Disable Wake on LAN

Turn on/off the **Enable Wake on LAN** switch to enable/disable the feature.




---

### Verify the feature

1. You can download a free Wake on LAN software online and follow the Settings. Make sure you have entered the correct channel port and MAC address.
  2. Enable Wake on LAN.
  3. Shut down the system by pressing the power button on the enclosure for around 5 seconds or the shutdown button on PAC Storage User Interface Firmware.
  4. Send the magic packets via a free Wake on LAN tool. The system will be powered on.
-

## Enclosure View

Go to **Main menu > Settings > Device > System > Enclosure View**

You will see the following display of the front and rear views with detailed information of both RAID and JBOD view from the scroll down list:



✓ RAID view:



✓ JBOD view:



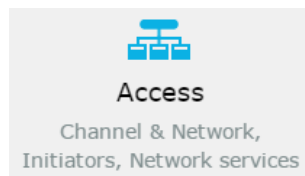
# Access

The Data Access menu contains the following sub-Settings


1. Channel and Network Settings
2. Initiators
3. Network Services
4. VLAN

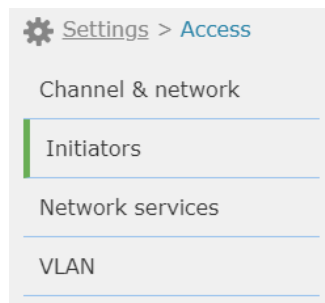
**Go to**

**Settings > Access**



## Data Access Menu

The Data Access menu for the selected device will appear. Users can switch to the sub-setting pages or click  [Settings](#) to go back to the previous setting page.





## Channel and Network

The Channel and Network setting allows users to modify the Settings of host channels, management ports, and trunk groups.

You can configure a channel interface for block-level data services (e.g. iSCSI, Fibre and SAS) or for file-level data services (e.g. CIFS/SMB, AFP, NFS and FTP).

Go to

**Settings > Access > Channel & Network**

### The Channel and Network Settings

**Channel & Network**

You can configure a channel interface for block-level data service (e.g. iSCSI, Fibre, SAS) or for file-level data service (e.g. CIFS/SMB, AFP, NFS, FTP, etc.)

Channel 0

iSCSI 10G Block-level Data Service (iSCSI)

● Controller A: --

● Controller B: --

Channel 1

iSCSI 10G Block-level Data Service (iSCSI)

● Controller A: --

● Controller B: --

Channel 2

iSCSI 1G Block-level Data Service (iSCSI)

● Controller A: --

● Controller B: --

Channel 3

iSCSI 1G Block-level Data Service (iSCSI)

● Controller A: --

● Controller B: --

## Host Channel Settings

Each host channel comes with a default ID: AID (one that is managed by controller A) and/or a BID (controller B). But this may not be sufficient if your subsystem is configured as a complex dual-active controller.

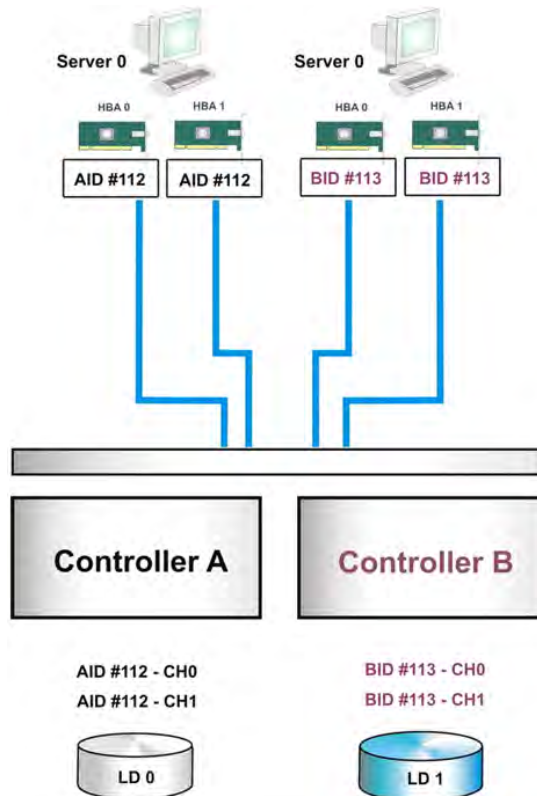
In a dual-active controller configuration, you need to manually create more Slot A or Slot B Channel IDs to distribute the workload between partner controllers.

### Host ID

A logical drive can be associated with either Controller A IDs or Controller B IDs through the host LUN mapping process. The IDs appear to the application servers as storage volumes. You may present storage volumes to the host using the LUN numbers under channel IDs. A maximum of 1024 LUNs and 32 LUNs under each ID are supported.

### Multiple Paths

When there are multiple paths between the subsystem controller and the host adapter, you may need to optimize the path using Multipath. For details, see Working with Multipath.



### Cross-Controller Mapping

Cross-controller mapping allows you to associate a logical drive with both controller A and controller B IDs. However, it is only beneficial when it is difficult to make fault-tolerant host linking between controllers and host HBAs (for example, using SAS-to-SAS storage systems).

**Controller Failure** When a controller fails, its host IDs will be taken over and managed by the surviving controller.

## Host Channel Parameters

Note: For an iSCSI 40G hostboard, both of its channels can only be set to either file-level or block-level.

**Go to** **Settings > Access > Channel & Network**

**Configuring Host Parameters (iSCSI)**

1. Click on the host channel to modify.
2. Click **Edit**.

**Parameters** **Channel type** Choose **File-level Data service** or **Block-level Data service**. The network channel is then set to the chosen type.

**Type** (Configurable)

- Static: specifies a fixed IP address.
- DHCP (Auto): allows the router/switch to pick an available IP address for the subsystem.
- Disabled: disables the IPV6 address protocol (applied when IPV4 is used instead of IPV6).

**IP Address** (Configurable) Specifies the IP address in IPV4 or IPV6 format. Note that each slot has its own IP configuration.

Notes on valid IP address format:

1. IP addresses starting with "FF" are reserved (multicast). For example, FF05:: and FFEF:: are not acceptable.
2. Route IP address can start with "FF".
3. The following addresses are not acceptable for IP address and route address:

FF01:0:0:0:0:0:1

FF02:0:0:0:0:0:1

FF02:0:0:0:0:1:FF00:0

FF01:0:0:0:0:0:0:2

FF02:0:0:0:0:0:0:2

FF05:0:0:0:0:0:0:2

0:0:0:0:0:0:0:0

**Subnet  
Mask,  
Default  
Gateway or  
Route**

(Configurable) Allows users to specify the surrounding subnet and gateway for the subsystem to specify the network subdivision.

**Test  
Connection**

After configuring the above network Settings, click on **Test Connection** to check controller connectivity.

1. Select the desired command in the **Command** drop-down menu:  
  
**ping**: Check network connection and data transmission speed.  
  
**tracert**: Track the routing path of sent packets over the network.
2. To test connectivity over the default route, select **Use default routing**.
3. Enter one or more supported arguments and their required values in the **Command arguments** field.

To find out the supported arguments, click **Available**

arguments.

4. Click **Test** to run the test. The result is displayed in the **Output** field.
5. To clear previous output results, click **Clear**.

**Set as the global default route**

Use this network channel as the default route that the system uses to communicate with other systems.

This option is only available for file-level channels.

**Advanced Parameters**

Scroll the host channel setting page to the bottom and click the **Advanced** button. The advanced setting page will pop up.

Host Channel Settings

ID

AID

☒ 0

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ 6

☐ 7

☐ 8

☐ 9

☐ 10

☐ 11

BID

☐ 0

☒ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ 6

☐ 7

☐ 8

☐ 9

☐ 10

☐ 11

MCS Group

☐ 0

☐ 1

☐ 2

☒ 3

Apply

Cancel

**ID**

Specifies the LUN mapping ID number.

**MCS Group**

MC/S (Multiple Connections per Session) protocol allows combining several channels to improve performance and failover rates.

**Fibre Channel Configurations**

There are fewer configurable parameters for a Fibre Channel port (you may choose the default data rate for some channels).

Current Data Rate:	8.0 Gbps
Default Data Rate:	Auto
Current Transfer Bandwidth:	Serial
host board:	FC 16G #1(slot A:8441430 (0x80CE56)) FC 16G #1(slot B:8462248 (0x811FA8))
Node Name	
AID 112:	200000D023064DBB
BID 113:	200000D023164DBB
Port Name	
AID 112:	210000D023064DBB
BID 113:	210000D023164DBB

**Fibre Channel Parameters**      **ID (Advanced setting)**      Click **Advanced** and specify the LUN mapping ID number.

**Data Rate**      Specifies the data rate of the Fibre Channel.

**InfiniBand Channel Configurations**      Configure the parameters for an InfiniBand Channel port.

Host Channel Settings

Current Data Rate:	--
Default Data Rate:	56.0 Gbps
Current Transfer Bandwidth:	
host board:	InfiniBand 56G #1(slot A:8804565 (0x8658D5)) InfiniBand 56G #1(slot B:8867761 (0x874FB1))
Node Name	
AID 0:	200000D0230800D1
BID 1:	200000D0231800D1
Port Name	
AID 0:	210400D0230800D1
BID 1:	210400D0231800D1
Advanced	
Apply Cancel	

Click **Advanced** to set the LUN mapping ID number.

The image shows a 'Host Channel Settings' dialog box. It has a title bar with a close button. Below the title bar, there is a section labeled 'ID'. Under 'ID', there are two lists: 'AID' and 'BID'. Both lists contain checkboxes for values 0 through 11. In the 'AID' list, checkbox 0 is checked. In the 'BID' list, checkbox 1 is checked. At the bottom right of the dialog, there are 'Apply' and 'Cancel' buttons.

**Note:**

1. If you have two InfiniBand 56Gb/s host boards on one controller, the controller must have at least 16GB of memory.
2. InfiniBand channel ports only support Linux hosts.

---

**InfiniBand Channel  
Parameters**

**Channel ID**

Specifies the LUN mapping ID number.

---

## Configuring IP Address (IPv4) of Management Port

You may change the IP address of the device, but doing so will disconnect the user interface in the old address. Make sure that you have noted down the new IP address and reconnect with the user interface using the new address.

<b>Go to</b>	<b>Settings &gt; Access &gt; Channel &amp; Network</b>	
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Scroll the page to the bottom, finding the Management port section and click the <b>Edit</b> button.</li> <li>2. Select the IP address type: <b>DHCP, Static</b></li> <li>3. If you select <b>Static</b>, enter the IP address, subnet mask, and the gateway address.</li> </ol>	
<b>Notes</b>	<p>You are not allowed to assign any of the following system reserved IP addresses to your subsystem:</p> <p>127.x.x.x</p> <p>128.0.x.x</p> <p>191.255.x.x</p> <p>192.0.x.x</p> <p>223.255.255.x</p>	
<b>Parameters</b>	<b>(IP) Address</b>	<p>Specifies the IP address of the subsystem. To use DHCP, select <b>DHCP</b> from the drop down list.</p> <p>Example: 192.168.4.246, DHCP</p>
	<b>Subnet mask</b>	<p>Specifies the subnet mask for the IP address. When using DHCP, leave this parameter blank.</p>
	<b>Default gateway</b>	<p>Specifies the IP address of the network gateway. When using DHCP, leave this parameter blank.</p>
<b>Note on Using DHCP</b>	<p>The default IP address is set as "DHCP client." If the DHCP server cannot be found, a default IP address "10.10.1.1" will be loaded.</p> <p>With DHCP, the IP address may change when cable disconnection or other network errors occur. If you are accessing the subsystem from the PAC Storage User Interface Firmware suite, you will have to re-connect with the subsystem with the new IP address.</p>	





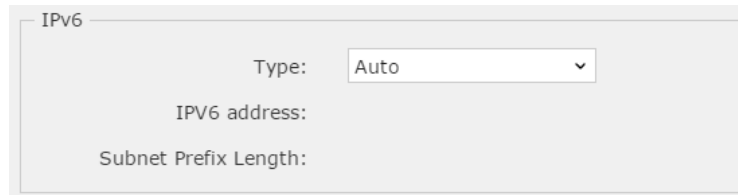
## Configuring IP Address (IPv6) of Management Port

---

**Go to** Settings > Access > Channel & Network

---

- Steps**
1. Scroll the page to the bottom, find the Management port section and click the **Edit** button.
  2. Select **Auto** and let the system configure IPv6



The screenshot shows a configuration panel for IPv6. At the top left is the label "IPv6". To its right is the "Type:" label followed by a dropdown menu currently showing "Auto". Below these are two labels, "IPv6 address:" and "Subnet Prefix Length:", each followed by an empty input field.

## Enabling Jumbo Frames

Enabling jumbo frames allows larger payloads per packet by increasing Ethernet networking throughput and reducing CPU utilization during large file transfers.

Note: If this storage system is connected to network devices (e.g. routers and switches), ensure all network devices support jumbo frames and are properly configured.

<b>Go to</b>	<b>Settings &gt; Access &gt; Channel &amp; Network</b>
<b>Steps</b>	<ol style="list-style-type: none"><li>1. Go to the <b>Jumbo frames</b> section.</li><li>2. Turn on jumbo frames. The data frame size increases to <b>9K</b> (bytes).</li></ol>

## Trunking Host Interfaces to Increase Bandwidth

Increase network bandwidth by combining (trunking) multiple LAN interfaces into one, creating a link aggregation configuration.

Trunking offers the following benefits:

- Increased bandwidth: bandwidths of multiple interfaces will be added up.
- Improved security: when one LAN interface fails, the other interface will keep the network connection intact.

Note:

- Multiple LAN ports on your hardware must be connected to the network.
- The network switch must be compatible with trunking.
- The trunking option is available only for iSCSI-host models.
- If the channels you selected are set as block-level, enable LACP on the switch that is connected to the storage system.
- If the channels you selected are set as file-level, enable LACP or ALB on the switch that is connected to the storage system.

**Go to** **Settings > Access > Channel & Network > Trunk group**

### Steps

1. Click **Manage**.
2. Click **Create** to start creating a trunk group.
3. Select a desired type of network interface in the **Type** menu.
4. Select two or more network channels to form a trunk group.
5. Choose a trunk mode. For file-level channels, you can choose either mode. For block-level channels, only the LACP mode is available.

#### **Adaptive Load Balancing**

The system assigns client traffic to different channels in the trunk group to balance network workload.

While using this mode, you do not need to connect the system to any intermediate networking device.

#### **IEEE 802.3ad Dynamic Link Aggregation (LACP)**

The system assigns client traffic to different channels in the trunk group to balance network workload.

This mode provides fault-tolerant data transmission even when a channel in the trunk group fails.

While using this mode, you must connect the system

---

to an intermediate networking device (e.g. switch) that supports this mode.

6. Click **Next** to proceed.
7. Go to the **Jumbo frames** menu and choose whether to enable jumbo frame for the trunk group channel:

<b>Default</b>	The system applies the global trunk group setting (in <b>Settings &gt; Access &gt; Channel &amp; network &gt; Jumbo frames</b> ).
<b>Enable</b>	<p>Enable jumbo frame for this trunk group channel.</p> <p>This setting has higher priority than the global trunk group setting (in <b>Settings &gt; Access &gt; Channel &amp; network &gt; Jumbo frames</b>).</p>
<b>Disable</b>	<p>Disable jumbo frame for this trunk group channel.</p> <p>This setting has higher priority than the global trunk group setting (in <b>Settings &gt; Access &gt; Channel &amp; network &gt; Jumbo frames</b>).</p>

8. Specify the trunk group channel's IPv4 Settings under each controller. Then, select an option from the **Type** menu:

**DHCP:** This option lets the DHCP server assign the network Settings.

**Static:** This option allows you to customize the network channel Settings. Then, continue to specify the IP address, subnet mask, and the default gateway.

9. Specify the trunk group channel's IPv6 Settings under each controller. Then, select an option from the **Type** menu:

**Static:** This option allows you to customize the network channel's Settings. Then, continue to specify the IPv6 address, subnet prefix length, and the route.

**Auto:** This option automatically determines the network channel's Settings.

**Disabled:** Do not allow this network channel to communicate over IPv6.

10. Click **Next** to proceed.
11. Check the trunk group Settings.
12. Click **Apply** to form a trunk group.



## Changing Channel Type for Converged Host Board

The converged host board allows users to change the channel type of its physical ports. When the channel type is changed, the ports on the converged host board will switch to the new type after system reboot.

Currently the following channel types supported by the converged host board includes:

- Fibre Channel 8G
- Fibre Channel 16G
- iSCSI 10G & FCoE 10G

### Go to

**Settings > Access > Channel & Network**

Scroll down the page and find **Converged host board** and click **Edit**.

#### Converged host board

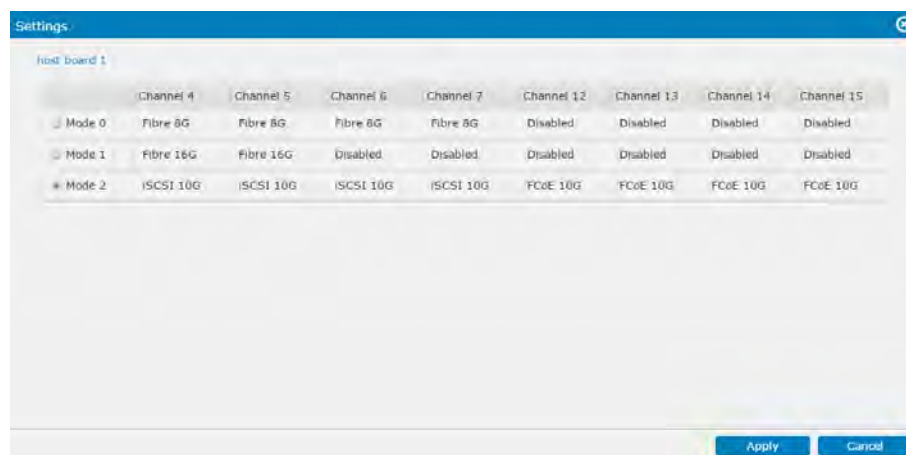
To change the converged host board to different work modes (e.g. 16Gb/s Fibre, 8Gb/s Fibre or 10Gb/s iSCSI SFP+). You can click Manage to modify.

Edit

(This option is available only when a converged host board is installed on your controller.)

### Steps

1. In the pop-up window, select one of the checkboxes to change the channel type of all physical ports on the converged host board to the one specified. Click **Apply**.



	Channel 4	Channel 5	Channel 6	Channel 7	Channel 12	Channel 13	Channel 14	Channel 15
Mode 0	Fibre 8G	Fibre 8G	Fibre 8G	Fibre 8G	Disabled	Disabled	Disabled	Disabled
Mode 1	Fibre 16G	Fibre 16G	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input checked="" type="radio"/> Mode 2	iSCSI 10G	iSCSI 10G	iSCSI 10G	iSCSI 10G	FCoE 10G	FCoE 10G	FCoE 10G	FCoE 10G

2. For the change to take effect, restart the storage subsystem.

### Parameters

#### Mode 0

If you select this mode, all 4 ports will be available for connectivity with their channel type changed to Fibre

---

8G.

---

**Mode 1**

If you select this mode, only the first two ports of the host board will be available for connectivity with their channel type configured as Fibre 16G.

---

**Mode 2**

If you select this mode, all 4 ports will be available for connectivity. The channel type can be selected iSCSI 10G or FCoE 10G based on the SFP+ that users insert.

---

**Notes and limitations**

- LUN mappings should be removed before changing the channel type.
- For FC 16G, its data rate can be optionally set as 16G/8G/4G; for FC 8G, its data rate can be optionally set as 8G/4G.
- If the channel type of the ports on the converged host board is set as Fibre 16G or Fibre 8G, then the storage subsystem can only be connected with other devices through the point-to-point (FC-P2P) topology, meaning Arbitrated Loop (FC-AL) is not supported by the converged host board.
- For Fibre Channel ports on other types of host boards, Arbitrated Loop is supported by Fibre 8G ports, allowing you to change their Fibre connection to either loop only or point-to-point only. Arbitrated Loop is not supported by Fibre 16G ports.
- For Fibre Channel ports on other types of host boards, their SCSI ID starts with 112. For a converged host board, its physical ports are all regarded as iSCSI ports even if their type is configured as FC 8G/16G, and their iSCSI IDs are specified according to the following rule:  
 Controller A: (accumulated iSCSI channel number) x 16  
 Controller B (if available): (accumulated iSCSI channel number) x 16 +1  
**Note:** The channel number starts with "0," which is also the number of the first physical port.



## Routing

You can configure network routing by specifying the destination, netmask and gateway that acts as an entrance to other IP networks.

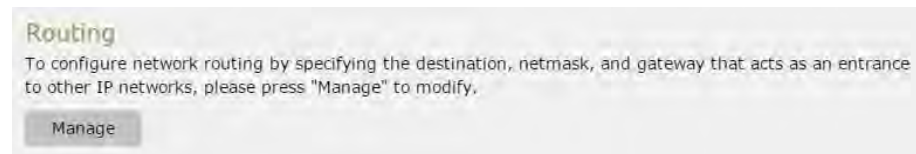
Note:

1. The primary controller has an additional routing option of the management port.
2. You can only edit the default route.
3. If the default route is the management port, the secondary route can be any route.

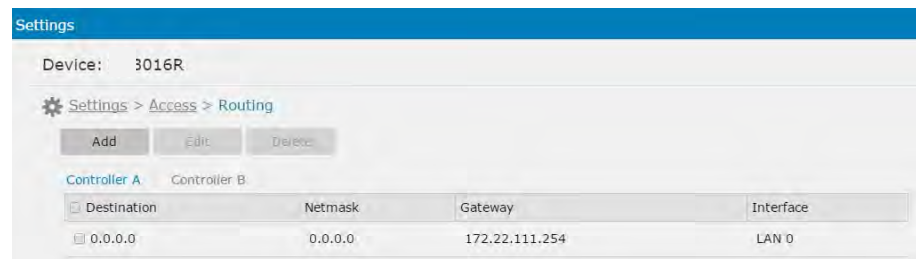
**Go to**

**Settings > Access > Channel & Network**

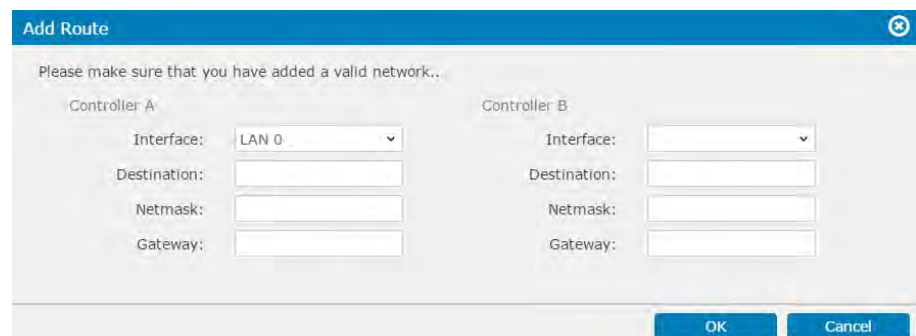
Scroll the page to the bottom and click the **Manage** button under **Routing**.



Then, click **Add** to add network routing information.



Enter the routing information and click **OK** to apply and save the Settings.



You can also select an item and make changes to it by clicking **Edit**.

Settings > Access > Routing

[Add](#) [Edit](#) [Delete](#)

Controller A | Controller B

<input checked="" type="checkbox"/> Destination	Netmask	Gateway	Interface
<input checked="" type="checkbox"/> 0.0.0.0	0.0.0.0	172.22.111.254	LAN 0

Change the routing information and click **OK** to apply and save the Settings.

**Edit Route**

Please make sure that you have added a valid network..

Controller A

Interface:

Destination:

Netmask:

Gateway:

Controller B

Interface:

Destination:

Netmask:

Gateway:

[OK](#) [Cancel](#)

## Initiators

This page allows users to create alias for iSCSI initiators and iSNS server.

---

**Go to**

**Settings > Access > Initiators**

[IQN](#) | [WWN](#) | [Initiator group](#) | [iSNS](#) |

### Authentication

Login authentication with CHAP

☐ Off

### IQN list

Add Edit Delete

<input type="checkbox"/> Initiator alias ^	Initiator group ^	Host IQN
--	-------------------	----------

## Configuring Alias for iSCSI Initiators

The Initiator function can be used to create aliases for iSCSI initiators.

**Go to**

**Setting > Access > Initiators**

Click in the **Initiator** tab to switch to the initiator configuration page.

**Add an Alias  
(for a iSCSI  
initiator)**

1. Click **Add** button and fill in the necessary information in the blanks.

**Host IQN:** Select one of the pre-defined host IQN or click the **Add** button and type in a new host IQN.

**Alias:** Assign a name for the iSCSI initiator. The name will represent the host IQN afterward.

**IP Address/Netmask:** Specifies the IP address and subnet mask, if necessary.

Multiple initiator ports on an application server can sometimes share the same IQN.

**CHAP authentication**

Username

Password

Confirm password

**Username/Password:** Specifies the user name and password for CHAP authentication. This information is the same as the CHAP target node name and CHAP secret in the OS setting.

**Mutual authentication**

Target username

Target password

Confirm target password

**Target Name/Password:** Specifies the target name and password for CHAP authentication. This information is the same as the CHAP initiator node name and CHAP secret in the OS setting.

The Target Name cannot exceed 32 bytes in length. For a Microsoft iSCSI software initiator, it is required that both the initiator and target CHAP password should be between 12 bytes and 16 bytes.

To enable CHAP, go to **Settings > Access > Initiators** and turn on the **Login Authentication with CHAP** switch to On.

**Authentication**

Login authentication with CHAP

☐ Off

2. Click **Next**. You can add the initiator in the existing Initiator group. Click **Apply** to complete the Settings.

#### Edit an iSCSI Initiator Alias

1. Tick the initiator on the IQN list and click the **Edit** button to change the Settings.

2. The alias information table will pop up. Modify the information according to your configuration.

## Initiator Group

1. Click in the **Initiator** tab to switch to the Initiator group page.

2. Click **Add** button to configure the Settings.
3. Specify the group name and select a group type from the drop down. Press **Next** to proceed.

4. Select a group member from the IQN list, note that at least one initiator should be selected.

5. To quickly create an IQN host, click **Add** above and specify the Settings.
6. Click **Apply** to finish the Settings.

**Add initiator group**

Select group members, at least one initiator should be selected.

Search

Initiator alias	Host IQN
writer	iqn.1991-05.com.microsoft:pc1.lft.local

You can also assign an IQN to a group on the **Initiators > Edit** page. Switch the tab to **Initiator group**, you can add the IQN to the existing group after selecting the group and clicking **Apply**.

### Unassign Group

1. Select the initiator and click the **Edit** button. Switch the **Initiator group** tab and select the Initiator group. Click **Remove** button on the top of the page to remove it from the group.

**Edit initiator**

General | CHAP authentication | **Initiator group**

Add Remove

☒ Initiator group

☒ A1

A warning will pop up. Click OK to unassign the IQN alias group.

**Warning**

Are you sure you want to remove the initiator from the selected group(s)?

OK Cancel

## Configuring iSNS Server in Storage Subsystems

iSNS(Internet Storage Name Service) is a common discovery, naming and resource management service for all IP storage protocols. PAC Storage 's iSNS implementation complies with RFC 4171 standards. iSNS discovers iSCSI initiators and targets within a domain and their related information. Windows iSNS server is available in Windows Server 2008 R2 and Windows Server 2012.

The iSNS functions can be embedded in an IP Storage switch, gateway or router, or centralized in an iSNS server. Initiators then can query the iSNS to identify potential targets.

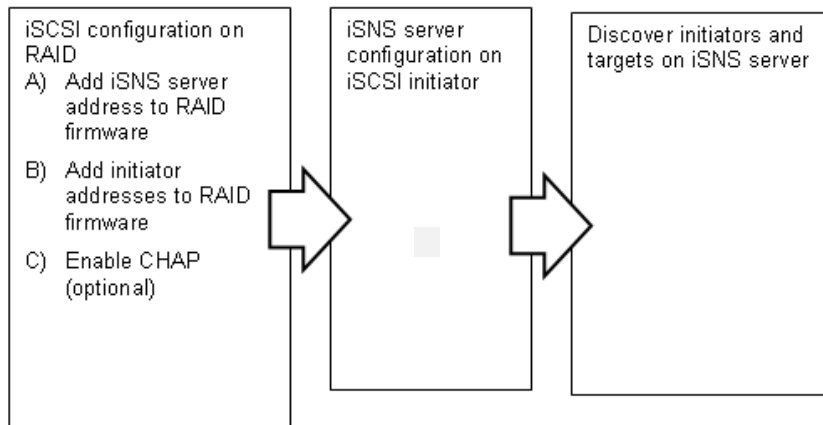
Microsoft's iSNS server is available for download. The iSNS server enables the interchange of data in a domain consisting of initiators and targets according to user preferences.

---

<b>Limitation</b>	Setting up iSNS is available only for iSCSI host models.
-------------------	--

---

### Example



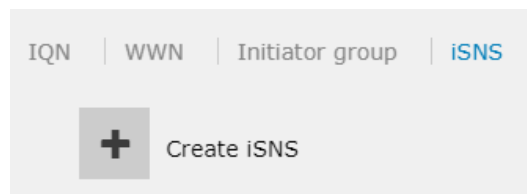

---

<b>Go to</b>	<b>Settings &gt; Access &gt; Initiators</b>
--------------	---

Click the **iSNS** tab to switch to the initiator configuration page.

### Steps

1. Click **Create iSNS** button to start the Settings.



2. On the Add iSNS page, enter the iSNS server IP address. Click OK to complete the Settings.

### iSNS Settings

**Add:** Click **Create iSNS** and enter the iSNS server IP address.

**Edit:** Select an iSNS server and click the **Edit** button to modify the IP address.



---

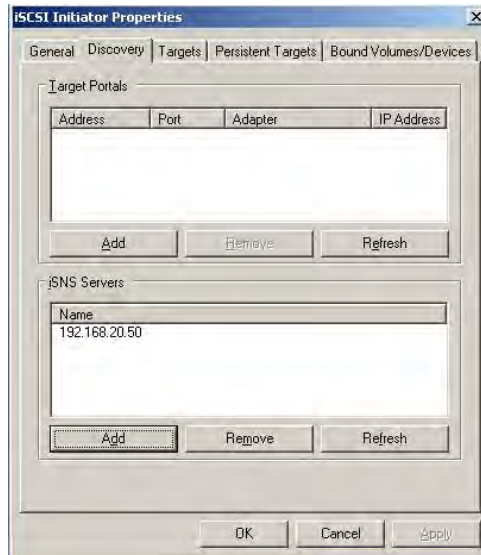
**Delete:** Select an iSNS server and click the **Delete** button. The iSNS server will be deleted from the list.

## Configuring iSNS Server in Windows OS

The sample process is based on Microsoft's iSCSI initiator software.

### Steps

1. Open the iSCSI initiator software and locate the iSNS server field by clicking the **Discovery** tab.



2. Click the **Add** button to key in an address. After an iSNS server address is added, you can check on host B (where the iSNS server is installed). If you have previously configured logical drives and mapped them to host IDs, the target LDs should have been scanned in and appear on the iSNS server configuration screen. Note that an iSNS server may take several minutes to find devices on the network at the initial setup.

An iSNS server is installed and operated using the administrator privilege. An incorrectly installed iSNS can still function, but the discovery function will not be available.

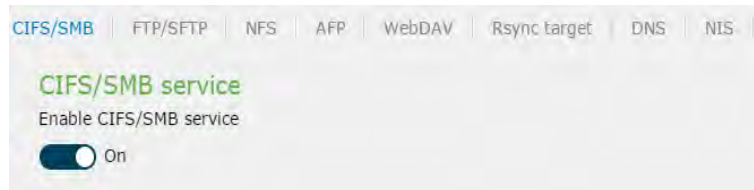
## Network Services

Activate and configure file service protocols to access your NAS system via network. Note that you have to turn on the switch before configuring the network services.

Go to

**Settings > System > Network Services**

**Networking  
Services**



## Configuring CIFS/SMB Service

CIFS (Common Internet File System) is a protocol developed by Microsoft to enable access to files stored on file servers across an IP network. CIFS evolves from Microsoft's Server Message Block (SMB). You can authenticate access through either Windows Domain, for users with Windows Active Directory (AD), or Windows Workgroup.

**Go to** **Settings > Access > Network services > CIFS/SMB**

### Steps

1. Turn on the CIFS/SMB service.

2. Specify the following Settings:

<b>Windows domain name</b>	It displays the name of the Windows Active Directory domain that the system joins in <b>Settings &gt; Privilege &gt; AD/LDAP</b> .
----------------------------	--

<b>Windows workgroup name</b>	Specify the name of a Windows workgroup for the system to join.  This setting is required if the system does not join any Windows Active Directory domain.
-------------------------------	--

<b>WINS Server</b>	Specify the primary and secondary WINS servers' IP addresses.
--------------------	---

3. Specify the advanced Settings to suit your needs:

<b>Inoperative client checking period</b>	Specify how often the system checks if a CIFS/SMB client is not operative.  The value must be between <b>10</b> to <b>864000</b> .
---	--

<b>Support creating multiple connections over SMB</b>	Select this option to allow the system to create multiple SMB connections to improve throughput and network fault tolerance.
---	--

4. Click **Save** to save the Settings.

## Configuring FTP/SFTP Service

FTP (File Transfer Protocol) is a standard network protocol used to exchange and manipulate files over a TCP/IP based network.

**Go to** **Settings > Access > Network services > FTP/SFTP**

### Steps

1. Turn on the FTP service.

2. Specify the FTP Settings:

<b>Listen port</b>	Specify a port for FTP transfers (default port: 21)
<b>Maximum number of failed login attempts</b>	<p>Specify how many failed login attempts are allowed from an FTP client. The number <b>0</b> means no limit.</p> <p>When the specified number is reached, the FTP client is banned from connecting to the system.</p>
<b>Login directory</b>	<p>Choose which directory the client is allowed to access upon login:</p> <p><b>User's home directory:</b> The client can access only the personal directory.</p> <p><b>Root directory:</b> The client can access the root directory.</p> <p><b>Customize:</b> You can customize the login directory for each client. Then, click <b>Manage</b> to add a mapping between a client and the login directory.</p>
<b>Enable anonymous FTP</b>	Select this option to allow a client to access files via FTP without unique user credentials.
<b>Enable FTP over SSL/TLS support (FTPS)</b>	<p>Select this option to enable SSL/TLS-encrypted FTP. Enable the auxiliary functions when necessary.</p> <ul style="list-style-type: none"> <li>● <b>Allow explicit FTP over TLS:</b> After connecting to the system, an FTP client can initiate a secure FTP connection by send this explicit command: <code>AUTH TLS</code></li> </ul> <p>To force all clients to use secure connections, select <b>Disallow plain unencrypted FTP</b>.</p> <ul style="list-style-type: none"> <li>● <b>Force PROT P to encrypt file transfers in SSL/TLS mode:</b> Enforce the <code>PROT P</code></li> </ul>

---

command to encrypt file transfers over SSL/TLS.

- **Listen for implicit SSL/TLS connections on the following ports:** Enable implicit FTP that builds SSL-protected connections via the specified port (default port: 990).

---

**Enable transfer speed limit**

Select this option and click **Transfer speed limit** to set speed limits on users or groups.

Then, choose a desired user or group and click **Set speed limit**. Then, specify the maximum upload and download limits.

Click **OK** to save the Settings.

---

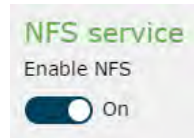
3. Click **Save** to save the Settings.
4. To protect FTP connections with SSH, turn on the SFTP service.

## Configuring NFS Service

NFS (Network File System) is a standard file transfer protocol for Unix/Linux networks, which allows users to access network files in a manner similar to accessing local files.

### Parameters

1. Click on the **NFS** tab to switch to the NFS setting page.
2. Click on the switch bar to enable the NFS service.



3. There are three NFS Versions: NFSv2, NFSv3 and NFSv4. By default, we support NFSv2 and v3. To enable NFSv4 support, click the **NFSv4 support** option and press **Apply**.



### NLM Support

PAC Storage PS/PSV family support NFSv2 & v3, as well as the Network Lock Manager (NLM). It provides UNIX record locking for any file that is shared over NFS. This locking mechanism enables NFS clients to synchronize their I/O requests with other clients to ensure the data integrity.

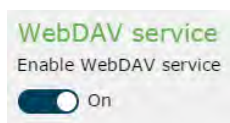
Note: The Network Lock Manager is used only for NFS Version 2 and NFS Version 3 installations.

## Configuring WebDAV Service

WebDAV(Web Distributed Authoring and Versioning) is an extension of the HTTP that allows users to perform remote Web content authoring operations. The WebDAV protocol provides a framework for users to create, change and move documents on a web server or web share.

### Parameters

1. Click on the **WebDAV** tab to switch to the WebDAV setting page.
2. Click on the switch bar to enable the WebDAV service.
3. Press **Apply** to save the Settings.



 A screenshot of a web interface showing the 'WebDAV Port Number' section. It has a title 'WebDAV Port Number' in green. Below the title, there are two input fields: 'For HTTP:' with the value '80' and 'For HTTPS:' with the value '8080'. At the bottom of the section is an 'Apply' button.

### Port for HTTP

WebDAV uses TCP ports 80 by default.

### Port for HTTPS

Port 8080 is default port for many web servers.

Note: If WebDAV is enabled, when you connect to your PAC Storage PS/PSV via a web browser, please enter **http://NAS IP:8816** in the web browser. If WebDAV is not enabled, you only have to enter **http://NAS IP** and it will automatically redirect to port 8816 (port 8817 for SSL connection).

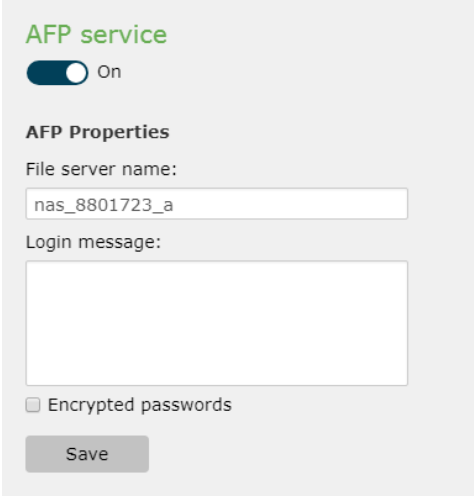


## Configuring AFP Service

AFP (Apple Filing Protocol) is the standard file transfer protocol for Mac OS X and Apple share servers.

### Parameters

1. Click on the **AFP** tab to switch to the AFP setting page.
2. Click on the switch bar to enable the AFP service.
3. Configure the Settings and press **Apply** to save the changes.



**AFP service**

☒ On

**AFP Properties**

File server name:

nas\_8801723\_a

Login message:

☐ Encrypted passwords

Save

<b>File Server Name</b>	Specifies the server name (the default setting is the name of your system).
<b>Login Message</b>	Specifies a custom message that appears at login.

## Configuring Rsync Target Service

Before setting up a PAC Storage PS/PSV as the Rsync Target (of third party), you need to configure the Rsync Target service first.

### Parameters

1. Click on the switch bar to enable the Rsync Target service.

Rsync target service



2. Specify the username and password of the user who can access the destination shared folder below the Rsync target properties section and press **Save**.

#### Rsync target properties

Port:

Username:

Password:

Save

3. Click on the **Add Rsync target** button. A window will pop up, asking users to specify the folder path and share name.

Rsync target

Folder Path:
Browse

Share Name:

Add
Cancel

4. After the Settings, Rsync target folder information will be shown on the target list.

Test

/Pool-1/Volume\_file/RsyncFolder/Test

Edit
Delete

**Rsync Target** Information for this case:

- **Share Name:** Test

- **Directory:** /Pool-1/Volume\_file/RsyncFolder/Test

## Configuring DNS Service

Users can configure the system to add one or more DNS servers.

### Parameters

1. Click on the **DNS** tab to switch to the DNS setting page.
2. Click on the **Add DNS server** button.



**DNS Server Address** Specifies the IP address of the DNS server

### Public DNS Servers

Provider	Primary DNS Server	Secondary DNS Server
Google	8.8.8.8	8.8.4.4
OpenDNS Home	208.67.222.222	208.67.220.220
DNS WATCH	84.200.69.80	84.200.70.40
Norton ConnectSafe	199.85.126.10	199.85.127.10
Level3	209.244.0.4	209.244.0.4

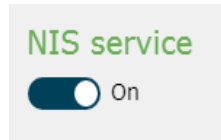
## Configuring NIS Service

You can enable NIS service and set the properties.

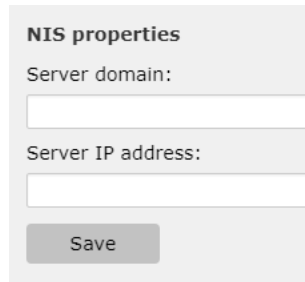
---

### Parameters

1. Click on the **NIS** tab to switch to the NIS setting page.
2. Click on the switch bar to enable the NIS service.



3. Enter the NIS server domain and server IP address and click **Save** to save the Settings.

A screenshot of the "NIS properties" configuration form. The title "NIS properties" is in bold. Below it are two input fields: "Server domain:" and "Server IP address:". At the bottom of the form is a gray button labeled "Save".

## Configuring Object Service

You can enable/disable object service. Currently OpenStack Swift and Amazon S3 are supported.

---

### Parameters

1. Click on the **Object** tab to switch to the object service setting page.
  2. Click on the switch bar to enable object service.
  3. To view service endpoints of all object storage services, click **All service endpoints** on the lower right corner.
- 

### Object Access Keys

You can create/delete object access keys for users by going to **Settings > Privilege > Users**. For more details, refer to the section Object Access Keys.

## Virtual Local Area Network (VLAN)

This page allows users to set VLAN. The range of VLAN ID can be set from **2~4094** (1 is default), the maximum VLAN for every channel is 8, each one of them has its own IP address.


Note: The VLAN function is only available for file-level channels.

Go to

**Settings > Access > VLAN**

### VLAN

Configure VLAN setting for a network interface, which is only accessible by devices with the same VLAN ID.

 Add VLAN

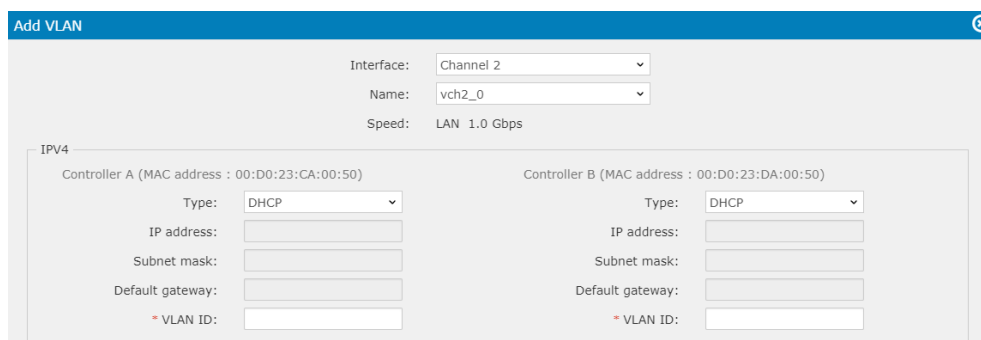
The VLAN list page displays the VLAN name, interface, IP, VLAN ID, link up/down status. Take over status when there is a fail over.

[Note] IPv6 is not supported.

## Create VLAN

**Configure  
VLAN**

1. Click the **Add** button and you will be directed to the following page:



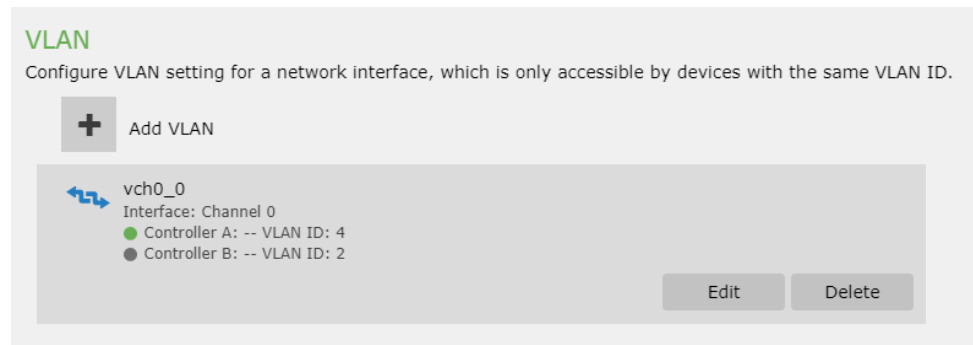
<b>Interface</b>	From the scroll down list, the system only displays the file-level channels.
<b>Name</b>	From the scroll down list, select the VLAN name. The VLAN name are automatically generated following the VLAN Naming Rule
<b>IPv4</b>	Choose your network type to DHCP or Static type, if DHCP is chosen, all IP configuration will automatically be set, please manually configure your IP address/subnet mask/default gateway if you choose Static configuration.
<b>VLAN ID</b>	Please input VLAN, each VLAN can also support one VLAN ID. For R-

---

models, both controllers must have a different VLAN ID.

---

2. Click **Apply** to finish setting up VLAN. Once VLAN is set, it will be displayed on the VLAN menu as follow:



Click **Edit** to edit VLAN and IP Settings, you will be directed back to the Add VLAN configuration page. You can also click **Delete** to remove the specific VLAN.

---

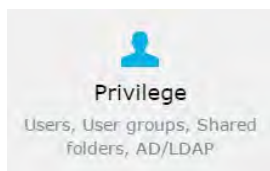
# Privilege

The Account setting menu contains the following sub-Settings.

1. Users Settings
2. User Group Settings
3. Shared Folders Settings
4. AD/LDAP Settings

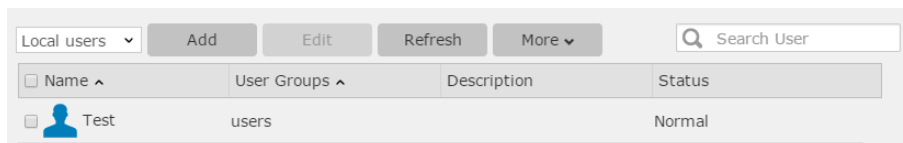
**Go to**

**Settings > Privilege**



## Accounts Privilege Setting Menu

The Account Setting menu for the selected device will appear. Users can switch to the sub-setting pages or click [Settings](#) to go back to the previous setting page.

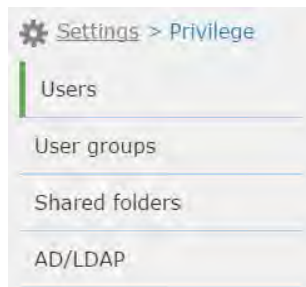




## Users

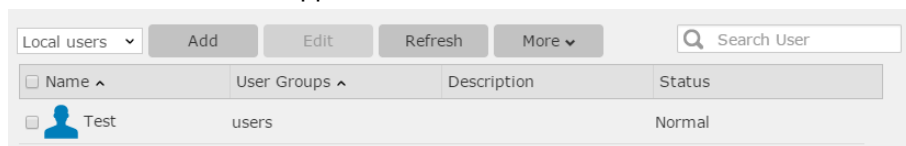
Go to

Settings > Privilege > Users



View

The account status will appear.



Parameters

<b>Name</b>	Lists the user names.
<b>User Groups</b>	Lists the group domain which the user belong to.
<b>Description</b>	Lists the descriptions for the user.
<b>Status</b>	Shows whether the user's password has expired or not

## Adding a User Account

User accounts can be created to allow access to shared files with unique usernames and passwords.

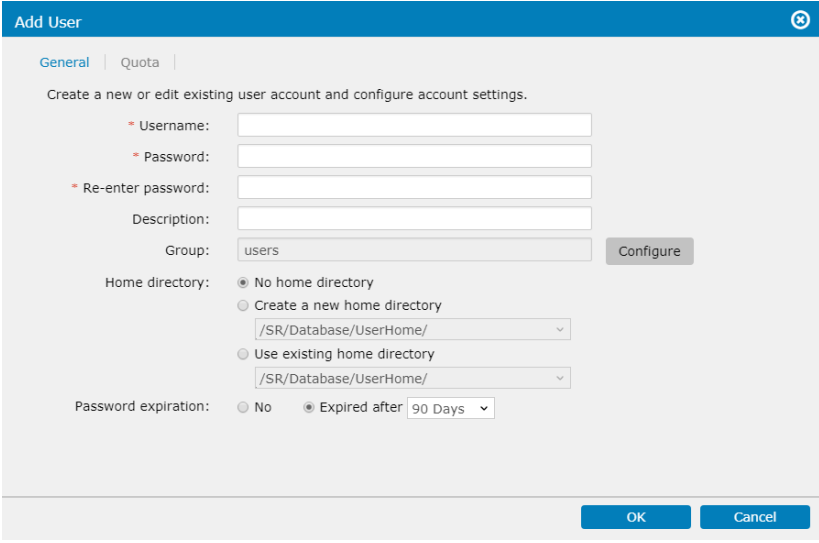
Go to

**Settings > Privilege > Users**

Press the **Add**  button to create a new user.

Steps

The **Add User** window will appear.



Note:

For more information about the **Quota** tab, refer to Quota Management section.

Parameters

<b>Username</b>	Specifies the new user name. No spaces are allowed.
<b>Password</b>	Enter the password for this user account. (default password policy requires at least 8 characters; you can change the setting by clicking Password Policy)
<b>Description</b>	Shows a description for this user.
<b>Group</b>	Specifies the group which this user belongs.
<b>Home Directory</b>	Creates a home directory (volume) for this user. When you check the box, the home directory path will automatically appear.
<b>Password</b>	Specifies the validity period of the user password. The

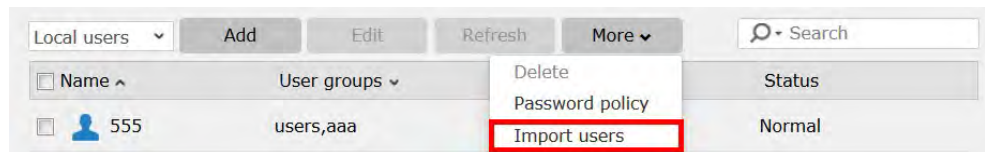
<b>Expiration</b>	user has to change the password when it expires.
-------------------	--

## Importing User Accounts in Batch

You can batch-create local user accounts by importing a user list.

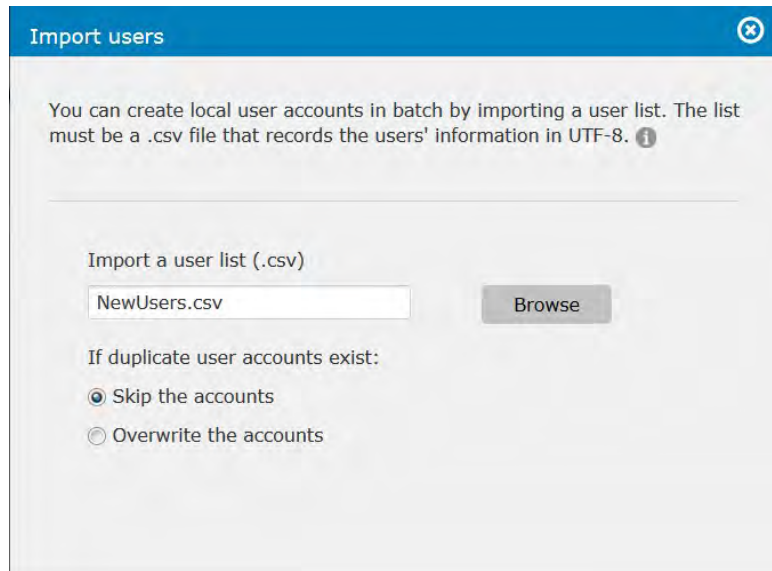
<b>Prerequisite</b>	Prepare a user list file in the .csv format in UTF-8 character encoding.  For each user, provide the following types of information from left to right in the same row, and separate each type with a comma (,):
Username (leftmost)	Specify a username.  To avoid import errors, do not include any comma (,).
Password	Specify a user password.  To avoid import errors, do not include any comma (,).
Description	Specify a user description.  To avoid import errors, do not include any comma (,).
Group name	Specify a user group to assign the user account to.
Password valid days	Specify how long the user password is valid: <b>30</b> (30 days), <b>60</b> (60 days), <b>90</b> (90 days), or <b>N</b> (no validity limit).
User home directory	Specify whether to enable a user home directory: <b>Y</b> (enable) or <b>N</b> (not enable).
Home directory path	Specify the home directory path in the format:  "/POOL_NAME/VOLUME_NAME".
User quota	Specify the numeric part of the user's space quota.  The specified number should be large than or equal to 0. "0" means "no limit on the user quota".
Quota unit (rightmost)	Specify the unit of the user's space quota: <b>MB</b> , <b>GB</b> , <b>TB</b> , or <b>PB</b> .

<b>Go to</b>	<b>Settings &gt; Privilege &gt; Users &gt; More &gt; Import users</b>
--------------	---



## Steps

1. Click **Browse** to select the user list file to import.



2. Select a policy to handle a duplicate user account found in the imported file:

<b>Skip the accounts</b>	The system skips duplicate accounts while importing the user list.
<b>Overwrite the accounts</b>	The system overwrites existing duplicate accounts with information imported from the user list.

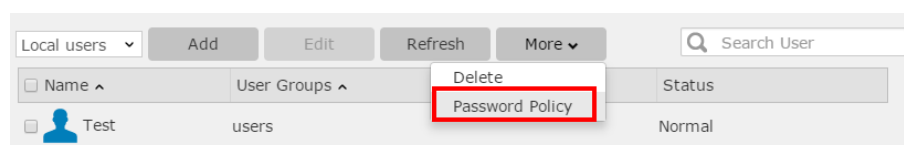
3. When the import is complete or an import error occurs, you can find a corresponding notification in the event log.

## Setting Password Policies

Set user password policies to allow PAC Storage User Interface Firmware and File Explorer users to manage their passwords.

Go to

Settings > Privilege > Users > More > Password Policy



Steps

1. Specify the password policies to improve login security.

Password policy

Enable the password policy to increase password complexity for better protection.

☒ Minimum length: 8 characters

☒ Maximum number of password(s) to keep: 3

☒ Minimum number of required letter(s): 2

☒ Minimum number of required upper case letter(s): 1

☒ Minimum number of required lower case letter(s): 1

☒ Minimum number of required digit(s): 1

☒ Minimum number of required special character(s): 1

☐ Allow local users to change their passwords

### Minimum length

Specify the least number of characters allowed for a password.

### Maximum number of password(s) to keep

Specify how many previous passwords the system remembers.

A user's new password cannot be the same with any remembered previous password.

### Minimum number of required letter(s)

Specify the least number of alphabetical characters allowed for a password.

### Minimum number of required upper case letter(s)

Specify the least number of uppercase characters allowed for a password.

---

<b>Minimum number of required lower case letter(s)</b>	Specify the least number of lowercase characters allowed for a password.
<b>Minimum number of required digit(s)</b>	Specify the least number of numeric characters allowed for a password.
<b>Minimum number of required special character(s)</b>	<p>Specify the least number of special characters allowed for a password.</p> <p>Accepted special characters are those available on the keyboard (including the space character).</p>
<b>Allow local users to change their passwords</b>	Select to allow local users to modify their own passwords without the system administrator's assistance.

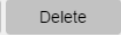
---

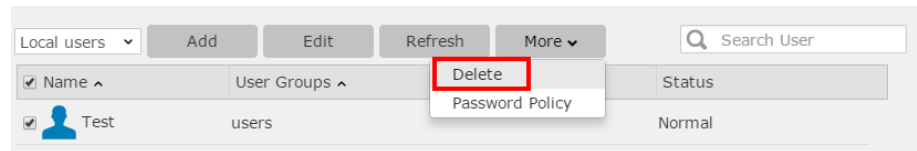
2. Click **OK** to apply the policies.
-

## Deleting a User Account

Go to

Settings > Privilege > Users

Select one or more of the users and click the **Delete**  button under **More**.



Steps

The system will ask whether to keep the directory of the corresponding user or not. Select one of the options and click **Delete User**.



Are you sure you want to delete the user account "infortrend" ?

To delete this user account, select what you want to do with the home directory for this account, and then click "Delete user".

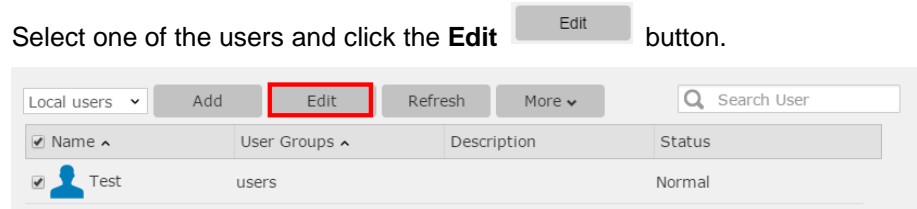
- ☒ Delete the home directory
- ☐ Keep the home directory for further use

## Editing a User Account

Go to

**Settings > Privilege > Users**

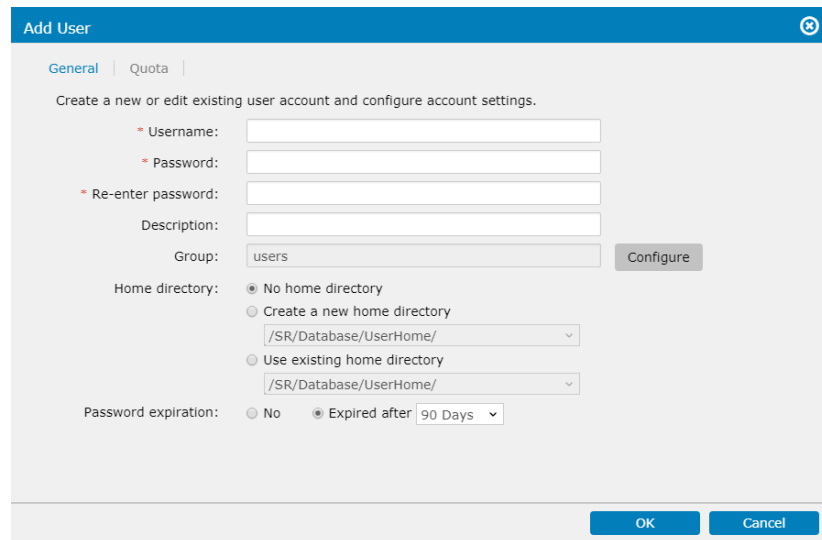
Select one of the users and click the **Edit** button.



Local users	Add	Edit	Refresh	More	Search User
Name	User Groups	Description	Status		
<input checked="" type="checkbox"/> Test	users		Normal		

### Steps

The parameters are the same as Adding a User Account. Modify the parameters and click **OK**.



**Add User**

General | Quota

Create a new or edit existing user account and configure account settings.

\* Username:

\* Password:

\* Re-enter password:

Description:

Group:  Configure

Home directory: ☒ No home directory  
☐ Create a new home directory  
☐ Use existing home directory

Password expiration: ☐ No ☒ Expired after 90 Days

OK Cancel



## Quota Management

Quota Management enables the system administrator to set maximum capacity limits for the users, so that the capacity of a volume will not be consumed by a small number of users, causing the rest of the users to have insufficient storage capacity available.

Note:

1. This operation can only be applied to file system enabled volumes.
2. When the specified capacity limit for a user is reached, write operations by the user to the volume will fail.

---

**Go to** **Settings > Privilege > Users**

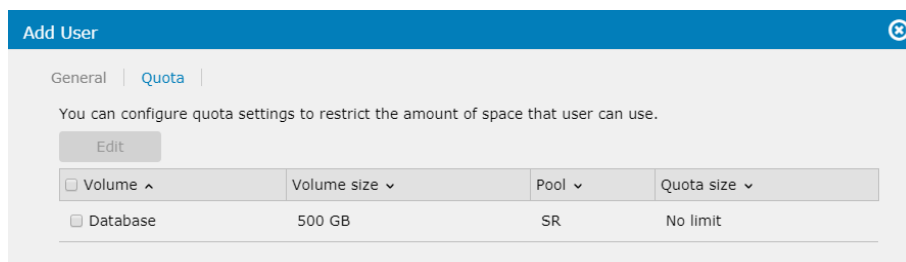
---

### Steps

When adding/editing a user, the administrator can set the quota size limit for the user.

1. Switch to the **Quota** page and select one or multiple volumes you want to set the limit for the user.

Note: By default, the quota size is “No limit” (i.e. until the whole volume space is used up).



**Add User**

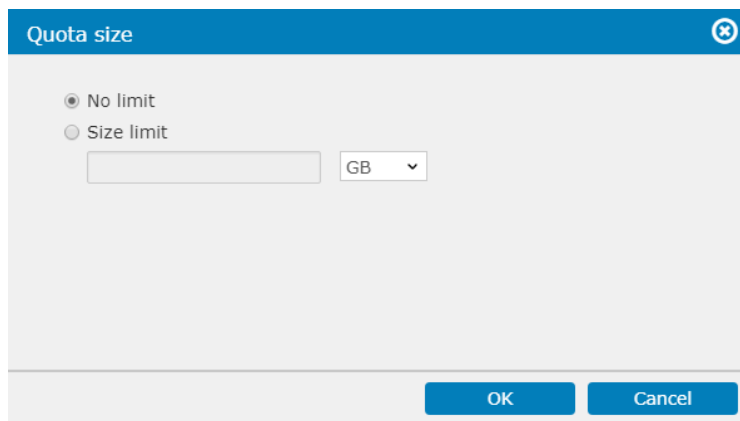
General | **Quota**

You can configure quota settings to restrict the amount of space that user can use.

**Edit**

Volume ^	Volume size v	Pool v	Quota size v
<input type="checkbox"/> Database	500 GB	SR	No limit

2. Click **Edit** to specify the limit size and click **OK**.



**Quota size**

☒ No limit

☐ Size limit

GB v

**OK** **Cancel**

3. The quota limit will be set. Click **OK** to apply the setting.

## Object Access Keys

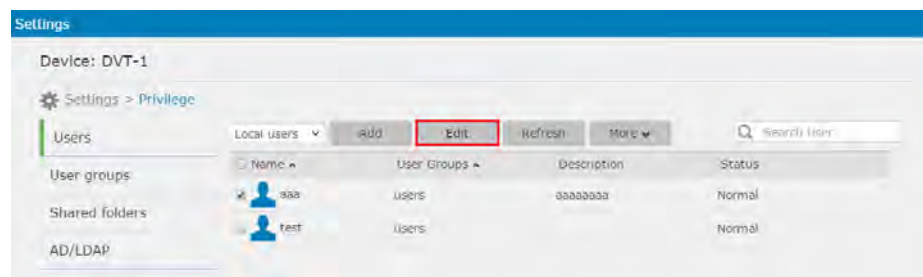
The administrator can create/delete object access keys for users.

Note: The maximum number of keys per user is 20.

**Go to**

**Settings > Privilege > Users**

Select a user and click the **Edit** button.

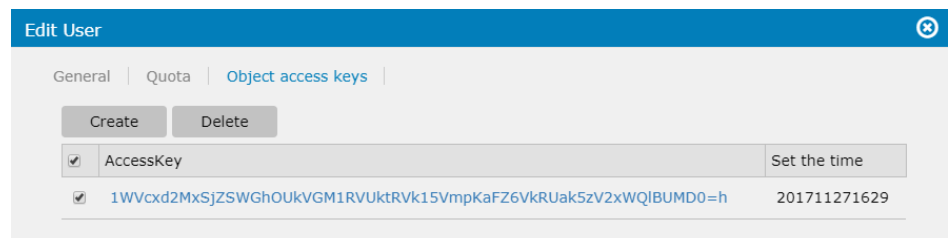


**Steps**

1. Switch to the **Object Access Keys** page.
2. Click the **Create** button to create an object access key. By clicking on the created key, you can view the key and endpoint information.



3. To delete one or more object access key(s), select the key(s) and click the **Delete** button.





## Access Object Storage

You can access the object storage via 3<sup>rd</sup> party software that can access the storage system through object protocol. For example, we used CloudBerry Explorer to access the object storage built on our PAC Storage PS/PSV to access and manage data. Please follow the instructions below to access object service. For more information, please visit <http://www.cloudberrylab.com>

### Go to

**File > New S3 Compatible Account > S3 Compatible**

### Steps

1. The account Settings page will appear. Enter the account information in the fields. Please refer to the **parameters** section below for the detailed information.

2. For the signature version, please select **version 2** from the drop-down list.
3. After completing the Settings, click the **Test Connection** button to verify the Settings. Press **OK** to finish.
4. Go back to the CloudBerry Explorer dashboard. Select the connection account from the **Source** drop-down list. Press **Refresh** button to update the status. Finally, you may configure the object storage via the CloudBerry Explorer.

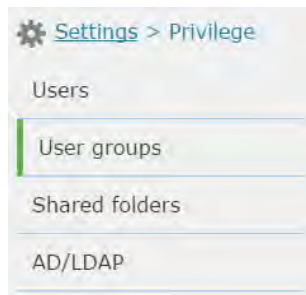
### Parameters

**Display name** The name of the connection.

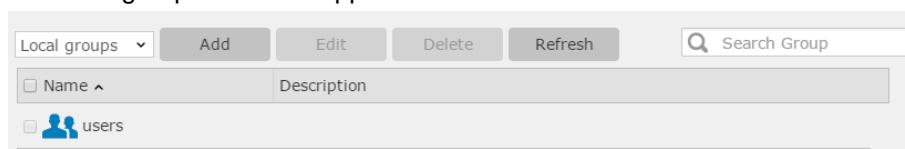
<b>Service point</b>	<p>Enter the <b>service endpoint</b> generate from object access keys in this field.</p> <div> <p>Note: If you want to connect over SSL, please select the network IP with port 8087.</p> </div>
<b>Access key</b>	<p>Enter the <b>access key</b> in the following format in the field:  <b>&lt;folder name&gt;:&lt;access key generated from object access keys&gt;</b></p> <p>EX: The source folder “aaa” with user’s access key “4VkZoYWQxWkh”, then the access key in this field may be “aaa: 4VkZoYWQxWkh”.</p>
<b>Secret key</b>	<p>Enter the <b>secret key</b> generate from object access keys in this field.</p>
<b>Use native multipart upload</b>	<p>Click the checkbox if you want to break large files into smaller segments and upload them in any sequence.</p>
<b>Signature version</b>	<p>Defines an authentication version.</p> <div> <p>Note: If your account is a S3 compatible account, please select version 2.</p> </div>

## User Group

**Go to** **Settings > Privilege > User Groups**



**View** The user group status will appear.



**Parameters**

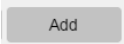
Name	
	Lists the user group names.

Description	
	Lists the descriptions of the user groups.

### Adding a User Group

Multiple users can be added into a group, making it easier to assign them to shared folders or to set the quota size limit for them.

**Go to** **Settings > Privilege > User Groups**

Press the **Add**  button to create a new group.

**Steps** Fill the Group Name and the Description information in the blank accordingly and select the Group Members that will be included in the new user group.

Add group
✕

Add a new group by configuring the name and checking the users for access rights.

\*Group name:

Description:

Group members:  Q

☒ Users ^

☒ Kevin

☒ SR

## Deleting a User Group

Multiple users can be added into a group, making it easier to assign them to shared folders.

**Go to**

**Settings > Privilege > User Groups**

Select one or more of the user groups and click the **Delete** button.

Local groups ▾
Add
Edit
Delete
Refresh

<input checked="" type="checkbox"/> Name ^	Description
<input checked="" type="checkbox"/> g1	test
<input type="checkbox"/> users	

**Steps**

A warning will pop up. Click **OK** to delete the user group.

Are you sure you want to delete the group?

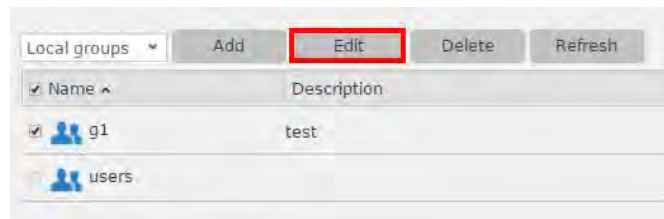
## Combining User Accounts into a Group (Editing a User Group)

Users can use the editing group function to combine multiple users into a group, making it easier to assign them to shared folders or to set the quota size limit for them.

**Go to**

**Settings > Privilege > User Groups**

Select one of the user groups and click the **Edit** button to edit the user group.



## Steps

Users can modify the Group Name and the Description information in the blank accordingly and add new group members that will be included in the user group.

Edit group

Edit the existing group parameters.

\*Group name:

Description:

Group members:

☐ Users ^

☒ Kevin

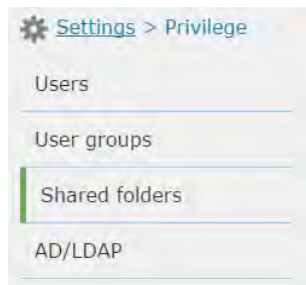
☐ SR



## Shared Folders

Go to

Settings > Privilege > Shared Folders



View

The shared folder status will appear.



Parameters

<b>Name</b>	The name of the shared folder
<b>Volume</b>	The source volume that contains the shared folder
<b>Pool</b>	The source pool that contains the shared folder
<b>Description</b>	The description for the shared folder
<b>Quota</b>	The storage limit of the shared folder

## Creating/Editing a Folder

### Before creating a Folder

A folder must be created on a file system enabled volume. For more information, please refer to the Create a Volume section.

**Go to** **Settings > Privilege > Shared Folders**

### Create/Edit a Folder

To create a folder, click the **Add** button. The folder configuration page will pop up.

Name	Volume	Pool	Description	Quota
RsyncFolder	Volume_file	Pool-1	Test	0 Byte
UserHome	Volume_file	Pool-1		0 Byte

To edit a shared folder, select the folder and click the **Edit** button. The folder configuration page will pop up.

**Folder configuration page:**

**Folder Name:** Specify a name for the new folder.

**Share Name:** Specify a name for the network sharing. Users only need to specify share name when CIFS, AFP or WebDAV is selected as an access protocol.

**Description:** Provide additional information of the shared folder.

**Location:** Choose the volume that stores the folder's directory. The volume must have file system enabled when created.

**Recycle bin:** Enable or disable a recycle bin for this shared folder. This option is only available when CIFS/SMB is selected.

---

**Parameters** Select the desired access protocols for the folder. You should enable the corresponding protocol services in Network Services first.

---

### CIFS/SMB

CIFS (Common Internet File System) and SMB (Server Message Block) enable access to files stored on file servers across an IP network in Windows OS environments. You can authenticate access through either Windows Domain, for users with Windows Active Directory (AD), or Windows Workgroup.

Three further options are available:

**Access-Based Enumeration:** This option hides folders or resources that the user is not allowed access to.

**SMB Encryption:** This option secures SMB/CIFS connections with AES-CCM encryption. The accessing client must support SMB 3.0 or above to build an encrypted SMB connection.

---

**Enable vfs\_fruit module (Not supported for Cloud):** This option increases compatibility of a SMB client running on the macOS system. This option is not available to a shared folder already connected to the cloud; a shared folder with this option enabled cannot be connected to the cloud.

---

## FTP

FTP (File Transfer Protocol) is a standard network protocol used to exchange and manipulate files over a TCP/IP based network.

---

## SFTP

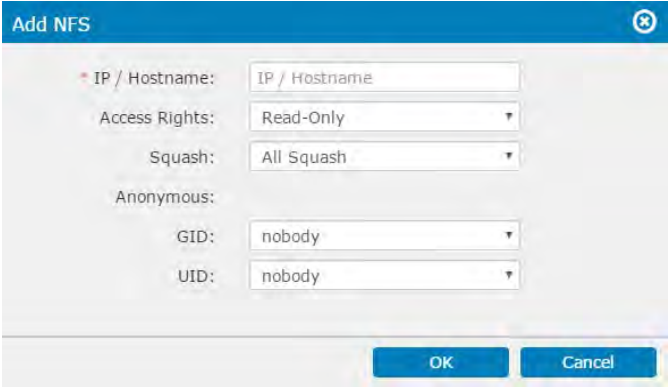
SFTP (SSH File Transfer Protocol or Secure File Transfer Protocol) is a network protocol that provides file access, transfer and management over any reliable data stream.

---

## NFS

NFS (Network File System) is a standard file transfer protocol for Unix/Linux networks, which allows users to access network files in a manner similar to accessing local files.

After you select this option, you will find further permission Settings on the **NFS Permission** tab by clicking **Add/Edit**:



**IP/Hostname:** Specify the IP address or hostname of a privileged user.

**Access rights:** Specify the user's access privilege: **Read only** or **Read/Write**.

**Squash:** Specify the access privileges for remotely accessing users:

- **All Squash:** All remote users are identified as anonymous users (i.e. non-administrator users) with limited privileges.

- **Root Squash:** A remote user with the root credentials is identified as an anonymous user with limited privileges. Remote users with other login credentials are identified as users listed at **Settings > Privilege > Users**, and have corresponding privileges.
- **No Root Squash:** A remote user with the root credentials is identified as a root user. Remote users with other login credentials are identified as users at **Settings > Privilege > Users**, and have corresponding privileges.

**Anonymous GID and UID:** Assign a group and user identifier to anonymous users.

---

## AFP

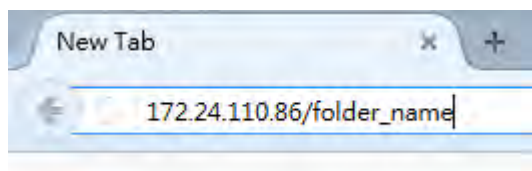
AFP (Apple Filing Protocol) is the standard file to transfer protocol for Mac OS X and AppleShare servers.

---

## WebDAV

WebDAV (Web Distributed Authoring and Versioning) is an extension of HTTP that allows users to perform remote Web content authoring operations.

To access a folder via WebDAV, please enter "Data port IP address/folder name" in a browser.



## Object

This data protocol allows your storage device to transfer small-chunk data (i.e. objects) with storage devices running OpenStack Swift or other object storage protocols.

To check all object storage service endpoints, click **All service endpoints**.

When you select this option to share the folder, all the other protocol options (e.g. FTP, CIFS/SMB) are disabled.

---


### Accessing Privilege

Click the **Permission** tab to assign the folder-access permissions to local/domain users and groups.

---

General | NFS Permission | **Permission** | Quota

You can edit the user and group access permissions of the shared folder.

Local users 

Name ^	Read/Write	Read only	No right
Other	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AAA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
testuser123	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ttt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
testuser	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
555	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note:

1. When a user is assigned permissions in both the **NFS Permission** and **Permission** tabs, the system grants the user with only the lower-level permission.
2. The system determines a user's permissions in the **Permission** tab in the priority order: user permissions > group permissions > "Other".

When the folder-hosting volume is enabled with advanced ACL, the priority order is: user permissions > group permissions > "Everyone". To check the "Everyone" permissions, go to **Settings > Privilege > Shared folders**, choose a shared folder, and click **Edit > Permission > Customize**.

---

### Customize permission

You can assign advanced access control list (ACL) permissions to better control folder access.

Before you proceed, check Adding a Volume to enable advanced ACL for the folder-hosting volume.

1. Go to the **Permission** tab and select **Customize** for a desired user.
  2. On the pop-up, select the desired advanced permissions.
-

3. Specify the **User/Group** on the top of the page and select a **access type** from the drop down. You can also apply the permission to its subfolder/files by configuring via the **Applies to** drop down list. If you want to **apply the permission to objects or containers within the folder**, tick the checkbox below the drop-down list.
4. In the permission section, set the management permissions for the configured user.

**Change permission:** The configured user have the right to change the access permission Settings.

**Take ownership:** The configured user have the right to set himself as the file owner.

In Read subsection, you can set the advanced read permission Settings.

**Traverse folders/execute files:** The user have the permission to traverse folders and their subfolders.

**List folders/read data:** If the configured target is a folder, the user can read the contents of the folder; if the configured target is a file, the user can read the file contents.

**Read attribute:** Allow the user to read attributes (i.e. read-only, hidden, etc.) of the

file or folder.

**Read extended attributes:** Allow the user to read extended attributes of the file or folder.

**Read permissions:** Allow the user to read the file or folder contents.

At the bottom of the page, you can also set the advanced write permission Settings.

**Create files/write data:** Allow the user to create a new file within the folder. If the configured target is a file, the user is allowed to add data to the existing file without modifying the original content.

**Create folders/append data:** If the configured target is a folder, the user is allowed to create a new subfolder; if the configured target is a file, the user is allowed to add contents into the existing data without modifying its original content.





**Write attribute:** Allow the user to modify attributes (i.e. read-only, hidden, etc.) of the file or folder.

**Write extended attributes:** Allow the user to modify extended attributes of the file or folder.

**Delete subfolders and files:** Allow the user to delete subfolders and files of the folder. Note that even if the user does not have delete permission, he/she can still delete subfolders and files within the folder.

**Delete:** Allow the user to delete a specific folder.

- Click **Apply** to save the Settings and you will be redirected to Privilege Settings page. You can examine all the permission Settings on the list and **Add/Edit/Delete** the permission by clicking the buttons on the top of the page. If you want to **Replace all child object permission entries with inheritable permission entries from this folder**, tick the checkbox at the bottom of the page. Click **Apply** to complete the Settings.

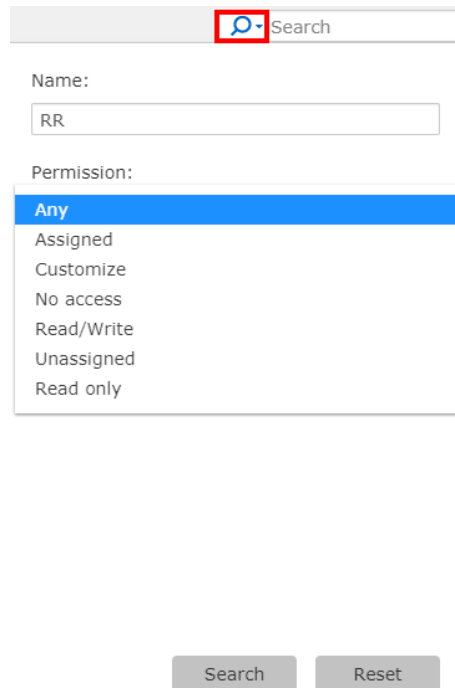
Privilege settings		
<div> <div>Add</div> <div>Edit</div> <div>Delete</div> </div>		
<input type="checkbox"/> Name ^	Type	Permission
<input type="checkbox"/>  Admin	allow	Customized
<input type="checkbox"/>  Everyone	allow	Customized
<input type="checkbox"/>  test	allow	Read/Write
<input type="checkbox"/>  users	allow	Customized

- You will be redirected to Add/Edit folder page, click **Save** after configuring all the Settings.



## Advanced Search

Click on the left side button in the Search bar, the advanced search tool will appear.  
Specify the user name and access permission for applying the search.



The image shows the Advanced Search interface. At the top, there is a search bar with a magnifying glass icon on the left and the word 'Search' on the right. Below the search bar, there are two input fields. The first is labeled 'Name:' and contains the text 'RR'. The second is labeled 'Permission:' and has a dropdown menu open. The dropdown menu lists the following options: 'Any' (highlighted in blue), 'Assigned', 'Customize', 'No access', 'Read/Write', 'Unassigned', and 'Read only'. At the bottom of the form, there are two buttons: 'Search' and 'Reset'.

## Parameters Access Rights

- Read only: allows the user to read.
- Read/Write: allows the user to read and write.
- No access: deny user's access.
- Customize: the access other than the above access rights.
- Any: Sort the users according to the name only.
- Unassigned: users who have not been set up for access.
- Assigned: all users with configured access rights.

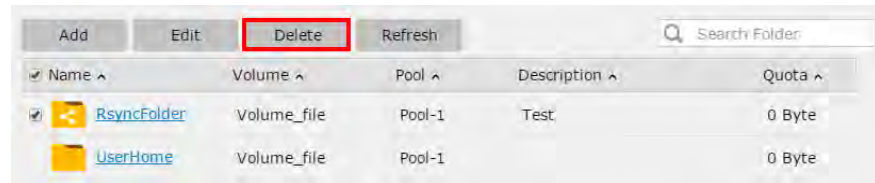
## Deleting a Folder

Go to

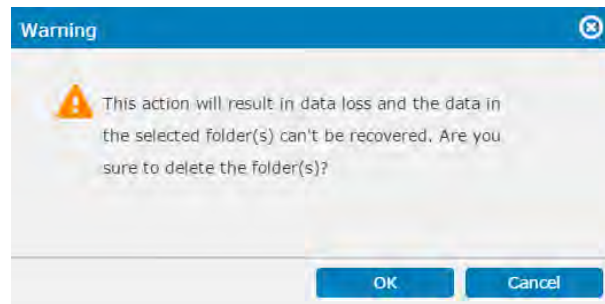
Settings > Privilege > Shared Folders

Steps

1. Select a folder and click the **Delete** button.



2. A warning message will appear. Click **Yes** to confirm.

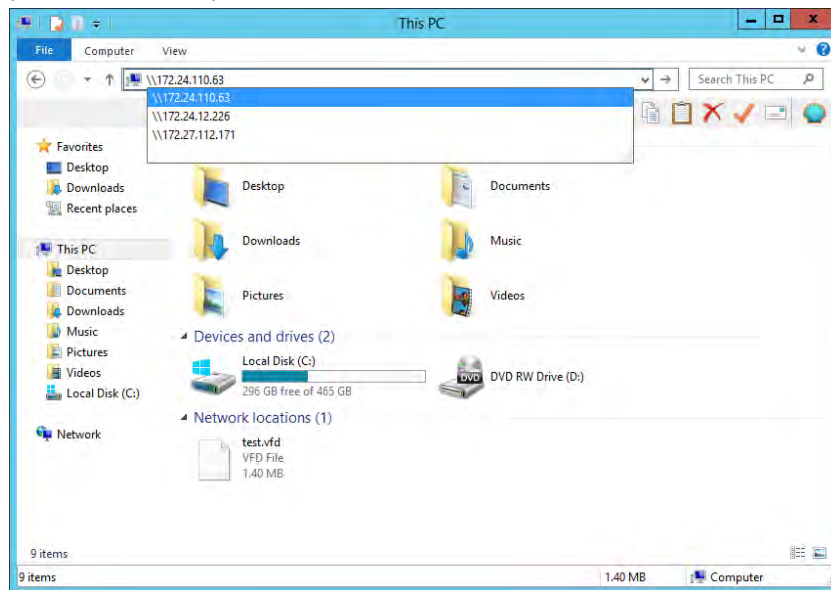


## Accessing a Folder

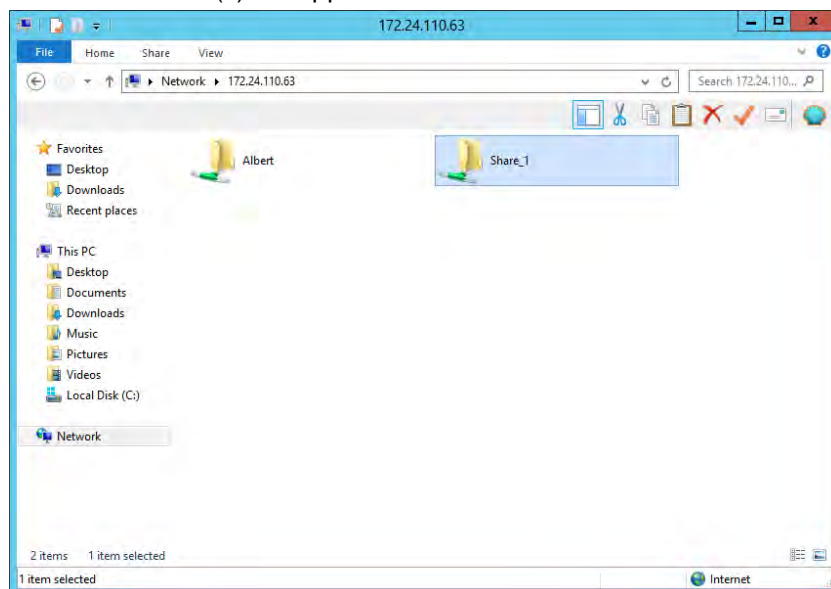
After sharing folders, users can access the sharing folder via folder browser.

### Steps

1. Check IP address of Host Channel Parameters.
2. Open folder browser and enter the IP address.  
(\\xxx.xxx.xxx.xxx)



3. The shared folder(s) will appear in the browser.

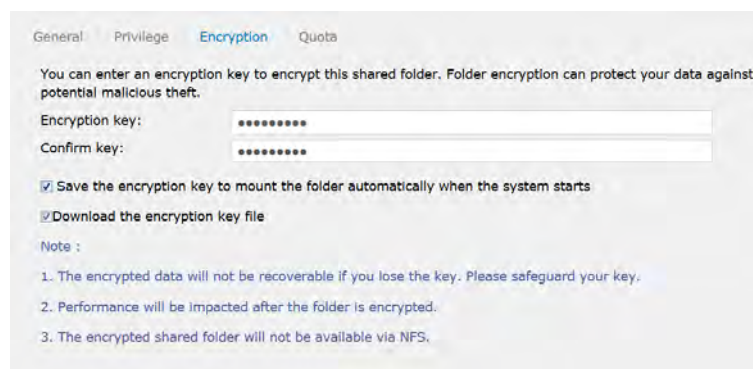


## Encrypting a Folder

Folder Encryption provides data protection in the case of malicious attacks on the system or theft of hard disks. The PAC Storage User Interface Firmware can perform AES 256-bit encryption on the data in the shared folders for protection against unauthorized access. When creating the folder, the administrator can set an encryption key which can be stored in the system based on user selection to automatically decrypt the folder at boot-up. The user can also choose to download the key to the local host for safekeeping.

When a NAS or domain user connects to the PAC Storage PS/PSV, an encrypted shared folder that is unlocked will allow authorized users to access the data as other regular shared folders. Users will not be able to see an encrypted shared folder that is locked.

### Add a new folder and enable folder encryption



1. Click on the **Encryption** tab.
2. Enter the encryption key in the field **Encryption key** and re-enter it in **Confirm key**.

The key must be at least 8 characters long and can contain any characters on the keyboard, including space (but the key cannot start or end with the space character). The maximum length is 32 characters. If this field is empty, the folder will NOT be encrypted.

3. Further options are available:
  - **Save the encryption key to mount the folder automatically when the system starts:** The system will remember the provided encryption key and mount this shared folder for access upon the system startup.
  - **Download the encryption key file:** You can download the encryption key into a text file and keep it in a safe location. If the key is lost, you will never be able to recover data in this shared folder.
4. Click **Save** to enable the Settings.

Note:

1. Please safeguard the encryption key. The encrypted data will not be recoverable if you lose the key.
2. The encryption process will slightly affect the system performance.
3. The encrypted shared folder will not be accessible via NFS.
4. You cannot encrypt a shared folder after it is created.

### Lock a folder

1. Go to **Settings> Privilege > Shared folders**. If a shared folder is locked, there will be an icon with a lock next to the name. If a shared folder is unlocked, there will be an icon with an opened lock next to the name. Select the shared folder to lock and click on the **Edit** tab.



Name	Volume	Pool	Description	Quota
<input checked="" type="checkbox"/> Shared_Folder	Volume_Target	Pool-1		0 Byte
<input type="checkbox"/> TargetFolder	Volume_Target	Pool-1		0 Byte
<input type="checkbox"/> UserHome	Volume_Target	Pool-1		0 Byte

2. Click on the **Encryption** tab. Check the box **Lock the folder now** to lock the shared folder. You can choose to save the key in the system for automatic mounting of the folder at system start-up. You can also download the key file to the local host for safekeeping (click on **Download Encryption Key File**).
3. Click **Save** to enable the Settings.

### Unlock a folder

1. Go to **Settings > Privilege > Shared folders**.  
If a shared folder is locked, there will an icon with a lock next to the name.  
If a shared folder is unlocked, there will an icon with an opened lock next to the name.
2. Select the shared folder to unlock and click on the **Edit** tab. Then, click on the **Encryption** tab.



Name	Volume	Pool	Description	Quota
<input checked="" type="checkbox"/> Shared_Folder	Volume_Target	Pool-1		0 Byte
<input type="checkbox"/> TargetFolder	Volume_Target	Pool-1		0 Byte
<input type="checkbox"/> UserHome	Volume_Target	Pool-1		0 Byte

3. Enter the encryption key or import a key file. Click **Save** to enable the Settings.

---

Add/Edit Folder

General

Privilege

Encryption

Quota

Currently the encrypted shared folder is locked and thus inaccessible. Please use one of the following ways to unlock the folder:

☒ Enter the encryption key.

☐ Import the encryption key file

\*\*\*\*\*

Browse

Save

Cancel

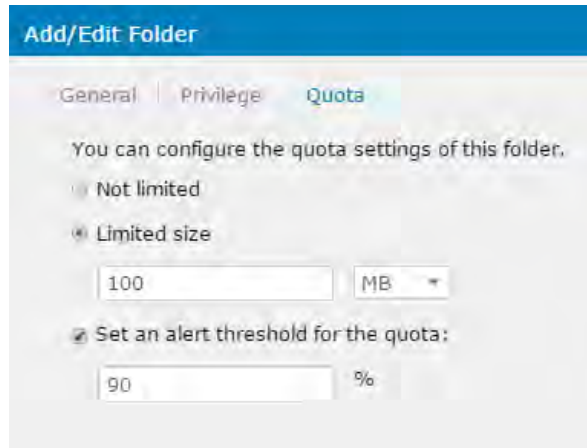
## Quota Management for a Folder

Quota Management for a shared folder enables the system administrator to set a maximum capacity limit for the folder.

Go to

Settings > Privilege > Shared folders

### Set folder quota



**Add/Edit Folder**

General | Privilege | **Quota**

You can configure the quota settings of this folder.

☐ Not limited

☒ Limited size

100 MB

☒ Set an alert threshold for the quota:

90 %

1. Go to the **Quota** page and set the capacity limit for the folder.

Note: By default, the quota size is **Not limited** (i.e. until the whole volume space is used up).

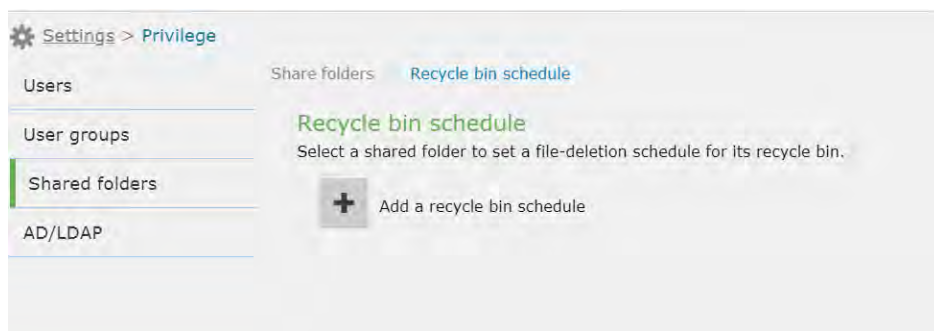
2. You can choose to have the system issue an alert when the capacity utilization of the folder reaches the specified threshold in percentage. Click the check box **Set an alert threshold for the quota** and enter an integer value between 1 and 99.
3. Click **Save** to apply the Settings.

## Recycle Bin Schedule

After enabling the recycle bin for a shared folder, you can set up a schedule to empty it.

Go to

**Settings > Privilege > Shared folders > Recycle bin schedule**



Steps

1. Click on **Add a recycle bin schedule**.
2. On the pop-up, select a desired shared folder. Then, click **Next**.
3. Complete the following Settings:

<b>Specify the name of the schedule</b>	Assign a name to this recycle bin schedule.
<b>Current date/time</b>	Check current time.
<b>Select the initialization policy</b>	<p>Select when to begin emptying the recycle bin:</p> <p><b>Start now:</b> The system immediately runs the schedule and empties the recycle bin.</p> <p><b>Specify a start date and time:</b> The system runs the schedule from the specified time.</p>
<b>Select the activate frequency</b>	<p>Select how often to empty the recycle bin:</p> <p><b>Once, Daily, Weekly, or Monthly.</b></p>
<b>File deletion policy</b>	<p>Select how to empty the recycle bin:</p> <p><b>Delete all files:</b> The system deletes all files from the recycle bin.</p> <p><b>Delete old files:</b> The system deletes files past the specified retention days.</p> <p><b>Delete files when the recycle bin reaches the maximum size:</b> When the recycle bin exceeds the maximum size, the system deletes</p>



---

files following the selected action: **Delete large files first** and **Delete old files first**.

Recycle bin schedule

\* Specify the name of this schedule

New\_Schedule\_20181024\_13350

Current date/time

2018-10-24 13:32:13

Select the initialization policy

☒ Start now

☐ Specify a start date and time

Select the activate frequency

☒ Once

☐ Daily

☐ Weekly

☐ Monthly

4. Click **Next**.
  5. Check the schedule Settings and confirm them by clicking **OK**.
-

## AD/LDAP Settings

The Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) are the standard application protocols for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

Note: To join the storage device to a Windows AD domain, do not include any underline (\_) character in the file server names (in **Settings > System > File server name**).

### Windows Active Directory Settings

<b>Go to</b>	<b>Settings &gt; Privilege &gt; AD/LDAP</b>	
	Select <b>Windows Active Directory</b> from the drop down list.	
<b>Parameters</b>	<b>AD Server (IP Address)</b>	Specifies the IP address of the AD server.
	<b>AD Security</b>	Specifies how the system will communicate with the AD server. You can select none or an encrypted connection with TLS.
	<b>Username / Password</b>	The root username and password.
	<b>DNS authentication</b>	<p>Select the option according to the DNS server's authentication requirement.</p> <p><b>No authentication required:</b> Select this option if the DNS server does not require any authentication.</p> <p><b>Same with AD server:</b> Select this option if the DNS server requires the same authentication information provided by the AD server.</p> <p><b>Manual:</b> Select this option and provide the username and password if the DNS server requires specific authentication information.</p>
	<b>Number of trusted domains</b>	<p><b>Only this AD domain:</b> The storage device trusts only the AD domain that it joins.</p> <p><b>Multiple AD domains:</b> The storage device trusts multiple AD domains. Click <b>Add trusted domain</b> to</p>

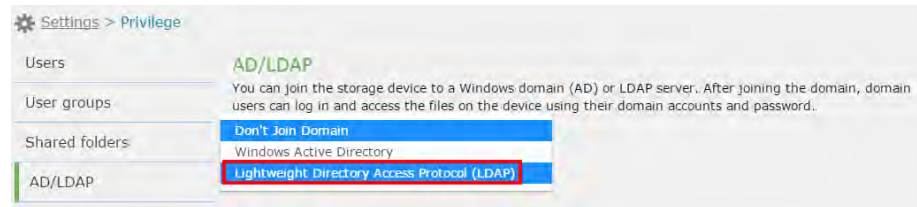
	specify the AD domains to trust.
<b>Mapping backend</b>	<p>Specify how to pull the domain user data from the AD server.</p> <p><b>RID:</b> The system pulls the domain users from the domain server and creates a new GID and UID for each domain user.</p> <p><b>AD:</b> The system pulls the domain users from the domain server. The domain users continue to use the GIDs and UIDs assigned by the domain server.</p>
<b>Authentication Level</b>	Specifies the Authentication level.
<b>Check domain</b>	Click this button to check if all the provided domain information is valid.
<b>Create home folder</b>	<p>Choose a local folder to create a home folder for the domain users.</p> <p>Choose <b>Don't create</b> if you do not want to create a home folder.</p>
<b>Update interval</b>	Choose how often to update the domain user and group information with the domain server: <b>Daily</b> , <b>Weekly</b> , or <b>Monthly</b> . Then, choose desired dates or days and set the start time.
<b>Update the user list</b>	Click this button to sync updates regarding domain users and groups from the domain server.

## Lightweight Directory Access Protocol Settings

Go to

**Settings > Privilege > AD/LDAP**

Select **Lightweight Directory Access Protocol** from the drop down list.



**Parameters**

**LDAP Server (IP Address)**

Specifies the IP address of the LDAP server (Directory System Agent).

**LDAP Security**

Specifies how the system will communicate with the LDAP server. You can select none or an encrypted connection with TLS.

**Base DN**

Specifies the LDAP domain.  
For example: dc=aadomain,dc=aa.local

**Root DN**

Specifies the LDAP root.  
For example: cn=admin, dc=aadomain,dc=aa.local

**Password**

The root username and password.

**Update interval**

Choose how often to update the domain user and group information with the domain server: **Daily**, **Weekly**, or **Monthly**. Then, choose desired dates or days and set the start time.

**Create the user's home directory**

Select an available directory or choose not to create any.

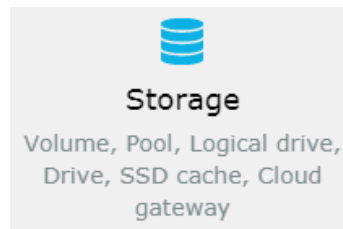
# Storage

The Storage setting menu contains the following sub-Settings.

1. Pool
2. Volume
3. Drive
4. SSD cache
5. Storage Maintenance


**Go to**

**Settings > Storage**




---

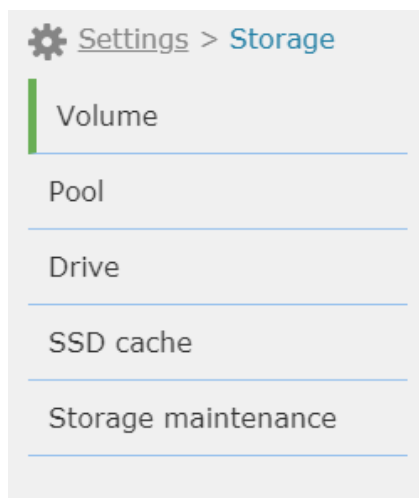
## Storage Provisioning Menu

The Storage Provisioning menu for the selected device will appear. Users can switch to the sub-setting pages or click  [Settings](#) to go back to the previous setting page.

## Volume

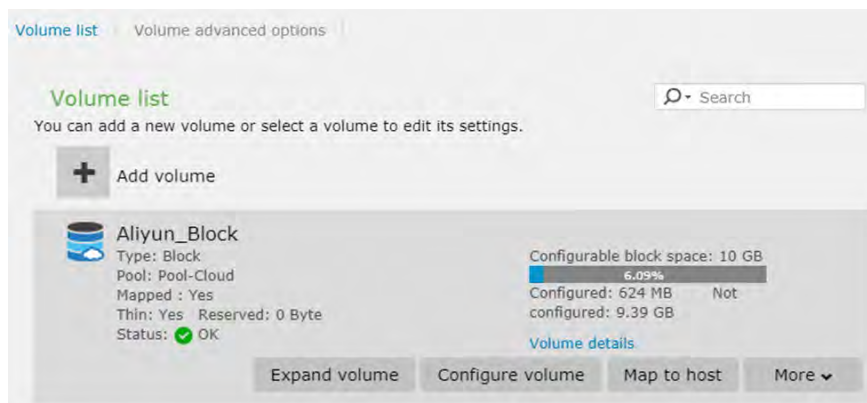
Go to

Settings > Storage > Volume



View

You can add a volume or select a volume to edit its Settings from the volume list tab.



Parameters

**Volume Name**

Shows the volume name.

**Capacity**

Shows the capacity of the volume, including the total, used, and free capacity.

**Type**

Shows the type as file-level or block-level.  
If the volume is configured in block-level, the capacity progress bar may be turned in blue; if it is set to file-level, the progress bar may be shown in green.

**Pool**

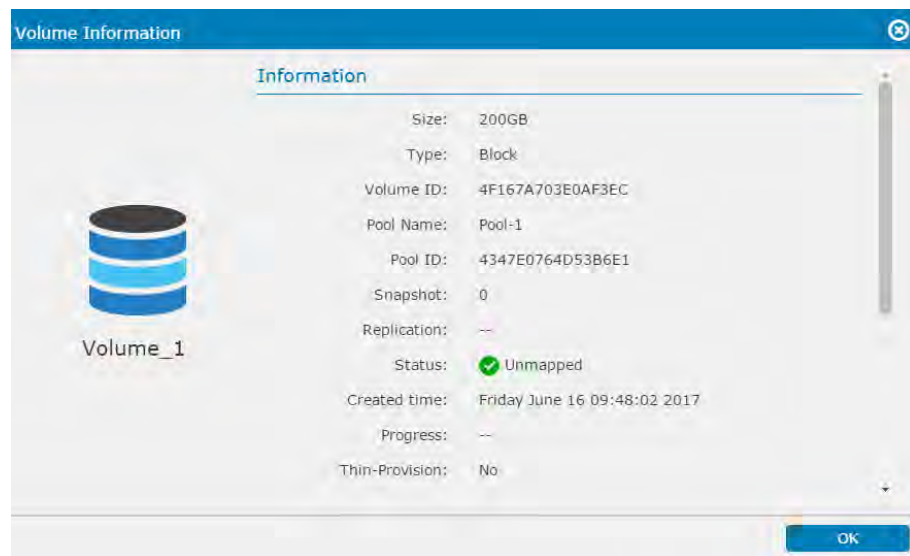
Tells which pool allocated capacity to the volume.

**Mapped**

Shows whether the block-level volume is mapped or not.

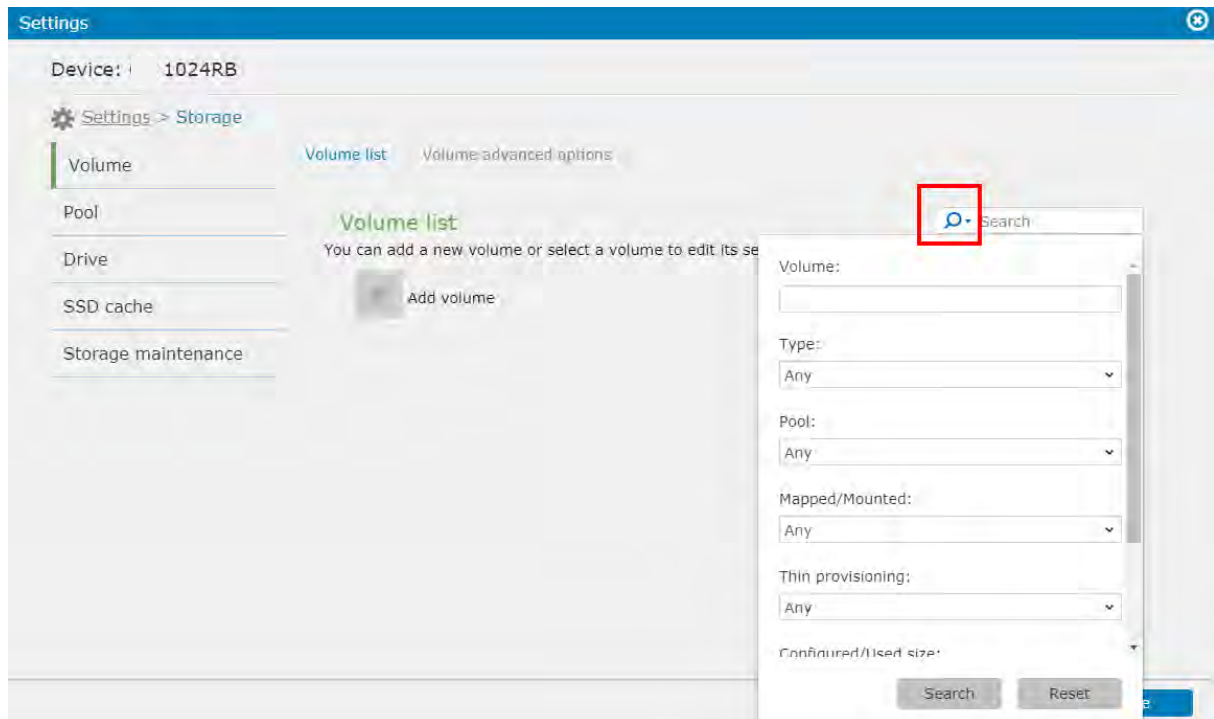
<b>Mounted</b>	Shows whether the file-level volume is mounted or not.
<b>Thin-Provision</b>	Shows whether the volume has enabled thin provisioning or not.
<b>Status</b>	Shows the volume status.

Click **Volume Details** to see more information.



## Advanced Search

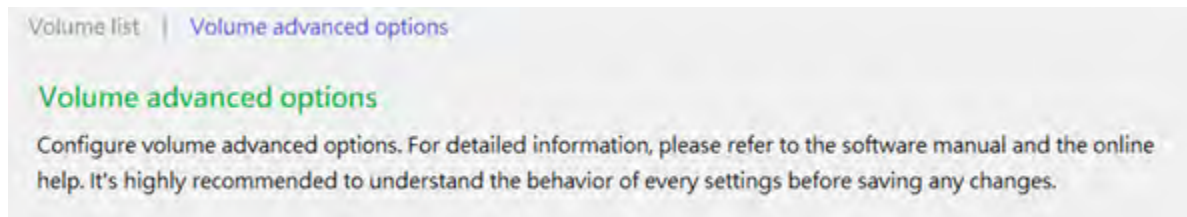
You can use the Advanced Searching bar from the top-right corner of the page to search using multiple advanced conditions. Once you open advanced searching, the following window will be displayed:



<b>Parameters</b>	<b>Name</b>	Select a pool for the volume to claim capacity.
	<b>Type</b>	Select a volume type.
	<b>Pool</b>	Enter the name of the volume.
	<b>Mapped/Mounted</b>	Select "Yes" or "No" whether to searched volume has mapped/mounted, "Any" is set as factory default.
	<b>Thin provision</b>	Select "Yes" or "No" whether the searched volume has Thin provision function, "Any" is set as factory default.
	<b>Configured/Used size</b>	Select "Yes" or "No" whether the searched volume has Configured/Used size. "Any" is set as factory default.
	<b>Configurable/Total size</b>	Select "Yes" or "No" whether the searched volume has Configured/Total size. "Any" is set as factory default.



## Volume advanced options



Select “Volume advanced options” tab on the right of the “Volume list” tab and the following window will be displayed:

Volume list | [Volume advanced options](#)

## Volume advanced options

Configure volume advanced options. For detailed information, please refer to software manual and online help. It's highly recommended to understand the behavior of every setting before saving any changes.

Maximum number of queued I/O

1024

LUN per host SCSI ID

32 LUNs

Tags reserved per host-LUN connections

4

Peripheral device type

(0D) Enclosure services

Peripheral device qualifier

Connected

☐ Device supports removable media

LUN applicability

First undefined LUN

Cylinder/Head/Sector

Default (variable/ variable/ ...

Save

<b>Parameters</b>	<b>Maximum number of queued I/O</b>	Specifies the maximum number of I/O operations per host channel that can be accepted from servers.
	<b>LUN per host SCSI ID</b>	Fibre Channel technology can address up to 126 devices per loop, and theoretically more than a million, using the FC switches. Each configured RAID volume is

	<p>associated with host IDs and appears to the host as a contiguous volume.</p> <p>Choose the parameter for your LUN per host SCSI ID</p>
<b>Tags reserved per host-LUN connections</b>	<p>Specifies that each nexus has at least this number of tags accessible per nexus to prevent the host sending less tags due to busy state.</p> <p>Set the parameter for the tags that are reserved per host-LUN connections.</p>
<b>Peripheral device type</b>	<p>The firmware default is Enclosure Service Device, which enables a brand new system to appear to host to enable in-band management. Different host operating systems require different adjustments.</p> <p>Select the peripheral device type from the scroll down list.</p>
<b>Peripheral device qualifier</b>	<p>Select the qualifier for your peripheral device to "Connected" or "Supported but not Connected" from the scroll down list.</p>
<b>Host devices support removable media</b>	<p>Enable or Disable Host devices support removable media for searching.</p>
<b>LUN applicability</b>	<p>Select "First Undefined LUN" or "Only Undefined LUN 's".</p>
<b>Cylinder/Head/Sector</b>	<p>In Solaris, the capacity of a drive is determined by the cylinder/head/sector count.</p> <p>Select the valuables from the scroll down list.</p>

Press **Save** button to complete volume advanced options, if nothing was changed in this page, the Save button will display as "**Disabled**"

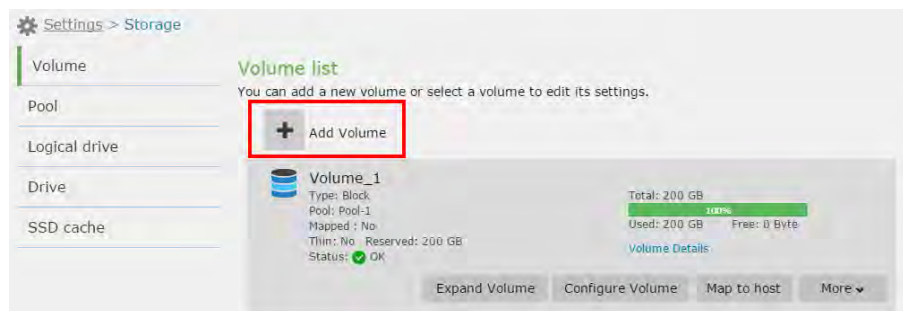
## Adding a Volume

The maximum size of a single volume is 2PB. Make sure that the size of the pool is in line. Please note that you cannot make the size of the volume larger than the size of the pool. For the latest status,

please check with technical support.

**Go to**      **Settings > Storage > Volume**

Click **Add Volume**, the volume configuration table will be shown.



**View**      The configuration window will appear.

Create volume

Configure volume parameters.

Select a pool used for creating this volume

FileExplorer

Select a volume type

Block-level volume for SAN

\* Specify a volume name

\* Specify the space allocated to this volume. Available free space: 228.67 GB

GB

☐ Use data deduplication to reduce storage overhead (thin provisioning will be enabled to make this feature available)

[Deduplication settings](#)

☐ Use thin provisioning to create the volume with a size (as reported to the application) exceeds the available free space. Maximum space supported: 2 PB

PB

☐ Enable WORM (Write-Once, Read-Many) to lock files within volume from modification and unauthorized deletion (this feature only available on file-level for NAS).

[WORM settings](#)


**Parameters**      **Pool**      Select a pool for the volume to claim capacity.

**Volume Type**      Select a volume type.

Select a volume type

Block-level volume for SAN

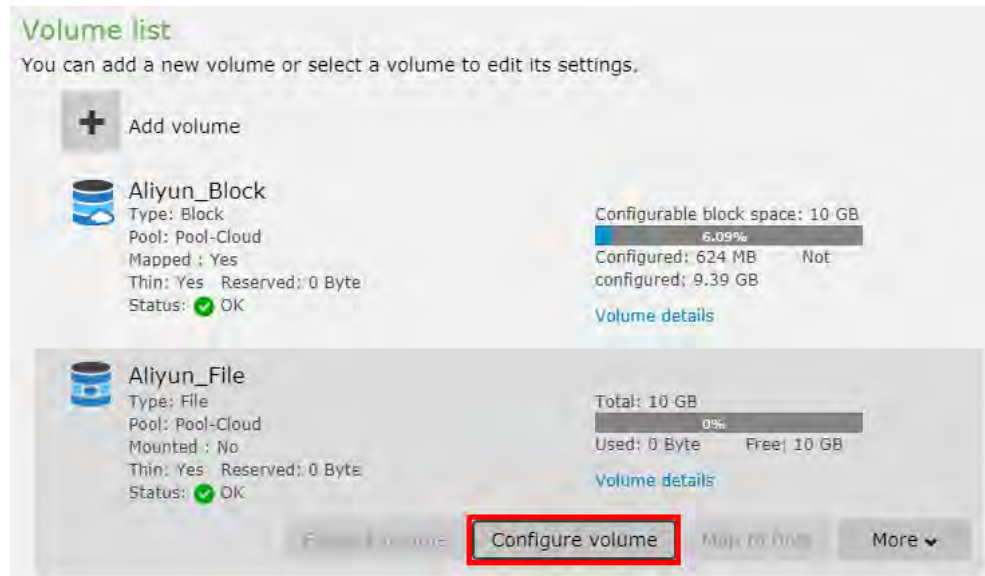
File-level volume for NAS

<b>Volume Name</b>	Enter the name of the volume.
<b>Advanced ACL</b>	<p>Enable this option to apply NTACL for better control over folder access. This option is only available on file-level volumes, and cannot be disabled once enabled.</p> <div> <input type="checkbox"/> Enable advanced ACL to get better access control for the folders.  </div>
<b>Data Deduplication (Beta)</b>	<p>Enable this function to reduce storage overhead. A pop up warning message will be displayed if your pool's available space must exceed more than 30GB.</p> <div> <input type="checkbox"/> Use data deduplication to reduce storage overhead (thin provisioning will be enabled to make this feature available)  <a href="#">Deduplication settings</a> </div> <p>Note:</p> <ol style="list-style-type: none"> <li>To try out this beta feature, contact the vendor for the special firmware update.</li> <li>You must set up thin provisioning to enable this function.</li> </ol>
<b>Thin Provisioning &amp; Minimum Reserved Space</b>	Enables thin provisioning. Enter the volume size to set the volume capacity that will be physically allocated as a safe reserve. If the reserve reaches 100%, the volume becomes fully-provisioned (all space is allocated from the pool). For more information, refer to the next section.
<b>Volume Size</b>	<p>Specifies the size and unit of the volume. If Thin Provisioning is enabled, the total size of volumes can exceed the size of the pool.</p> <div>The minimum size of a volume is 10GB.</div>
<b>Enable WORM</b>	Enable WORM (Write Once Read Many) functionalities. Refer to Creating a WORM Volume for more details.
<b>Enable case-insensitive file and folder names</b>	<p>Enable this option so that the system does not distinguish folders or files sharing the same name but in different cases.</p> <p>For example, folders named "xyz" and "XYZ" are treated as the same.</p>
<b>Host LUN Mapping</b>	Maps the volume to all host ports. If you want to select the host port, you may manually map it later. For more information, refer to the next section.

## Renaming a Volume

Go to **Settings > Storage > Volume**

1. Select the volume and click **Configure Volume**.



2. Change the volume name and click **OK**.

**Configure volume**

Select a pool used for creating this volume  
Pool-2 ▼

Select a volume type  
Block-level volume for SAN ▼

Specify a volume name  
Cloud\_Volume

Specify the space allocated to this volume. Available free space: 235.29 GB  
10 GB ▼

## Creating a WORM Volume

The PAC Storage PS/PSV supports WORM (Write Once Read Many) functionalities by allowing administrators to create a WORM volume with the following features:

- Files in a WORM volume are read-only and cannot be modified, renamed or deleted during the retention period after the Settings are manually changed (automatic lock is not enabled) or the lockout wait time expires (automatic lock is enabled).
- Compliance WORM and Enterprise WORM are supported.
  - Compliance WORM: No one is allowed to delete the WORM files during the retention period.
  - Enterprise WORM: system administrators are allowed to delete the WORM files during the retention period.
- CIFS/SMB, NFS and FTP are supported.
- Files can be locked automatically or manually.

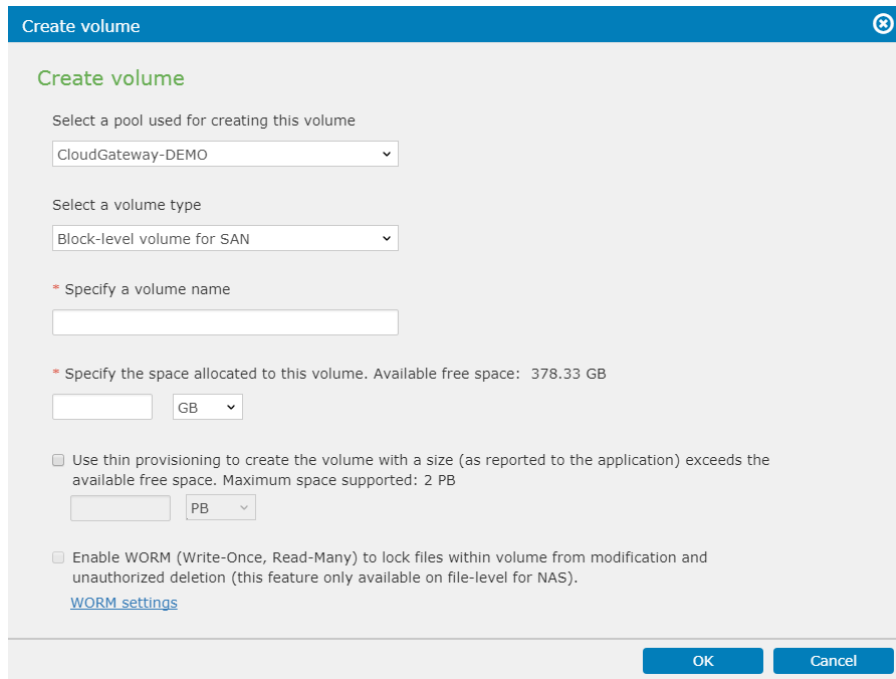
Due to the WORM characteristics, there are the following limitations with WORM volumes:

- Cloud cache and Cloud tiering are not available for WORM volumes.
- Snapshots of WORM volumes are read-only.
- Rollback with snapshots is not available for WORM volumes.
- Remote replications on WORM volumes should have the source and the target in the same mode (both compliance or both enterprise), and the target should be a new volume.
- Retention period cannot be extended. Files with expired status cannot be locked again.

---

**Go to**      **Settings > Storage > Volume > Add Volume**

1. Select the volume type to **File-level volume for NAS** and then check **Enable WORM**. Click the **WORM Settings** button to configure the Settings.



**Create volume**

Create volume

Select a pool used for creating this volume  
CloudGateway-DEMO

Select a volume type  
Block-level volume for SAN

\* Specify a volume name  
[Text input field]

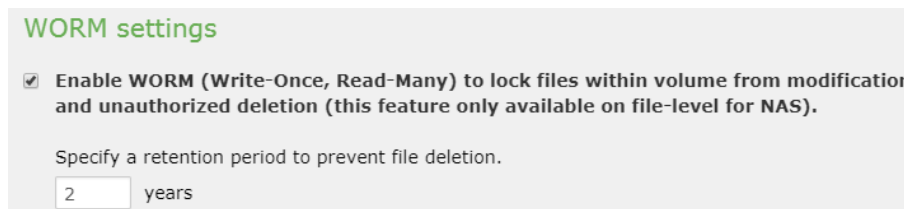
\* Specify the space allocated to this volume. Available free space: 378.33 GB  
[Text input field] GB

☐ Use thin provisioning to create the volume with a size (as reported to the application) exceeds the available free space. Maximum space supported: 2 PB  
[Text input field] PB

☐ Enable WORM (Write-Once, Read-Many) to lock files within volume from modification and unauthorized deletion (this feature only available on file-level for NAS).  
[WORM settings](#)

OK Cancel

- In the WORM Settings page, check the Enable WORM checkbox on the top of the page and specify a **retention period** of the volume.



**WORM settings**

☒ **Enable WORM (Write-Once, Read-Many) to lock files within volume from modification and unauthorized deletion (this feature only available on file-level for NAS).**

Specify a retention period to prevent file deletion.  
2 years

- Select a **WORM mode**. Please refer to the parameter description below.
- Select the **file locking mode**.  
You can either manually or automatically change file property into read-only.
- Click **OK** to save the Settings.

The other steps and options are the same as the creation procedures for regular volumes.

WORM volumes have an indication of WORM in the **Type** field in the list of volumes.



**Volume worm**

Type: File(WORM)

Pool: Block-File-System

Mounted : Yes

Thin: Yes Reserved: 0 Byte

Status: OK

Total: 10 GB

Used: 32 MB Free: 9.96 GB

[Volume details](#)

**Note:**

- WORM configurations of a WORM volume are NOT editable.



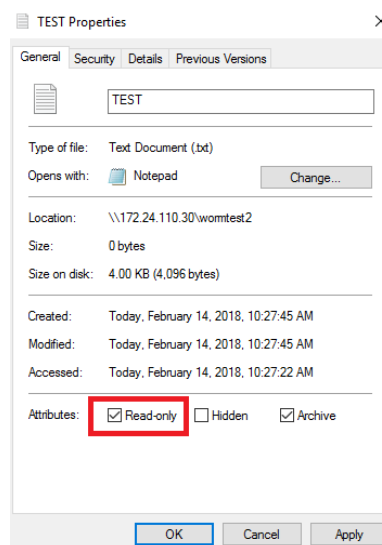
2. A volume without the WORM attribute enabled at creation cannot be changed to a WORM volume at a later time.
3. A WORM volume can be deleted by the administrator only if the retention periods for all the files in the volume have expired.

---

<b>Parameter</b>	<p><b>Mode:</b> Choose one from the two supported modes: Enterprise or Compliance.</p> <ul style="list-style-type: none"> <li>● <b>Enterprise</b> (default): Files within retention cannot be modified, renamed or deleted by common users, but can be deleted by system administrators. After retention, the files can be deleted but cannot be modified by common users and system administrators.</li> <li>● <b>Compliance:</b> Files within retention cannot be modified, renamed or deleted by common users and system administrators. After retention, the files can be deleted but cannot be modified by common users and system administrators.</li> </ul>
------------------	--

**Retention period (years):** The text field accepts a positive integer to specify the retention period of files in the volume. The maximum valid value is 999. The default value is 2.

**Manually change file property to read-only:** By enabling this option, users are able to change the permission to read-only under file's properties. Once changed to read-only, it will activate WORM function and can no longer be edited afterwards.



**Automatic file locking (hours):** If this option is enabled, when the specified waiting time has expired after a file is created and is being written, the file will automatically go into the read-only state (i.e. locked). Valid values are integers from 2 to 168 and the default value is 2.

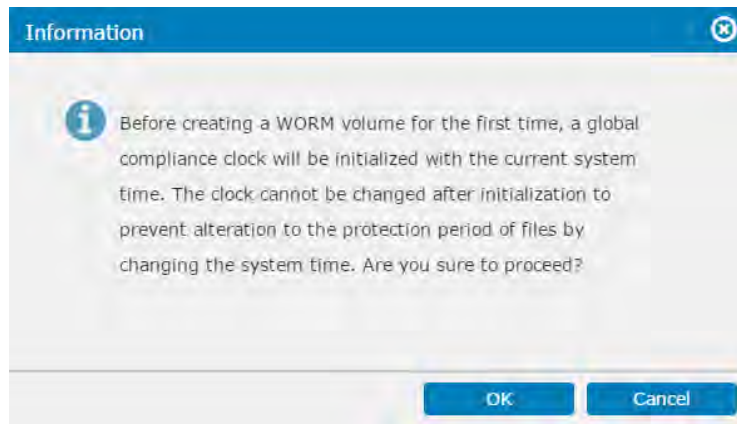
---

<b>Before the 1<sup>st</sup> WORM volume is</b>	<p>Before the first WORM volume is created, a confirmation window will pop up to inform the administrator to initialize the global compliance clock first.</p> <p>The global compliance clock can be initialized once only. It's not re-initialized even if there are no WORM volumes in the system.</p>
---	--

---

**created**

The retention time for WORM volumes will be based on the global compliance clock without being affected by system clock reset or change.



## About Thin Provisioning and Host Reclaim

Thin provisioning allows you to allocate a large amount of virtual capacity for a pool regardless of the physical capacity actually available. Actual space is used only when data writing occurs. By automatically allocating system capacity to applications as needed, thin provisioning technology can significantly increase storage utilization. Thin provisioning also greatly simplifies capacity planning and management tasks.

Dynamically allocating capacity affects the overall performance. If performance is a top priority (such as in AV applications), we recommend you disable thin provisioning (meaning to use full provisioning).

### Thin Provisioning Settings

Thin provisioning is configured during volume creation in a pool.

In the creation screen, thin provisioning options will appear in the lower half.



The screenshot shows a configuration window for a volume. At the top, it says "Specify the space allocated to this volume. Available free space: 378.33 GB". Below this, there is a text input field containing "10" and a dropdown menu set to "GB". Further down, there is a checked checkbox labeled "Use thin provisioning to create the volume with a size (as reported to the application) exceeds the available free space. Maximum space supported: 2 PB". Below the checkbox, there is another text input field containing "2" and a dropdown menu set to "PB".

After a new volume has been created, create one or more notification thresholds to make sure that the administrator receives warning/critical messages before all of the pool space is used up, and to give him or her ample time to expand the pool size.

We recommend you create multiple thresholds to stay on the safe side. (Example: notification for 70%, warning for 90%, critical for 95%, critical and purge snapshot images for 99%)

### Case 1: Full Provisioning (Thin Provisioning Disabled)

If you uncheck **thin provisioning** function, thin provisioning will be disabled and all of the configured pool size will be taken from the capacity actually available. The volume will be created as a continuous physical space reserved only for target application, and then will be initialized.

Full provisioning is suitable for mission-critical applications with large amount of uninterrupted data, such as audio/video streams. Dynamically allocating space and expanding usable area slows the I/O performance down, and therefore allocating a large physical capacity from the beginning optimizes the performance.

### Case 2: Thin Provisioning

To enable thin provisioning, check the **Use thin provisioning to create the volume with a size exceeds the available free space** box and enter the

---

#### Minimum Reserved space.

When the application uses up the minimum reserved area, additional space will be taken from the rest of the pool space and will be added to the volume dynamically.

The reserved space cannot exceed the actual available capacity.
---

---

#### **About Host Reclaim**

Thin provisioning keeps increasing the amount of physical storage on demand whenever new files are added. This works perfectly as long as all of the original files remain intact, but in reality some files will be deleted by host computers in the long run. As a result, available Pool capacity of your subsystem often appears less than its real available size. In order to make the most use of storage area, the size of deleted files/blocks should be checked occasionally to adjust the size of the logical volume.

The host reclaim function calculates the size of the deleted files in volumes and “shrinks” the pool size so that it reflects the currently used area. Host reclaim should be used in conjunction with thin provisioning and is especially useful for data replication such as snapshot and volume copy/mirror, allowing for shortened replication time and reduced target area.

Host Reclaim only works when the host computer is running Windows or Linux.
---



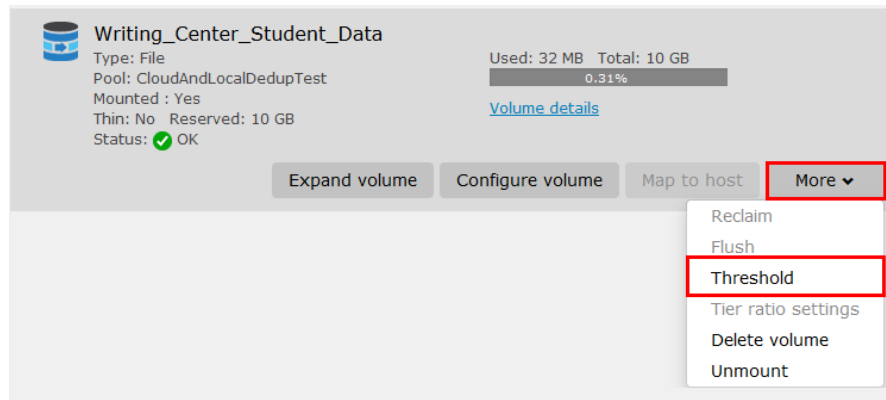
## Setting a Volume Threshold

Monitor volume usage by creating a threshold. The system will send out a notification when the volume usage reaches the threshold.

---

**Go to**                      **Settings > Storage > Volume**

Select the volume, click the **More** button, and select **Threshold**.



## Steps

Click **Add** to create a new threshold. You may also edit or delete existing thresholds.

Threshold

Add or edit threshold settings.

Total capacity: 10 GB

99.69%

Used Free

Add Edit Delete

Policy	Threshold
<input type="checkbox"/> Post notification events	50%
<input type="checkbox"/> Post warning events	70%

Cancel

On the pop-up window, enter the threshold value (% of the volume) and choose the notification type. Click **OK** to save the threshold.

Add Threshold

Create a threshold.

Threshold percentage: 60 %

Policy: Post notification events  
Post warning events  
Post critical events

OK Cancel

<b>Parameters</b>	<b>Post notification events</b>	Create a notification event when the amount of volume usage reaches the threshold.
	<b>Post warning events</b>	Create a warning event when the amount of volume usage reaches the threshold.
	<b>Post critical events</b>	Create a critical event when the amount of volume usage reaches the threshold.

## Note

**You can only set thresholds for a file-level volume.**

## Deleting a Volume

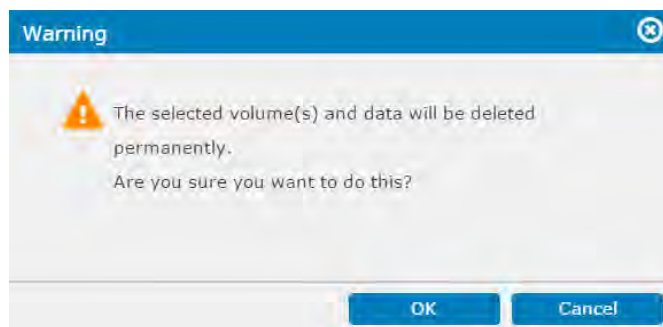
**Go to**                      **Settings > Storage > Volume**

Select the volume, click the **More** button and select **Delete volume**.



**Delete a volume**

A warning will pop up. Click **OK** to delete the volume. This action will also delete the LUN mappings and snapshots related to the volume.





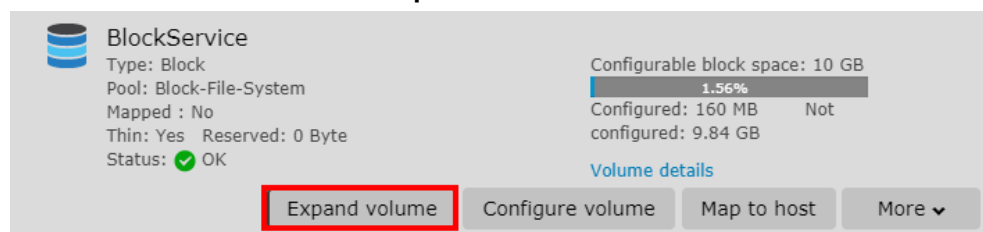
## Expanding a Volume

Expanding a volume's capacity is available only when there is available capacity.

Go to

**Settings > Storage > Volume**

Select the volume and click the **Expand Volume** button.



BlockService  
 Type: Block  
 Pool: Block-File-System  
 Mapped : No  
 Thin: Yes Reserved: 0 Byte  
 Status: ✔ OK

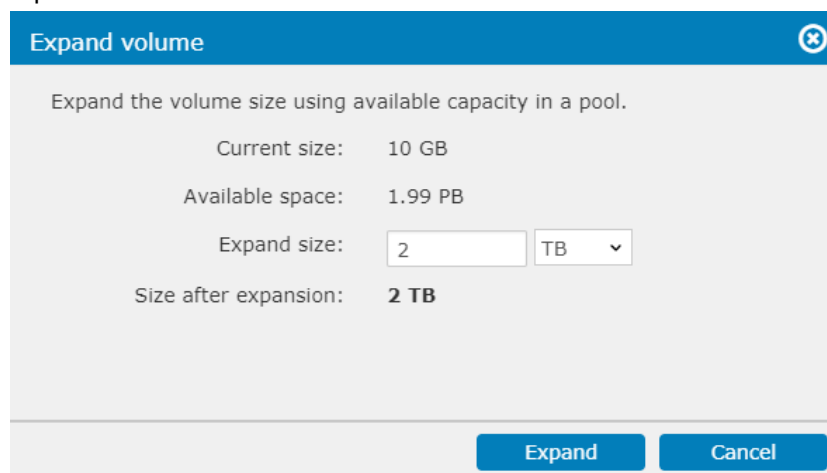
Configurable block space: 10 GB  
 1.56%  
 Configured: 160 MB Not  
 configured: 9.84 GB

[Volume details](#)

**Expand volume** Configure volume Map to host More ▼

**Steps**

The expansion setting window will appear. Specify the capacity you want to expand.



**Expand volume** ✕

Expand the volume size using available capacity in a pool.

Current size: 10 GB  
 Available space: 1.99 PB  
 Expand size:  TB  
 Size after expansion: **2 TB**

**Expand** **Cancel**

Expansion will begin. When it is completed, check that the size of the volume is increased by the specified amount.

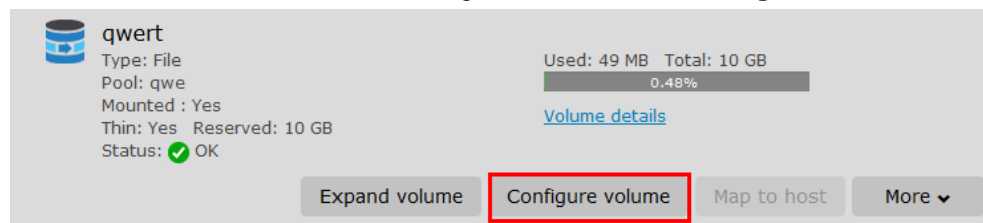
## Deduplicating Volume Data (Beta)

Performing data deduplication can significantly reduce volume usage and therefore minimize expense on storage expansion.

To try out this beta feature, contact the vendor for the special firmware update.

**Go to** **Settings > Storage > Volume**

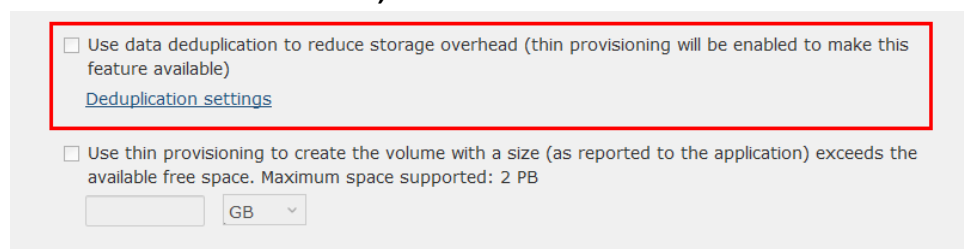
Click **Add volume**, or select an existing volume and click **Configure volume**.



The screenshot shows the configuration page for a volume named 'qwert'. It includes details such as Type: File, Pool: qwe, Mounted: Yes, Thin: Yes, Reserved: 10 GB, and Status: OK. A progress bar indicates 'Used: 49 MB Total: 10 GB' with '0.48%' usage. A 'Volume details' link is present. At the bottom, there are buttons for 'Expand volume', 'Configure volume' (highlighted with a red box), 'Map to host', and 'More'.

### Steps

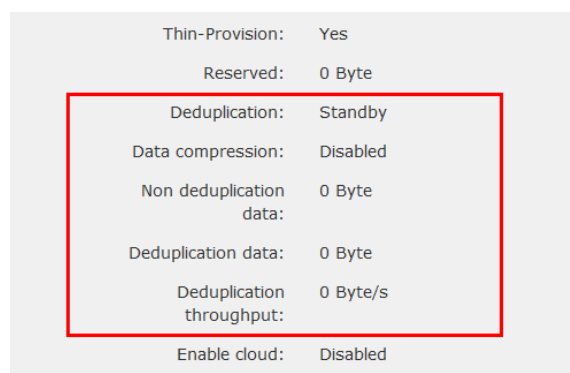
On the pop-up window, enable data deduplication by checking **Use data deduplication to reduce storage overhead (thin provisioning will be enabled to make this feature available)**.



The screenshot shows a pop-up window for deduplication settings. The first checkbox, 'Use data deduplication to reduce storage overhead (thin provisioning will be enabled to make this feature available)', is checked and highlighted with a red box. Below it is a link for 'Deduplication settings'. The second checkbox, 'Use thin provisioning to create the volume with a size (as reported to the application) exceeds the available free space. Maximum space supported: 2 PB', is unchecked. At the bottom, there is a text input field and a dropdown menu set to 'GB'.

To configure more deduplication Settings, click **Deduplication Settings**.

To view current deduplication status, select the volume and click **Volume details**.



The screenshot shows the 'Volume details' page. It lists various settings: Thin-Provision: Yes, Reserved: 0 Byte, Deduplication: Standby, Data compression: Disabled, Non deduplication data: 0 Byte, Deduplication data: 0 Byte, Deduplication throughput: 0 Byte/s, and Enable cloud: Disabled. A red box highlights the 'Deduplication' section, which includes 'Deduplication: Standby', 'Data compression: Disabled', 'Non deduplication data: 0 Byte', 'Deduplication data: 0 Byte', and 'Deduplication throughput: 0 Byte/s'.

## Parameters

### Enable data compression to save more space

The system compresses deduplicated data to further reduce volume usage.

### Enable background optimization

The system automatically pauses data deduplication when the system is busy, and resumes the operation when the system is not busy.

### Enable throughput optimization

Set a schedule to run data deduplication in times when the system is not busy.

## Notes

- To run data deduplication, also enable thin provisioning for the volume under deduplication.
- To store deduplicated data, reserve capacity large enough for creating a volume in the storage pool.
- Do not enable automated storage tiering to avoid slowing down the deduplication process.
- Do not enable Cloud Gateway for a deduplicated volume.
- Data deduplication is only available on specific models. For more information, please check PAC Storage's official website.

## Defragmenting a Volume

Defragmentation allows file fragments on the volume to merge into contiguous fragments, therefore boosting file access and storage efficiency.

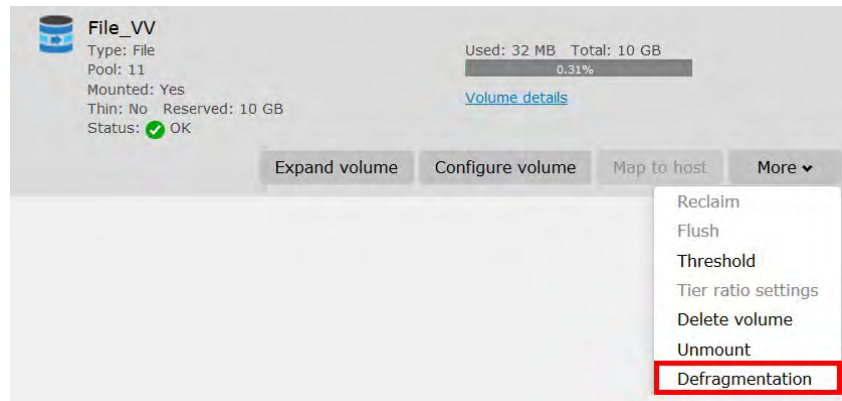
Note: Only file-level volumes can be defragmented.

### Go to

**Settings > Storage > Volume**

### Steps

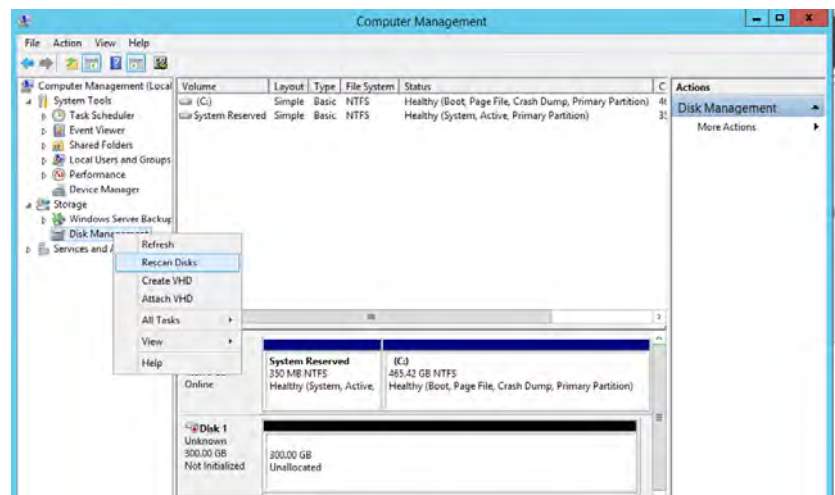
1. Select a volume and go to **Volume details** to check **Fragmentation factor**. If the factor is high, we recommend you defragment the volume to improve its access and storage efficiency.
2. Click **More > Defragmentation** to start defragmenting the volume.



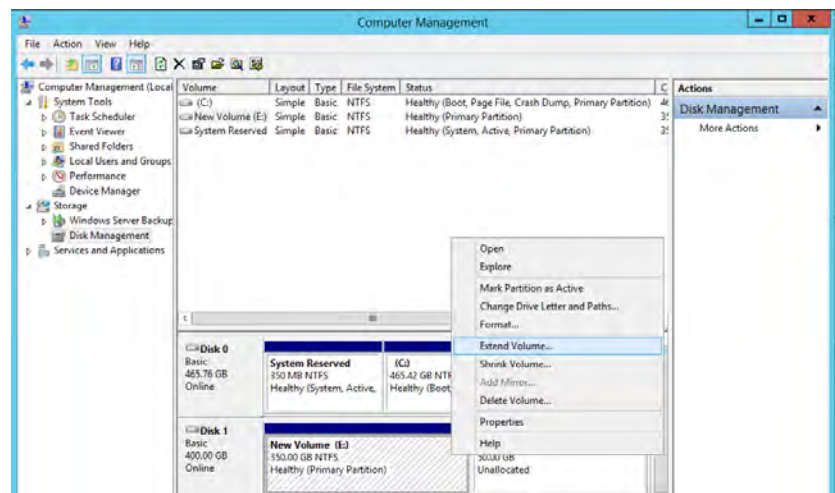
## Reflecting the Expanded Volume Status in Windows Server (Windows Server 2012 R2 for example)

### Steps

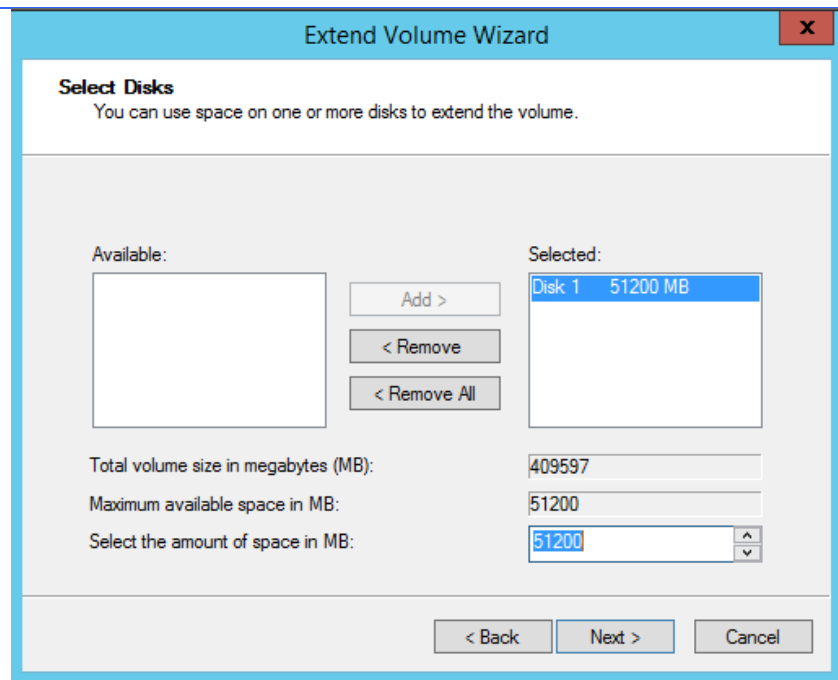
1. Open the Computer Management Utility.
2. Right-click on the Disk Management icon in the sidebar and select Rescan Disks.



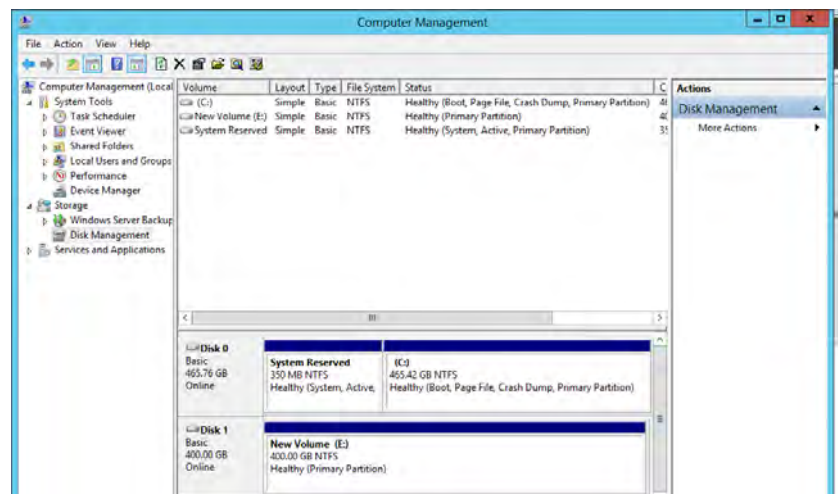
3. The expanded part of the volume will appear as a new unallocated disk space (see Disk 1 in the example below). Right-click on the Disk and select **Extend Volume**.



4. The Extend Volume Wizard will appear. Add available disk and click **Next**.



5. You should be able to see the extended volume.



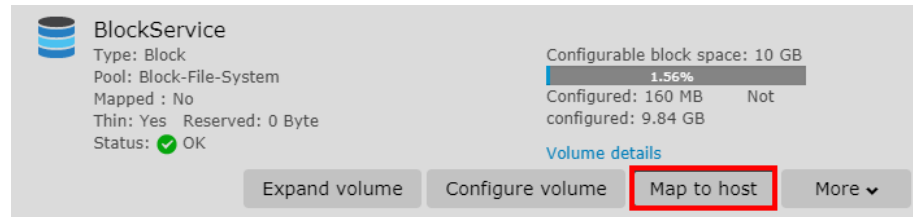
## Mapping a Volume to a LUN

There must be at least one volume available to create LUN mapping.

Go to

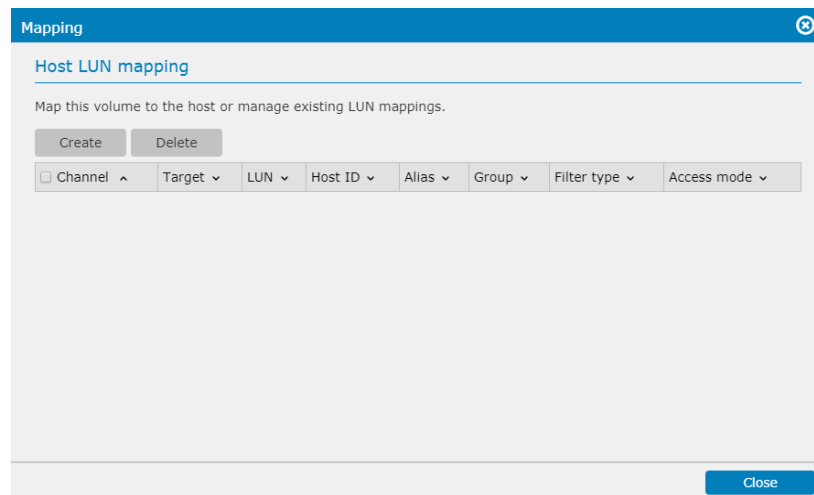
**Settings > Storage > Volume**

Select a “Type: Block” volume and click the **Map to host** button.

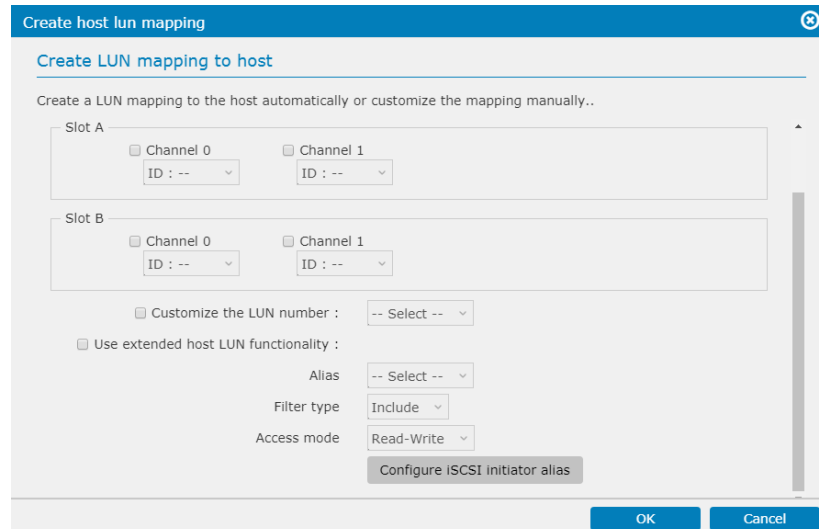


Steps

The Host LUN Mapping table will appear.



Click **Create** and the Host Mapping Configuration Window will be shown.



Click **OK**. The list of Host LUN Mapping configurations will appear in the window.

Channel	Target	LUN	Host ID	Alias	Group	Filter type	Access mode
0	0	1	--	--	--	--	--
0	1	1	--	--	--	--	--

### Automatic Configuration

Check the created LUN mappings if you want the system to create them automatically. For hybrid models, you need to select the host type.

Create a LUN mapping to the host automatically or customize the mapping manually.

☒ Create a host LUN mapping set automatically

☒ iSCSI 10.0 Gbps ☐ iSCSI 1.0 Gbps

☐ Customize host LUN mapping

### Manual Configuration

If you have manually configured the LUN mapping, check the Customize option and select the Channels.

☒ Customize host LUN mapping

☒ iSCSI 10.0 Gbps ☐ iSCSI 1.0 Gbps

Slot A

☐ Channel 0 ID : -- ☐ Channel 1 ID : --

Slot B

☐ Channel 0 ID : -- ☐ Channel 1 ID : --

☐ Customize the LUN number : -- Select --

You can also customize the LUN number to differentiate the channels.

☒ Customize the LUN number: 4

### Using Advanced LUN Mapping Features (Extended LUN/LUN Filter)

The differences between normal Host LUN mapping and Extended LUN mapping are as follows.

- Normal host LUN mapping simply presents a pool to the host links. If host links are made via an FC switch, all servers attached to the switch (or those within the same zone) can “see” the volume.
- The extended LUN mapping binds a pool with a specific HBA port and presents the volume to the HBA port.



## Extended LUN Mapping (Fibre Channel)

Extended LUN Mapping is available only for manual configuration.

**Go to** **Settings > Storage > Volume**

Select a "Type: Block" volume and click the **Map to host** button.

**Steps** Click **Use Extended LUN Functionality** and modify the parameters.

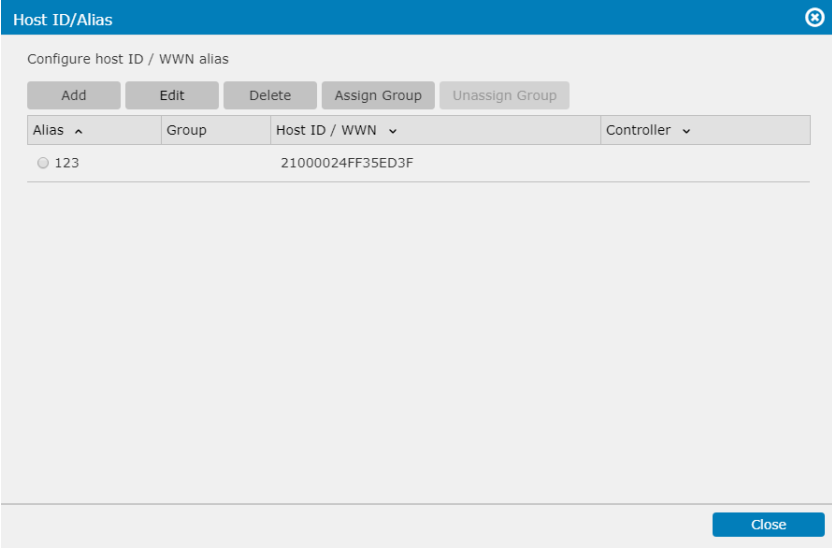
<b>Parameters</b>	<b>Host ID/Alias</b>	Specifies the host ID, referring to WWPN port name. You can also see OUI (Organizationally Unique Identifier) of a system: "00:D0:23"oui. Note: Avoid checking the OUI while mapping host LUN. To check the WWN information of your fiber channel adapter on your Windows server, open the <b>Device Manager</b> page. Right click on the fiber channel adapter in the <b>Storage controllers</b> section and select <b>Properties</b> for detailed information. If you cannot find the WWN information of the fiber channel adapter, go to Powershell command line interface and enter "get-initiatorport" for WWN information.
-------------------	----------------------	--

<b>Host ID Mask</b>	Works as a prefix mask in hexadecimal format.
---------------------	---

<b>Filter Type</b>	Specifies whether to allow (include) WWNs or to forbid (exclude) them from accessing after filtering.
--------------------	---

<b>Access Mode</b>	Specifies the access right of LUN mapping for the host: read-only or read-write.
--------------------	--

<b>Edit Host-ID/WWN</b>	1. Click <b>Configure Host ID/WWN Alias</b> . (Edit Host-ID/WWN List enabled only when Extended Host LUN Functionality has been enabled.)
-------------------------	---

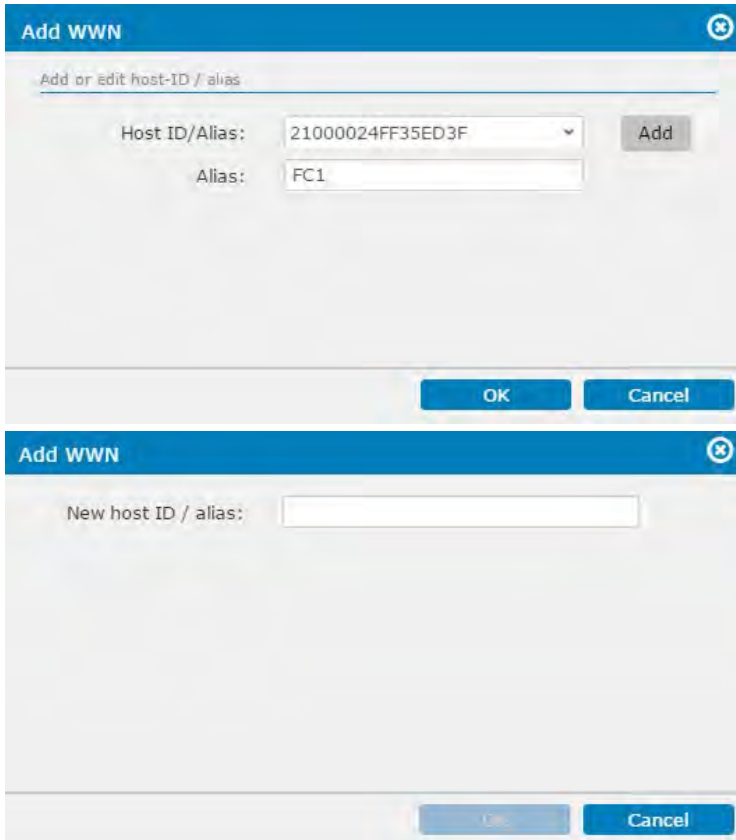


Host ID/Alias

Configure host ID / WWN alias

Alias ^	Group	Host ID / WWN v	Controller v
123		21000024FF35ED3F	

- In the Edit Host-ID/WWN list window, click **Add** to create an entry and enter the node name (WWN Name) for identifying HBA ports in SAN. An HBA card may have one node name and multiple port names. The node name can be a nickname such as "SQLserver\_port" instead of the real name.



Add WWN

Add or edit host-ID / alias

Host ID/Alias: 21000024FF35ED3F

Alias: FC1

---

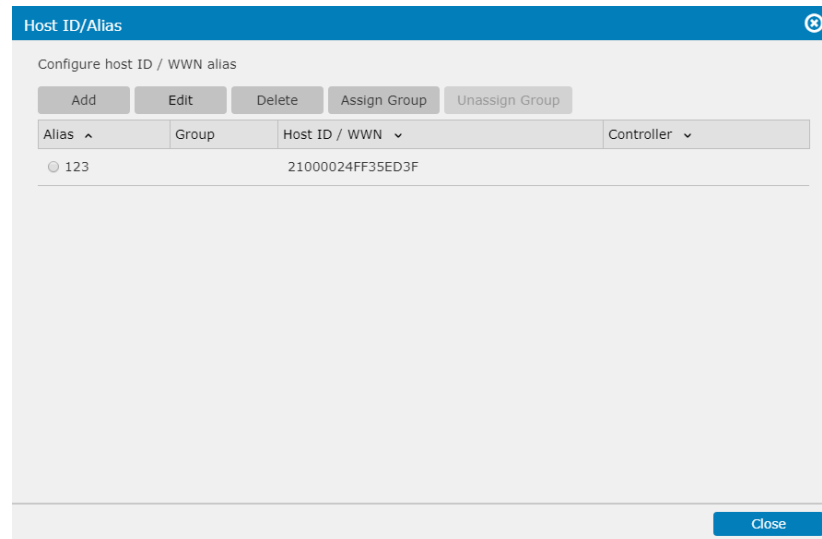
Add WWN

New host ID / alias:

- Click **OK**. Repeat the above process to create more LUN mappings

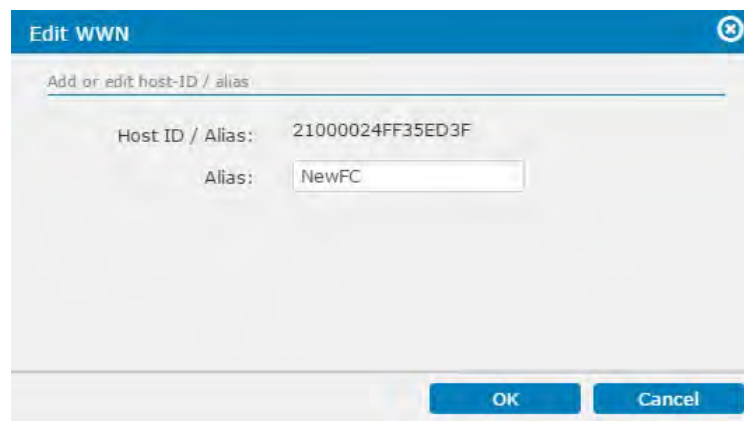
especially if you have multiple HBA ports accessing the same volume (e.g., in high-availability applications).

4. To delete a WWN Name from the List, Highlight a WWN in the list and click **Delete**.



The screenshot shows a window titled "Host ID/Alias" with a close button in the top right. Below the title bar is a subtitle "Configure host ID / WWN alias". There are five buttons: "Add", "Edit", "Delete", "Assign Group", and "Unassign Group". Below these buttons is a table with four columns: "Alias", "Group", "Host ID / WWN", and "Controller". The table contains one row with the values "123", an empty cell, "21000024FF35ED3F", and an empty cell. At the bottom right of the window is a "Close" button.

5. To edit the alias name of the WWN, click **Edit** and enter the new name.



The screenshot shows a dialog box titled "Edit WWN" with a close button in the top right. Below the title bar is a subtitle "Add or edit host-ID / alias". There are two labels: "Host ID / Alias:" and "Alias:". The "Host ID / Alias:" label is followed by the value "21000024FF35ED3F". The "Alias:" label is followed by a text input field containing the value "NewFC". At the bottom of the dialog box are "OK" and "Cancel" buttons.

### Assigning a WWN to a Group

A WWN group allows multiple host LUNs to be accessed in a single mask, which becomes useful in a clustered storage server environment.

1. To create a group and assign a WWN to it, highlight a WWN.
2. Click **Assign Group** and select the group from the drop down menu.

3. To add a new group, click **Add** and enter the group name.

4. The group name will appear in the list.

Alias	Group	Host ID / WWN	Controller
123	Group	21000024FF35ED3F	Slot A

5. To unassign a WWN from a group, click **Unassign Group**.

### Example

We have two HBA ports with the following WWNs.

1. HBA-1: 0x0000000000000001
2. HBA-2: 0x0000000000000002

Only HBA-1 should be able to access the volume, Therefore the filter type is “included.” The mask will become:

3. Mask: 0xFFFFFFFFFFFFFC (Binary: 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111)

---

Thus HBA ports that end with 0x....00, 01, 03 can access the volume but NOT 0x...02 (HBA-2).

If more HBA ports are added, for example:

4. HBA-3: 0x000000000000000A1 (Binary: 00000000 00000000 00000000 00000000 00000000 00000000 10100001)
5. HBA-4: 0x000000000000000A2 (Binary: 00000000 00000000 00000000 00000000 00000000 00000000 10100010)

The mask should be modified to reflect the changes such as:

6. For HBA-3: 0xFFFFFFFFFFFFF5C (Binary: 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111 01011100) (included)
  7. For HBA-4: 0xFFFFFFFFFFFFF5C (Binary: 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111 01011100) (included)
-

## Extended LUN Mapping (iSCSI Channel)

Extended LUN Mapping is available only for manual configuration.

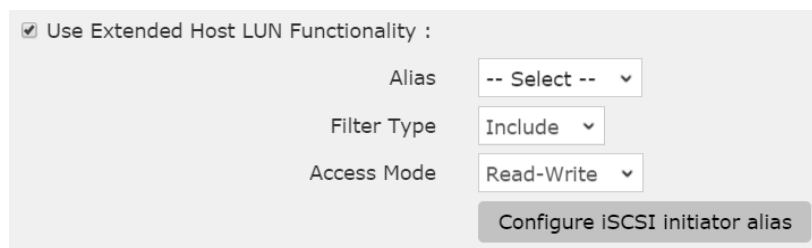
### Go to

**Settings > Storage > Volume**

Select a “Type: Block” volume and click the **Map to host** button. On the host LUN mapping page, click on **Create** and then select **Customize host LUN mapping**.

### Steps

Click **Use Extended LUN Functionality** and enter the parameters.



☒ Use Extended Host LUN Functionality :

Alias: -- Select --

Filter Type: Include

Access Mode: Read-Write

Configure iSCSI initiator alias

### Parameters

<b>Alias</b>	Specifies a pre-configured iSCSI initiator instance. To create a new initiator alias, click the Configure iSCSI Initiator Alias button.
<b>Filter Type</b>	Specifies whether to allow (include) initiators or to forbid (exclude) them from accessing after filtering.
<b>Access Mode</b>	Specifies the access right of LUN mapping for the host: read-only or read-write.

### Configuring iSCSI Initiator Alias

1. Click Configure iSCSI Initiator Alias.
2. Click **Add** to create an entry and enter the parameters.

3. Click **OK**. Repeat the above process to create more LUN mappings especially if you have multiple HBA ports accessing the same volume (e.g., in high-availability applications).

<b>Parameters</b>	<b>Host IQN</b>	Select one of the pre-defined host IQN or click the <b>Add</b> button and type in a new host IQN.
	<b>Alias</b>	Assign a name easy to remember for the iSCSI initiator.
	<b>Username/Password</b>	Specifies the user name and password for CHAP authentication. This information is the same as the CHAP target node name and CHAP secret in the OS setting.
	<b>Target Name/Password</b>	Specifies the target name and password for CHAP authentication. This information is the same as the CHAP initiator node name and CHAP secret in the OS setting. The Target Name cannot exceed 32 bytes in length. For a Microsoft iSCSI software initiator, it is required that both the initiator and target CHAP password should be between 12 bytes and 16 bytes.
	<b>IP Address/Netmask</b>	Multiple initiator ports on an application server can sometimes share the same IQN.
<b>Assign Group</b>	Click the checkbox on one of the iSCSI initiator aliases and click the <b>Assign Group</b> button to set IQN groups for the aliases. An iSCSI initiator can be	

---

included in multiple groups.

Configure iSCSI initiator alias

Alias ^	Group v	Host IQN v	User Name v	Target name v	IP address v	Netmask v
<input checked="" type="radio"/> server112		iqn.1991-05.com.microsoft:win-9uc15b7ofjk	admin		172.24.110.112	255.0.0.0

If no groups have been set before, click the **Add** button to claim a name for a new group. Otherwise, select a group for the iSCSI initiator. The alias group information can be seen in the Group column of the alias.

---

## Notes

- By mapping a volume to multiple ports on multiple HBAs, you acquire path redundancy. To manage fault-tolerant paths to a single volume, you should have MPIO enabled on Windows servers, Device Mapper on Linux, and Solaris MPXIO on Solaris platforms (SPARC machines). Refer to Working with Multipath.
  - To acquire HBA port names, you may access utility software/website from the HBA vendor.
  - In hybrid models, the iSCSI host channels are by default used for remote replication.
-



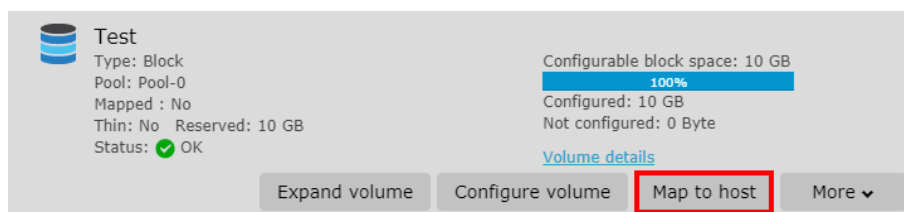
## Deleting a LUN Mapping

There must be at least one volume of a pool available.

**Go to**

**Settings > Storage > Volume**

Select a "Type: Block" volume and click the **Map to host** button.



**Test**  
Type: Block  
Pool: Pool-0  
Mapped : No  
Thin: No Reserved: 10 GB  
Status: ✔ OK

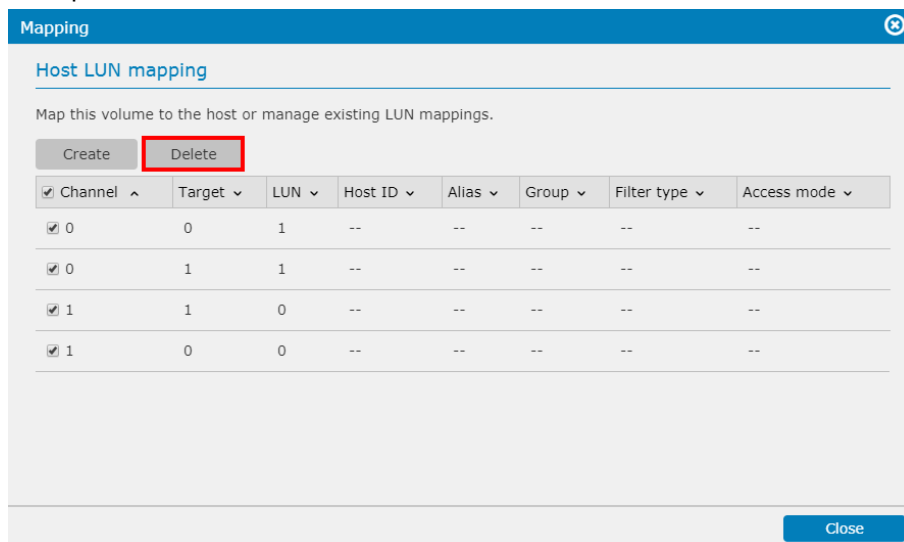
Configurable block space: 10 GB  
100%  
Configured: 10 GB  
Not configured: 0 Byte

[Volume details](#)

Expand volume Configure volume **Map to host** More ▾

**Steps**

The host LUN mapping table will pop up. Select the host LUN you want to unmap and click **Delete**.



**Mapping**

Host LUN mapping

Map this volume to the host or manage existing LUN mappings.

Create Delete

Channel	Target	LUN	Host ID	Alias	Group	Filter type	Access mode
<input checked="" type="checkbox"/> 0	0	1	--	--	--	--	--
<input checked="" type="checkbox"/> 0	1	1	--	--	--	--	--
<input checked="" type="checkbox"/> 1	1	0	--	--	--	--	--
<input checked="" type="checkbox"/> 1	0	0	--	--	--	--	--

Close

## About In-Band, Out-of-Band Flush

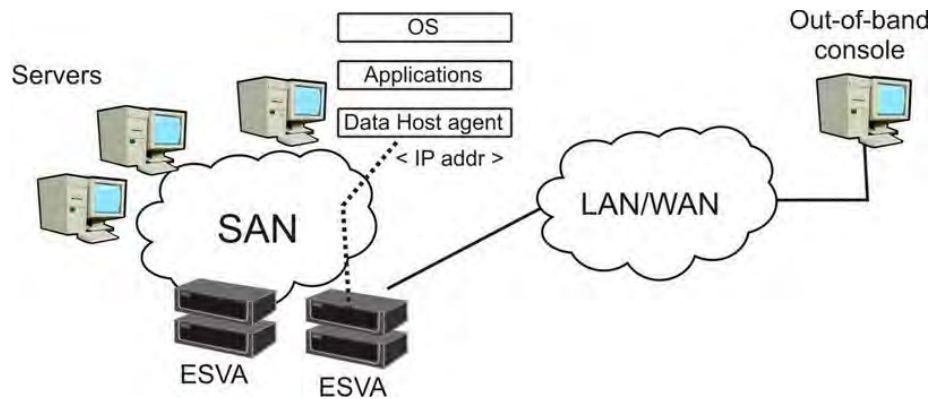
### In-Band VS. Out-of-Band

There are two types of cache memory flush, In-Band and Out-of-Band, depending on the connection between the host computer and the subsystem.

#### In-Band Flush

Cache memory flushing is triggered by the host computer itself, which is connected to the subsystem through in-band connection. This is the standard flush method when there is only one data host computer or Windows Virtual Machine (VM) is not running in the host computer.

#### Out-of-Band Flush



Out-of-Band Flush refers to cache memory flushing triggered by an out-of-band host computer. This method is required in the following cases:

- Multiple host computers with database applications are connected to the subsystem. In-band flush might be in conflict when more than one host computers tries to back up user data at the same time. In this case, out-of-band flush allows multiple servers to perform data flushing in series without conflict.
- Windows Virtual Machine (VM), installed on ESX server, is running in the host computer. VM itself cannot initiate cache data flushing on its own, and thus the host computer needs to use the out-of-band connection to initiate flushing indirectly.

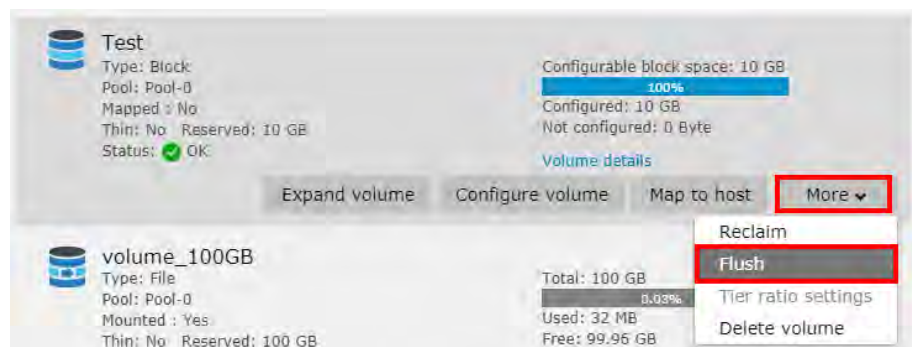
## Configuring Out-of-Band Flush

If you are holding data in VMs or in database forms, all data need to be flushed into storage subsystem before activating a backup job.

Go to

**Settings > Storage > Volume**

Select a “Type: Block” volume and click the **More** button and select **Flush**.

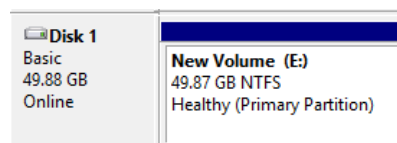


The Flush Settings window will appear.



Click **Add** to add a data host. In the Flush Agent Setting, enter the host agent IP address, select the OS type, and enter the following in the Disk field:

-For Windows, the Disk ID (the “1” in “Disk 1” for example)



-For Linux: /dev/ID (such as /dev/sdb)

-For Solaris: /dev/dsk/ID (such as /dev/dsk/sdb)



# Pool

Go to

Settings > Storage > Pool

Volume

Pool

Drive

SSD cache

Storage maintenance

View

Pool list

Pool advanced options

Pool list

You can add a new pool or select a pool to edit its settings.

+

Add pool

AA

Logical drives: 2

Volumes: 2

Status: On-Line

Allocated: 30.59 GB

Total: 272.45 GB

11.23%

Pool details

Parameters	Pool Name	Shows the Pool name
	Capacity	Shows the capacity of the pool, including the total and allocated capacity
	Allocated size	Shows the used percentage of the pool
	Logical Drives	The number of logical drive members
	Volumes	The number of volume members
	Status	Shows the status of the pool

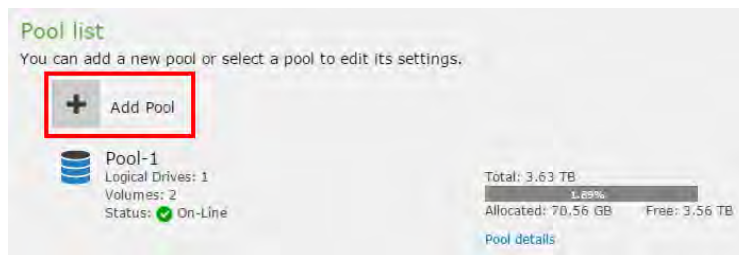
## Adding a Pool

Note:

1. A logical drive must be at least 10 GB in size to form a pool.
2. Check pool limitations in [Appendix – Pool](#).

**Go to**                      **Settings > Storage > Pool**

1. Click the **Add Pool** button.



You will be directed to the following Create pool webpage:

Create pool

Configure pool parameters

\* specify the pool name

select write policy in cache memory

Write-Back

[Write policy settings](#)

Select controller ownership policy for the pool

Asymmetric active/active mode (supports both file-level volume for NAS and block-level volume for SAN)

Both controllers are able to receive I/O requests, but only the controller being assigned to own this pool handles incoming I/O requests, while the other controller stands by and passes I/O requests to the assigned controller.

Assign a controller for this pool

Controller in SlotB

Symmetric active/active mode (only supports block-level volume for SAN)

Both controllers are able to receive and handle I/O requests for this pool, with nearly equal performance. To achieve better performance, at least two logical drives should be added into this pool.

Apply

Cancel

2. Specify your pool name (this field is required). It accepts underscore ( \_ ) characters.
3. Select the write back in cache memory from the scroll down list. There are two options:

**Write-back (default):** If you choose write-back option, writing is only done to the cache while backing storage is postponed until cache blocks containing the data are about to

---

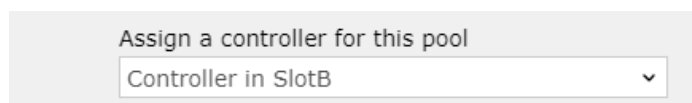
be modified or replaced by new content.

**Write-through:** If you choose Write-through option, data write is done synchronously both to the cache and to the backing storage.

You can set writing policy by clicking the write policy Settings, refer to General & Advanced Settings and go to **set cache parameters** category for details.

4. Select **Asymmetric Active/Active** or **Symmetric Active/Active mode** under “Select Controller ownership policy for the pool” (Note that this feature will only display/available with two controllers attached on the storage device).

**Asymmetric Active/Active:** read the description carefully, then assign a controller for this pool from the scroll down list. (Controller in SlotA / Controller in SlotB)



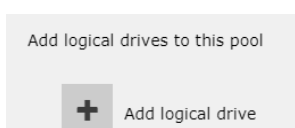
Assign a controller for this pool

Controller in SlotB

**Symmetric Active/Active mode:** read the description carefully. You do not need to assign a controller under this mode. Symmetric Active/Active configuration allows host IO to come from both controllers. The logical drives of the pool will be evenly distributed to the two controllers. You can create a symmetric pool with multiple logical drives, which will be automatically assigned to controller A or B at creation/boot-up.

Note: Currently, file-level volumes and Automated Storage Tiering functionality cannot be configured on a pool in Symmetric Active/Active mode.

5. Add Logical Drive:



Add logical drives to this pool

+ Add logical drive

Click the **Add logical drive** button, you will be directed to the below page to configure logical drive parameters:

---

**Add logical drive**

Configure logical drive parameters

Select drive members

☐ 1024RB (Available: 8, Selected: 0) Hide

- ☐ Slot 9 / FUJITSU MAY2036RC / HDD / SAS / 33.99 GB
- ☐ Slot 12 / ATA HGST HTE725050A7 / HDD / SATA / 465.5 GB
- ☐ Slot 19 / TOSHIBA AL14SEB030N / HDD / SAS / 279.14 GB
- ☐ Slot 20 / TOSHIBA AL14SEB030N / HDD / SAS / 279.14 GB
- ☐ Slot 21 / TOSHIBA AL14SEB030N / HDD / SAS / 279.14 GB
- ☐ Slot 22 / TOSHIBA AL14SEB030N / HDD / SAS / 279.14 GB
- ☐ Slot 23 / TOSHIBA AL14SEB030N / HDD / SAS / 279.14 GB
- ☐ Slot 24 / TOSHIBA AL14SEB030N / HDD / SAS / 279.14 GB

☐ JBOD2 (Channel4) (Available: 4, Selected: 0) Show

\* Specify logical drive name

Select RAID level

Select stripe size

Apply Cancel

Select drive members: displays enclosures and JBOD drive's information that are available to be created as Logical Drives, those drives that are damaged or in use are not displayed.

Note: For Symmetric Active/Active mode, if there is no expansion enclosure connected and there are single-type drives in the enclosure, the drive list will be hidden. All drives will be selected and assigned to the two LDs evenly.

Each drive information has its naming rule for example:

Slot # / Model number /HDD or SSD / SAS or SATA / Capacity

You can click the Hide button on the right to conceal or display drive members

6. Specify logical drive name: the name is preset (do not repeat Logical Drive name under the same pool).
7. Select a RAID protection level.
8. Select a stripe size for the logical drive, the default may be 128K.

Encrypted Drives: From here you can select how the drives to be encrypted from the scroll down list, there are three options

Disabled(Default)

Use an existing SED authentication



## Create a new SED authentication key

All the selected drives are Self-Encrypting Drives (SED). Select how the drives to be encrypted.

Use an existing SED authentication key

Select an existing key from the system from the scroll down list.

Press the SED key management link to direct you to SED key management page where you can choose two methods to upload your key file. Please refer to General & Advanced Settings and find SED key management category.

☒ Select an existing key from the system

[SED key management](#)


You can tick the Upload an SED key and browse for the SED key location.

☒ Upload an SED key (must be the ones generated from a compatible system)

Browse

Once you have completed Logical Drive setting, your newly created Logical Drive will appear under Add Logical Drive button:

Add logical drives to this pool

 Add logical drive



Logical\_drive\_1  
Type: RAID1  
Capacity: 25.99 GB

Edit

Delete




Logical\_drive\_2  
Type: RAID1  
Capacity: 271.14 GB

Edit: select this button to edit your logical drive in the “Configure logical drive parameters” page.

Delete: click this button to completely erase the Logical Drive.



- Back to the Create Pool main page, under Add Logical Drive, you can use Storage tiering function, tick the box if you wish to activate storage tiering (Note that this feature will only display/available with a storage tiering license, and it is not supported for Symmetric Active/Active controller mode)

Add logical drives to this pool


 Add logical drive

☐ Use storage tiering to retain frequently accessed data in higher storage tiers (usually formed with high performance drives), and move less frequently accessed data to lower tiers.

[Storage tiering settings](#)

#### 10. Click Storage tiering Settings

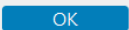

Storage tiering settings 

Storage tiering settings

☒ Use storage tiering to retain frequently accessed data in higher storage tiers (usually formed with high performance drives), and move less frequently accessed data to lower tiers. (Not supported for Symmetric active/active controller ownership policy)

Specify tier index for the logical drives. Logical drives formed with higher performance drives should be assigned with smaller tier indexes, such as tier 0.

Logical Drive Name ▾	Type ▾	Interface ▾	Capacity ▾	Tier Index
Logical_Drive_1	HDD	SAS	418.93 GB	0 ▾
Logical_Drive_2	SSD	SAS	136.48 GB	0 ▾

Please ensure the use storage tiering box is ticked for further configuration

In this page, specify tier index for the logical drives, Logical drives formed with higher performance drives should be assigned with the smaller tier index, such as tier 0.

#### Parameters

##### Pool Name

Enter a unique name for the volume.

##### RAID Level

**RAID 0:** at least 2 drives (best performance but no data protection).

**RAID 1:** at least 2 drives (average performance with excellent data protection).

**RAID 5:** at least 3 drives (improved performance with improved data protection).

	<b>RAID 6:</b> at least 4 drives (improved performance with excellent data protection).
<b>Storage Tiering</b>	Select whether to enable tiering.
<b>Tier Index</b>	If storage tiering is enabled, specify the tier index.
<b>Write Policy</b>	<p>Changes the writing cache policy for this pool.</p> <ul style="list-style-type: none"> <li>● Default: The writing cache policy follows system setting.</li> <li>● Write-Back: Writing data will be stored into the cache memory first and will be written into the disk drive later.</li> <li>● Write-Through: Writing data will be stored into the disk drive directly.</li> </ul> <p>The Write-Back and Write-Through setting overrides the write cache policy for the system.</p> <div> <p>When a critical event occurs, the writing policy may automatically switch to the more conservative Write-Through.</p> </div>
<b>Assignment</b>	<p>Specifies which controller (Slot A or Slot B) this pool will be assigned to.</p> <p>Note: Before changing the pool assignment, the system needs to be reset to activate the assignment change.</p>
<b>Stripe Size</b>	Specifies the stripe size of the array.
<b>SED Security</b>	<p>Specifies whether you want to protect the member drives with SED (Self Encrypting Drives) security.</p> <div> <p>Before enabling this option, the following requirements should be met:</p> <ul style="list-style-type: none"> <li>● A SED authentication key is created.</li> <li>● All member drives support SED.</li> </ul> </div>



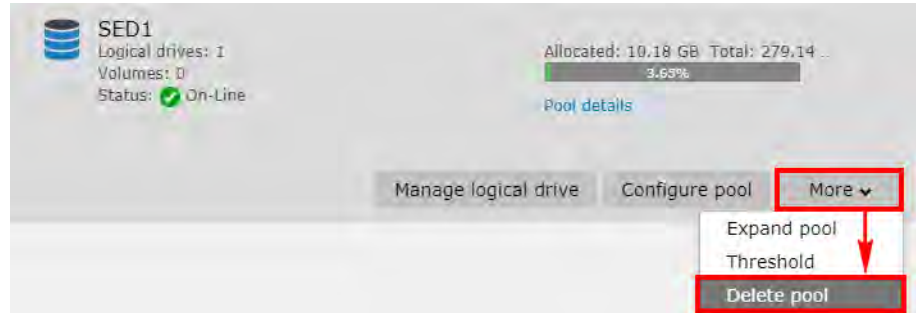
## Deleting a Pool

Go to

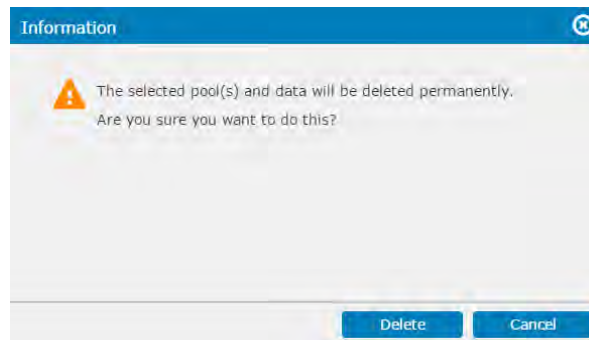
Settings > Storage > Pool

Steps

Select the pools you want to delete, click **More** and select **Delete pool**.



A warning message will appear. Click **Delete** to confirm and delete the pool.

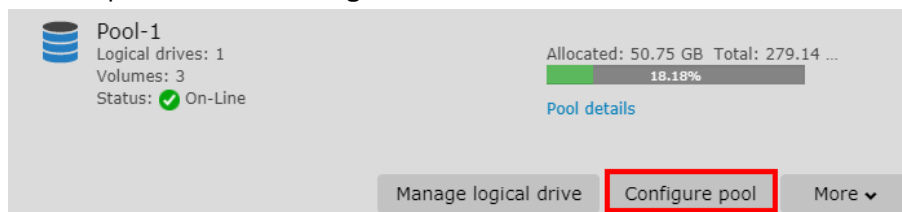


## Configuring a Pool

Go to

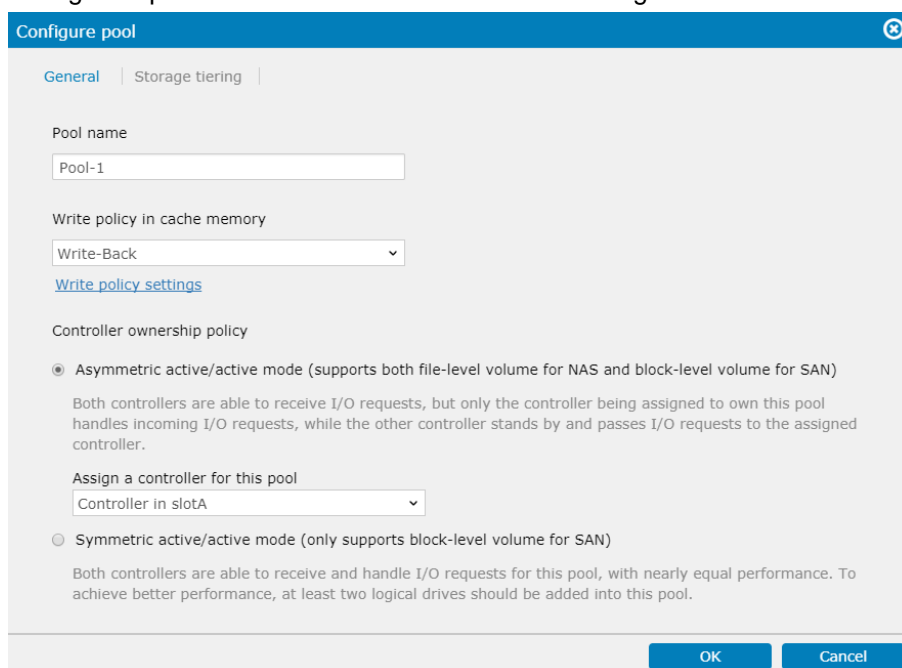
**Settings > Storage > Pool**

Select a pool and click **Configure Pool**.



### Steps

Change the parameters and click **OK** to confirm changes.



### Parameters

#### Name

Specifies the pool name.

#### Write Policy

- When “Write-back” (by default) is enabled, writing requests from the host will be held in cache memory and distributed to disk drives later. Write-back caching can dramatically improve writing performance by caching unfinished writing in memory and commit them to the drives in a more efficient manner. In the event of power failure, a battery backup module can hold cached data for days (usually 72 hours).
- When “Write-through” is enabled, host writing will be directly distributed to individual disk drives. Write-through mode is safer if your controller is not configured in a redundant pair and there is no battery backup or

---

UPS device to protect cached data.

---

<b>Assignment</b>	Specifies which controller (Slot A or Slot B) this pool will be assigned to.
-------------------	--

---

<b>SED Security</b>	Specifies whether you want to protect the member drives with SED (Self Encrypting Drives) security.
---------------------	---

---

Before enabling this option, the following requirements should be met:

- A SED authentication key is created.
  - All member drives support SED.
- 

Please note that after automatic failover, if you want to reassign the pools that were originally assigned to the failed controller to the replacement controller, you will have to restart the replacement controller after the reassignment.

## Expanding a Pool

For the PAC Storage PS/PSV storage devices, there are three ways to expand the capacity of a Pool

1. Create new logical drives and add them into the Pool. (Highly recommended)
2. Add new disk drives and expand the original Logical Drive.
3. Replace the original drives with higher capacity drives.

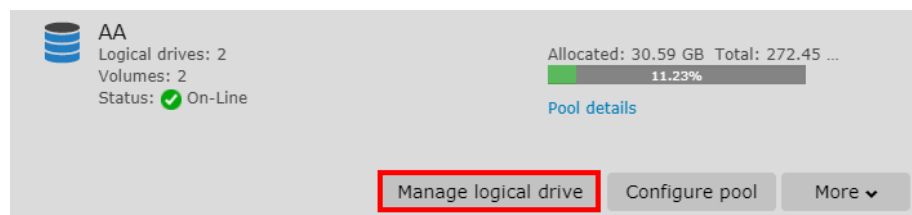
We recommended creating new logical drives in order to expand capacity of a pool. Adding new disks or replacing original disks with new ones requires reading data from old disks and writing data to the new ones, which consumes a lot more time than simply adding a logical drive to the pool.

The following steps show how to add new Logical Drives into a Pool.

**Go to**

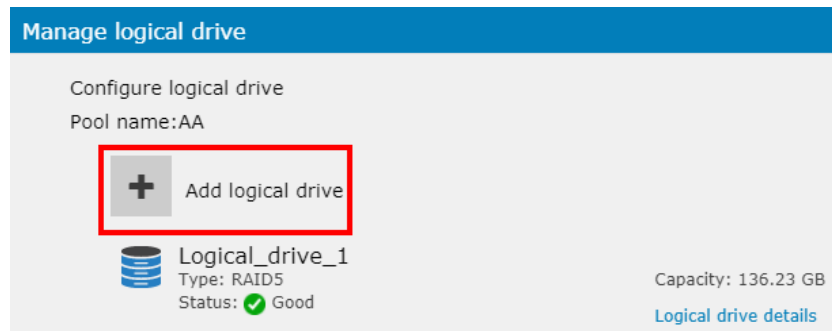
**Settings > Storage > Pool**

Select a pool and click the **Manage Logical Drive** button.



**Steps**

Click **Add logical drive button**.



After a new Logical Drive has been added, select the Pool and click **Expand Pool** under **More**. In the window that appears, click **Expand** to expand the pool capacity with the new logical drive.

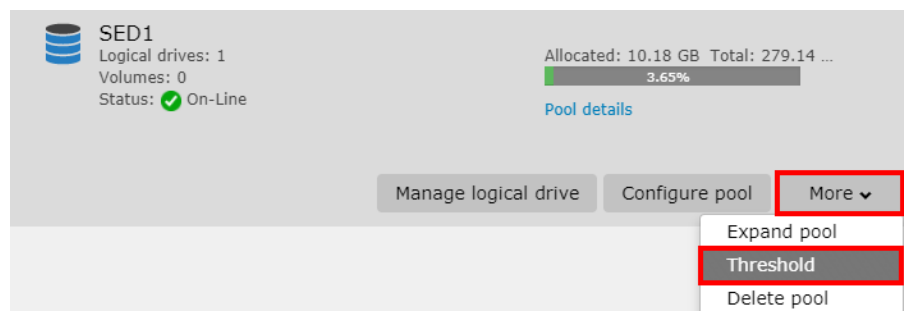


## Pool Capacity Threshold

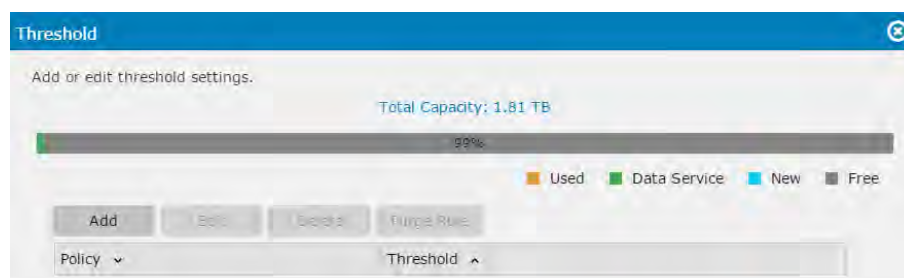
Go to

Settings > Storage > Pool

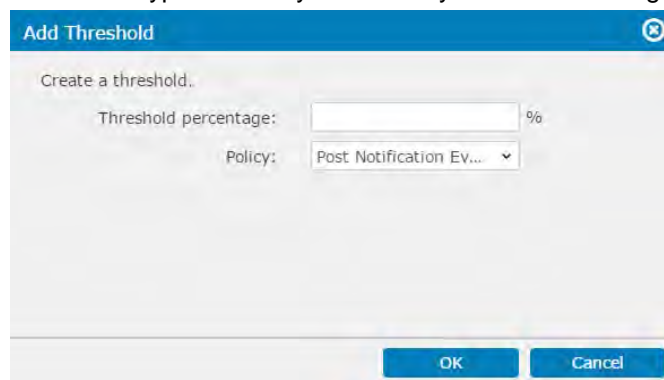
Select a pool and click the **More** button and select **Threshold**.



### Steps



Click **Add** and enter the threshold value (% of the pool). Choose the notification type. You may also modify or delete existing thresholds.



### Parameters

<b>Post Notification Event</b>	Creates a notification event when the amount of pool content reaches the threshold.
<b>Post Warning Event</b>	Creates a warning event when the amount of pool content reaches the threshold.
<b>Post Critical Event</b>	Creates a critical event when the amount of pool content reaches the threshold.
<b>Post Critical Event</b>	Creates a critical event and purges all snapshot

<b>+ Run Purge</b>	images when the amount of pool content reaches the threshold.
<b>Post Critical Event + Disassociate Snapshot Images</b>	Creates a critical event and makes all snapshot images invalid when the amount of pool content reaches the threshold.

## Configuring Purge Rules

This setting is applicable only when there is a policy with the “Post Critical Event + Run Purge” option.

Purge refers to removing old snapshot images to prevent the storage capacity from being occupied by rarely used snapshot image files.

Click **Purge Rule** in the **Threshold** page.



Highlight the purge setting and click **Edit**. The purge rule screen will appear.

<b>Purge Parameters</b>	<b>Purge Threshold</b>	Specifies the threshold policy: duration (by time) or the number of snapshot images (by SI count).
<b>Value</b>		Specifies the values.

## Storage Tiering

Tiering creates vertical layers inside a pool to improve data I/O performance compared to the traditional, monolithic pool.

For more information about storage tiering, please refer to Application Note - Automated Storage Tiering.

---

<b>Tier Levels</b>	<p>The storage system may have four tier levels to choose from: tier 0-4 with tier 0 being the fastest. Here are the recommended tier levels for RAID and drive types.</p> <p>Tier 0: SSD</p> <p>Tier 1: SAS</p> <p>Tier 2: Near-line SAS</p> <p>Tier 3: SATA</p> <p>SSD and SAS drives have fast I/Os but are expensive so they are more suitable for performance-oriented usage. NL-SATA drives are slower but are less expensive, and therefore they are suitable for capacity-oriented usage.</p>
--------------------	---

---

<b>Host I/O Priority</b>	<p>The host always writes to the highest tier in a given pool.</p> <p>Data service (snapshot, volume copy, volume mirror) will occur at the lowest tier.</p>
--------------------------	--



## **Pool Advanced Options**

You can further configure your pool by selecting the Pool advanced options tab located on the top-right corner of the Pool's page.

Pool list
Pool advanced options

### Pool advanced options

Configure pool advanced options. For detailed information, please refer to the software manual and the online help. It's highly recommended to understand the behavior of every settings before saving any changes.

#### Write policy in cache memory

Periodically flush data in cache memory to disks on write-back

Disabled

☒ Synchronize cache memory between both controllers on write-through

☒ Adaptive write policy on write back

☒ Force the system to use write-through cache policy during controller backup module (CBM) error or failure.

☐ Force the system to use write-through cache policy during power supply failure

☐ Force the system to use write-through cache policy during cooling fan failure

☐ Force the system to use write-through cache policy during abnormal status of critical components  
[Critical component option](#)

#### Other pool advanced options

☐ Verify write on normal access

☐ Verify write during logical drive initialization

☐ Verify write during logical drive rebuild

Rebuild priority

Normal

AV optimization mode

Disabled

Maximum drive response timeout

Disabled

Read-ahead option for media editing

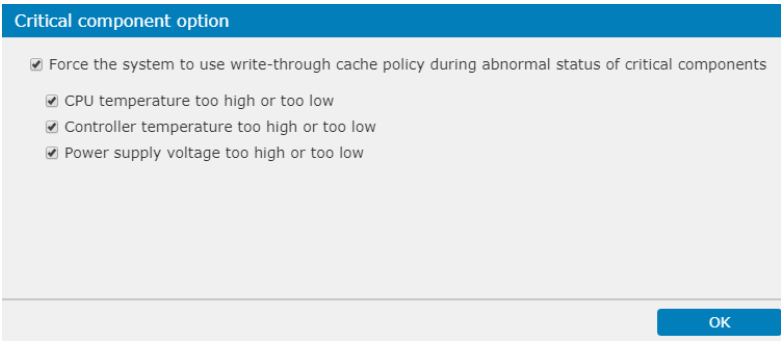
Disabled

Read-ahead option for NAS file transfer

256K

Save

Close

<b>Parameters</b>	<b>Synchronize cache policy</b>	Synchronize cache memory between both controllers on write-through
	<b>Adaptive write policy</b>	Apply adaptive write policy on write back
	<b>Force write-through cache policy during CBM Failure</b>	Force the system to use write-through cache policy during CBM failure. The CBM failure is when monitors the CBM status or if the battery is under-charged.
	<b>Force write-through cache policy during power supply</b>	This will force the system to use write-through cache policy during power supply failure.
	<b>Force write-through cache policy during fan failure</b>	This will force the system to use write-through cache policy during cooling fan failure
	<b>Force write-through cache policy during critical components</b>	Force the system to use write-through cache policy during abnormal status of critical components. Click the “critical components option” link to select under which components abnormality force to use write-through cache policy:
	<b>Critical component option</b>	
	<b>Verify write on normal access</b>	Performs Verify-after-Write during normal I/Os. Users may disable or enable this option. (This option might take up system resource)
	<b>Verify write during logical drive initialization</b>	Performs Verify-after-Write when initializing a logical drive. Users may disable or enable this option. (This option might take up system resource).
	<b>Verify write during logical</b>	Performs Verify-after-Write during the rebuild process. Users may disable or enable this option. (This option might take up system

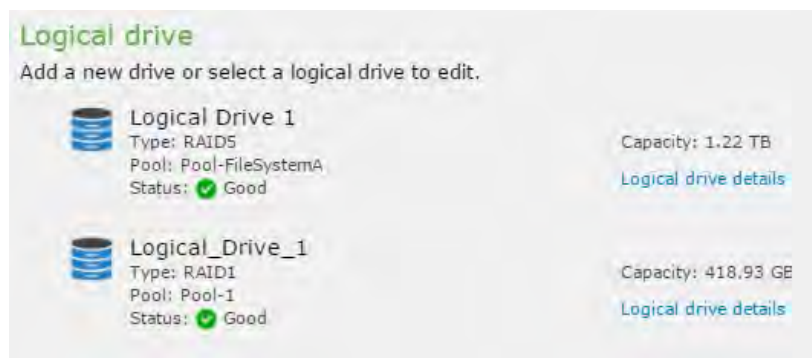
<b>drive rebuild</b>	resource).
<b>Rebuild priority</b>	Set the rebuild priority to High, Normal, Low.
<b>AV optimization</b>	Fine-tunes array performance for AV applications
<b>Maximum drive response timeout</b>	Sets the waiting period for read/write request.
<b>Read-ahead option for media editing</b>	SD Stream (50Mb/s) HD Stream (100Mb/s) 2K/4K Stream (100Mb/s+)
<b>Read-ahead option for NAS file transfer</b>	256K, 512K, 1M and 2M

## Logical Drive

Go to

**Settings > Storage > Pool**

You can set the logical drive when creating or configuring the storage pool.



Click on **Logical drive details** to see the detailed information of the logical drive.



**Limitations**

See Appendix – Logical Drive

**Parameters**

**Logical Drive Size**

Specifies the logical drive size. The maximum capacity of a drive will be reduced when it becomes a part of a logical drive because a part of the drive will be used for system purposes. By setting the drive size lower than the maximum capacity, you should be able to “hide” the system area.

If you set the drive size to be lower than the maximum size, you can later expand it.

To create a pool, the size of logical drive must be



		equal or larger than 16GB.
<b>Index</b>		Shows drive index.
<b>ID</b>		Shows drive ID.
<b>RAID Level</b>		Specifies the RAID level.
<b>Stripe Size</b>		<p>The default stripe size is 128KB for all RAID levels except for RAID 3 (16 KB). We do not encourage you to change the size unless there is a reason to do so. For example, smaller stripe sizes are ideal for I/Os that are transaction-based and randomly accessed. For more details and examples, see Optimizing the Stripe Size.</p> <div> <p>The stripe size here refers to the “Inner Stripe Size” specifying the chunk size allocated on each individual data drive for parallel access instead of the “Outer Stripe Size” which is the sum of chunks on all data drives.</p> </div>
<b>Logical Drive Status Message</b>	<b>Online Initializing</b>	Drive is on-line and currently initializing.
	<b>Online Expanding</b>	Drive is on-line and currently expanding.
	<b>Offline Initializing</b>	Drive is being shutdown and currently initializing.
	<b>Offline Expanding</b>	Drive is being shutdown and currently expanding.
	<b>Drive Missing</b>	A member drive is missing (likely a result of loose drive insertion)
	<b>Good</b>	In good condition
	<b>Checking/Updating parity</b>	The system is checking/updating the Parity of the Logical Drive.
	<b>Fatal Fail</b>	The logical drive became inaccessible, likely a result of two or more member drives having failed.
	<b>Incomplete</b>	One or more member drives missing or failed
	<b>Invalid</b>	Logical drive has not been properly initialized

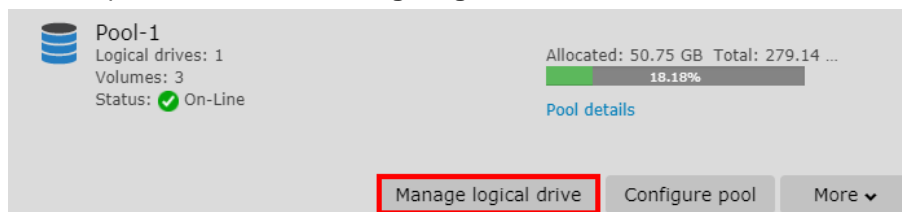
	(It will occur when firmware is being upgraded during logical drive initialization. The status will return to normal (GOOD) once the subsystem reboots.)
<b>Shutdown</b>	Logical drive has been shut down. Users have to restart the Logical Drive to bring it back online.
<b>Rebuilding</b>	Currently in rebuild process
<b>Degraded</b>	One or more member drives has failed, but the Logical Drive is still working because of RAID protection.
<b>Adding</b>	One or more non-member drives are being added into the Logical Drive.
<b>Migrating</b>	Data is migrating within tiers in the Logical Drive.
<b>Add/Migrate Paused</b>	An Adding/Migrating process is being paused.

## Configuring Logical Drive Parameters

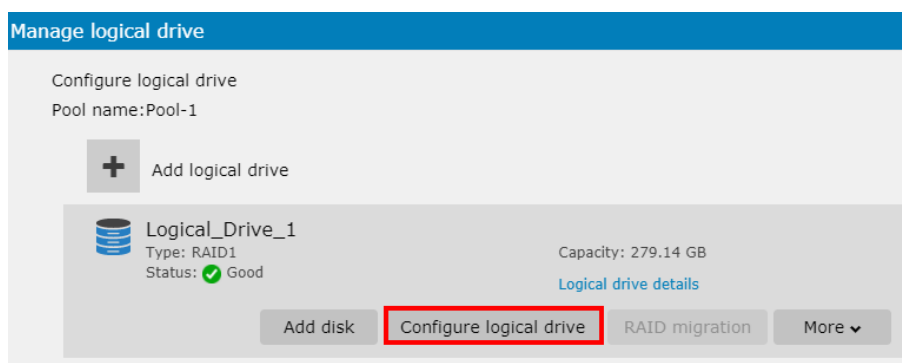
Go to

**Settings > Storage > Pool**

Select a pool and click the **Manage logical drive** button.

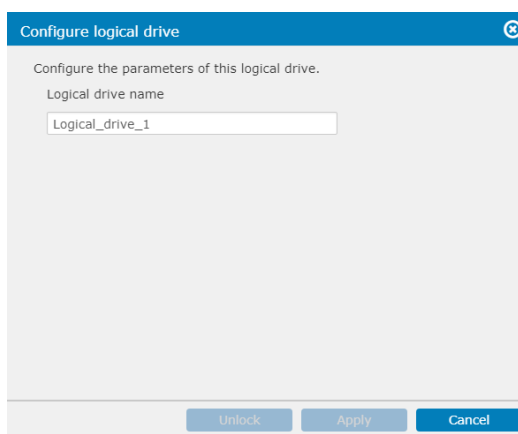


In the Configure logical drive page, click **Configure logical drive** button.



Steps

The following window will be shown. Click **Apply** to save your changes.



Parameters

**Logical Drive Name**

Specifies the name for this logical drive.  
The maximum number of characters is 32.

**SED Security**

Enhances data security with SED for all logical drives on your subsystem. Once enabled, all LDs will be SED-protected, therefore this mechanism is called "global key."

Before enabling this option, the following requirements should be met:

- A SED authentication key is created
- All member drives support SED.

## Migrating a Logical Drive to another RAID Level

Migration allows you to change the RAID level of a logical drive to another. You may need to add or delete member drives due to the minimum required number of drives for a RAID level.

Migrating works only for logical drives with RAID 5 or RAID 6 level.

Source Logical Drive must be RAID 5 or 6.

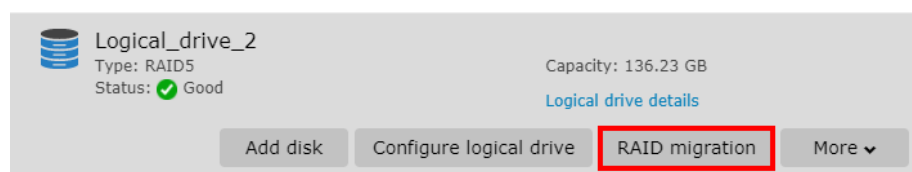
You cannot migrate a logical drive if it is already part of a pool.

### RAID 5 VS RAID 6

	Member Drives	Capacity	Redundancy
<b>RAID 5</b>	N = 3 or more	N-1	Single disk failure
<b>RAID 6</b>	N = 4 or more	N-2	Dual disk failure

### Steps

Select a logical drive and click the **RAID migration** button. Please note that this operation can only be implemented on RAID5 or RAID6 logical drives.



Current RAID level and the RAID level afterward will be displayed. Select the drives to be added into or to be removed from the logical drive. Click the **Migrate** button to start the RAID migration process.

Example 1: Migrate from RAID 5 to RAID 6.

**RAID migration**

Change the RAID level configuration of selected logical drive with RAID migration.

Current RAID Level: RAID5  
Change To Level: RAID6

Please select an unused drive to add into RAID group.

Slot	Capacity	Device
<input checked="" type="checkbox"/> 8	418.93 GB	Channel 6 JBOD --
<input type="checkbox"/> 9	558.66 GB	Channel 6 JBOD --
<input type="checkbox"/> 10	558.66 GB	Channel 6 JBOD --
<input type="checkbox"/> 11	418.93 GB	Channel 6 JBOD --
<input type="checkbox"/> 12	418.93 GB	Channel 6 JBOD --

Migrate Cancel

Example 2: Migrate from RAID 6 to RAID 5.

**RAID migration**

Change the RAID level configuration of selected logical drive with RAID migration.

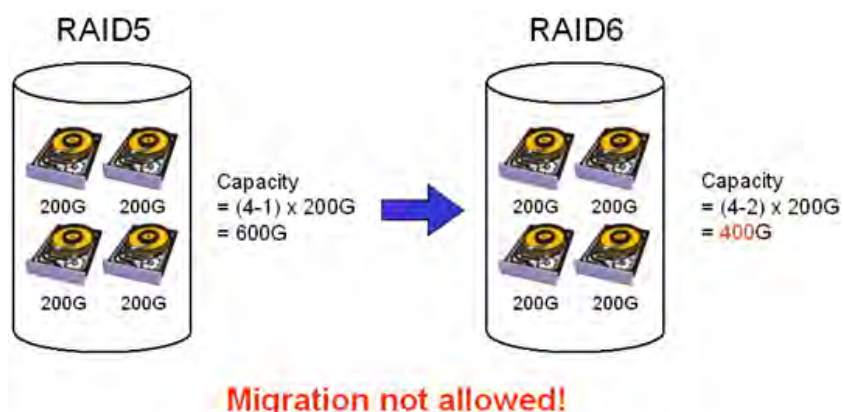
Current RAID Level: RAID6  
Change To Level: RAID5

The last used drive will be removed from the RAID group.

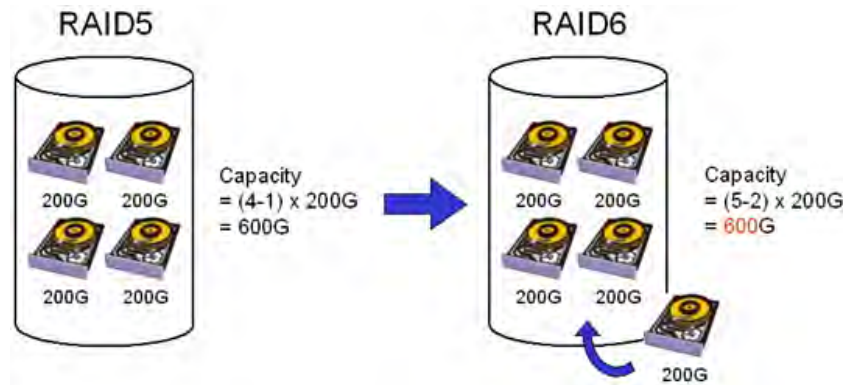
Slot	Capacity	Device
8	418.93 GB	Channel 6 JBOD --
9	558.66 GB	Channel 6 JBOD --
10	558.66 GB	Channel 6 JBOD --
11	418.93 GB	Channel 6 JBOD --

Migrate Cancel

**Migration Examples** The usable capacity of the to-be RAID6 array is smaller than the usable capacity of the original RAID5 array.

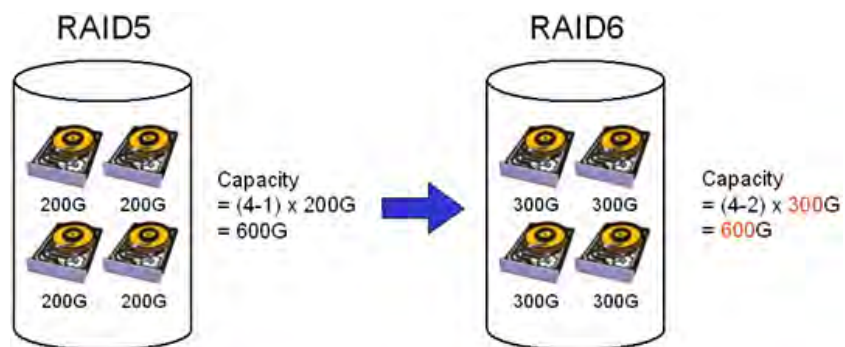


The additional capacity for migrating to a RAID6 array is acquired by adding a new member drive.



**Migration condition met by adding drive(s)!**

The additional capacity for composing a RAID6 array is acquired by using larger drives as the members of the array. Members of an existing logical drive can be manually copied and replaced using the “Copy & Replace” function in the **Disk** section.



**Migration condition met by using larger drive(s)!**

## Configuring Power Saving Mode

This feature reduces power consumption for logical drives or non-member disks such as spare drives. When there is no host I/O, disk drives may enter two power-saving modes: Level 1 for idle mode and Level 2 in spin-down mode.

The power-saving policy for physical drives has priority over the power-saving policy for logical drives.

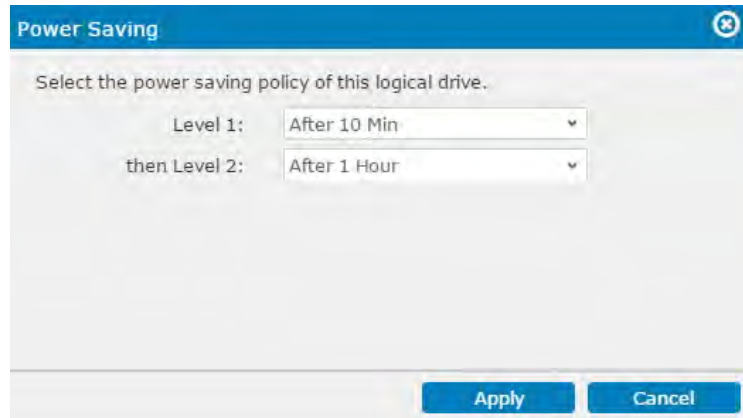
If a logical drive relocates, its power saving mode will be cancelled.

**Go to** **Settings > Storage > Logical Drive**

**Steps** Select a logical drive, click **More** and select the **Power Saving** option.



The power saving page will appear. Click **Apply** when ready.



### Waiting Period

You may also configure the waiting period for switching to the power saving mode.

- Level 1: 1 to 60 minutes without I/O requests
- Level 2: 1 to 60 minutes of Level 1 state

## Expanding a Logical Drive

To expand a logical drive/volume, you have to follow these steps:

1. Add new disk drives or replace them with higher-capacity devices.
2. Expand the logical drive to which the disk drives belong.

### Notes and Limitations

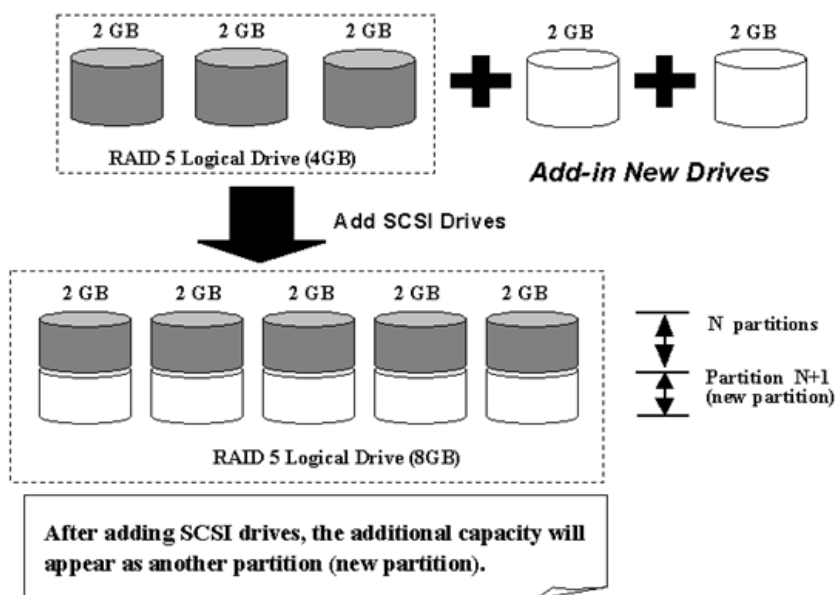
- When adding new drives to an existing logical drive, the new drives will be recognized as a new volume. Also, the new drive(s) must have the same or larger capacity than the existing member drives.
- RAID 0 or N RAID logical drives cannot be expanded because they lack parity information and therefore may cause unrecoverable data loss during expansion.
- If expansion is interrupted due to power failure or other reasons, the expansion process will stop. You may need to manually restart the expansion.

## Adding Drives to a Logical Drive

The new drive(s) will be recognized as a new volume.

The new drive(s) must have the same or larger capacity than the existing member drives.

We strongly recommend adding a drive with the same capacity as the existing member drives.

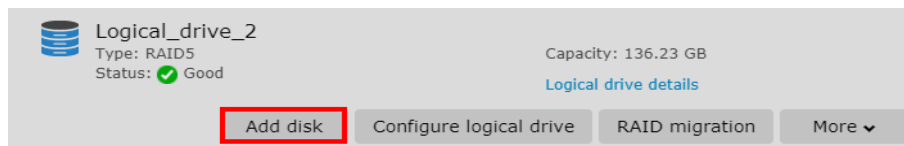




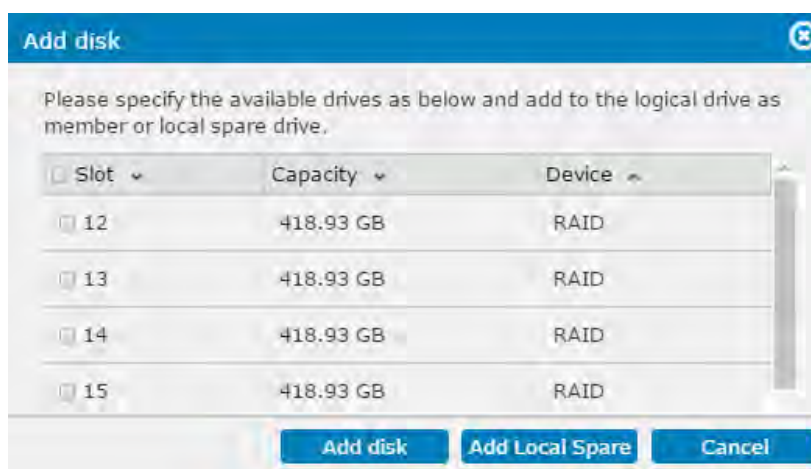
**Go to** Settings > Storage > Logical Drive

**Steps**

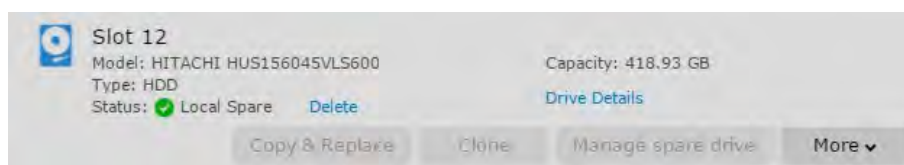
1. Select a logical drive and click **Add disk**.



2. In the pop up window, select one or more disks to be added as a member drive or a spare drive.



3. If a local spare drive has been added, the newly added drive will be marked as Local Spare in the **Drive** page.



4. If member drives have been added, the **Adding Disk** progress will appear in the **Status** column. (Depending on the RAID level of the logical drive, you may need to add more than one drive at a time.)
5. Drive status is displayed in the **Drive** page (**Settings > Storage > Drive**).

## Expanding the Size of a Logical Drive

You can expand the size of a logical drive only if there is available space in the member drives.

The expanded area will become a new volume. After this, you need to expand the size of the pool it belongs to.

**When All Disk Capacity Has Been Used**

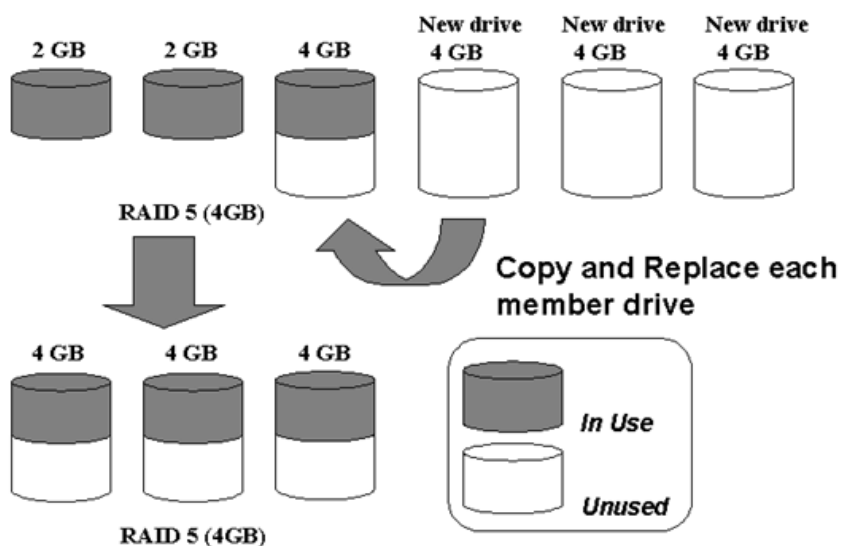
You cannot expand a logical drive if all disk drive capacity has been used up for the logical drive. In that case, there are two options:

1. You may add more member drives.
2. You may copy and replace member disk drives with larger capacity drives, and then use the additional capacity to expand the logical drive following the steps in this section.

You must replace all member drives.

**Expand the size of a logical drive by replacing higher capacity drives**

You can expand the size of a logical drive by replacing its member drives with higher capacity drives.



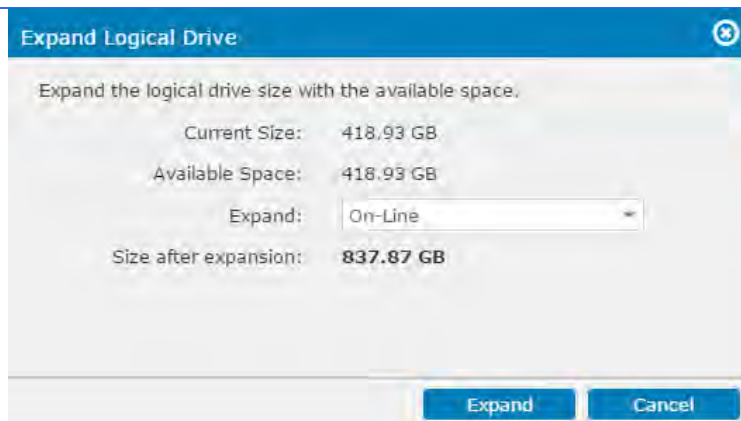
*After all the member drives have been replaced, execute the "Expand logical drives" to make use of the unused capacity.*

**Go to**

**Settings > Storage > Logical Drive**

**Steps**

The expanded logical drive page will appear. Select the initialization mode and click **Expand**.



<b>Parameters</b>	<b>Expandable Size</b>	Shows the available size to be expanded. The available size is automatically calculated by (Total capacity) – (Current logical drive capacity).
	<b>Execution (Initialize) Mode</b>	Shows how the expansion will be executed: online (expansion continues in the background while users carry on with their tasks using the logical drive; this is a slower process) or offline (during expansion, users cannot use the logical drive; This is a faster process).

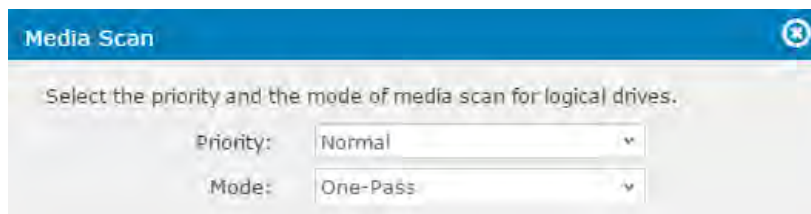
## Scanning a Logical Drive Manually

You can only scan a logical drive after its initialization is completed.

<b>Steps</b>	Select a logical drive, click the <b>More</b> button and then click the <b>Media Scan</b> option.
--------------	---



The scan configuration window will appear.



<b>Parameters</b>	<table> <tr> <td data-bbox="470 560 758 600"><b>Priority</b></td><td data-bbox="758 560 1406 660">The higher the priority, the faster the scanning but the system performance will decrease.</td></tr> </table>	<b>Priority</b>	The higher the priority, the faster the scanning but the system performance will decrease.
<b>Priority</b>	The higher the priority, the faster the scanning but the system performance will decrease.		
	<table> <tr> <td data-bbox="470 660 758 712"><b>Mode</b></td><td data-bbox="758 660 1406 712">Scans once (Execution Once) or continuously.</td></tr> </table>	<b>Mode</b>	Scans once (Execution Once) or continuously.
<b>Mode</b>	Scans once (Execution Once) or continuously.		

## Rebuild a Logical Drive

The Rebuild menu appears only for RAID 1, 3, 5, or 6 logical drives with one or more failed member drives.

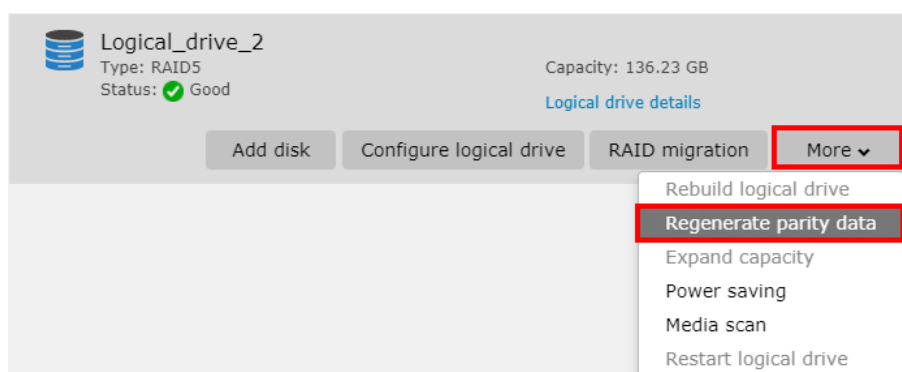
A failed drive is indicated as “BAD” when you view the logical drive’s member drive status.

<b>Steps</b>	Select the logical drive that is in a degraded state and click the <b>Rebuild logical drive</b> button. If the logical drive does not go back to a healthy state after rebuilding, remove it and create the logical drive anew.
--------------	---

## Regenerating Parity

This function does not apply to RAID0 or NRAID logical drives. You may regenerate parity to determine whether data parity inconsistency exists.

<b>Steps</b>	Select a logical drive. Click the <b>More</b> button and then click the <b>Regenerate parity data</b> option.
--------------	---



The parity data will be regenerated immediately.

## Restarting a Logical Drive

After moving a logical drive (all member drives) into another enclosure, or if a pool element has gone offline or has been locked, Logical Drive will be in the “Shutdown” status, and you need to restart the logical drive to bring it back online.

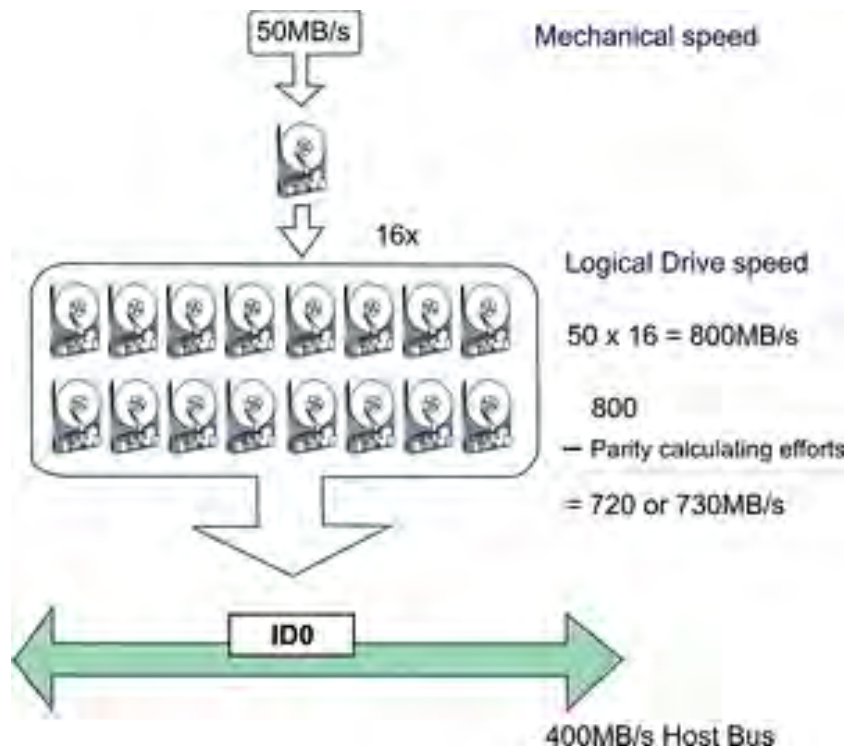
**Steps** Select a logical drive that is currently in the Shutdown status. Click the **More** button and choose the **Restart logical drive** option. The logical drive will be restarted immediately.

## Optimizing Logical Drive Access

In an environment that spans multiple enclosures, including all disk drives into one logical drive may not be a good idea. A logical drive with too many members may cause difficulties with maintenance tasks such as rebuilding.

RAID arrays deliver a high I/O rate by having all disk drives spinning and returning I/O requests simultaneously. If the combined performance of a large array exceeds the maximum transfer rate of a host channel, you will not be able to enjoy the performance gain by simultaneous disk access.

### Example



The diagram shows a logical drive consisting of 16 members. The host bus bandwidth apparently becomes a bottleneck here, which will compromise the benefit of simultaneous disk access.

## Optimizing Stripe Size

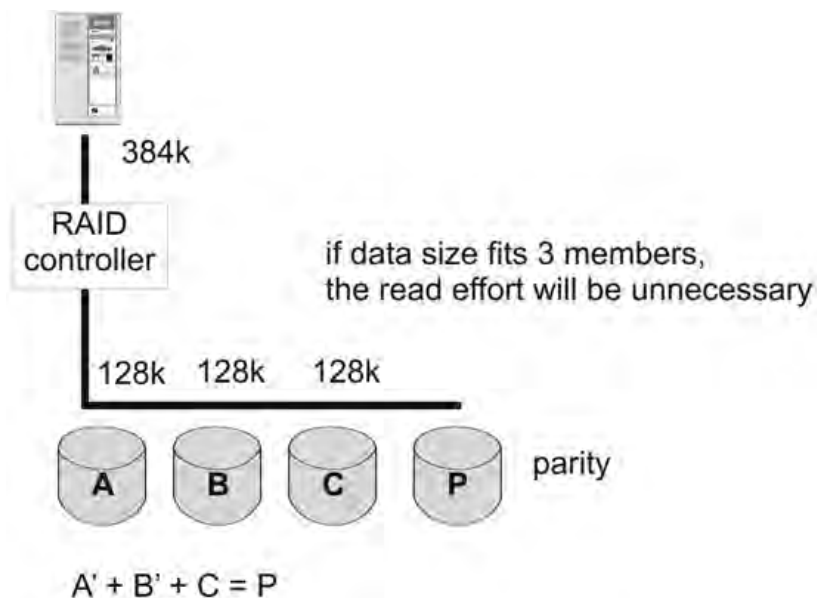
The stripe size should only be changed when you can test the combinations of different I/O sizes and are sure of performance gain.

For example, if the I/O size is 256k, data blocks will be written to two of the member drives of a 4-drive array while the RAID firmware will read the remaining member(s) in order to generate the parity data.

We will use RAID 3 in the example below.

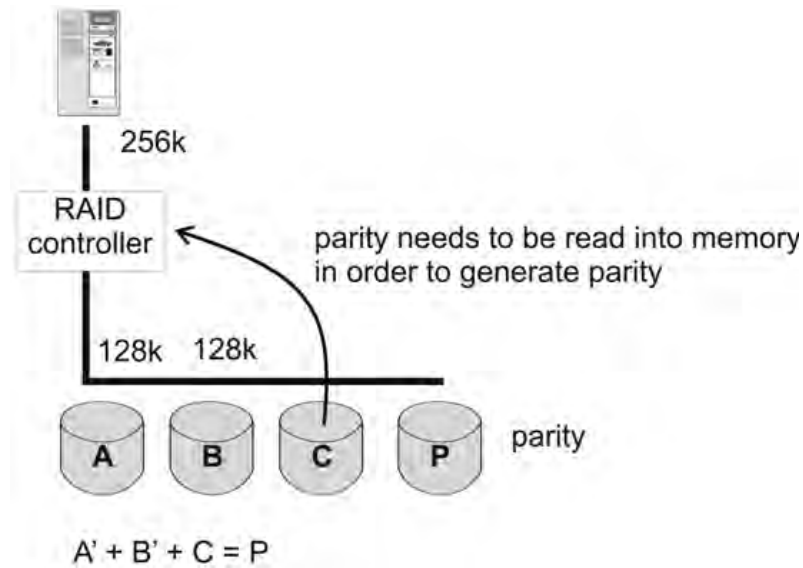
### I/O Size = Stripe Size

In an ideal situation, a 384k I/O size allows data to be written to 3 member drives while the parity data is simultaneously generated without consulting data from other members in the array.



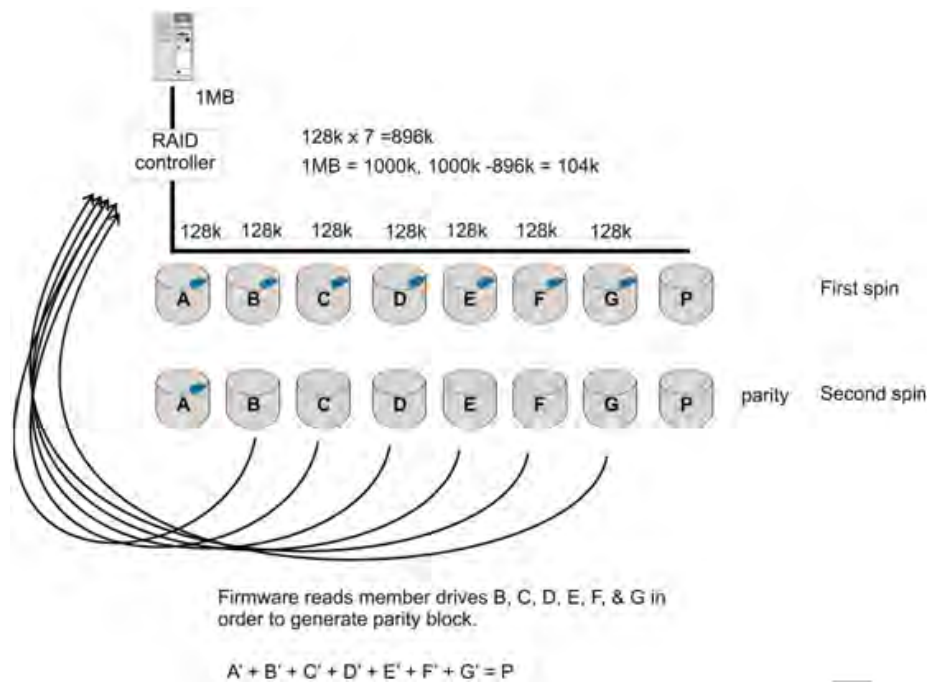
### I/O Size > Stripe Depths

If the I/O size is larger than the combined stripe depths, the extra data blocks will be written to the member drives on the successive spins, and the read efforts will also be necessary for generating parity data.



### Summary

Although the real-world I/Os do not always perfectly fit the array stripe size, matching the array stripe size to your I/O characteristics can eliminate draPS on performance (hard drive seek and rotation efforts) and will ensure optimal performance.



## Calculating Logical Drive Performance

The following is a simple example using an 8-member RAID5.

### Capacity

RAID5 LD capacity = [no. of HDDs - 1 (parity drive)] x single-drive capacity

---

Exp.  $(8-1) \times 1\text{TB} = 7\text{TB}$

---

**Performance**

- MB/s in pure reads: [no. of HDDs - 1 (parity drive) x 100MB/s (15k SAS approx.)] x 85% (15% parity and I/Os handling overhead)  
Exp.  $(8-1) \times 100 \times 85\% = 595 \text{ MB/s}$
- Random IOPS: [no. of HDDs - 1 (parity) x 180 IOPS (15k SAS approx.)] x 85% (15% parity and I/Os handling overhead)  
Exp.  $(8-1) \times 180 \times 85\% = 1071 \text{ IOPS}$



## Protecting a Logical Drive with Self-encrypting Drives (SED)

You can create and manage a local encryption key to protect a logical drive on the storage device when the logical drive is purely made up of self-encrypting drives (SED).

Note:

- You can create a local encryption key only when the system does not host a global encryption key.
- To encrypt all SED logical drives with a global encryption key, refer to SED Key Management.

Go to	Settings > Storage > Pool						
Steps	<ol style="list-style-type: none"> <li>1. Click on the storage pool made up of SED drives.</li> <li>2. Click <b>Manage logical drive</b>.</li> <li>3. Click on the desired logical drive to encrypt.</li> <li>4. Click <b>More &gt; Modify SED authentication key</b>.</li> <li>5. Go to the <b>SED security</b> drop-down menu and select how to encrypt the SED logical drive:</li> </ol>						
	<table> <tr> <td><b>Disabled</b></td><td>The system does not encrypt the SED logical drive.</td></tr> <tr> <td><b>Use an existing SED authentication key</b></td><td> <p>Encrypt the SED logical drive with an existing key:</p> <p><b>Select an existing key from the system:</b> Select a global key or a local key stored in the system.</p> <p><b>Upload an SED key:</b> Click <b>Browse</b> to upload a key file. Only the key file generated by an PAC Storage system is compatible.</p> </td></tr> <tr> <td><b>Create a new SED authentication key</b></td><td> <p>Encrypt the SED logical drive with a new key:</p> <p><b>Generate and download a key file from the system:</b> Click <b>Generate</b> to create a .key file that contains the SED authentication key. Then, upload the key file for confirmation by clicking <b>Browse</b>.</p> <p><b>Enter the key manually:</b> Enter a custom key and confirm it.</p> <p>You must keep this key in a secure place. This key cannot be recovered once lost or forgotten.</p> </td></tr> </table>	<b>Disabled</b>	The system does not encrypt the SED logical drive.	<b>Use an existing SED authentication key</b>	<p>Encrypt the SED logical drive with an existing key:</p> <p><b>Select an existing key from the system:</b> Select a global key or a local key stored in the system.</p> <p><b>Upload an SED key:</b> Click <b>Browse</b> to upload a key file. Only the key file generated by an PAC Storage system is compatible.</p>	<b>Create a new SED authentication key</b>	<p>Encrypt the SED logical drive with a new key:</p> <p><b>Generate and download a key file from the system:</b> Click <b>Generate</b> to create a .key file that contains the SED authentication key. Then, upload the key file for confirmation by clicking <b>Browse</b>.</p> <p><b>Enter the key manually:</b> Enter a custom key and confirm it.</p> <p>You must keep this key in a secure place. This key cannot be recovered once lost or forgotten.</p>
<b>Disabled</b>	The system does not encrypt the SED logical drive.						
<b>Use an existing SED authentication key</b>	<p>Encrypt the SED logical drive with an existing key:</p> <p><b>Select an existing key from the system:</b> Select a global key or a local key stored in the system.</p> <p><b>Upload an SED key:</b> Click <b>Browse</b> to upload a key file. Only the key file generated by an PAC Storage system is compatible.</p>						
<b>Create a new SED authentication key</b>	<p>Encrypt the SED logical drive with a new key:</p> <p><b>Generate and download a key file from the system:</b> Click <b>Generate</b> to create a .key file that contains the SED authentication key. Then, upload the key file for confirmation by clicking <b>Browse</b>.</p> <p><b>Enter the key manually:</b> Enter a custom key and confirm it.</p> <p>You must keep this key in a secure place. This key cannot be recovered once lost or forgotten.</p>						

Configure SED key

Modify SED authentication key

SED key status

None

SED security

Create a new SED authentication key

☐ Generate and download a key file from the system (Type: File)

☒ Enter the key manually(Type: String)

Please remember the key and keep it security.

.....

Please enter the key again to confirm

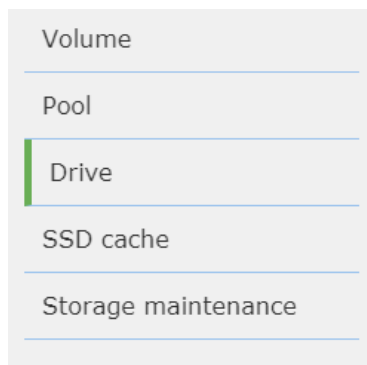
.....

6. Click **Apply** to encrypt the SED logical drive.

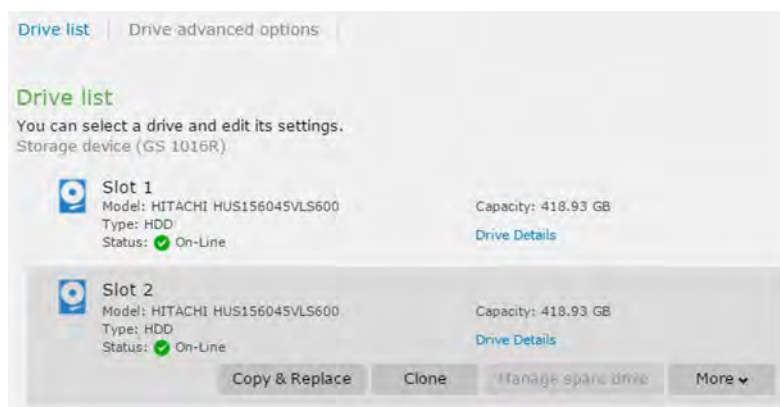
## Drive

Go to

**Settings > Storage > Drive**



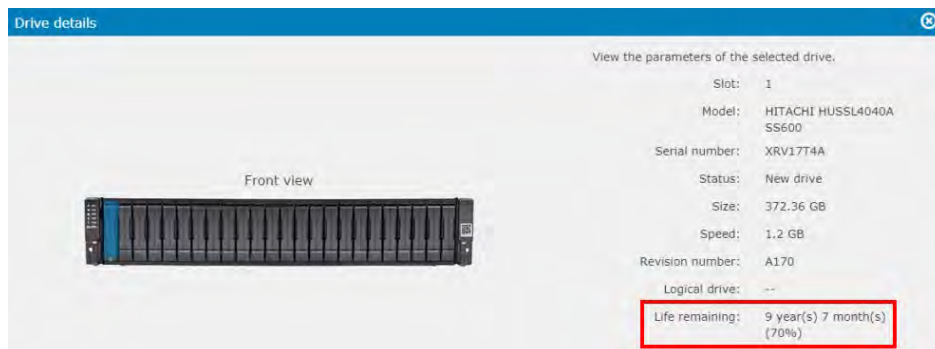
Click on the controller enclosure or the disk enclosure to see the drive list.



Click **Drive Details** to see the details of the hard drive.

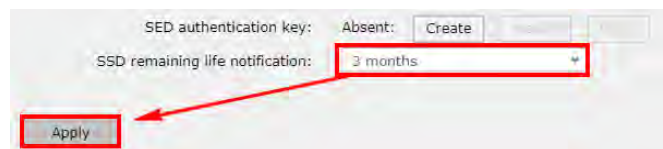


For PAC Storage PS 3025A series, SSD's life span is displayed under "Life remaining" in year/month/percentage format.



<b>Drive Status</b>	<b>Global Spare</b>	Global spare drive
	<b>Local Spare</b>	Local spare drive
	<b>Enclosure Spare</b>	Enclosure spare drive
	<b>Initial</b>	Currently initializing
	<b>On-Line</b>	In good condition
	<b>Off-Line</b>	The Logical Drive has been shutdown.
	<b>Rebuilding</b>	Currently in rebuilding process
	<b>New Drive</b>	An unformatted new drive which has not been included in a logical drive or configured as a spare drive
	<b>Used</b>	An used drive which has not been included in a logical drive or configured as a spare drive
	<b>Formatted</b>	Formatted drive with a reserved section
	<b>Bad</b>	Failed drive
	<b>Drive Absent</b>	A drive does not exist in this slot
	<b>Adding</b>	Being added to a logical drive
	<b>Ceding</b>	Being dismissed from a logical drive (such as when migrating from RAID 6 to RAID 5)
	<b>Copying</b>	Copying data from a member drive to be replaced

<b>Cloned</b>	Clone drive holding the replication of data from a source drive
<b>Cloning</b>	Cloning data
<b>Missing</b>	Drive missing (The drive does not respond; it might need to be re-inserted or replaced)  This status might appear temporarily after booting up and before I/O distribution, which is not a sign of error.
<b>SB-Missing</b>	Spare drive missing
<b>Exiled</b>	Turned off by firmware for being unreliable
<b>Media scan</b>	The system is scanning the drive to check whether it's still reliable.
<b>Read-only</b>	The drive is being tested for read only operations.
<b>Read-Write</b>	The drive is being tested for both read and write operations.
<b>Life remaining</b>	The life remaining of the SSD drive. The status shows the life span of the SSD drive  For PAC Storage PS 3025A series, you can even set notification timer for the SSD remaining life span. Go to Settings > Systems > General > Advanced Settings > Drive-side category. Press <b>Apply</b> to complete the Settings.



### About Exiled Drives

When the firmware finds a drive unreliable, it will isolate the drive from logical drives or pools and turn it off. The drive's status will then change into "EXILED." The firmware will then rebuild its logical drive to a spare drive (local spare drive > enclosure spare drive > global spare drive).

You need to replace the exiled drive as soon as possible.

Here are possible reasons for a drive to be exiled:

- Cannot be scanned during boot-up
- A member drive of a logical drive was removed and then re-inserted. In this case, the system will not automatically let the drive rejoin its logical drive.
- Here are some tips for exiled drives:
  - You can put the exiled drive back to “NEW” status by removing its 256MB reserved space. This method is recommended only for debug purposes.
  - If you move an exiled drive to another enclosure, its status will change to “USED” because there is no association with existing logical drives any more.
  - A “BAD” drive will turn into an “EXILED” drive if it can be scanned during boot-up.

#### Drive Types and Applicable Features

	Member Drive	Spare Drive	Formatted Drive	Unformatted Drive
Assign as Spare Drive			✓	✓
Delete Spare Drive		✓		
Format Drive				✓
Unformatted Drive			✓	
Scan Drive		✓		
Clone Drive	✓			
Identify Drive	✓	✓	✓	✓
Show Drive Information	✓	✓	✓	✓
Run Read/Write Test				✓

#### About Aligning the Drive Size

The basic read/write unit of a hard drive is a block. If members of a logical drive

have different block numbers (capacity), the smallest block number will be taken as the maximum capacity to be used in every drive when composing a logical drive. We strongly recommend you use drives of the same capacity.

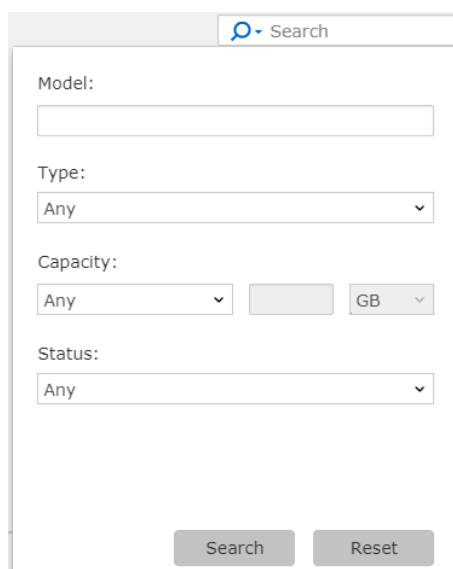
---

**Spare Drives**

You may assign a spare drive to a logical drive with an equal or smaller block number but you should not do the reverse.

## Advanced Search

A search bar is located at the top-right of the device list. There are two types of searching, regular searching and advanced searching. The advanced searching option helps user to search for specific drives.



The image shows a search interface with a header bar containing a magnifying glass icon and the word "Search". Below this, there are four sections for filtering:

- Model:** A text input field.
- Type:** A dropdown menu currently showing "Any".
- Capacity:** A dropdown menu currently showing "Any", followed by a numeric input field, and then a unit dropdown menu currently showing "GB".
- Status:** A dropdown menu currently showing "Any".

At the bottom of the form are two buttons: "Search" and "Reset".

Advance options	Model	Enter the model name.
	Type	The options are: "Any", "SSD", "HDD". (default is set to "Any")
	Capacity	The options are: "Any", "Less than", "Equal to", Greater than". (default is set to "Any")
	Status	Select one option from the scroll down list.

Press **Search** to start searching for results, or press **Reset** button to set all parameters to their factory default.



## Drive advanced options

To set advanced option for your drive, you can select the Drive advanced options tab on the top-right corner of the Drive page.

Once changes are made, press the **Save** button to save your configuration.

<b>Parameters</b>	<b>Auto rebuild on drive swap</b>	Specifies how frequently the system checks if there are removed drives. If a replacement drive is detected, the firmware will automatically rebuild the logical drive. (This option affects system performance)
	<b>Disk access delay time</b>	Specifies the delay time before the subsystem tries to access the hard drives after power-on. The default is determined by the type of drive interface. You may adjust this parameter to fit the spin-up speed of different disk drive models.
	<b>Drive I/O timeout (sec)</b>	Specifies the time interval for the controller to wait for a drive to respond. If the drive does not respond within the drive I/O timeout value, the drive will be considered as a failed drive.

When the drive itself detects a media error while reading from the drive platter, it usually retries the previous reading or re-calibrates the read/write head. When a disk drive encounters a bad block on the media, it will attempt to reassign the bad block to a spare block.

During channel bus arbitration, a device with higher priority can use the bus first. A device with lower priority will sometimes receive an I/O timeout when devices of higher priority keep utilizing the bus.

The default setting for “drive I/O timeout” is 7 seconds. It is recommended not to change this setting. Setting the timeout to a lower value will cause the controller to judge a drive as failed while a drive is still retrying, or while a drive is unable to arbitrate the drive bus. Setting the timeout to a greater value will cause the controller to keep waiting for a drive, and it may sometimes cause a host timeout.

---

**Action done to drive predictable failure (S.M.A.R.T)**

S.M.A.R.T monitors selected disk drives attributes that are susceptible to degradation over time. If a failure is likely to occur, S.M.A.R.T reports to the host, the host then prompts the user to backup data from the failing drive.

---

**Maximum number of tags**

Specifies support for Tagged Command Queuing (TCQ) and Native Command Queuing (NCQ). TCQ is a traditional feature on SCSI, SAS, or Fibre Channel disk drives, while NCQ is recently implemented with SATA disk drives. The queuing feature requires the support of both host adapters and hard disk drives. Command queuing can intelligently reorder host requests to streamline random accesses for IOPS/multi-user applications.

---

**Power Saving level 1 & 2**

Set the activation time for power saving, this feature reduces power consumption for non-member disks such as spare drives. When there is no host I/O, disk drives may enter two power-saving modes: Level 1 for idle mode and Level 2 in spin-down mode.

Note: The power saving policy for physical drives has priority over the power-saving policy for logical drives. If a logical drive physically relocates, its power saving mode will be cancelled.

---

**SSD remaining life notification**

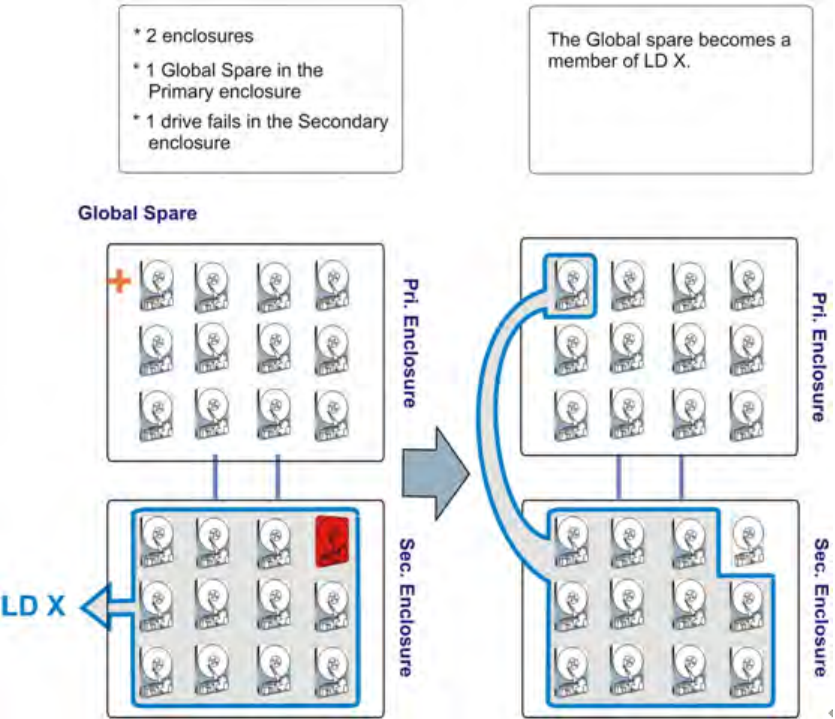
The user will be notified of the SSD remaining life according to the percentage set in this option.

---

## Spare Drive Types

A spare drive replaces a failed disk drive. A spare drive is assigned to a logical drive. When a member drive of that logical drive fails, the spare drive takes place of the failed drive and becomes part of that logical drive. The logical drive starts rebuilding the data using parity information.

<b>Types</b>	<b>Local spare</b>	A local spare drive is dedicated to a logical drive. It can be used for replacing any of the member drives, even across subsystem enclosures, but it cannot be used for a different logical drive, even if that logical drive resides in the same enclosure.
	<b>Global spare</b>	A global spare drive is not dedicated to a specific logical drive. It can be used to replace any disk drive.
	<b>Enclosure spare</b>	An enclosure spare drive is dedicated to the enclosure it resides. It can be used for a member of any logical drives, as long as it resides in the same enclosure.
<b>Why Enclosure Spare?</b>	<p>If a global spare drive replaces a disk drive of a logical drive that spans multiple enclosures, the chance of removing the wrong drive increases, e.g. accidentally mixing SAS and SATA drives of different RPM's, etc.</p> <p>The Enclosure Spare helps prevent the situation by rebuilding drives that only reside in the same enclosure.</p>	



## Adding/Deleting a Spare Drive

If an available drive (unassigned to a logical drive) is not present, you may not see the spare drive menu at all.

The capacity of spare drives must be equal to or greater than that of member drives.

### Mixing SATA and SAS Drives

You cannot use a SATA spare drive for SAS logical drive, and vice versa. We strongly recommend you avoid mixing SATA and SAS drives in the same logical drive, pool, or enclosure.

### Go to

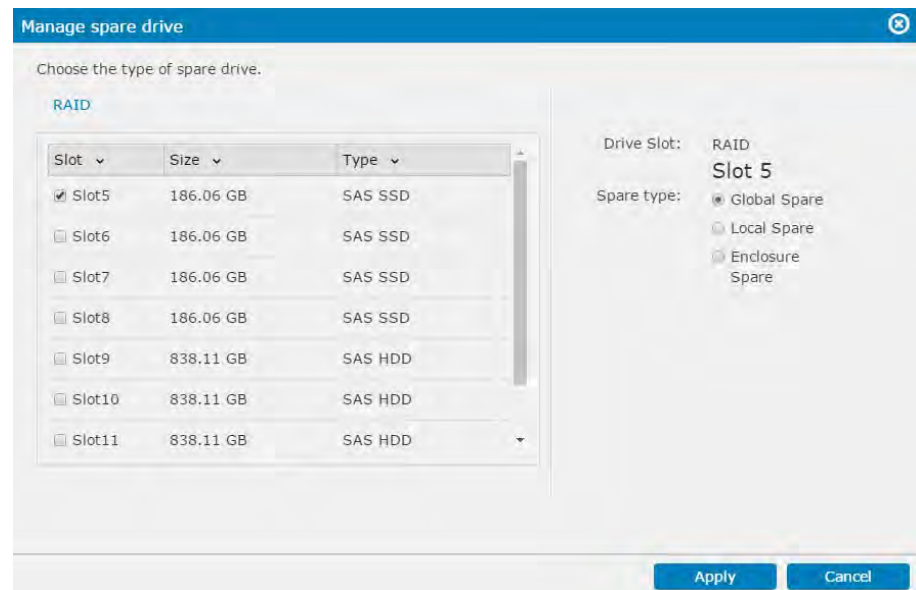
**Setting > Storage > Drive**

Click the **Manage Spare Drive** button.



### Add & Delete a Spare Drive

The Manage Spare window appears with a list of available drive(s) on the system. Select a drive and choose the spare type.



The drive status will be changed to the chosen spare type.

To delete a spare drive, click **Delete** in the drive status. The drive status will be changed back.

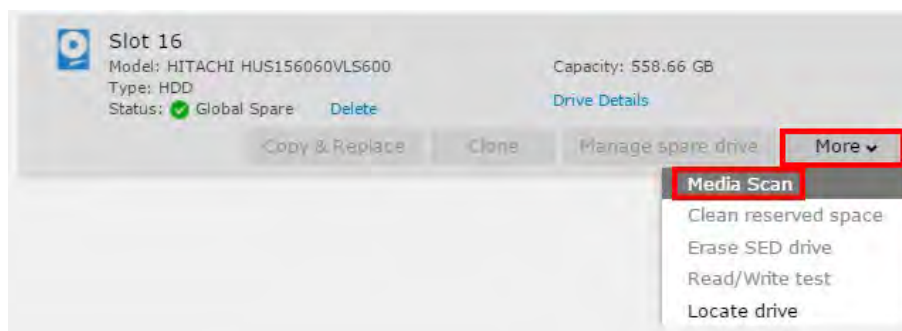
## Scanning a Spare Drive

To scan a spare disk drive, it must be an enclosure spare drive or a global spare drive.

### Go to

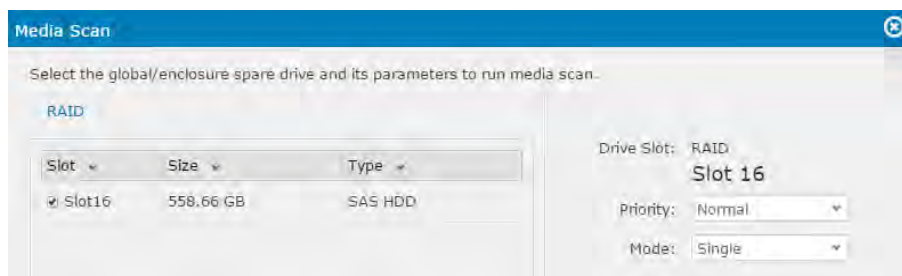
**Settings > Storage > Drive**

Select the drive and click **More** and select **Media Scan**.

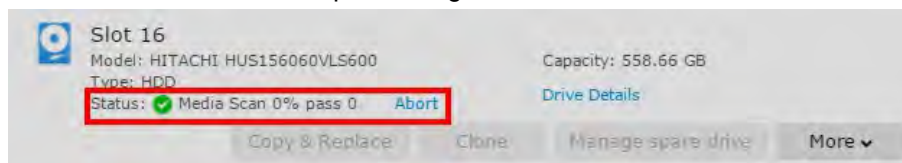


### Steps

Click on the drive you wish to scan. Select **Priority** and **Mode** and click the **Scan** button to begin scanning.



The Scanning process can be seen in the drive status column. To stop the scan, click the **Abort** button to stop scanning.



### Parameters

#### Priority

Specifies the priority of this scan: Low, Normal, Mid-High and High.

#### Mode

Specifies the mode of the scan: Single (once), Continuous (repeated).

## Running Read/Write Test

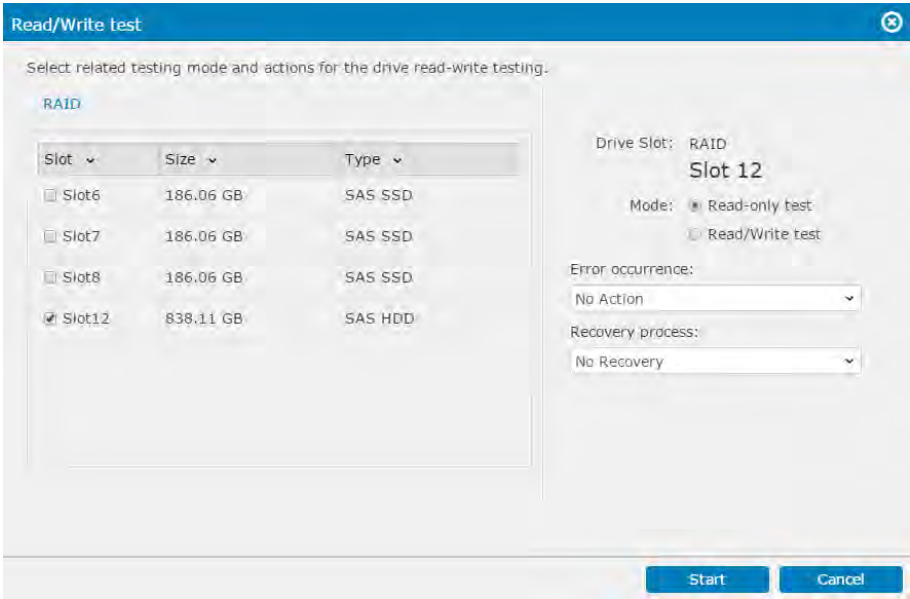
This function can only be performed on new (unformatted) drives.

Go to **Settings > Storage > Drive**

Select the drive, click the **More** button and select the **Read/Write test** option.



**Steps** The Read/Write test configuration table will pop up, listing the new (unformatted) drives. Finish the configuration and click the **Start** button. For detailed information, see the parameter descriptions below.

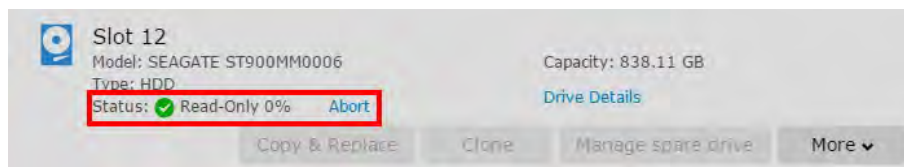


<b>Parameters</b>	<b>Mode</b>	Specifies whether to test write and read capability or read only.
	<b>Error Occurrence</b>	Specifies what to do when an error is found during testing: abort test (any error), abort test (on hardware errors), or continuing testing.
	<b>Recovery Process</b>	Specifies what recovery action to take when errors are found during testing, such as marking bad blocks, reassigning bad blocks or reassigning bad blocks followed by marking them if they fail.



## Aborting Read/Write Test

The Read/Write status can be seen in the drive status column. To abort the test, click the **Abort** button.



## Removing a Drive Reserved Space

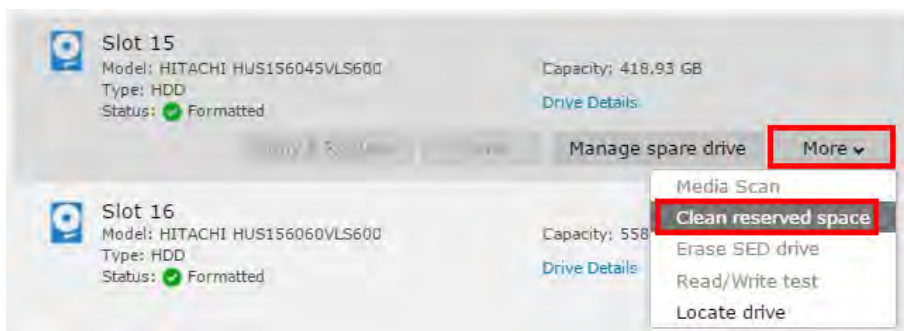
A formatted drive includes a reserved section (256MB block) to be used for event logs, configuration Settings and storage virtualization so these contents will not be erased upon system reset. You may remove the reserved section (unformatting a drive) to bring the drive status to “new.” This operation is necessary for debugging purposes, especially if you intend to do a read/write test on a drive; otherwise it is not recommended.

To bring back the reserved space, you can run the formatting operation.

### Go to

**Settings > Storage > Drive**

Select the drive, click the **More** button and select the **Clean reserved space** option.



### Steps

Select the drives to be unformatted, and click **Clean**.



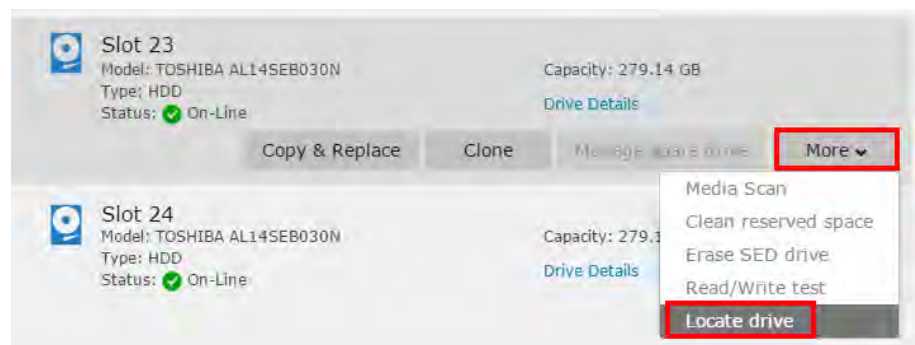


## Identifying a Drive

You may flash the LED on the drive trays to identify the drive hardware-wise on a storage subsystem enclosure.

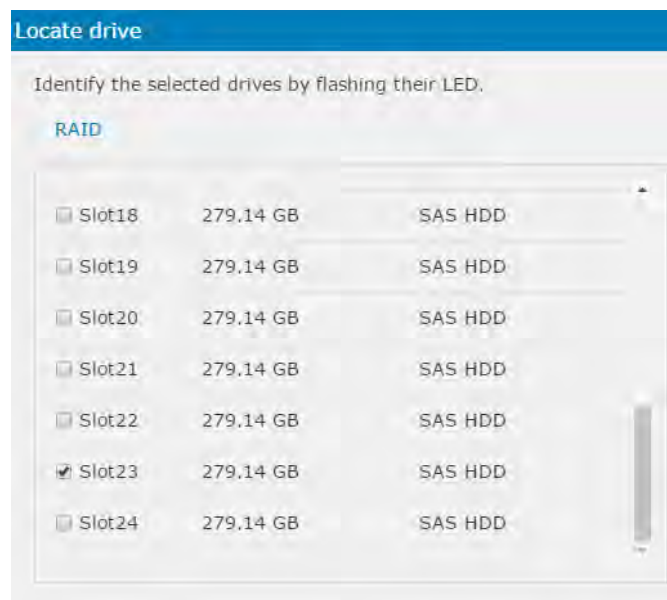
**Go to** **Settings > Storage > Drive**

Select the drive, click the **More** button and select the **Locate drive** option.



### Steps

1. Select the drive you would like to identify.



2. Select how the hard drive LED(s) will be flashed and click **Apply**.

Drive Slot:

RAID

Slot 23

Mode:

☒ Flash selected drives
 ☐ Flash all drives
 ☐ Flash all but selected drives

The LED of the selected (or unselected) drives will turn blue for five to ten seconds.

Parameters	Flash Selected Drive	Flashes only the LED of the selected drive.
	Flash All Drives	Flashes the LED of all drives in the subsystem enclosure.
	Flash All but Selected Drives	Flashes the LED of all drives in the storage subsystem enclosure but the selected drive.

## Preventing/Recovering a Failing Drive

When a drive fails, a spare drive can rebuild its content and take over its role. However, if you know a drive is likely to fail in the future, you can preemptively create its backup copy by either cloning its content to a spare drive or replacing it after copying the content to a non-member drive.

## Cloning a Drive

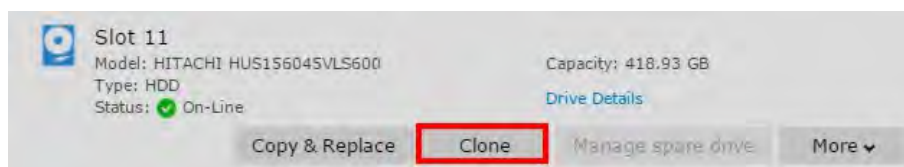
### Prerequisites

- The source drive must be a member of a logical drive.
- The target drive must be a spare drive and it must be available when the cloning occurs (the existing spare drive will automatically be chosen as the target drive).
- The capacity of the target drive must be larger than the source drive.

### Go to

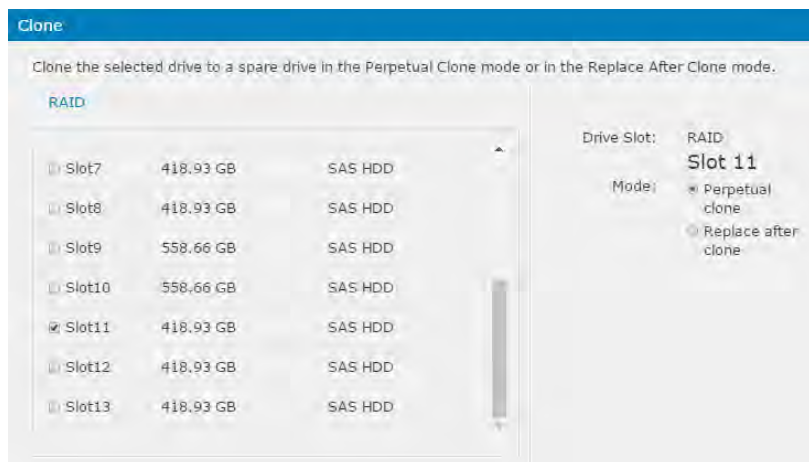
**Settings > Storage > Drive**

Select the drive and click the **Clone** button.



## Steps

1. Select the drive to be cloned (Slot 11 in this example). The “source” drive must be a member of a logical drive.



2. Select **perpetual clone** or **replace after clone**.
3. Click **Apply**.  
The spare drive is automatically chosen as the target drive. To view the process and/or abort cloning, click the spare drive (Slot 14 in this example).
4. The cloning process can be seen in the spare drive status column. To abort, click the **Abort** button.



## Parameters

### Perpetual clone

Perpetual cloning refers to copying the content of the source drive into the target drive. The source drive will remain a member of the logical drive it belongs to. When the source drive fails, the target drive will take over its role.

### Replace after clone

Replacing refers to copying the source drive into the target drive and then assigning the target drive to the role occupied by the source drive. The source drive will be disassociated from the logical drive it belongs to and will become a “used drive.”

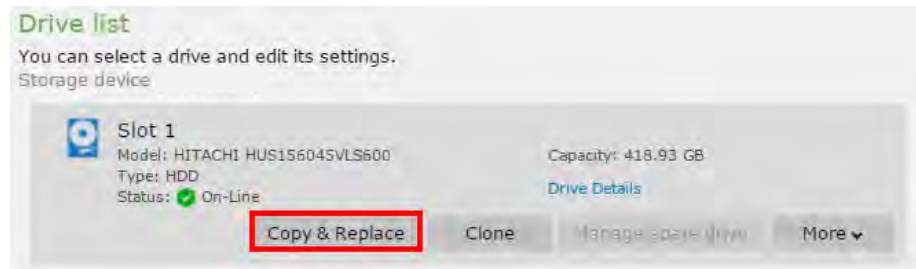
## Copying & Replacing a Drive

- The source drive must be a member of a logical drive.

- The destination (target) drive must not be a member of a logical drive nor a spare drive.
- The capacity of the target drive must be larger than the source drive.

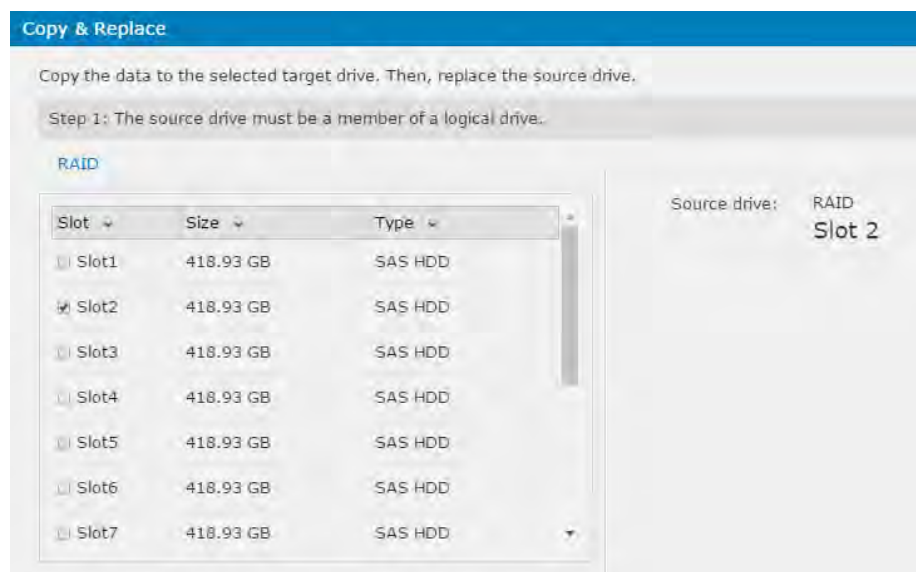
**Go to** **Settings > Storage > Disk**

Select the drive and click the **Copy & Replace** button.

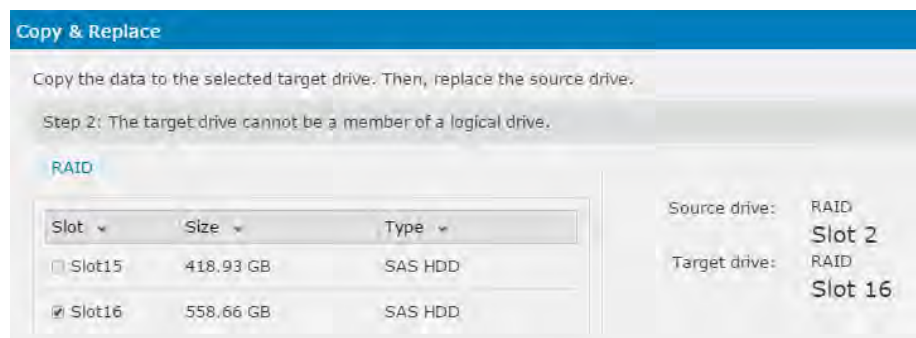


## Steps

1. Select the drive to be the source drive (Slot 2 in this example). The source drive must be a member of a logical drive.



2. Select the drive to be the target drive (Slot 16 in this example). The target drive must not be a member of a logical drive nor a spare drive.



3. Click **OK**. The content of the source drive will be copied to the target drive, and the target drive will take the place of the source drive. The copying process cannot be seen in the spare target drive status column.

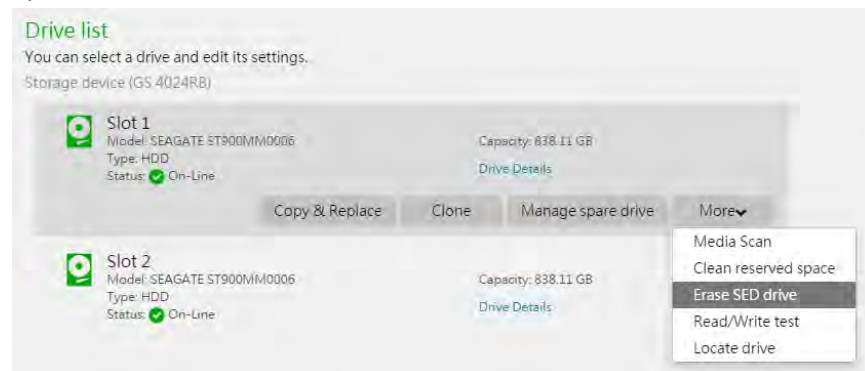
To abort, click the **Abort** button

## Erasing SED drive

### Steps

### Settings > Storage > Drive

1. Select the drive, click the **More** button and select the **Erase SED drive** option.



2. When selecting the SED drives, the operation will delete all data on the drive, including the local authentication key. The operation is only available when the selected SED drives do not belong to any logical drives.

## SSD Cache

The SSD cache pool is a pool composed of SSD drives, designed to accelerate application workloads by automatically copying the most frequently accessed data (a.k.a. hot data) to the lower latency SSD drives. When the data is requested by a host computer next time, the subsystem will retrieve it from the SSD cache pool (instead of the other drives), thus boosting data reading performance for the host. The SSD cache pool is especially useful for applications with intensive random reading requests, such as OLTP and databases.

Since the SSD cache pool works similar to a cache, data stored in it will be removed after the controller is reset or shut down.

---

•

### Notes and limitations

The SSD cache pool can only accelerate the reading process for host computers. Writing data from host computers to the SSD cache pool is currently not supported.

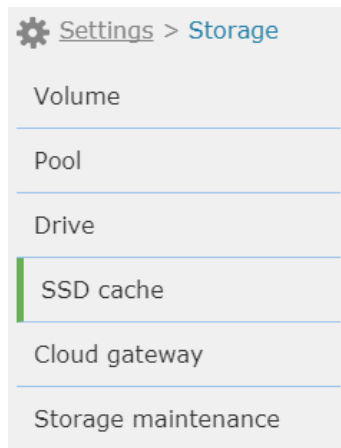
DRAM Size	Max SSD cache pool capacity
4GB	200GB
8GB	400GB
16GB	600GB
32GB	1000GB
64GB	1600GB
128GB	3200GB
256GB	3200GB
512GB	3200GB
1024GB	3200GB

- "Sequential read" is not supported by the SSD cache pool, meaning using the SSD cache pool will not enhance the reading performance for sequential data, such as multimedia files. However, the SSD cache pool can enhance the random reading performance for databases and OLTP.
- It is required to reset the controller only after configuring the SSD cache pool for the first time but not for future configuration.
- It is not allowed to designate drives located in expansion enclosures as member drives of the SSD cache pool.
- One controller can manage up to 4 member drives in the SSD cache pool.
- RAID configuration is not available for member drives in the SSD cache pool.
- Data stored in the SSD cache pool will be removed every time the subsystem reboots.
- The available SSD cache pool capacity will depend on system memory size:

## Enabling/Disabling SSD Cache Function

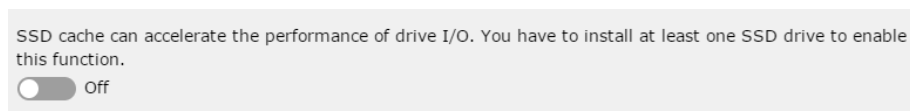
Go to

Settings > Storage > SSD Cache



**Enable/Disable the SSD Cache Function**

Click the switch bar to enable/disable the SSD cache function.



**Add SSDs into SSD Cache Pool**

You will be asked to add new SSD disks into the SSD cache pool if no SSDs have been added into SSD cache pool before.



You can see the list of installed SSDs and SSD Cache Pool Information. To add more SSDs, click the **Add disk** button.



### SSD cache pool information

Size: 372.12 GB

Member count (added/maximum): 2/8

Note: The available SSD cache size depends on the system memory size. Please refer to the user manual for details.



Add disk

Storage device (GS 3024RUB)



Slot 7

Model: HGST HUSMM1620ASS200

Serial No.: 0PY3UD3A

Life Remaining: 100%

Status: ✔ On-Line

Capacity: 186.06 GB

SED Drive: No

[Drive Details](#)

Remove



Slot 8

Model: HGST HUSMM1620ASS200

Serial No.: 0PY3U57A

Life Remaining: 100%

Status: ✔ On-Line

Capacity: 186.06 GB

SED Drive: No

[Drive Details](#)

### Remove SSDs from SSD Cache Pool

Select the SSDs and click the **Remove disk** button to remove them from the SSD cache pool.



Slot 7

Model: HGST HUSMM1620ASS200

Serial No.: 0PY3UD3A

Life Remaining: 100%

Status: ✔ On-Line

Capacity: 186.06 GB

SED Drive: No

[Drive Details](#)

Remove

## Storage Maintenance

In this page, the system lists the invalid LUN and isolated logical drive when there are errors in the volumes (LUNs) or logical drives.

---

<b>Go to</b>	<b>Settings &gt; Storage &gt; Storage maintenance</b>
--------------	---

---

<b>Invalid LUN</b>	<p>When users remove the drives which belong to a mapped LUN from the storage system, PAC Storage PS/PSV will list the “invalid” LUN in the page to inform you that the LUN cannot retrieve its data from the current disks.</p>
--------------------	--

To remove the LUN from the list, you can delete the volume from the list, or you can re-insert the disks to the storage systems, the LUN status will be returned to normal and you can find it in the volume list.

---

<b>Isolated Logical Drive</b>	<p>The page lists the logical drives which are not yet assigned to a storage controller. The error may occur when the system fails to delete the storage pool properly.</p>
-------------------------------	---

# Scheduling & Backup

Scheduling & Backup is a function to make your data always available. The Scheduling & Backup setting menu contains the following sub-Settings.

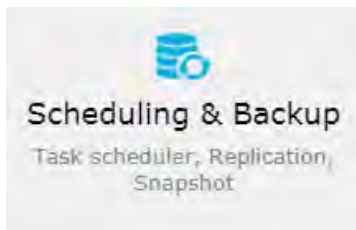
1. Task scheduler
2. Replication
3. Snapshot

**Go to**

**Settings > Scheduling & Backup**

**Backup & Restore  
Menu**

The Scheduling & Backup menu for the selected device will appear. Users can switch to the sub-setting pages or click  [Settings](#) to go back to the previous setting page.



## Task Scheduler

This chapter describes how to create a scheduled task (snapshot, volume mirror) and backup or restore schedule Settings.

**Go to**                      **Settings > Scheduling & Backup > Task list > Task list**

---

**View**                      The list of scheduled tasks will appear in the list.

**Schedule list**

You can schedule a task for folder replication, media scan, snapshot, volume replication or tier migration.

Create schedule

All schedules

<b>New_Schedule</b> Type: Volume mirror Last result: --	Last runtime: -- Next runtime: 06/13/2018 13:25
---	--

Edit
Delete
View details

## Creating Schedules: General Rules

Go to

Settings > Scheduling & Backup > Task list

---

Operations

Click **Create Schedule**.

Select a type of task.

**Create schedule**

Select the type of scheduled task you want to add.

- ☒ Create a folder rsync schedule
- ☐ Create a media scan schedule
- ☐ Create a snapshot schedule
- ☐ Create a volume replication schedule
- ☐ Create a tiered migration schedule

## Creating a Folder Rsync Schedule

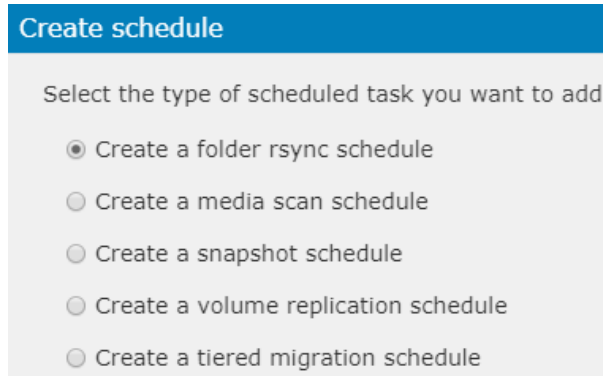
Go to

Settings > Scheduling & Backup > Task list

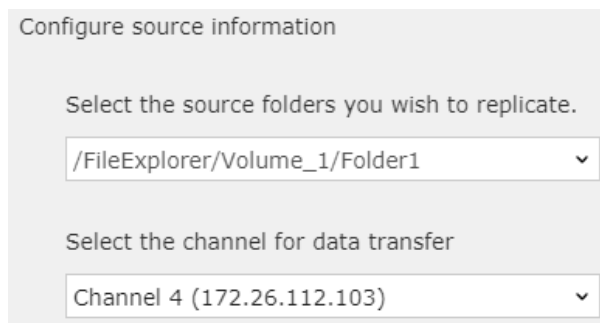
Editing/Viewing  
a Schedule

1. Click **Create Schedule**.

Select the task option create a folder rsync schedule. Press **Next** to proceed.



2. Specify the **source folder** you wish to replicate and the host **channel for data transfer**. Click **Next** to proceed. As you select the source folder, the channel drop-down list will show the available file channel(s) of the controller(s), depending on where the source folder resides on and the source folder you chose.



Note: If you select the data channel in the Auto mode, the system will automatically select the channel to perform the file replication.

3. On the target information configuration page, fill in the target system information. In the target type, you can choose either an PAC Storage PS/PSV system or a 3<sup>rd</sup> party system (Rsync compatible server). Note that once you chose the **PAC Storage PS/PSV** type, the security blank will automatically turn into **Encryption**.
4. Enter the host channel IP address of the target model in the **Rsync target IP address**. The default port is set to 22.

5. For the **Target Username** and **Password**, please enter the user information that can access the target folder with complete permission (read+write). In the **Target directory name** field, please enter a valid directory of the target folder, which you may find in Shared Folders section.

Configure target information

Rsync target type  
▼

Security level  
Encryption (security shell) ▼

\* Rsync target IP address      Port  
172.24.110.69      22

\* Target user name  
SR

\* Target password  
••••••••

\* Target directory name  
/Pool-NAS/HQ\_Data/HQ\_Sync

6. You can also decide whether to duplicate the folder access control list (ACL) of the files by selecting the checkbox **“Duplicate the source folder ACL Settings to target”** at the bottom of the page. For detailed information of these features, please refer to *PAC Storage PS/PSV File Replication Feature Guide Application Note* on our website.

☐ Compress file data

☐ Delete other files on remote destination

☐ Handle sparse files efficiently

☒ Duplicate ACL settings of the source folder to target

7. Click **Next** to display the detailed information for the folder rsync schedule. Click **OK** to complete the Settings.

Configure schedule parameters.

Controller time

2018-06-12 06:24

\* Specify the name of this schedule

New\_Schedule\_20180612\_14293

Select the start date and time

2018-06-12  06 : 19

Select the activate frequency

- ☐ Once
- ☐ Several time in a day
- ☒ Daily
- ☐ Weekly
- ☐ Monthly



## Creating a Disk Scan Schedule

**Go to** Settings > Scheduling & Backup > Task list

**Steps** 1. Click **Create Schedule**.

Select the task option create a media scan schedule. Press **Next** to proceed.

2. Select the drives that need to be scanned.

Slot	Size	Logical drive	Device
1	1.81 TB	Logical_Drive_1 (3B63EDDA)	
2	1.81 TB		RAID

### Destination Type:

Select **Member Drives of a Logical Drive**: Click a drive that belongs to a logical drive in the front panel, and all member drives (including local spare drives) for that logical drive will be selected.

Select **All Logical Drives**: All drives that are members of logical drives will be selected.

**All Global/Enclosure Spare Drives**: Only global/enclosure spare drives will be selected.

**All Assigned Drives**: All drives that are part of a pool or a volume will be selected.

**All Eligible Drives**: All healthy drives, whether a part of a logical drive or not, will be selected.

Click **Next**. The schedule parameters will appear.

Controller time  
2018-06-12 06:11

Select the initialization policy

☒ Start now  
☐ Specify a start date and time

Select the activate frequency

☒ Once  
☐ Daily  
☐ Weekly

Configure the advanced options

☐ Execute on controller initialization  
☐ Execute on all target elements at once

3. Click **Next**. The summary of the scheduled task will appear. Click **OK** to finish the Settings.

**Summary**

Confirm the summary of the created schedule.

<b>Schedule type</b>	Media scan
<b>Destination type</b>	Select member drives of logical drive
<b>Select target</b>	All member drives of: Logical_drive_1 (6B6E1D27)
<b>Schedule settings</b>	
Start date:	--
Start time:	--
Period:	Once
<b>Options</b>	
Execute on controller initialization:	NO
Execute on all target elements at once:	NO
Priority:	Normal

---

**Parameters**    **Start Date / Start Time / Period**    Specifies the start date, start time, and period of this schedule.

---

**Options**    Choose whether to perform scan when the controller is initialized or to scan all drives at once. If you choose the priority as high, scanning will be executed immediately but the system performance may be affected.

### Summary

Confirm the summary of the created schedule.

<b>Schedule Type</b>	Media Scan
<b>Destination Type</b>	Select Member Drives of Logical Drive
<b>Select Target</b>	All member drives of: Logical_Drive_1 (3B63EDDA)
<b>Schedule Settings</b>	
Start Date	20170616
Start Time	15:08
Period	Once
<b>Options</b>	
Execute on Controller ...	NO
Execute on All Target ...	NO
Priority	Normal

Click **OK**. The scheduled task will appear in the list.

## Creating a Snapshot-taking Schedule

Note:

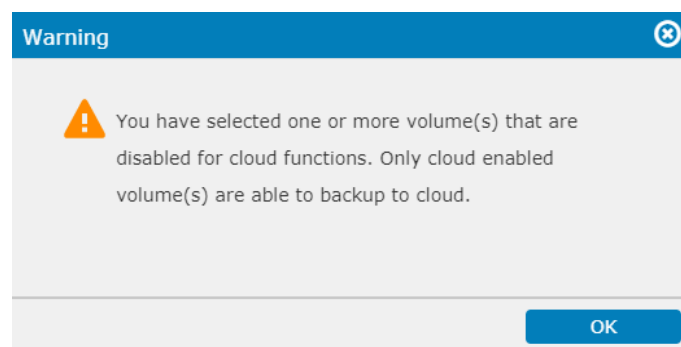
- The interval between two snapshots must be 10 minutes or longer.
- If a snapshot being processed takes longer than the interval, the next snapshot will be abandoned and the currently processed snapshot will be completed.

**Go to**                      **Settings > Scheduling & Backup > Task list**

---

- Steps**
1. Click **Create Schedule**.
  2. Select **Create a snapshot schedule**. Then, click **Next** to proceed.
  3. Choose one or more volumes to snapshot.
  4. Specify an identifying name in the **Tag** field. This name tag is assigned to snapshots created through this scheduled task.
  5. Specify a task description in the **Description** field.
  6. Go to **Cloud-integrated options**. To back up snapshots to the cloud once they are created, select **Backup the selected cloud-integrated volume snapshot to the cloud storage device**. Then, click **Next** to proceed.

Note: You can only backup the snapshot to cloud for the cloud-integrated volume. The cloud icon indicates that the volume has successfully connected to the cloud. If the system detects that a volume has not connected to the cloud, a warning message will pop up.



For more information, please refer to Cloud Backup.

7. Assign an identifying name to the scheduled task.
8. Specify a time for the scheduled task to start running.
9. Choose how often to run the scheduled task: **Once**, **Several times in a day**, **Daily**, **Weekly**, or **Monthly**.

If you choose an option other than **Once**, specify the following Settings:

<b>Termination policy</b>	<p>Choose whether to set an end time for the scheduled task:</p> <p><b>Continuous, the schedule won't be terminated on its own:</b> Select this option if you do not wish to set an end time for the task.</p> <p><b>Specify a termination date and time:</b> Select this option if you want the scheduled task to stop running when it reaches the specified time.</p>
<b>Prune rule</b>	<p>Choose a policy to manage snapshots when the maximum number of snapshots is reached:</p> <p><b>Rotate snapshots when the maximum number of snapshots is reached:</b> Select this option to remove the oldest snapshots until the number of snapshots is within limit. Then, set a limit on the maximum number of snapshots.</p> <p><b>Delete a snapshot when its retention period is reached:</b> Select this option to remove snapshots that have reached its retention period after creation. Then, specify a retention period for snapshots.</p>

10. Click **Next** to proceed.
11. Check the task Settings.
12. Click **OK** to create a scheduled task with the specified Settings.

## Creating a Volume Replication Schedule

**Note** At least one volume mirror pair must exist to create a volume mirror schedule task.

**Go to** Settings > Scheduling & Backup > Task list

**Steps** 1. Click **Create Schedule**.

Select the task option create a volume replication schedule.

Create schedule

Select the type of scheduled task you want to add.

☐ Create a folder rsync schedule
 ☐ Create a media scan schedule
 ☐ Create a snapshot schedule
 ☒ Create a volume replication schedule
 ☐ Create a tiered migration schedule

2. Select the available volume mirror pairs and click **Next**.

Create schedule

Select the volume mirror pair for the scheduled sync task.

Available volume mirror pairs.

Name ▾	Type ▾	Priority ▾	Progress ▾	Status ▾	Description ▾
<input checked="" type="radio"/> Pairtest	Async	Normal	--	Completed	--

3. Enter your schedule parameters.

**Create schedule**

System time  
2018-06-12 14:02

\* Specify the name of this schedule

New\_Schedule\_2018061

Select the start date and time

2018-06-12

📅

14

:

05

Select the activate frequency

☒ Once

☐ Several time in a day

☐ Daily

☐ Weekly

☐ Monthly

4. Click **Next**. The summary of the scheduled task will appear.

**Summary**

---

Confirm the summary of the created schedule.

<b>Schedule type</b>	Volume Mirror
<b>Select target</b>	Pairtest
<b>Schedule settings</b>	
Name:	New_Schedule_20180612_140538
Start date:	20180612
End date:	20180612
Repeat:	Once
Start time:	14:05
End time:	--

5. Click **OK**. The scheduled task will appear in the list.

#### Changing the IP Address

Scheduled asynchronous volume mirror will fail if the remote IP (host server IP for In-band or subsystem IP for out-of-band) changes between (a) and (b).

- (a) When the volume pair is created
- (b) When the scheduled async volume mirror begins

It is best if you can keep the IP address fixed after creating the volume pair. However, if you need to change it, follow these steps.

1. Restart the PAC Storage User Interface Firmware.
2. Re-discover the new IP address or add it manually.
3. Open the PAC Storage User Interface Firmware from the subsystem with the updated IP address.
4. Remove the existing schedule.
5. Sync/async the volume pair to fix the broken link due to the changed IP address.
6. Create a new schedule with the updated IP address.

You can change the remote IP from the firmware (LCD menu or terminal interface) after creating a volume mirror (remote replication) pair. Note that if you do this, the remote pair will be broken. In order to remove a broken pair, you must first unassign the target in the PAC Storage User Interface Firmware.

Changing the remote IP after creating a remote replication pair is not allowed in the PAC Storage User Interface Firmware. If you wish to change the IP, you need to first unassign the target volume of the remote replication pair. After changing the IP, you can safely reassign the pair by syncing/asyncing it manually.

## Creating a Tiered Data Migration Schedule

This feature only works when one or more logical volumes or pools that reside in multiple tiers exist in the subsystem.

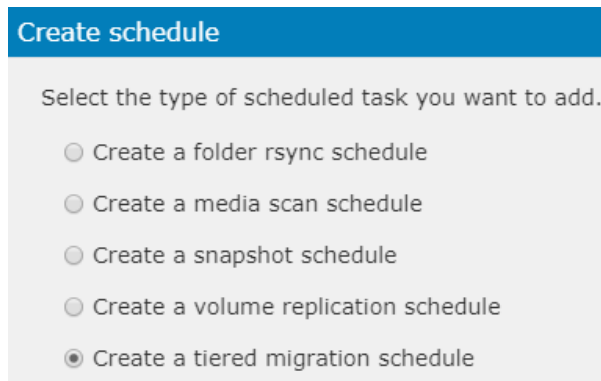
---

**Go to**                      **Settings > Scheduling & Backup > Task list**

---

**Steps**                      1. Click **Create Schedule**.

Select the task option create a tiered migration schedule. Click **Next** to proceed.



2. The list of pools will appear. Select one and click **Next**. Please note that the selected pool must have more than one tier level in the logical volume.



Select pool for the scheduled tier migration task.


Name ▾	ID ▾	Size ▾	Status ▾
<input type="radio"/> Pool-1	37692A6F43D3CE92	2.45 TB	On-line
<input checked="" type="radio"/> Pool-2	5F144B7B45554472	837.85 GB	On-line

2. The schedule parameters will appear. Click **Next**.


Configure schedule parameters.

Target Pool-2 (5F144B7B45554472):  
Volume\_tier (3760173D5351449D)

\* Name

Start Date  

Start Time  :

End Date   ☐ Repeat

Frequency ☒ Once  
☐ Daily  
☐ Weekly  
☐ Monthly

Priority  ▾

3. The summary of the scheduled task will appear. Click **OK**. The scheduled task will appear in the list.

**Summary**

Confirm the summary of the created schedule.

**Schedule Type** Tiered Migration

**Select Target** Pool-2;  
Volume\_tier

**Schedule Settings**

Name New\_Schedule\_20170619\_091454

Start Date 20170619

End Date 20170619

Repeat Once

Start Time 09:14

Priority Normal

## Creating a Volume Defragmentation Schedule

You can set up a scheduled task to regularly defragment a file-level volume.

---

**Go to**                      **Settings > Scheduling & Backup > Task list**

---

- Steps**
1. Click **Create schedule**.
  2. Select **Create a file-level volume defragmentation schedule**. Then, click **Next**.

3. Select a volume to defragment, and click **Next**.
4. Specify a name for the scheduled task.

5. Set an initialization policy to determine when to start the first run: **Start now** or **Specify a start date and time**.
6. Set an activation frequency to determine how often to run the task: **Once**, **Several times in a day**, **Daily**, **Weekly**, or **Monthly**.

7. Set a defragmentation time limit to determine how long the task can run: **No limit** or **Customize**.
8. Set a termination policy to determine when to end the defragmentation task. You can let the task run until it is complete or specify an end time.
9. Click **Next** to check the schedule Settings.
10. Click **OK** to create the schedule.

## Set Email Notification

You can set up email notification to inform you of backup task status.

Note:

- To use this function, you must enable email notification in **Settings > System > Notification > Email**.
- The email notification reports the status of folder rsync, volume replication, and snapshot tasks.

<b>Go to</b>	<b>Settings &gt; Scheduling &amp; Backup &gt; Task list &gt; Advanced</b>
--------------	---

---

<b>Step</b>	Turn on <b>Inform me of task status updates via email</b> .
-------------	---

The system then sends you email notifications when the following task events occur: start, stop, and completion.

# Replication

## Creating a Volume Replication Pair

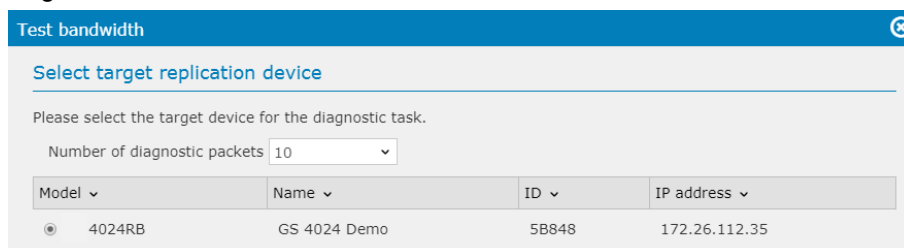
### Go To

**Settings > Scheduling & Backup> Replication > Volume replication**

### Test bandwidth

You can perform a test for channel bandwidth to check if the connection is suitable for your volume replication tasks.

1. Click **Test bandwidth** button.
2. A target replication device list will be shown on the page. The system will only display the systems that have been added in the Central PAC Storage User Interface Firmware. You can specify the amount of diagnostic data packet (64K per each, valid values: 1-10000) and select the target device you wish to diagnose and click **Next**.



Model	Name	ID	IP address
<input checked="" type="radio"/> 4024RB	GS 4024 Demo	5B848	172.26.112.35

3. In the Diagnostic result page, the system shows the Name, ID, IP address of the source and target model on the top of the page. This page lists only block-level channels.

To refresh the results, select **Auto refresh** to automatically refresh the diagnostic test in every 10 seconds, or click **Refresh**. The result displays the link status on the page, including the packets transferred/received, time, and latency. You can also export the test result to your PC by clicking the **Export log** button.

Test bandwidth

Diagnostic result

The following result shows the bandwidth of all channels from the source device to the target device.

Source device Model: 1016R, Name: GS 1016R, ID: 64DBB, IP address: 172.24.110.64

Target device Model: 2024RTB, Name: GS 2024RTB, ID: 8009F, IP address: 172.24.110.130

Number of diagnostic packets: 10 ☐ Auto refresh (10 seconds)

Source	Link	Target	Connected	Received	Time	Rate	Xfer	Lost	Latency
SlotA/CH:0	Down	--	--	--	--	--	--	--	--
SlotB/CH:0	Down	--	--	--	--	--	--	--	--
SlotA/CH:1	Up	SlotA/CH:0	OK	10/10	6.736ms	92.78MB/s	1.16MB	0B	<1ms
		SlotA/CH:1	OK	10/10	6.841ms	91.36MB/s	1.13MB	0B	<1ms
		SlotB/CH:1	OK	10/10	6.729ms	92.88MB/s	1.15MB	0B	<1ms

Step 2 / 2

Export log

Refresh

Cancel

## Data replication channels

You can run data replication over specified network channels to improve network usage efficiency.

1. Click **Choose channels**.
2. On the pop-up, select either option:

**Use any available network channels:** The system dynamically uses any available network channels to run data replication.

**Use selected network channels:** Select specific network channels to run data replication.

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

## Create a volume replication pair

1. Click **Create a replication pair** and select a method for pair creation in the next page. If you have an existing source volume for data replication, continue to Step 2; if not, skip to Step 3.

Create Replication Pair

Select method for pair creation

For replication pair creation, users are allowed to leverage existing volume with data as the source volume, or create a new volume as source without pair initialization process.

☒ Select existing volume for replication pair creation

☐ Create a new volume as the source of replication pair

2. Select a source volume on the system and press **Next**.

Create replication pair

Select source volume

Select the device where the source volume is located, and then assign the volume to the replication source.

Source device: 1016R

Volume name ▾	Pool ▾	Status ▾	Size ▾
<input checked="" type="radio"/> Cloud_Gateway	SR		100 GB
<input type="radio"/> 123	CloudGateway-DEMO		10 GB
<input type="radio"/> Database	SR		500 GB
<input type="radio"/> test_cloud	SR		10 GB

Previous

Next

Cancel

3. Create a new volume to be the source volume. Press **Next** to proceed.

4. Select the target pool and specify a name for the target volume. If you want to create replication pairs between two devices, you will need an advanced license for remote replication actions.

Note: Before you start the remote replication process, we recommend you test the bandwidth between the two devices to verify whether the devices are connected.

Select target pool

Select the device where the target pool is located, and then assign the volume to the replication target.

Target device:

Target volume name:

Pool name ▾	Logical drive amount ▾	Status ▾	Total capacity ▾
<input checked="" type="radio"/> DR-DEMO	1	On-line	418.92 GB
<input type="radio"/> SR	2	On-line	2.04 TB
<input type="radio"/> CloudGateway-DEMO	1	On-line	418.92 GB
<input type="radio"/> Pool-for-DR	1	On-line	558.65 GB

4. Configure the replication pair.

### Replication pair name

Specify a name for the replication pair.

### Volume copy

Select this option if you want to copy the source volume to the target volume.

**Task name:** Specify a name for this volume copy task.

**Task execution time:** Select **Now** to immediately run the volume copy task. To run the task at a specific time, select **By schedule** and specify the execution time.

**Task priority:** Select a priority level to the task.

**Timeout threshold:** Select a timeout limit for the task. When the target volume stays unresponsive over the timeout limit, the system stops the task.

---

**Volume mirror** Select this option if you want to mirror the source volume to the target volume.

**Task priority:** Select a priority level to the task.

**Mirroring type:** Select **Synchronous mirror** if you want to mirror changes in the source volume in real time. This option is not recommended over WAN connections as high I/O latency may cause the process to fail.

If you do not want to perform volume mirroring in real time, select **Asynchronous mirror**, and you can further choose whether to create a snapshot in the target volume to avoid data loss.

**Timeout threshold:** Select a timeout limit for the task. When the target volume stays unresponsive over the timeout limit, the system stops the task.

## 6. Detailed information for the replication pair.



Summary

View the summary of the newly created pair.

Summary:

Name: test

Type: Synchronous volume mirror

Priority: Normal

Schedule: None

Summary of source:

Device: 4024 Demo, 172.26.112.35

Pool name: FileExplorer

Volume name: test

Size: 10 GB

Summary of target:

Device: 4024 Demo, 172.26.112.35

## Parameters

### Synchronous / Asynchronous

When the synchronous mode is enabled, the host will write data to both the source and target at the same time. In the asynchronous mode, the host I/O will be allocated to the source volume only, thus allowing higher bandwidth and optimized performance. New data will be written later into the target in batch, avoiding heavy I/O traffic.

Note: To run replication properly, the system must reserve free space equal to or larger than the size of data to replicate.

### Configure Sync Point

This option can only be enabled in asynchronous mode. The system takes snapshots in the target volume for every asyncing tasks. Users will be able to recover the source volume according to the asyncing time.

### Remote Timeout Threshold

The remote timeout threshold option allows you to avoid breaking a remote replication pair when the network connection between the source and the target becomes unstable or too slow. You may choose how long the controller will wait (timeout). The replication pair will receive better protection if the timeout period is long, but fewer interruptions impact the host performance. The reverse is also true: shorter timeout > less impact > more risk of breaking the pair apart.

#### Enabled:

Depending on the situation, the controller either splits or halts the volume mirror when there is no network activity for the length of the timeout period.

**Disabled:**

Host I/O may be impacted seriously when the network connection becomes unstable.

This option is for remote replication pairs only. If you create a local replication pair, this option will be disabled.

**How Remote  
Timeout  
Threshold Works**

**Stage 1: Syncing has been interrupted**

Background syncing will be stopped for the Wait (timeout) period (default: 30 seconds) and will retry.

**Stage 2: Fails to sync to the remote target**

If the target volume cannot be found, the un-synced data blocks will be marked. The system will continue syncing the next data blocks. An event will be posted.

**Stage 3: Still fails to sync to the remote target**

The system attempts to sync the marked data blocks for several times. If the target volume is still not found, sync will be aborted and uncompleted sync data will be marked. An event will be posted.

If the system reboots before the sync retry count reaches the threshold, sync operation will restart after the reboot and the retry count will be reset.

**Stage 4: Replication pair will be marked as abnormal**

The status of the split replication pair will be updated as abnormal so that users can avoid creating host LUN mapping via such target volume.

**Viewing the  
Progress**

The newly created replication pair will be initialized upon creation or according to the schedule.

The length of each process depends on the capacity of the replication pair. In some cases, the process finishes within a matter of seconds.

When initialization has been completed, the status of the replication pair will change to Completed.

Progress▼	Status▼	Description▼
Completed		

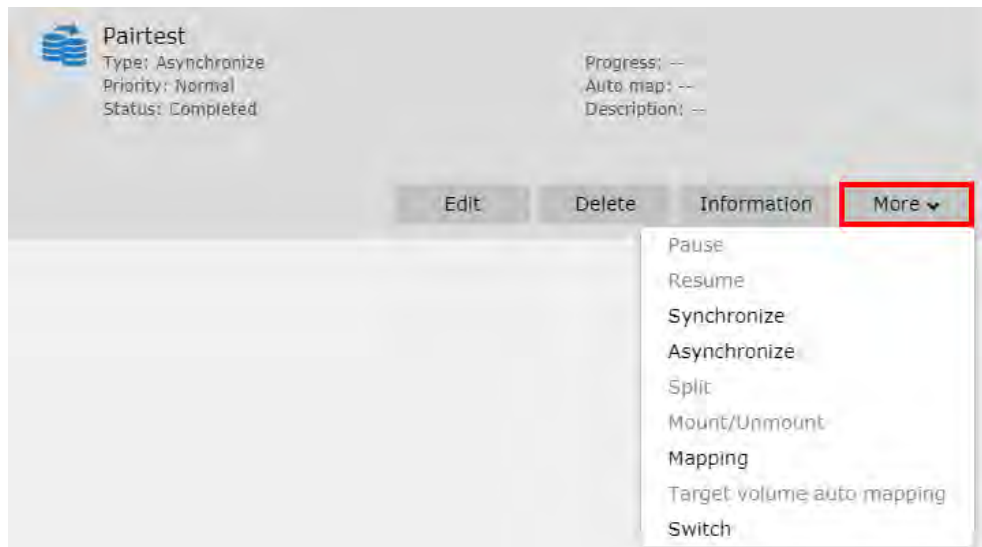
If network connection is lost during the process, the status of the replication pair will change to Non-Complete.

## Replication Pair Actions

**Go To**      **Settings > Scheduling & Backup > Replication**

---

**Replication pair actions**      Select a replication pair and click the **More** button. The available actions are as follows:



### **Pause/Resume:**

These are two options only available during volume copy tasks. Users are able to pause the process and resume it afterward.

### **Synchronize/Asynchronize:**

For volume mirror pairs, users can choose to activate Synchronize or Asynchronize mirror tasks.

### **Split:**

To stop a mirroring synchronize replication pairs, users will have to split the syncing process. After being split, the replication pair can be re-generated a Synchronize or Asynchronize replication task.

### **Mount/Unmount:**

For volumes with file system enabled (file level volumes), users can choose to mount/unmount the source or the target volume of the replication pair. Please note that the target volume cannot be mounted when the replication pair is in the "Mirror" status.

### **Mapping:**

For volumes with file system disabled, users can choose to map/unmap the source or the target volume of the replication pair. Please note that the target volume cannot be mapped when the replication pair is in the "Mirror" status.

### **Target volume auto mapping:**

This function helps achieve continuous data transaction when a replication pair gets

broken. When the host (recovery) agent fails to locate the source volume of a replication pair due to a disaster such as power outages, it will try to map the target volume to the host for failover. Because the target volume is a copy of the source, users can continue their operations using the data on the target side. This function only works on Remote replication pairs with source volumes already being mapped.

**Note:**

**1. Because the failover job is engaged by the agent and needs the mapping operation, it will still cause downtime on the host for seconds or even minutes (depends on the work environment).**

**Switch:**

Swap the roles (source and target) of a replication pair.

**Note:**

1. To switch the roles, you need to split the replication pair and delete the pair schedules. Make sure there is no important data transaction going on at the moment.
2. In a replication pair, the target must have equal or higher capacity than the source. Therefore, to switch the roles properly, it is best that the source and the target pair have the same amount of capacity.



Make sure the following have been done before proceeding with the role switch operation: (1) Delete the pair schedule or stop the schedule service (Ndmp service). (2) Unmap the source.

**Functions**    **Information**    Shows the detail and status of the replication pair.

Replication pair information	
<b>Pair details</b>	
Pair ID:	6714C4464DE8130F
Created at:	06/12/2018 03:08 AM
Completed on:	--
Split on:	06/12/2018 03:08 AM
Sync commenced on:	06/12/2018 03:08 AM
<b>Source details</b>	
Name:	qweqwe
Pool:	testmap
Volume ID:	7788BD027D22878F
Mapped:	No
<b>Target details</b>	
Name:	RR
Pool:	testmap

**Edit**    Click **Edit** to change the configurations of the replication pair. Some of

the set parameters cannot be modified after creation, but you can still see the Settings.

Edit replication pair

Volume pair name:

Description:

Operation priority:

Normal

Remote timeout threshold:

30 Seconds

Incremental recovery:

Supported

Target snapshot:

Enabled

OK

Cancel

## Delete

Click **Delete** to remove a replication pair.

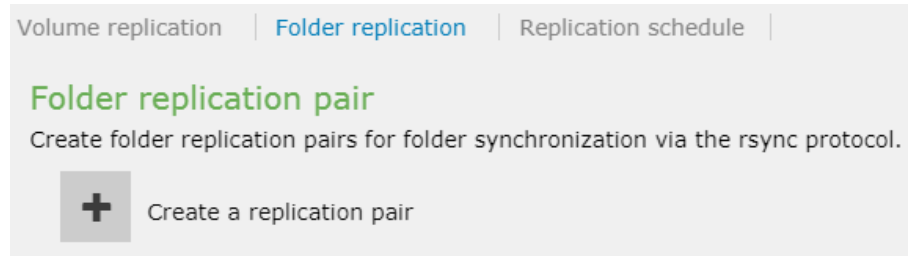
## Creating a Folder Replication Pair

Go To

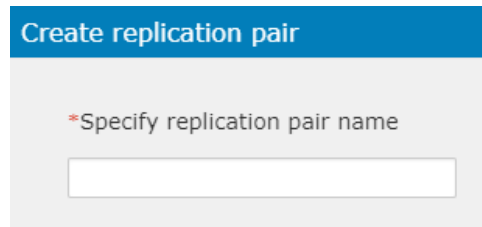
Settings > Scheduling & Backup> Replication > Folder replication

Create a folder replication pair

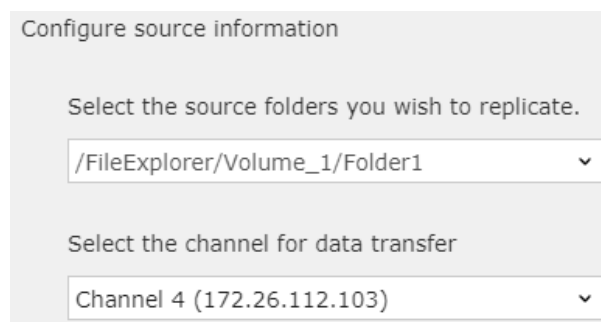
1. Click **Create a replication pair** button.



2. Specify replication pair name and press **Next**.



3. Specify the **source folder** you wish to replicate and the host **channel for data transfer**. Click **Next** to proceed. As you select the source folder, the channel drop-down list will show the available file channel(s) of the controller(s), depending on where the source folder resides on and the source folder you chose.

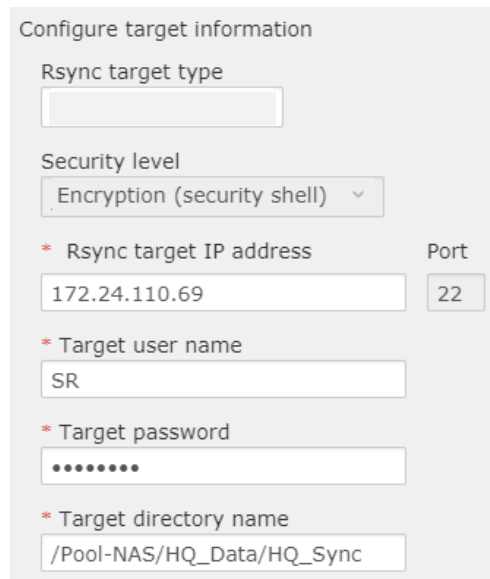


Note: If you select the data channel in the Auto mode, the system will automatically select the channel to perform the file replication.

8. On the target information configuration page, fill in the target system information. In the target type, you can choose either an PAC Storage PS/PSV system or a 3<sup>rd</sup> party system (Rsync compatible server). Note that once you chose the **PAC**

**Storage PS/PSV** type, the security blank will automatically turn into **Encryption**.

9. Enter the host channel IP address of the target model in the **Rsync target IP address**. The default port is set to 22.
10. For the **Target Username** and **Password**, please enter the user information that can access the target folder with complete permission (read+write). In the **Target directory name** field, please enter a valid directory of the target folder, which you may find in Shared Folders section.



Configure target information

Rsync target type

Security level  
 Encryption (security shell) ▾

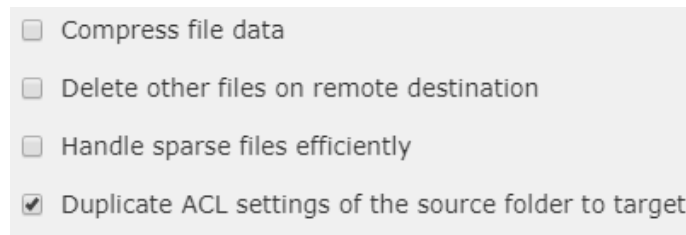
\* Rsync target IP address      Port  
     

\* Target user name

\* Target password

\* Target directory name

11. You can also decide whether to duplicate the folder access control list (ACL) of the files by selecting the checkbox **“Duplicate the source folder ACL Settings to target”** at the bottom of the page. For detailed information of these features, please refer to *PAC Storage PS/PSV File Replication Feature Guide Application Note* on our website.



☐ Compress file data

☐ Delete other files on remote destination

☐ Handle sparse files efficiently

☒ Duplicate ACL settings of the source folder to target

12. Click **Next** to display the detailed information for the folder rsync schedule. Click **OK** to complete the Settings.

## Summary

Confirm the summary of the created schedule.

<b>Schedule type</b>	Folder Rsync
<b>Select source</b>	/FileExplorer/Volume_1/Folder1
<b>Select target</b>	
Type:	
Security:	Encryption (security shell)
IP address:	172.24.110.69
Port:	22
Username:	SR
Directory:	/Pool-NAS/HQ_Data/HQ_Sync
Compress file data:	NO
Delete other files on ...	NO
Handle sparse files e...	NO



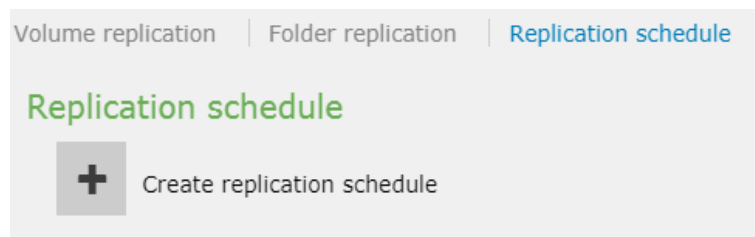
## Creating a Replication Schedule

Go To

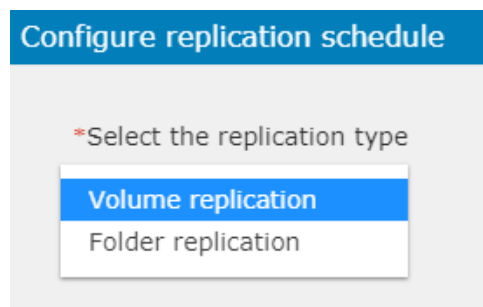
Settings > Scheduling & Backup> Replication > Replication schedule

Create  
replication  
schedule

1. Click **Create replication schedule** button.



2. Select a replication type from the drop-down list and press **Next**.



3. Select a replication pair on the list and press **Next**.


*Select a replication pair		
Name ^	Source v	Target v
<input checked="" type="radio"/> Pairtest	172.26.112.35: testmap/qweqwe	172.26.112.35: testmap/RR

4. Configure the replication schedule by specifying the **schedule name**, **start date and time**, and **activate frequency**. If you set the activate frequency other than Once, specify a **termination policy** of the schedule. Press **Next** to proceed.

System time  
2018-06-12 13:14

\* Specify the name of this schedule

Select the start date and time


  :

Select the activate frequency

☐ Once  
☐ Several time in a day  
☒ Daily  
☐ Weekly  
☐ Monthly

Specify the termination policy

☐ Continuous, the schedule won't be terminated on its own  
☒ Specify a termination date and time

  :

- Click **Next** to display the summary for the replication schedule. Click **OK** to complete the Settings.

### Summary

Confirm the summary of the created schedule.

<b>Schedule type</b>	Volume Mirror
<b>Select target</b>	Pairtest
<b>Schedule settings</b>	
Name:	New_Schedule
Start date:	20180612
End date:	20180615
Repeat:	Daily
Start time:	13:25
End time:	--

- Edit Replication Schedule**
- Click Edit button in the below the schedule.

 <b>New_Schedule</b> Type: Volume mirror Last result: --	Last runtime: -- Next runtime: 06/13/2018 13:25
<div> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">View details</a> </div>	


2. You can edit the schedule parameters on the edit schedule page. Press **Next** to proceed.

### Edit schedule

Configure schedule parameters.

System time  
2018-06-12 13:32

\* Specify the name of this schedule

Select the start date and time  
 
 :

Select the activate frequency  
☒ Once  
☐ Several time in a day  
☐ Daily  
☐ Weekly  
☐ Monthly

3. On the summary page, you can confirm the schedule Settings and click **OK** to complete the Settings.

### Summary

Confirm the summary of the created schedule.

**Schedule type** Volume mirror

**Select target** Pairtest (6714C4464DE8130F)

#### Schedule settings

Name: New\_Schedule

Start date: 20180612

End date: --


Repeat: Daily

Start time: 13:25

End time: --

### Delete Replication Schedule

1. Click **Delete** button below the schedule.



New\_Schedule

Type: Volume mirror

Last result: --


Last runtime: --

Next runtime: 06/13/2018 13:25

Edit
Delete
View details

2. A pop-up window will appear. Click **OK** to delete the schedule.

Information




Are you sure you want to delete schedule?

OK
Cancel

### View Replication Schedule Details

1. Click **View details** button below the schedule.



New\_Schedule

Type: Volume mirror

Last result: --

Last runtime: --

Next runtime: 06/13/2018 13:25

Edit
Delete
View details

2. The summary of the create schedule will pop-up. Click **Cancel** to exit the page.

## Summary

Confirm the summary of the created schedule.

**Schedule type**      Volume mirror

**Select target**      Pairtest (6714C4464DE8130F)

### Schedule settings

Name:      New\_Schedule

Start date:      20180612

End date:      --

Repeat:      Daily

Start time:      13:25

End time:      --

## Snapshot

The following sections explain snapshot related operations.

### Number of Snapshots

#### Number of Snapshots

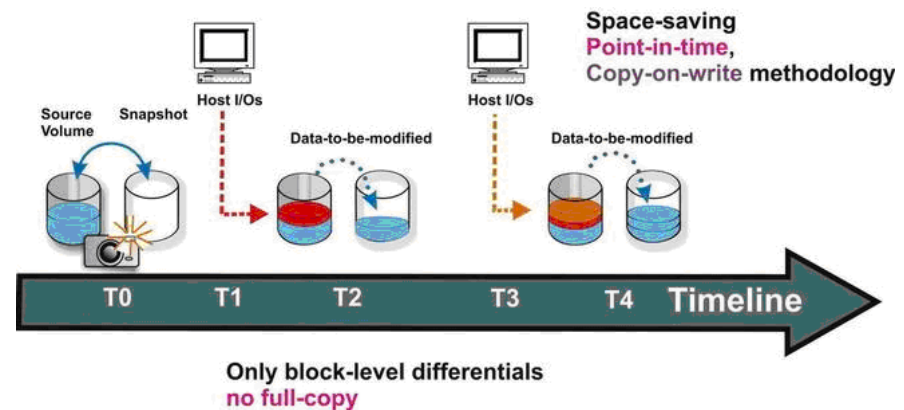
The maximum number of snapshot images per source volume is 256.  
The maximum number of snapshot images per system is 4096.

#### Space Concerns

The storage space required for storing snapshot images is automatically allocated from a pool.

When you create a pool via the PAC Storage User Interface Firmware, you will be notified if more than 70% of the pool's space is used. Make sure you always have enough space.

The space required for taking snapshots is determined by how frequently your data changes.



Use the prune rule option in the snapshot scheduler window to put a cap on the maximum number and lifespan of snapshots.

#### What to Evaluate when Planning

When planning snapshots, evaluate the following:

How many data changes will occur within a time frame?

How many snapshots will you need to recover?

How long can you tolerate loss of data (i.e. how frequently do you need to take snapshots)?

#### Case Study: Calculating the Required Space

Here we calculate the required data space based on these assumptions.

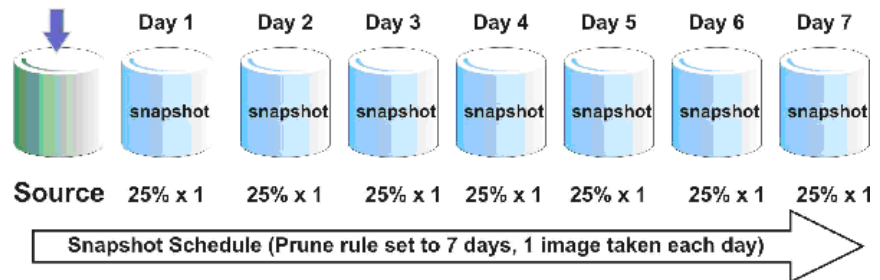
25% of data is expected to change every day.

A snapshot is taken every day.

You need 7 snapshots to preserve data protection.

The lifespan of a snapshot is 7 days.

25% data is changed everyday!



The storage space required from a volume will be:  $(25\% \times 1) + (25\% \times 1) + (25\% \times 1) + (25\% \times 1) + (25\% \times 1) + (25\% \times 1) + (25\% \times 1) = 1.75$  times of the source volume size.

### Pruning vs. Purging Snapshot Images

To use the storage space efficiently, there are two mechanisms, pruning and purging, that allow you to automatically remove older snapshot images.

#### Pruning

Pruning refers to removing older snapshot images when the threshold size is reached or the retention period has expired. Pruning occurs based on the threshold conditions, regardless of the availability of storage space. Pruning can be configured when you create snapshot images.

#### Purging

Purging refers to removing older snapshot images when the used storage space hits the threshold (= available space becomes insufficient). Purging will continue until the used storage space becomes lower than the threshold setting or all snapshot images are deleted or marked as invalid (the original data will always remain intact). Purging can be configured when you create notification thresholds for pools.

Purging takes priority over pruning and is considered as a critical issue for the overall system. When purging occurs, you may take one of the following actions:

- Increase the size of the pool to expand the available storage space.
- Remove unnecessary data from existing LVs or pools or reconfigure them to use storage space more efficiently
- Increase the pruning threshold (least recommended)



If a snapshot image is marked as invalid during purging, the image can no longer be used and needs to be deleted immediately.

### **Creating/Editing/Deleting a Snapshot**



Go to

**Settings > Scheduling & Backup > Snapshot**

[Snapshot list](#) | [Snapshot Schedule](#)

### Snapshot list

You can create a snapshot for an existing volume to backup your important data or roll back the data with a snapshot version.

<input type="checkbox"/> Creation Time	Volume	Pool	Status	Size
<input type="checkbox"/> <a href="#">2018/03/30 15:55:46</a>	HQ_Data Tag:Snapshot_201...	Pool-NAS	✓ Unmounted	19.97 GB

**Take a snapshot**

1. Click **Take snapshot** button, the page for creating a snapshot will pop up. Specify the pool and the volume to take a snapshot.

### Create snapshot

Please select the volume to take a snapshot for it

Select volume

☐ Block (34472A5832BB4951)

☐ SR\_Cloud\_Block (4AD9081C0E499EF5)

☐ vmtest (61E2D04B4DCECDAA)

☐ Pool-NAS (079E668A144A0EB8)

☒ HQ\_Data (56EB1A7464A4E8A9)

☐ Infortrend (17D658615BD0B1C8)

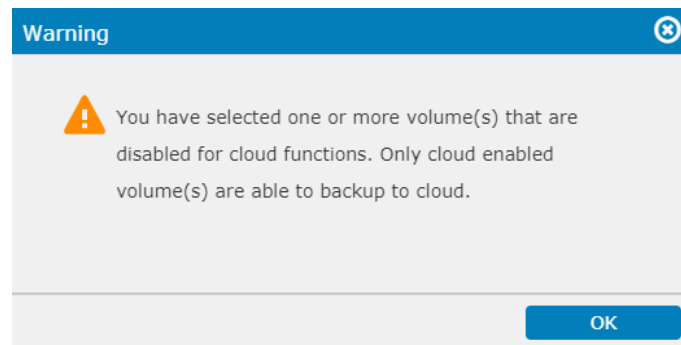
If you want to back up the snapshot images to the cloud, tick the **Backup the selected cloud-integrated volume snapshot to the cloud storage device** checkbox at the bottom of the page.

☒ Backup the selected cloud-integrated volume snapshot to the cloud storage device  
 You can select multiple volumes from different pools to take snapshots. If you enable this function, the selected volume(s) must be a cloud-integrated volume.

☒ Empty local snapshot space after uploading snapshot image to the cloud.

It is also optional that to delete the local snapshot images after uploading the snapshot to the cloud. The feature is enabled by default.

[Note] You can only backup the snapshot to cloud for the cloud-integrated volume. The cloud icon indicates that the volume has successfully connected to the cloud. If the system detects that a volume has not connected to the cloud, a warning message will pop up.



For more information, please refer to [Cloud Backup](#).

2. According to your needs, specify the label and description of the snapshot image for easy management.

Tag

Snapshot\_test

Description

test

3. Press **OK** to complete the Settings.

## Edit Snapshots

You can modify the name and description of the snapshot.

1. Select a snapshot from the list and click the **Edit** button.

**Snapshot list**

You can create a snapshot for an existing volume to backup your important data or roll back the data with a snapshot version.

Take snapshot **Edit** Delete Roll back More ▾ Search

<input type="checkbox"/> Creation Time ▾	Volume ▾	Pool	Status	Size
<input checked="" type="checkbox"/> 2018/06/11 17:26:13	HQ_Data Tag:Snapshot_test	Pool-NAS	✓ Unmounted	0 Byte
<input type="checkbox"/> 2018/03/30 15:55:46	HQ_Data Tag:Snapshot_201...	Pool-NAS	✓ Unmounted	19.97 GB

2. You can edit the **Tag** and **Description** of the snapshot. Press **OK** to save the Settings.

Edit a snapshot

Pool

Pool-NAS

Volume

HQ\_Data

Creation Time

2018-06-11 17:26:13

Tag

Snapshot\_test

Description

test

☐ Backup the selected cloud-integrated volume snapshot to the cloud storage device  
You can select multiple volumes from different pools to take snapshots. If you enable this function, the selected volume(s) must be a cloud-integrated volume.

## Delete Snapshots

1. Select a snapshot image. Click the **Delete** button.

Snapshot list | Snapshot Schedule

### Snapshot list

You can create a snapshot for an existing volume to backup your important data or roll back the data with a snapshot version.

Take snapshot | Edit | **Delete** | Roll back | More

<input type="checkbox"/>	Creation Time	Volume	Pool	Status	Size
<input checked="" type="checkbox"/>	<a href="#">2018/06/11 17:26:13</a>	HQ_Data Tag:Snapshot_test	Pool-NAS	✓ Unmounted	16 MB
<input type="checkbox"/>	<a href="#">2018/03/30 15:55:46</a>	HQ_Data Tag:Snapshot_201...	Pool-NAS	✓ Unmounted	19.97 GB

2. A window will pop up to confirm the action. Click **OK** and the snapshot will be deleted immediately.

Warning

Are you sure you want to delete the snapshot?

OK

Cancel

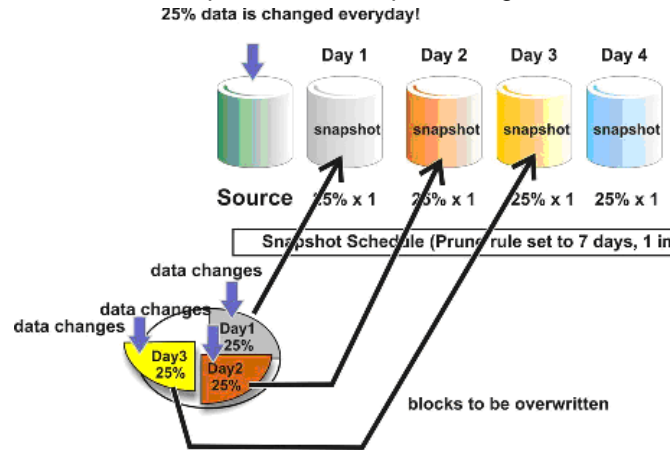
3. If the deletion is successful, a message as shown below will pop up.

The operation has been completed.



## Recovering Source Volume from a Snapshot (Rollback)

If you roll back a source volume to a specific state, all images must remain intact as data is sequentially stored in different snapshot images. The below example shows a source volume with 3 daily snapshots. If you want to roll back to day 1, all 3 images must be intact, ready to be referred to in order for past data to be pieced together.



Go to

Settings > Scheduling & Backup > Snapshot

### Rolling Back a Snapshot

If the source volume has been mapped/mounted, you must unmap/unmount the volume before rolling back a snapshot.

1. Select a snapshot image and click the **Roll back** button, and the source volume will be rolled back immediately.

Snapshot list | Snapshot Schedule

**Snapshot list**

You can create a snapshot for an existing volume to backup your important data or roll back the data with a snapshot version.

Take snapshot Edit Delete **Roll back** More Search

Creation Time	Volume	Pool	Status	Size
<input checked="" type="checkbox"/> 2018/06/11 17:26:13	HQ_Data Tag:Snapshot_test	Pool-NAS	Unmounted	16 MB
<input type="checkbox"/> 2018/03/30 15:55:46	HQ_Data Tag:Snapshot_201...	Pool-NAS	Unmounted	19.97 GB

2. If the rollback is successful, the operation-completed message will pop up.

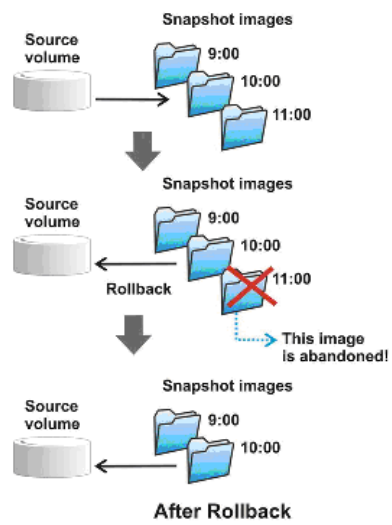
The process can take up to several minutes depending on the size of the source volume.

You may re-establish host LUN mappings for the source volume.

### Note on Rollback Timing

If a source volume is rolled back based on a snapshot image, snapshot images taken after that image will be deleted. In the example below, the snapshot image taken at 11:00 will be lost because the original source volume it was referring to

was replaced by the image taken at 10:00.

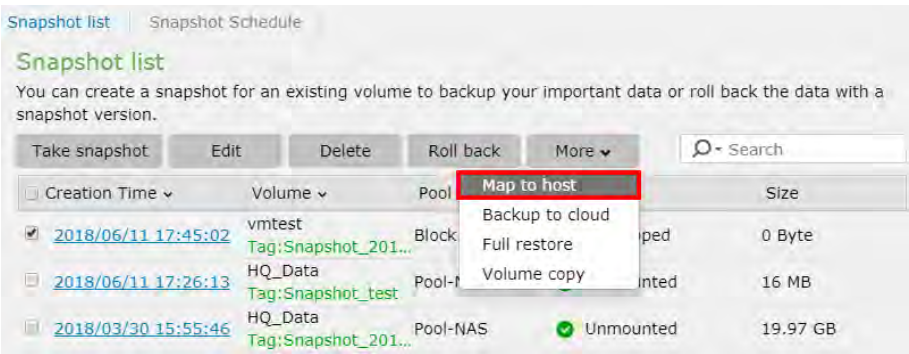


## Mapping/Unmapping a Snapshot Image to a Host

The mapping process is twofold. After mapping a snapshot in the PAC Storage User Interface Firmware, you need to assign a drive letter to it in the host computer environment.

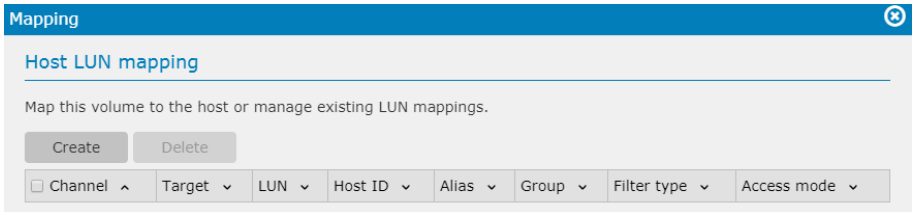
**Go to**                      **Settings > Backup & Restore > Snapshot**

- Steps**
1. Select a snapshot that was taken in a block-level volume and click the **Map to host** button.

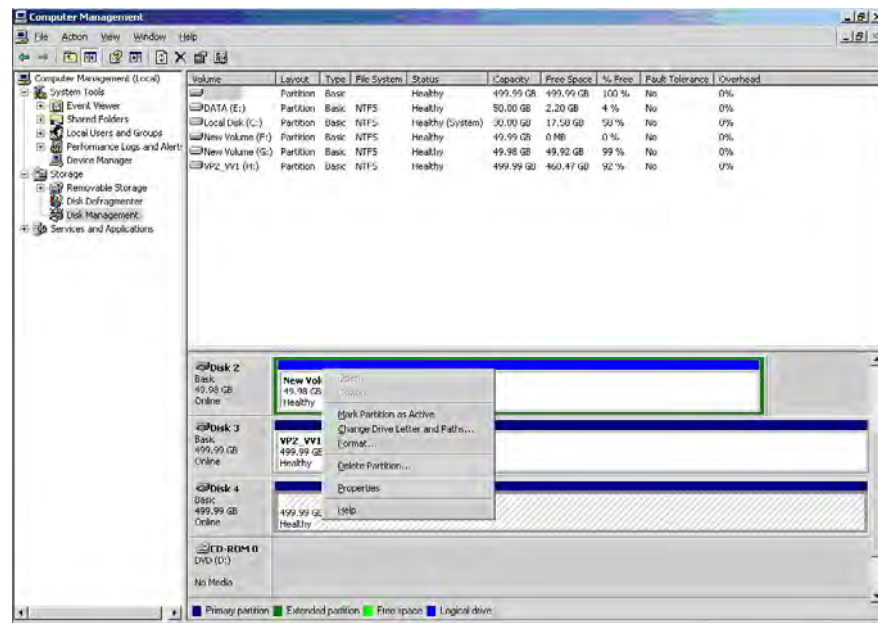


Note that a snapshot taken in a file-level volume will not be able to be mapped to a host. You can select the **Mount** option instead.

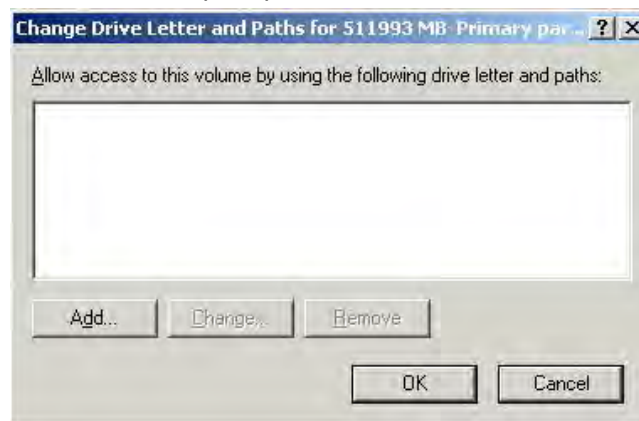
2. The Host LUN Mapping window will appear. The rest of the steps are the same as those for mapping a volume.



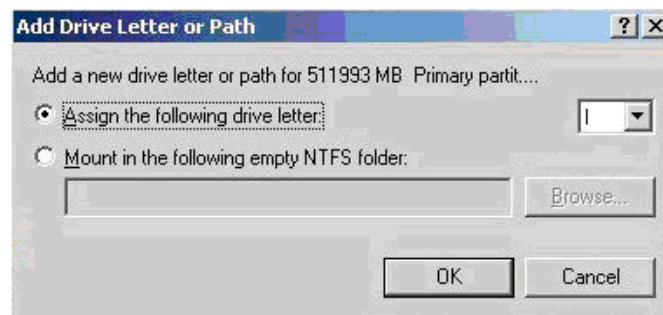
- Assign a Drive Letter to the Snapshot**
- Before accessing data in the snapshot, you need to assign a drive letter to it. Here are the procedures for a Windows Server environment.
1. When an image is mapped, it will appear as a new drive to the computer.



3. Right-click on the disk and select **Change Drive Letters and Path**.
4. Click **Add** in the prompt.



5. Select the drive letter and click **OK**.



6. You should be able to access the data in the snapshot.



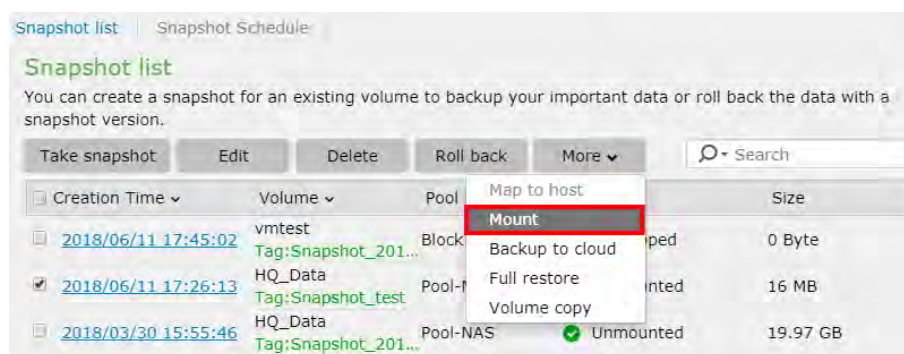
## Mounting/Unmounting a Snapshot Image

The mounting process is twofold. After mounting a snapshot in the PAC Storage User Interface Firmware, you need to assign a drive letter to it in the host computer environment.

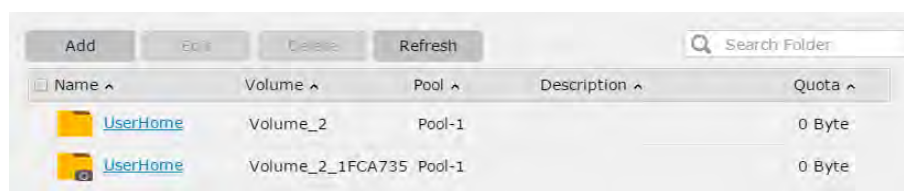
**Go to** **Settings > Scheduling & Backup > Snapshot**

### Mount a snapshot image

1. Select a snapshot that was taken in a file-level volume. Click **More** and select the **Mount** option. This option is not available for snapshots taken in block-level volumes.



2. After the snapshot is mounted, go to the shared folders page (**Settings> Privilege> Shared folders**). The mounted snapshot will be named as the folders in the volume with the snapshot name. Check the snapshot folder. Click **Edit** and select the sharing protocols. For detailed information about editing folders, refer to [Creating/Editing a Folder](#).



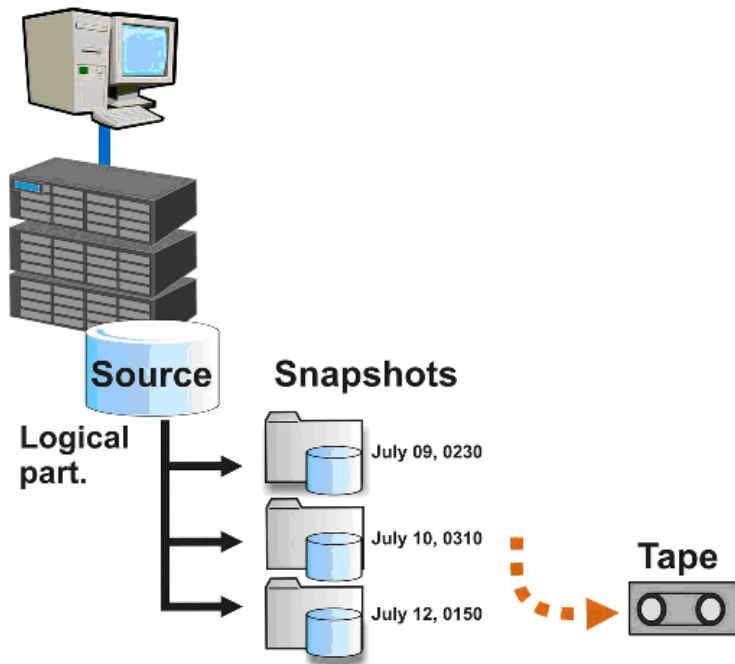
### Unmount a snapshot image

- To unmount a snapshot, select a mounted snapshot. Click **More** and select the **Unmount** option. The snapshot will be unmounted.

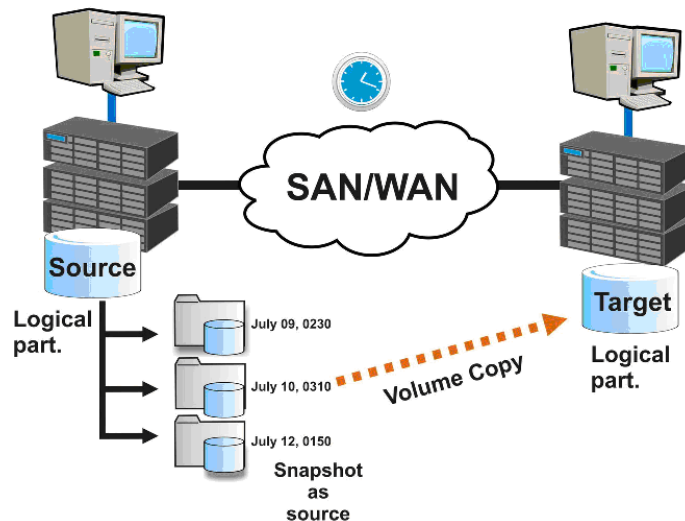
## Backing up Snapshot Images

The following discusses three ways to back up snapshot images using tape storage and/or Volume Copy/Mirror functions described later in this manual.

**Using Tape Backup** Snapshots are saved to tape media during system low time.

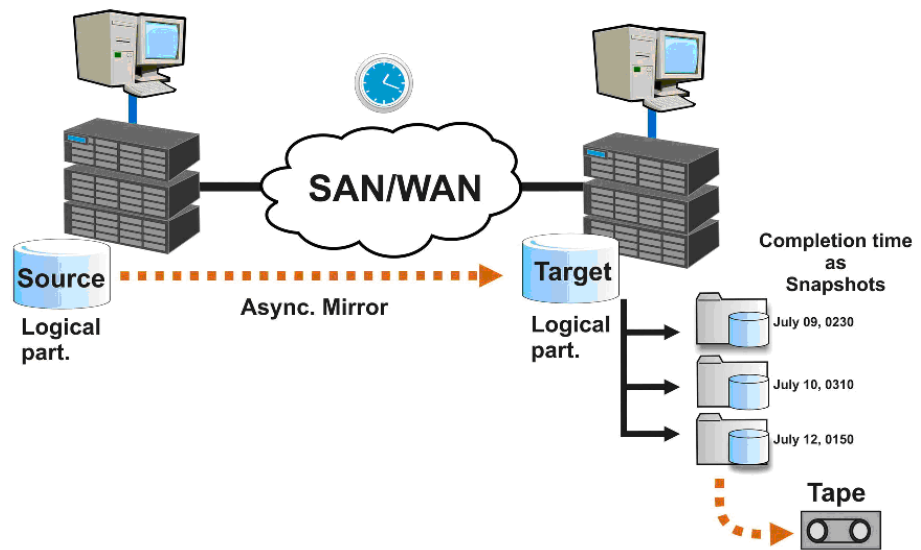


**Using Volume Copy** After snapshot images are taken, they are copied to another location using the Volume Copy function.



**Using Asynchronous Mirror**

Snapshots can be saved (mirrored) to a remote location using the Asynchronous Mirror function. Other backup methods, such as tape media, can be used at the remote site.



### Cloud Backup

During the process of creating a snapshot, users can select whether to back up the snapshot to the cloud. The snapshot will be stored in both the PAC Storage PS/PSV and the cloud bucket. This policy can also be applied to snapshot schedules.

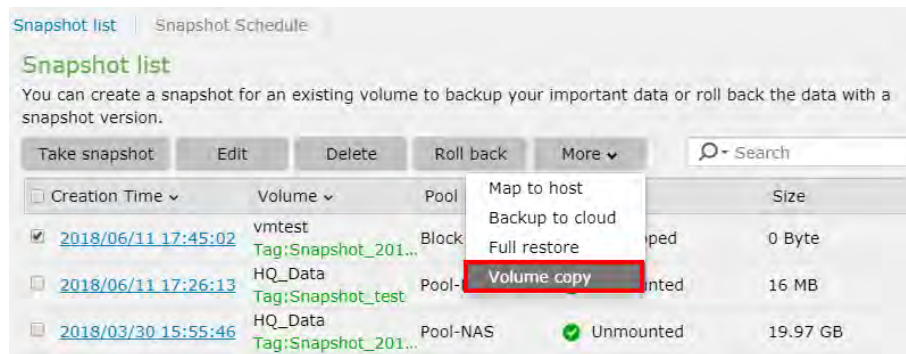
## Creating a Volume Copy from a Snapshot Image

To create a volume copy, you must have at least one snapshot image ready. Snapshot volume copy allows you to do both read and write operations on the target volume copied from the snapshot.

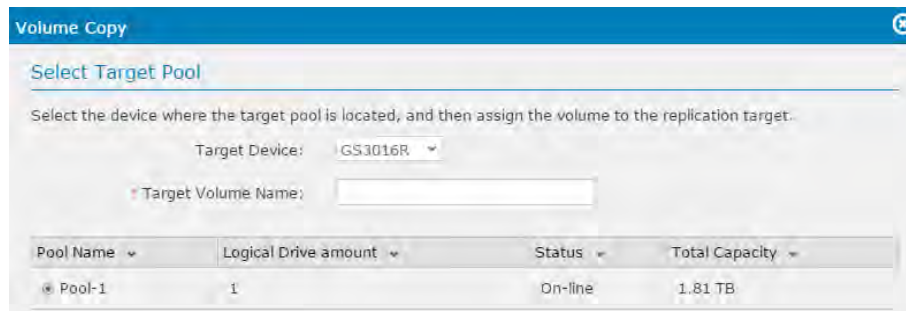
**Go to**                      **Settings > Scheduling & Backup > Snapshot**

### Steps

1. Select a snapshot. Click **More** and choose the **Volume Copy** option.



2. The pop-up window for volume copy will be displayed. Type in a volume name for the new volume and select an existing pool to store the new volume.



3. Choose a type of volume copy and follow the instructions until it is completed.
  - (a) Synchronous mode: the host will write data to both the source and target at the same time, and the data in the target volume cannot be accessed.
  - (b) Asynchronous mode: the host I/O will be allocated to the source volume only, thus allowing higher bandwidth and optimized performance. New data will be written later into the target in batch, avoiding heavy I/O traffic. Data can be accessed when the source volume isn't transferring data to the target volume.
  - (c) Volume copy: the source volume will be copied to the target volume once. Any changes to the source volume later will not be applied to the target volume.

Volume Copy

Configure Replication Pair

Configure the replication parameters including the mode, priority and type.

Volume Mirror

Operation Priority:
Normal

Volume Mirror Type:
Synchronous Mirror
Asynchronous Mirror

☐ Configure the sync point inside the target volume (target snapshot)

Remote Timeout Threshold:
30 Seconds

Volume Copy

☒ Schedule:
2017-06-16
14
:
10

Schedule Name:

Operation Priority:
Normal

Remote Timeout Threshold:
30 Seconds

Previous
Next
Cancel

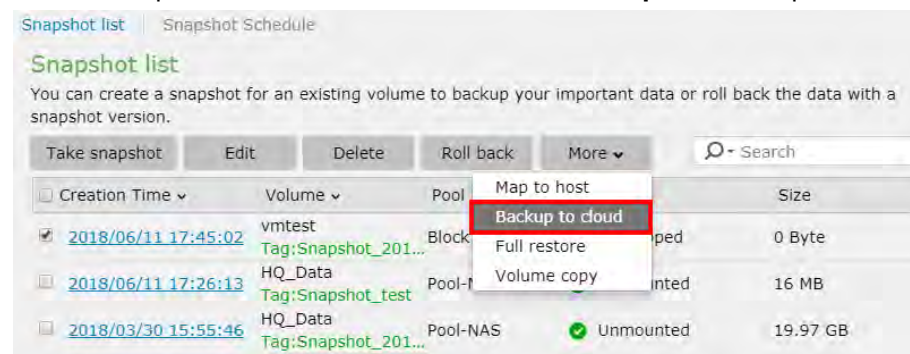
## Backup to cloud

When creating a snapshot or a snapshot schedule, enabling the **Backup to cloud** option will allow the system to upload the snapshot image to the configured cloud bucket. The snapshot image will be stored not only on the local device but also in the cloud bucket as backup.

Please note that cloud features are available only for block-level services.

### Steps

Select a snapshot. Click **More** and choose the **Backup to cloud** option.



If the pool has been mapped with a cloud provider, the snapshot will be created and stored in the local device and then uploaded to the cloud bucket directly. The snapshot icon will have an extra cloud drawing.

If the pool has not been mapped to any cloud provider, the system will guide you to create a mapping relationship between the pool and a cloud provider.

Note: You can select multiple volumes from different pools to take a snapshot.

If you enable "backup to cloud," you can only select multiple volumes from the same pool and a cloud provider has to be configured for the pool.

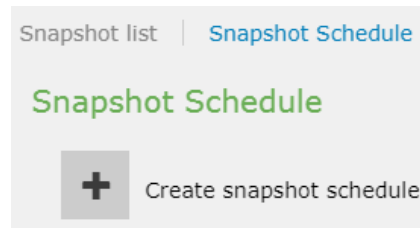
## Snapshot Schedule

You can configure the snapshot schedule for specific or multiple volumes on the system.

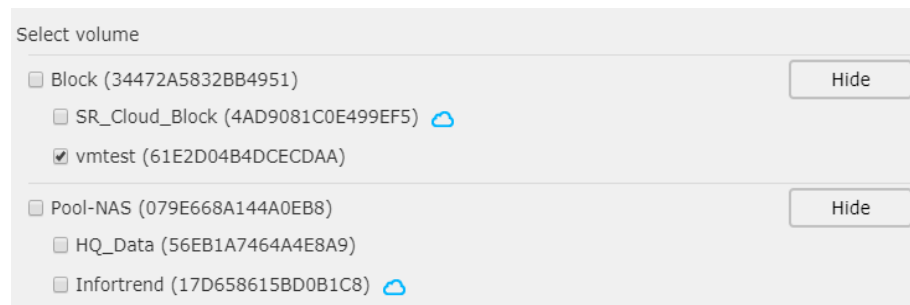
**Go to** Settings > Scheduling & Backup > Snapshot > Snapshot Schedule tab

### Steps

1. Click the **Create snapshot schedule** button.



2. The window of snapshot schedule wizard will pop up. Specify the volume you want to take snapshot from the list. Click **Next** to proceed.



You can also specify the Tag and Description of the snapshot.

Tag

Snapshot\_20180611\_180058

Description

test

If the volume is cloud-integrated, you can backup the snapshot image to the cloud by ticking **Backup the selected cloud-integrated volume snapshot to the cloud storage device** option.

3. On the snapshot schedule Settings page, you can specify the **schedule name**, **start date and time**, and **activate frequency** of the schedule. If the activate frequency is configured other than Once, you may also configure the **termination policy** and **Prune role** of the snapshot schedule.

System time  
2018-06-11 18:35

\* Specify the name of this schedule  
New\_Schedule\_20180611

Select the start date and time  
2018-06-11 18 : 03

Select the activate frequency  
☐ Once  
☒ Several time in a day  
 Backup every 10 minutes  
☐ Daily  
☐ Weekly  
☐ Monthly

Specify the termination policy  
☒ Continuous, the schedule won't be terminated on its own  
☐ Specify a termination date and time

Prune rule  
☒ Purge snapshot images by image count  
 Keep the number of images within: 256  
☐ Purge snapshot images by retention period

4. After all Settings have been completed, you can view the summary page and check the Settings before activating the schedule. You can also go back to the previous page by clicking **Previous** button. Press **OK** to complete the Settings.

**Summary**

Confirm the summary of the created schedule.

<b>Schedule type</b>	Snapshot
<b>Select target</b>	vmtest (61E2D04B4DCECDAA)
<b>Schedule settings</b>	
Name:	New_Schedule_20180611_180358
Start date:	20180611
End date:	--
Repeat:	10 minutes
Start time:	18:03
End time:	23:59
Prune rule:	By Image Count:256
Backup to cloud:	No



## Step 2 Configure Pool

Select an existing pool or create a new one. The disaster recovery process will create a new volume that claims capacity from the pool and then import the snapshot image to the new volume.

**Note:** The volume will be unmapped after the disaster recovery process. You will need to establish host LUN mapping for the volume in order to be able to access it. Refer to Mapping a Volume to LUN.

**Disaster Recovery**

**Configure Pool**  
Configure pool parameters for disaster recovery by creating a new pool or selecting an existed pool.

Pool: ☐ Use existed pool for disaster recovery  
☐ Create a new pool for disaster recovery

Pool Name: Pool-1

Write Policy: Default

Total selected volume: 0

SSD	Size
2	
Slot13	59.37 GB
Slot14	59.37 GB

RAID Level: 2

Previous Next Cancel

## Step 3 Configure Volume

Users can choose to restore all data in the selected bucket or choose to restore specific volumes.

**Configure Volume**  
You can restore all data or select some volumes from cloud for disaster recovery.

☐ Restore all data from cloud directly. **(Selected)**  
☐ Select the specific volume(s) for directly fully restored. Restore all others later using cloud gateway policy.

Total selected: 0

Volume Name	Volume Size	Total/Uncompressed Size
Volume_1	10 GB	0 Byte

Snapshot name	Used Size	Size	Created time
Snapshot_20160930_174240	0 Byte	10 GB	2016/9/30 9:43:14

## Summary

Verify whether the summary page showing the exact configuration that you just set. Click **Next** to carry out the disaster recovery process or click **Previous** to modify the configuration.

Summary

Confirm the summary of disaster recovery.

Cloud provider:

Cloud vendor:	Amazon S3 Storage
Region:	Singapore
Node Name:	s3-ap-southeast-1.amazonaws.com
Encryption:	No
Compression:	No
Use SSL:	No

Pool Informations:

Pool Name:	Pool-DR
Storage Tiering:	Disable
Write Policy:	Default
Assignment:	SlotA
Member drives (SAS):	Tier Index:0 / 10 Drives
	RAID Level: Non RAID
	Stripe Size: 128K

# Application

This section introduces additional software features provided in PAC Storage PS/PSV system.

The system setting menu contains the following sub-Settings.

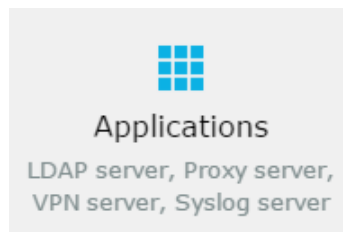
1. Anti-Virus
2. File Explorer
3. LDAP Server
4. Proxy Server
5. Syslog Server
6. VPN Server

## Anti-Virus

With Antivirus, you can set up a schedule to periodically scan the files on the storage system. Files infected with virus will be quarantined to protect your storage environment from virus, spyware and other malware.

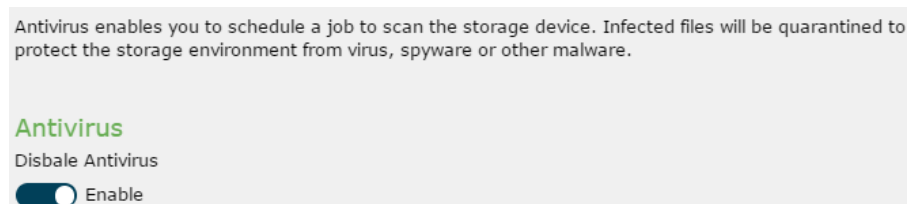
---

**Go to**                      **Settings > Applications > Antivirus**




---

**Enable/disable Antivirus**      Click on the switch bar to enable/disable the antivirus function. When antivirus is disabled, no scheduled scan jobs will be executed.




---

**Update virus database**      Click on the **Update now** button and the system will connect to the ClamAV website to update the ClamAV Virus Database.

For dual controller models, the virus databases will be individually updated for each

---

controller and the update information is displayed respectively.

### Antivirus

☒ On

Quarantined file(s) 0

Status Ready to scan

### Virus pattern update

You can manage virus pattern and its update schedule.

Virus definitions(Controller A):	2017/12/05 (Version 24101)
Virus definitions(Controller B):	2016/06/13 (Version 21723)

Manage Update now

## Set working folder

The antivirus service needs a working directory to save the log files and infected file(s) (quarantine zone). If the working directory is not specified, the service cannot be activated.

In the case of dual controller models, each controller needs its own working folder.

Specify the working folder(s) and click **Apply** to save the Settings.

### Antivirus

☒ On

Quarantined file(s) 0

Status Ready to scan

Location for logs and quarantined files(Controller A)

/SR/Database/AntiVirus

Location for logs and quarantined files(Controller B)

Not configured yet.

Note: You will have to configure the folder for logs and quarantine files to enable the functions "Virus pattern update", "Scan jobs", "Logs" and "Quarantine".

Save

## Virus pattern update

Click **Manage** under virus pattern update to set the frequency of updating virus patterns.

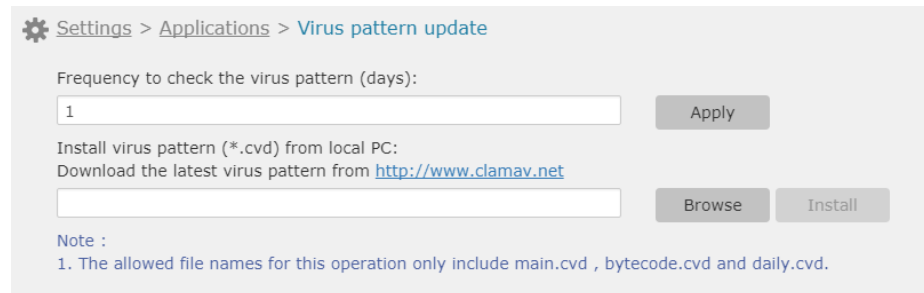
### Virus pattern update

You can manage virus pattern and its update schedule.

Virus definitions(Controller A):	2017/12/05 (Version 24101)
Virus definitions(Controller B):	2016/06/13 (Version 21723)

Manage Update now

Then, you will see the following window.

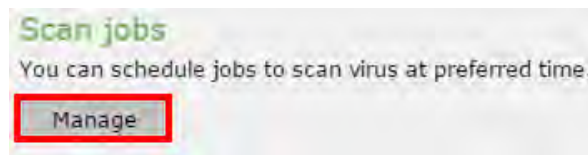


**Frequency to check the virus pattern:** Enter the frequency to check the virus pattern. Valid values are 1-99 days and the default is 1.

**Install virus pattern from local PC:** This dialog box can be used to update the ClamAV Virus Database (.CVD file). If online update cannot work properly, click the button **Browse** to select the .CVD file in the local host and click **Install** to upload the file to the storage device. Virus patterns can be downloaded from <http://www.clamav.net>.


## Scan jobs

Click **Manage** under scan jobs to manage virus scan jobs.



Then, you will see the following window. The status of each scan job will be displayed. For each scan job, you can click **Scan now** to start scanning, **Edit** to modify it, or **Delete** to remove it.



To configure the global Settings of scan jobs, click the icon . You will see the following window.

The screenshot shows a 'Settings' window with three main sections:

- File filter:**
  - Radio buttons: ☐ Scan all files; ☒ Only scan potentially dangerous file types listed below.
  - A text box containing a list of file extensions: \*.386; \*.bat; \*.bin; \*.blf; \*.bl; \*.bmp; \*.bmw; \*.boo; \*.chm; \*.cih; \*.cla; \*.class; \*.cmd; \*.cnm; \*.com; \*.cpl; \*.cxq; \*.cyw; \*.dbd; \*.dev; \*.dlb; \*.dll; \*.dlx; \*.drv; \*.eml; \*.exe; \*.ezt; \*.gif; \*.hlp; \*.hsq; \*.hta; \*.ini; \*.iva; \*.iws; \*.jpeg; \*.jpg; \*.js;
  - Buttons: Apply, Reset.
- Action to take when detecting infected files:**
  - Radio buttons: ☒ Only report virus detection; ☐ Move infected files to quarantine zone.
  - Button: Apply.
- Scan options:**
  - Text input: Maximum file size for scanning (MB): 25.
  - Checkbox: ☐ Scan compressed file content.
  - Button: Apply.

At the bottom right of each section is a blue 'Cancel' button.

**File Filter:** You can choose to scan all files or only scan the specified file types.

**Action to take when detecting infected files:** You can specify what action to take when infected files are found, to only report virus detection or to move infected files to the quarantine zone.

**Scan Options:** You can set the size limit of a file to scan. Files larger than the limit will not be scanned. The default is 25MB and the maximum limit is 4096 MB. You can also specify whether to scan the content of compressed files.

Click **Apply** to save the Settings.

---

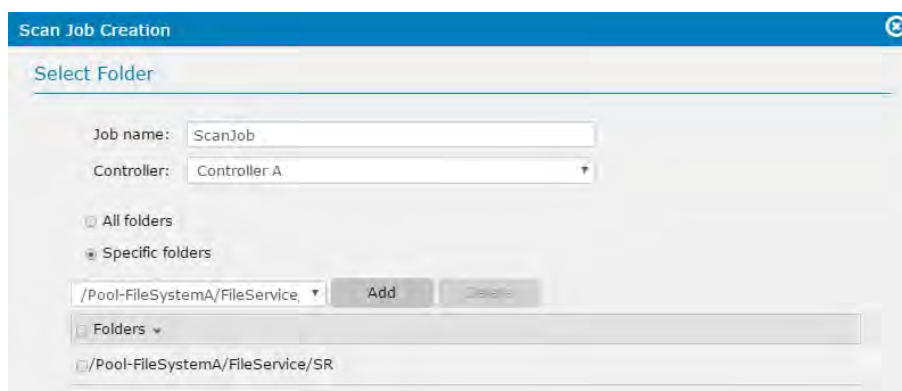
**Add a scan job** To add a scan job, click **Add job** and a wizard will guide you through the steps.

---



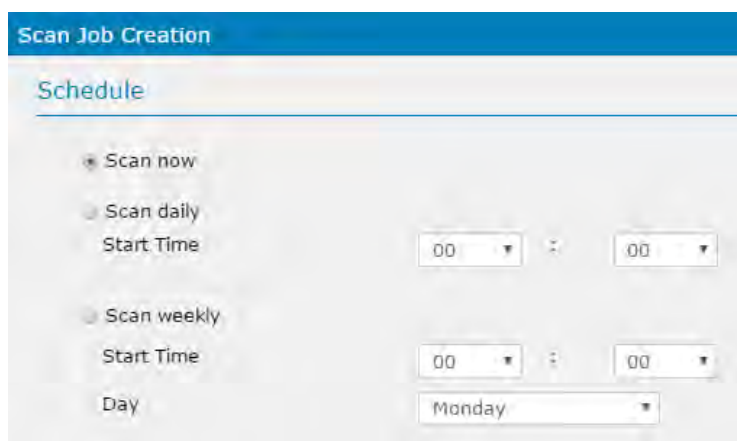
**Step 1:** Set the job name and select the folder(s) to be scanned.

Enter a job name. Select the controller in the case of dual controller models. Then, select the folder(s) and click the button **Add** to include them in the scan folder list. To remove folder(s) from the scan folder list, select them and click **Delete**.



Note: If you choose to scan all folders for a dual controller model, the system will automatically divide the job into two jobs, respectively for controller A and B.

**Step 2:** Configure the scan schedule. The options include scan now, scan daily(specify the time) and scan weekly(specify the time and day).



## Scan logs

Click **Manage** under logs to manage the scan results of scan jobs.

## Logs

You can view the results of each virus scan.

**Manage**

You will see the following window. All the scan results are listed in the table. Each scan result is saved in a log file.

Settings > Applications > Logs

Download logs Delete Settings

Job name	Last scan	Controller	Duration	Infected files
ScanJob	2017-06-19 13:35:42	SlotA	00:00:24	0

**Download logs:** You can choose to download one or more log files by selecting them and click this button. If multiple selections are made, the log files will be saved as a zip file.

**Delete:** You can select one or more scan results and delete them by clicking this button.

**Settings:** The following window will pop up if you click this button. You can specify the number of days to keep the logs. The valid range is 1-99 and the default is 10. Click **Apply** to save the setting.

Settings

Retention time to keep the logs (days)

10

Apply Cancel

## Quarantine

Click **Manage** under quarantine to manage the files in quarantine.

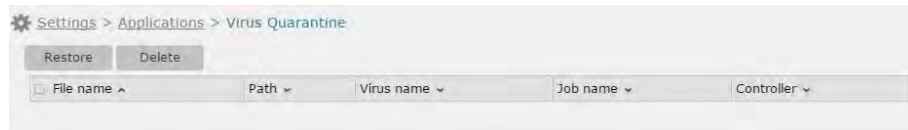
## Quarantine

When detecting infected files, the system will quarantine them. You can permanently delete quarantined files or restore the files to their original locations.

**Manage**

You will see the following window. All infected files will be displayed.





**Restore:** Select one or more files and click this button to restore the file(s) to their original location(s).

**Delete:** Select one or more files and click this button to permanently delete the file(s).

---

## File Explorer

File Explorer is a file management tool that allows authorized users to access local shared folders and attached USB storage devices with a web browser.

Note:

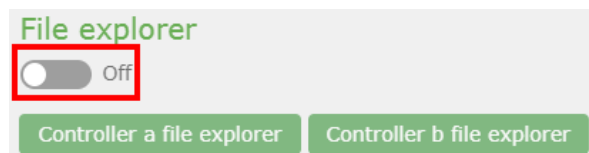
- Compatible USB file systems are EXT3, EXT4, exFAT, FAT32, HFS+, and NTFS.

---

**Go to**      **Settings > Applications > File Explorer**

---

**Enable File Explorer**      Click on the switch bar to enable the File Explorer function. The File Explorer function is disabled by default.

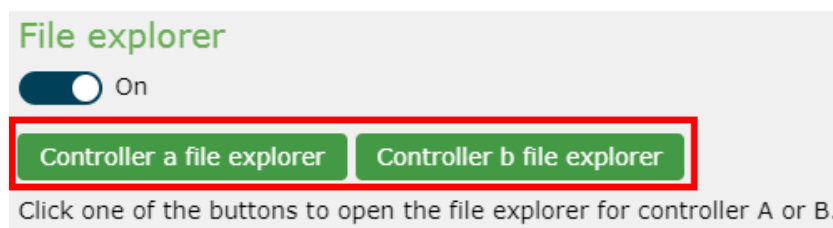



---

**Open File Explorer**      You can open File Explorer through PAC Storage User Interface Firmware or your browser.

- Open File Explorer through PAC Storage User Interface Firmware**

Click the button Controller a file explorer or Controller b file explorer to re-direct PAC Storage User Interface Firmware to connect to the PS/PSV file system via the data port of controller A or B.



Then, login with the username and password that have been registered with the device through PAC Storage User Interface Firmware.

- Open File Explorer through your browser**

Entry point: **http://device\_ip:port/**

Port number: **8989**

Note:

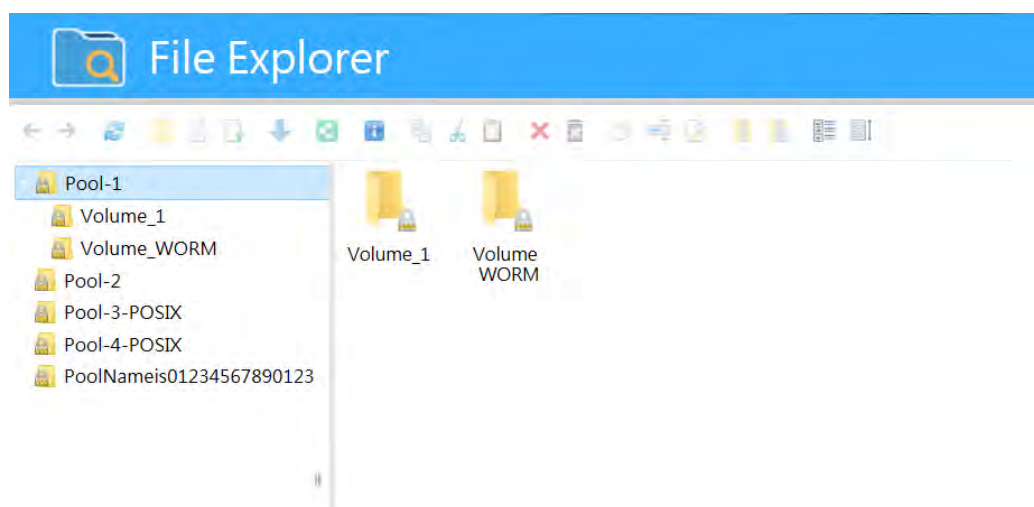
- The port number is not configurable.
  - Please make sure File Explorer is enabled or else you will get an http error 404.
  - The login user has to have the application privilege to access File Explorer.
-

4. The user login authentication will include both NAS local account authentication and domain (AD/LDAP) authentication.
5. The account “admin” is used for system management only.
6. Please make sure there is a channel configured for file-level service.

**File  
Explorer  
View**


After logging in, you will see the folders under *VolumeID/VolumeName*.


Only the administrator can create and manage shared folders in this directory and must follow the rules for creating shared folders. “UserHome” and “ImportedUser” are home directories for local users and domain users and cannot be deleted or renamed.




← Back: return to the previous page.

→ Forward: go to next page.

 Reload: reload the page.

 New folder: create a new folder under the folder highlighted in the left pane.

 New text file: create a new text file under the folder highlighted in the left pane.

 Upload files: upload file(s) to a folder.



Download: download the highlighted file/folder.



Share: share a folder.



Get info: show the information about the selected file. When multiple files are selected, only the total number selected will be displayed.



Copy: copy a highlighted file/folder.



Cut: cut a highlighted file/folder.



Paste: paste a copied/cut file/folder.



Delete: delete the selected file(s)/folder(s).



Empty recycle bin: delete all files from the recycle bin.



Duplicate: duplicate the selected file(s)/folder(s).



Rename: rename the highlighted file.



Edit file: edit the highlighted text file.



Extract files from archive: extract a zip file.



Create archive: create a zip file.



Icon view: view the files/folders in icons.



List view: view the files/folders in a list.

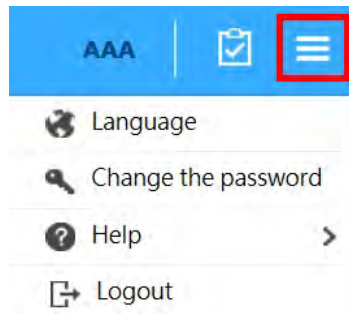


Sort: sort the files/folder.

---

Note: Hot-key operations including Ctrl-C=Copy, Ctrl-X=Cut, Ctrl-V=Paste, Ctrl-A=Select All are supported.


**Menu Icon** Click on the top-right menu icon to find the **Language**, **Change the password**, **Help**, and **Logout** options.

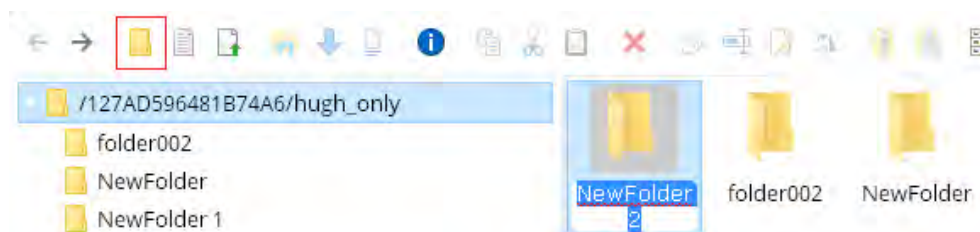


Note:


To display the **Change the password** option, go to PAC Storage User Interface Firmware and click **Settings > Privilege > Users > More > Password policy > Allow local users to change their passwords**. Then, log in to File Explorer again as a local user.

**Create a new folder**

Click the icon  to create a new folder under the folder highlighted in the left pane.



**Work with a text file**

Click the icon  to create a new text file under the folder highlighted in the left pane.

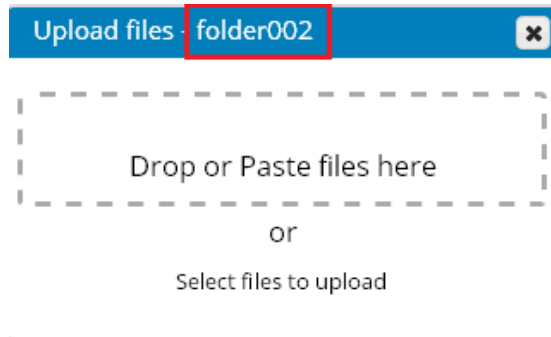


Select a text file and click the icon  to edit it.

**Upload files**

1. Select a folder on the list.
2. Click on the **Upload** icon on the top tool bar to upload files.

3. Drag and drop or select files to upload. You can upload multiple files or file folders at a time.




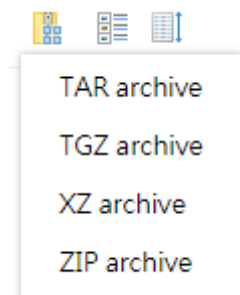
Note:

- Each file to upload cannot exceed 5GB in size.
- If the destination folder is modified during the upload process, the upload is terminated and you need to re-upload files to complete the process.
- You can select a destination folder by clicking on the bottom left folder icon during the upload process.



#### Work with zip files

- Create a zip file


Select the file(s) to compress and click the icon . A popup menu will appear for you to select the zip file type.

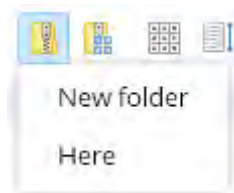


You can also specify the zip file name.

Name	Permissions
 Archive.xz	read and write
 folder002	read and write

- Extract a zip file

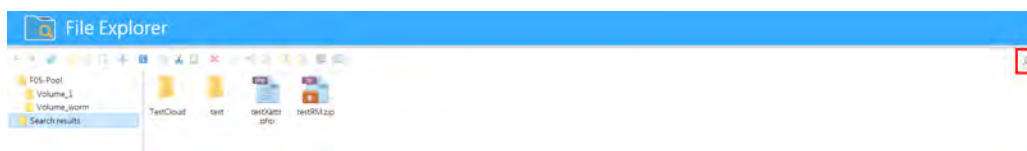
Select one or multiple zip files to extract and click the icon . A popup menu will appear for you to select a folder to place the extracted files.




### Search for files

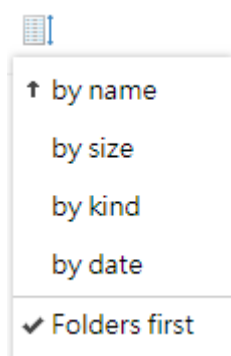
Basic search: Enter keywords in the top-right search bar to show all matching files and folders in the current folder.

Advanced search: To locate files and folders using more search criteria, click on the downward arrow icon on the search bar and provide relevant information.



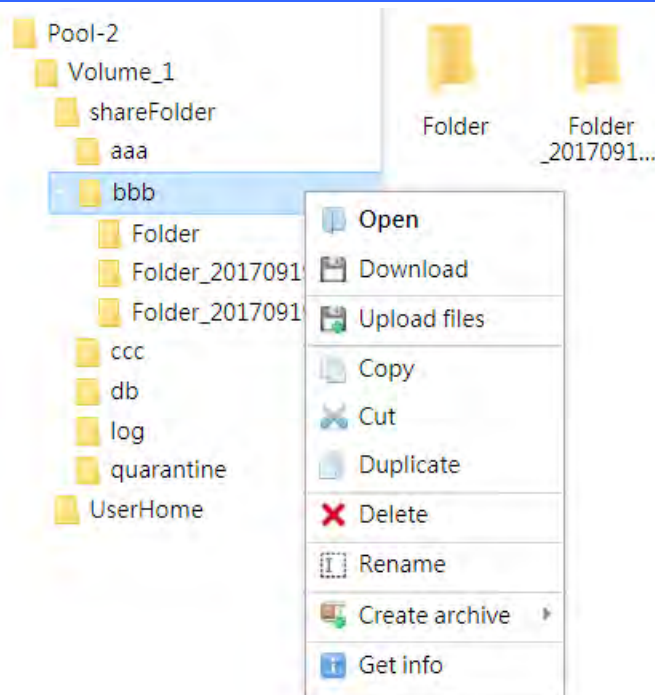
### Sort files/folders

Click the icon  to sort the files/folder. A popup menu will show the available sorting options.



### File System Hierarchy (Tree-view)

Right-click on the tree nodes and a popup menu will display the available operations for the folder/subfolder.




Note: When you right click on a pool or volume, the popup menu does not support the "Download" function since it is just a directory link.

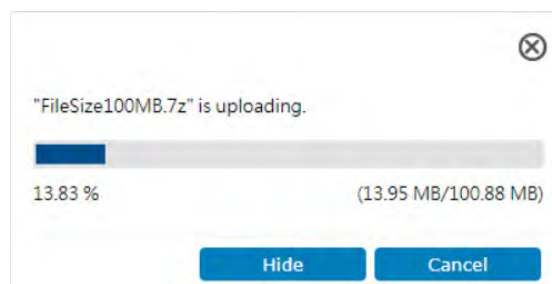
## Progress Bar

For file operations (e.g. copy, move, and upload, etc.), you can check the real-time progress.

To check an operation's progress in the background, click on the upper-right

**Background Job List** icon  above the top toolbar.

To terminate the operation in the background job list, click the  icon and then the red trash can icon.

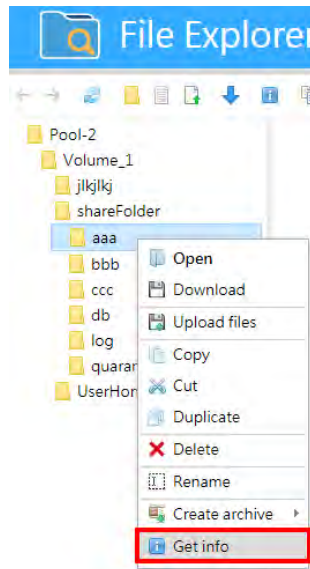




## Shared folder's and Subfolder's Permission

### Properties

Right-click on a shared folder or a subfolder. A pop-up menu will display the available operations for the shared folder/subfolder. Click **Get info** button to proceed.



### Note:

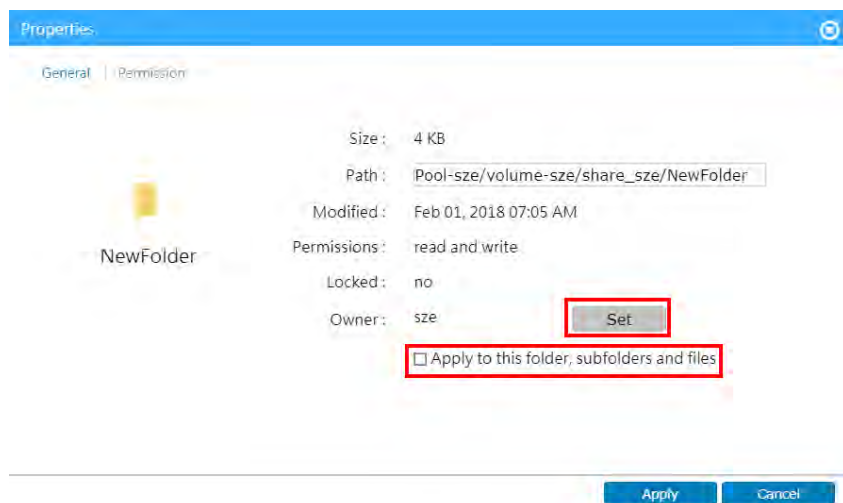
The top-down folder hierarchy is **Pool > Volume > Shared folder (= UserHome) > Subfolders**. The Pool, Volume, and UserHome folder permission Settings are not available.

You can examine basic information of a subfolder and change its ownership.

### General

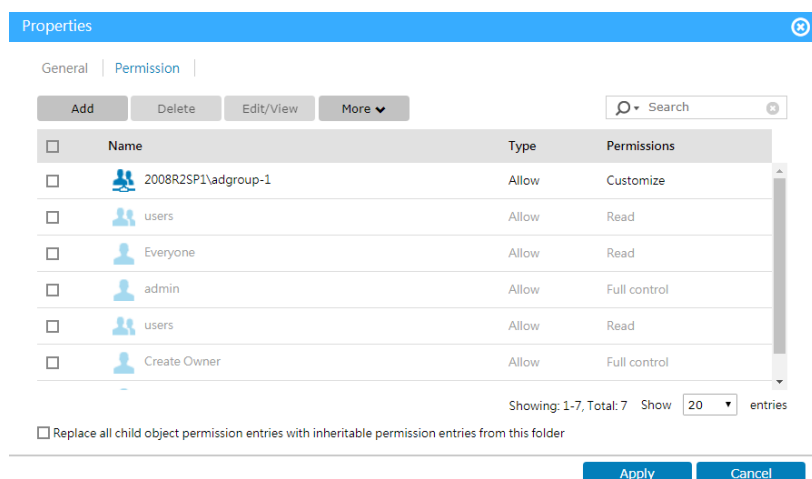
The system administrator can change the subfolder owner. Click **Set**. On the pop-up, select a user from listed local users or domain users. Click **OK** to complete the change.

To allow the owner take ownership of folders and files inside this subfolder, select **Apply to this folder, subfolders and files**.



## Permission

After the general Settings, you can check the permission of the users who have been set the access privilege in the **Permission tab**.



To add extra permission Settings, you can press **Add** button on the top of the page. You can remove a user from the permission list by selecting a user then click delete button and you can Edit/View the permission setting. You can also inherit the folder's user permission from its parent folder. Press **Apply** to complete the setting.

To determine how this subfolder should inherit permission Settings from the parent folder, click **More** to select a type:

**Exclude inherited permission:** Do not inherit the parent folder's access privilege Settings.

**Convert inherited permission into explicit permission on this object:** Inherit the parent folder's access privilege Settings. You can

change the inherited Settings..

**Include inherited permission:** Inherit the parent folder's access privilege Settings. You cannot change the inherited Settings.

To pass this subfolder's permission Settings to its child folders, select **Replace all child object permission entries with inheritable permission entries from this folder.**

Note:

- The system administrator and the folder owner can assign administration, read, and write permissions.
- A user with the **Change permission** permission can assign read and write permissions.

Create customized permission

User / Group name

Browse

Inherit from

Access Type

Applies to

☐ Only apply the permissions to objects and/or containers within this folder

Permissions

Administration

☐ All
 ☐ Change permission
 ☐ Take ownership

Read

☐ All
 ☐ Traverse folders / execute files
 ☐ List folders / read data
 ☐ Read attributes

OK

Close

## Quota

You can set a storage quota limit to a shared folder listed at **Settings > Privilege > Shared folders**. Subfolders do not have an individual quota limit.

General
NFS Permission
Permission
Quota

You can configure the quota settings of this folder.

☐ Not limited  
☒ Limited size

\*

☒ Set an alert threshold for the quota

%

<b>Not limited</b>	This shared folder has unlimited storage space until the volume's storage is full.
<b>Limited size</b>	This shared folder has limited storage space as you specify.
<b>Set an alert threshold for the quota</b>	Set a usage threshold for the folder by percentage. When the usage reaches the specified volume percentage, the system will send a notification to the administrator via email and SNMP.

## Advanced Search

Likewise, you can use the search bar, pagination and **Advanced Search** to look for the specific user(s).

Properties

General
Permission

Add
Delete
Edit/View
More

<input type="checkbox"/>	Name
<input type="checkbox"/>	2008R2SP1\adgroup-1
<input type="checkbox"/>	users
<input type="checkbox"/>	Everyone
<input type="checkbox"/>	admin
<input type="checkbox"/>	users
<input type="checkbox"/>	Create Owner

☐ Replace all child object permission entries with inheritable permission er

☒ Advanced Search

Name

User / Group

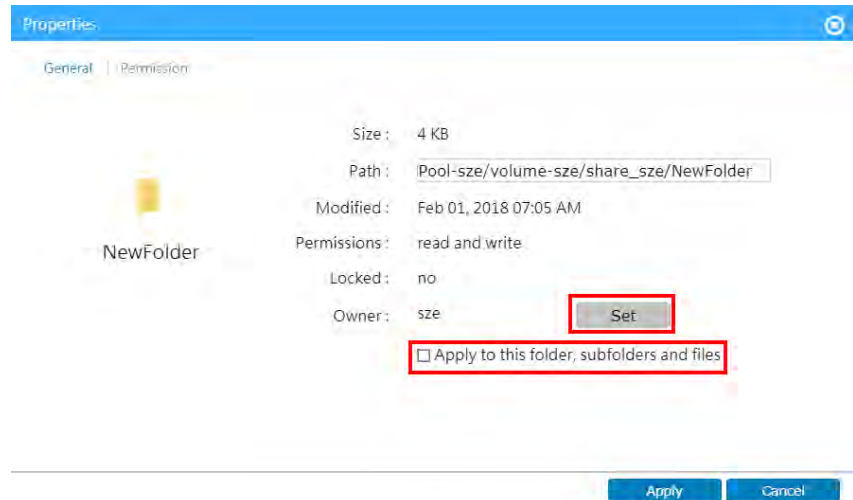
Type

Permission

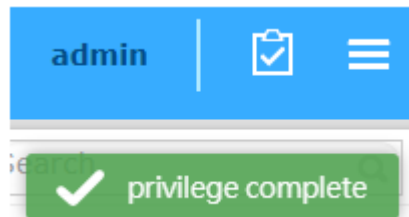
Search
Reset

Apply
Cancel

Back to the folder properties Settings page, you can decide whether to apply the owner permission to its subfolders and files. Press **Apply** to finish the Settings.



The system will display a privilege complete window to inform you that the Settings were successfully configured.



**Note**

1. When a user is assigned permissions in both the **NFS Permission** and **Permission** tabs, the system grants the user with only the lower-level permission.
2. The system determines a user's permissions in the **Permission** tab in the priority order: user permissions > group permissions > "Other".

When the folder-hosting volume is enabled with advanced ACL, the priority order is: user permissions > group permissions > "Everyone". To check the "Everyone" permissions, go to **Settings > Privilege > Shared folders**, choose a shared folder, and click **Edit > Permission > Customize**.

## Share Subfolders

You can share subfolders in a shared folder via common file transferring protocols. To share a folder, right-click a desired one, select **Share**, and complete the following Settings.

### General

#### 1. Specify basic information of the shared subfolder.

Edit share folder

General
NFS Permission
Permission
Quota

Folder name:

Share name:

Description:

Location:

Recycle bin:  

▼
i

The folder can be accessed with the following protocols  
☒ CIFS / SMB

<b>Folder name</b>	The shared subfolder's name is displayed.
<b>Share name</b>	Set an identifying name to this shared subfolder. When other users are accessing it, they identify it with this name.
<b>Description</b>	Specify additional identifying information.
<b>Location</b>	The shared subfolder's location is displayed.
<b>Recycle bin</b>	Enable or disable a recycle bin for this shared folder. This option is only available when <b>CIFS/SMB</b> is selected.

#### 2. Select the protocols for accessing the shared subfolder: **CIFS/SMB**, **FTP**, **SFTP**, **NFS**, **AFP**, **WebDAV**, and **Object**.

When you select the CIFS/SMB protocol, you can apply further options:

<b>Enable access-based enumeration</b>	Let users only see files and folders that they have read access to.
<b>SMB encryption</b>	Encrypt data transfers over SMB connections.
<b>Enable vfs_fruit</b>	Increase compatibility with an SMB client running on the

**module** macOS system.

**NFS Permission** When you select the NFS protocol in the **General** tab, you can click **Add** to create an access privilege entry.

General | **NFS Permission** | Permission | Quota |

You can edit the client permissions of the shared folder accessed via NFS.

**Add** **Edit** **Delete**

<input type="checkbox"/> Client	Privilege	Squash	AnonymousGID	AnonymousUID
<input type="checkbox"/> *	ro	all	65534	65534

Display item: 1-1, Total: 1 Show 20 entries

**IP / Hostname** Specify the IP address or hostname of a privileged user.

**Access rights** Specify the user's access privilege: **Read only** or **Read/Write**.

**Squash** Specify the access privileges for remotely accessing users:

**All Squash** All remote users are identified as anonymous users (i.e. non-administrator users) with limited privileges.

**Root Squash** A remote user with the root credentials is identified as an anonymous user with limited privileges.

Remote users with other login credentials are identified as users listed at **Settings > Privilege > Users**, and have corresponding privileges.

**No Root Squash** A remote user with the root credentials is identified as a root user.

Remote users with other login credentials are identified as users listed at **Settings >**

**Privilege > Users**, and have corresponding privileges.

**Anonymous GID** Assign a group identifier to anonymous users.

**Anonymous UID** Assign a user identifier to anonymous users.

## Permission

Specify access privileges for selected protocols other than NFS.

General | **Permission**

<input type="checkbox"/> Name	Type	Permissions
<input checked="" type="checkbox"/> size	Allow	Customize
<input checked="" type="checkbox"/> admin	Allow	Full control
<input type="checkbox"/> users	Allow	Customize

Display item: 1-3, Total: 3 Show  entries

☐ Replace all child object permission entries with inheritable permission entries from this folder

1. Click **Add** to add a new user or group.

**User/Group name** Assign a name to the new user/group.

**Inherit from** It displays the parent folder that this shared subfolder inherits its privilege Settings from.

**Access Type** Allow or deny access from the user/group.

**Applies to** Select the scope of files/folders that allow access.

**Only apply the permissions to objects and/or containers within this folder** Apply the access privilege Settings only to first-level child files and child folders.

2. Continue to assign the access privileges to the user/group over this shared subfolder.

**Administration** Assign the administration privileges to the user/group:

**All** Assign all administrative privileges.



	<b>Change permission</b>	Change access permissions of this shared subfolder.
	<b>Take ownership</b>	Have the ability to be the owner of this shared subfolder.
<b>Read</b>	Assign the read privileges to the user/group:	
	<b>All</b>	Assign all read privileges.
	<b>Traverse folders / execute files</b>	Enter and exit child folders and execute child files.
	<b>List folders / read data</b>	List child folders and read child files.
	<b>Read attributes</b>	Read attributes of child files and folders.
	<b>Read extended attributes</b>	Read extended attributes of child files and folders.
	<b>Read permissions</b>	Read access permissions of child files and folders.
<b>Write</b>	Assign the write privileges to the user/group:	
	<b>All</b>	Assign all write privileges.
	<b>Create files / write data</b>	Create files in child folders, and write data into child files.
	<b>Create folders / append data</b>	Create folders in child folders, and write data into child files with the original data unchanged.
	<b>Write attributes</b>	Change attributes of child files and folders.
	<b>Write extended attributes</b>	Change extended attributes of child files and folders.
	<b>Delete subfolders and</b>	Delete child folders and files.

---

**files**

---

**Delete**

Delete the shared subfolder.

---

3. Click **More** to decide how this shared subfolder should inherit the access privilege Settings from its parent folder.
- 

**Exclude inherited permissions**

Do not inherit the parent folder's access privilege Settings.

---

**Convert inherited permissions into explicit permissions on this object**

Inherit the parent folder's access privilege Settings. You can change the inherited Settings.

---

**Include inherited permissions**

Inherit the parent folder's access privilege Settings. You cannot change the inherited Settings.

---

4. To pass the access privilege Settings to its child folders, select **Replace all child object permission entries with inheritable permission entries from this folder**.
-

## LDAP Server

LDAP Server provides directory services including centralized access control, authentication and account management.

**Go to** Settings > Applications > LDAP Server

### LDAP Server

1. Turn on the switch on the top of the page to enable the LDAP server.
2. Press the **Change** button to specify the database location, domain name, and the password.
3. Click on **Apply** to save the LDAP Server Settings.

**LDAP server**

Before you enable the LDAP server, please configure the domain name and the password first.

☒ On

Fully qualified domain name : domain.com

Password : \*\*\*\*\*

**Change**

### LDAP server-user management

Click on **Manage** under the Manage users section. You can choose to **edit/delete** an existing user or add a new user.

Add ▾ Edit Delete <input type="text" value="Search User"/>				
<input type="checkbox"/> Name	User Groups	Email	Description	Status
<input checked="" type="checkbox"/> user1	Domain_users, Group1	none	user1	Normal
<input type="checkbox"/> user2	Domain_users, Group1	none	user2	Normal
<input type="checkbox"/> user3	Domain_users, Group1	none	user3	Normal
<input type="checkbox"/> user4	Domain_users, Group1	none	user4	Normal
<input type="checkbox"/> user5	Domain_users, Group1	none	user5	Normal
<input type="checkbox"/> user6	Domain_users, Group1	none	user6	Normal

To add domain users, click **Add** and select a method.

**Add ▾ Edit**

Single user

Multiple users

Import user list

### Case 1: add a single user

Select the **Single user** option, fill in the necessary information and click **Next**.

Add

Please enter the following user information.

Name

adtest

\* Password

\*\*\*\*\*

\* Confirm Password

\*\*\*\*\*

Email

Description

test

☐ User must change the password at the first time logon.

☐ User cannot change the password.

☐ Account expiration

☐ Disable now

Valid until: 2017-06-19

step 1 of 2

Next

Cancel

The system will ask to add the new domain user into a group.

Please select user groups to join.

Add

Edit

Delete

Search User

<input type="checkbox"/> Name	Description
<input checked="" type="checkbox"/> Domain_users	A domain user group
<input type="checkbox"/> Group1	G1

## Case 2: add multiple users

Select the **Multiple users** option, fill in the necessary information and click **Apply**.

Note: To join the users into different user groups, go to the **Manage Groups > Group member** page and select the users to be added into the domain user group.

### Case 3: add multiple users via a “.csv” file

Select the **Import user list** option, select the “.csv” format user list and click **Import**. You can verify the users in the **Content preview** area. If all Settings are correct, click **Apply**.

Note: To join the users into different user groups, go to the **Manage Groups > Group member** page and select the users to be added into the domain user group.

### LDAP server- group management

Click on the **Manage Groups** at the bottom of the LDAP server page. You can choose to edit/delete an existing group or add a new group.



### Add a user group

Click the **Add** button and enter the group name and description.

### Edit group Settings

Select a user group and click **Edit**. In the group editing page, you can modify the group description and the members in the group.

**Backup/Restore** Click **Backup / Restore** at the bottom of the LDAP server page.

## LDAP database

Note: There has to be at least one shared folder to save the database and it cannot be a reserved folder, e.g. UserHome and ImportedUser. The shared folder must be created on a pool assigned to the primary controller (Slot A).

### Backup/restore LDAP database

You can back up the database of LDAP server for recovery.

Backup / restore

Then, the following page will pop up. Switch **Backup Database** to **Enable**. Specify the **backup frequency**, **start time** and **destination folder** which will be used to save the backup data. All level 1 folders (except reserved folders, e.g. UserHome and ImportedUser) will be listed.

Click **Apply** to save and apply the Settings. Click **Export Database Now** to download the database to the local host.

To restore a database from the local host, click **Browse** to select the database in the local host and then click **Restore** to upload the selected database to PAC Storage PS/PSV and activate restoration.

Settings > Applications > Backup/Restore LDAP Database

### Backup Database

☒ On

Repeats  
Daily

Start Time  
00 : 00

Destination folder  
/Pool-FileSystemA/FileService/SR

Apply Export Database Now

### Restore Database

Please press "Browse" to upload a backup file and restore the database.

Browse

## Proxy Server

Proxy Server acts as an intermediary for requests from clients seeking resources from other servers. With proxy servers, organizations can manage the connection and separate irrelevant contents from the outer network environment. The cache function of a proxy server also benefits network performance by providing real-time services to clients in the network and reducing the traffic to resources outside the network.

The proxy server function is presented with the features:

- Cache the web contents which clients have accessed
- Access control functions
- User authentication

Note:

1. Please remember to configure the DNS service before enabling Proxy Sever. Refer to the section Configuring the DNS Service.
2. You can configure extra memory space to be used as cache for Proxy Server. However, you are advised to first confirm there is enough memory capacity for other functions to avoid impact to system performance.

---

### Go to

**Settings > Applications > Proxy Server**

---

### Activate proxy server

Click the switch to **On** to enable proxy server.

Specify the Settings and click Apply.

Proxy server provides caching and access control for HTTP-based services. With caching, visited web content can be retrieved from proxy server to speed up services effectively. With access control, you can deny users from accessing restricted web services, keeping your network safe.

#### Proxy server

☒ On

Available channel interface(s) to access proxy server

Controller A (Channel 2: -- ,Channel 3: 172.24.110.69) ▼

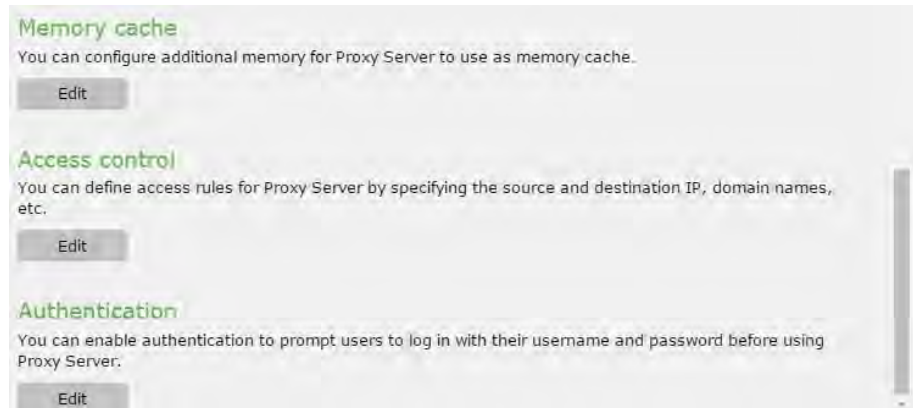
\* Port

3128

You can also configure additional memory for Proxy Server to use as cache, define access rules and enable user authentication.

---





## Parameters

**Available channel interface(s) to access Proxy Server:** Controllers found are listed in this field, as well as the available ports on the controller. The location field also shows available folders corresponding to the value in this field. This is only for dual-controller products. The default value is the primary controller.

**Port:** This is the port number to listen to client requests. The default value is 3128.

**Location:** Available shared folders in the selected controller are listed in this field, including the pool and the volume, sorted alphabetically. The default is the first enumerated folder. If there is no available folder, the service cannot be activated.

**Cache Size (GB):** This specifies the cache size in GB. The default value is 10.

**Max. file size for disk cache (KB):** This is the maximum size of a single cache file. The default value is 1024000.

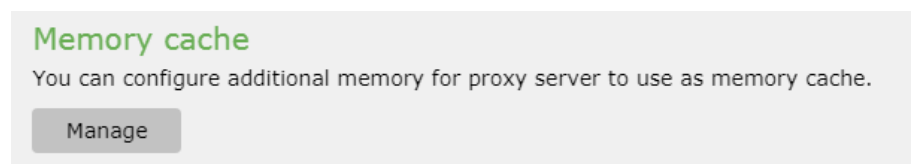
**Min. file size for disk cache (KB):** This is the minimum size of a single cache file. The default value is 0.

**Cache swap floor (%):** The system will stop swapping when the space occupied is lower than the specified percentage of cache size here. The default value is 90.

**Cache swap ceiling (%):** The system will start swapping when the space occupied is higher than the specified percentage of cache size here. The default value is 95.

## Set additional memory cache

Click **Manage** under Memory Cache.



Then, you can enable additional memory cache for proxy server by clicking the

switch to **On**.

**Cache size (MB):** This specifies the memory size to be used as cache. The value should never exceed the available memory size. The default value is 16.

**Maximum file size for memory cache (KB):** Files of sizes larger than this value will not be cached in memory. The default value is 8.

Click **Apply** to save and apply the Settings.

## Access control

Click **Manage** under Access Control to define the access rules for proxy server.

You can add, edit, delete a rule or change a rule to higher priority (the Up tab) or lower priority (the Down tab) by selecting the rule(s) and clicking the respective tab.

Action	Type	IP or hostname
<input checked="" type="checkbox"/> Deny	Source IP	172.24.110.11
<input type="checkbox"/> Allow	Source IP	172.24.110.75
<input type="checkbox"/> Allow	Source IP	172.24.110.36

To add a rule of allowing/denying particular connections, click the **Add** tab and the following window will appear.

**Action:** To allow or to deny the connections

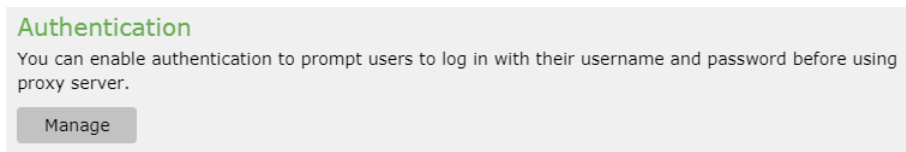
**Type:** Specify the field to compare the connections with. The value can be one of *source IP*, *source host name*, *source MAC address*, *destination IP*, and *destination host name*.

**IP address:** The value of the specified field to be verified.

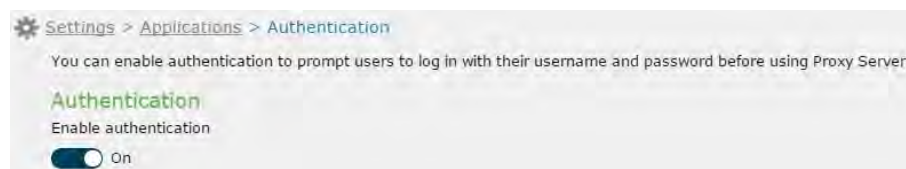
Click **OK** to save and apply the Settings.

## Enable authentication

To enable user authentication before using proxy server, click **Manage** under Authentication.



Then, click the switch to **On**.



## Syslog Server

Organizations have to save records of their operations for audit purposes to comply with ISO certification requirements on information security. To ensure that log data on various systems can be gathered and stored safely, businesses often install Syslog servers to collect logs from Syslog clients, such as Firewall, mail servers, routers, switches, UPS and NAS.

PAC Storage PS/PSV supports operations with Syslog servers with the following features:

- Supporting TCP and UDP
- Archiving log data
  - The logs are archived and stored in the specified shared folder when the size of the logs exceeds the specified threshold.
- Viewing logs
  - The fields include: Severity, Facility, Hostname, Application, Time, and Message, following the format of Syslog.

Go to	Settings > Applications > Syslog Server
<b>Activate Syslog Server</b>	<p>Click the switch to <b>On</b> to enable Syslog Server. Enter the parameters and click <b>Apply</b>.</p> <div> <p>Syslog server allows the storage device to receive the logs sent from syslog clients (e.g. NAS, router, UPS, etc.). This will help you archive all important logs centrally and safely.</p> <p><b>Syslog server</b></p> <p><input checked="" type="checkbox"/> On</p> <p>Available channel interface(s) to access Syslog server</p> <p>Controller A (Channel 2: -- ,Channel 3: 172.24.110.69) ▾</p> <p>Transfer protocol</p> <p>TCP ▾</p> <p>* Port</p> <p>514</p> <p>Archive the current logs when their size exceeds (MB)</p> <p>100</p> <p>Location for archived logs</p> <p>/Pool-NAS/HQ_Data/DB ▾</p> <p>Save</p> </div>
Parameter	Available channel interface(s) to access Syslog Server: Controllers found are

listed in this field, as well as the file-level ports on the controller. The location field also shows available folders corresponding to the value in this field. This is only for dual-controller products. The default value is the primary controller.

**Transfer Protocol:** PAC Storage PS/PSV listens to and receives log data according to the specified protocol. Users may select to use TCP or UDP. The default is TCP.

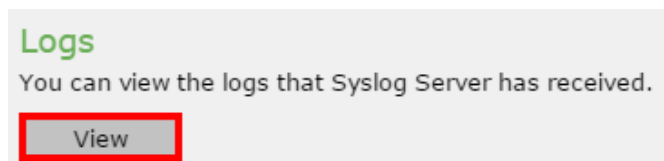
**Port:** The port number to receive log data. The default is 514.

**Archive the current logs when they exceed (MB):** The maximum value is 999. The default value is 100.

**Location for archived logs:** Available shared folders in the selected controller are listed in this field, including the pool and the volume, sorted alphabetically. The default is the first enumerated folder. If there is no available folder, the service cannot be activated.

## View logs

Click on **View** to see the received log data.



The fields of logs include *Severity*, *Facility*, *Hostname*, *Application*, *Time*, and *Message*.

Clicking **Refresh** will update the view with the latest log data.

Refresh					
Severity ▾	Facility ▾	Hostname	Application	Time	Message
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx
Error	Daemon	InfoNAS	qlogd	20016-12-11 15:24:30	xxxxxxxxxxxxxxxxxxxx

Note: Only logs that are not archived will be displayed on this page. Archived logs are stored in the specified folder and will not be shown on this page.

## VPN Server

Virtual Private Network (VPN) is a private network that extends across a public network or Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPNs can provide functionality, security and/or network management benefits to the user.

PAC Storage PS/PSV provides VPN service with the following features:

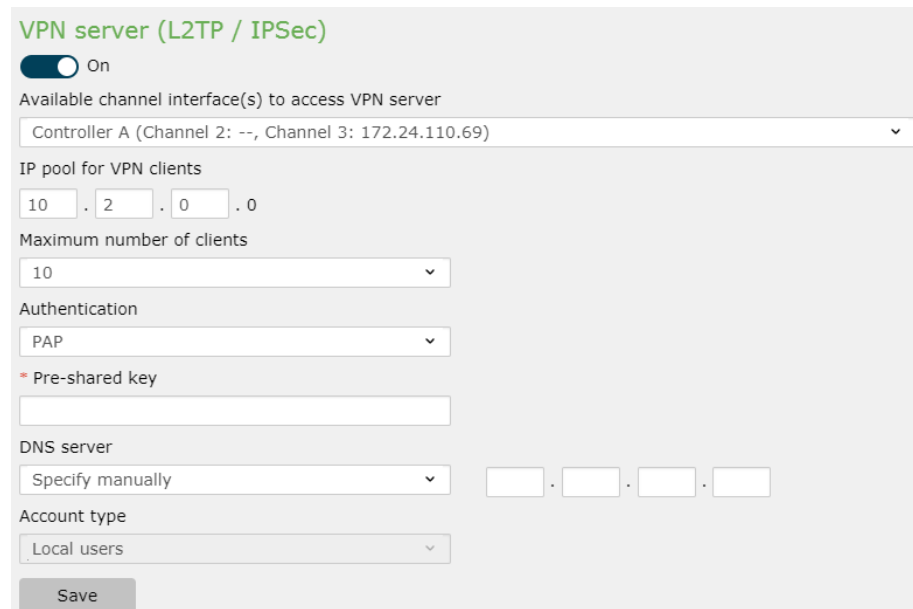
- L2TP/IPSec
- Viewing and managing current connections
- Privilege control for local and domain users
- Support for clients from Windows, Mac, iOS, and Linux

Go to

Settings > Applications > VPN Server

**Activate VPN service**

Click the switch to **On** to enable VPN server. Enter the parameters and click **Apply** to save the Settings.



The screenshot shows the 'VPN server (L2TP / IPSec)' configuration page. At the top, there is a toggle switch labeled 'On'. Below it, a dropdown menu shows 'Available channel interface(s) to access VPN server' with the selected option 'Controller A (Channel 2: --, Channel 3: 172.24.110.69)'. The 'IP pool for VPN clients' is set to '10 . 2 . 0 . 0'. The 'Maximum number of clients' is set to '10'. The 'Authentication' method is set to 'PAP'. There is a field for 'Pre-shared key' with a red asterisk indicating it is required. The 'DNS server' is set to 'Specify manually' with four empty input boxes for IP address. The 'Account type' is set to 'Local users'. A 'Save' button is at the bottom.

**Note:**

1. Please make sure UDP port 1701, 500, and 4500 are open on your router or firewall Settings for VPN connection.
2. To grant users the permission for VPN service, please edit their application

privileges in **Settings > Privilege > Users**.

#### Parameter

**Available channel interface(s) to access VPN server:** The controllers found are listed in this field, as well as the file-level ports on the controller(s). This is only for dual-controller products. The default value is the primary controller.

**IP pool for VPN clients:** The range of IP addresses the server may assign to clients. The default value is 10.2.0.0.

**Maximum number of clients:** The value can be 10, 20 or 30. The default is 10.

**Authentication:** Authorization protocols MS-CHAPv2 and PAP are supported. The default is MS-CHAPv2, which is available to either domain or local users.

**Pre-shared key:** The key for clients to log into the service. The default is null but a given string for PSK (pre-shared key) is required.

**DNS server:** User may specify the DNS server address in the VPN. The default is "Don't specify."

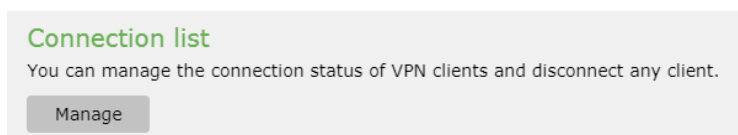
**Don't specify:** clients use their own DNS configuration.

**Specify manually:** Provide an address of DNS server which clients will use in the VPN. The DNS server address should be provided if this option is selected.

**Account type:** This option appears when the authentication protocol is set as *MS-CHAPv2*. Choose to provide the service to local user accounts or domain user accounts. The default is to domain user accounts.

#### View connection list

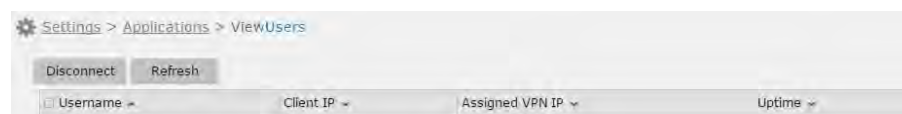
Click on Manage to see and manage user connections.



A window listing all the connections will pop up.

To disconnect a user, check the box next to the username and click **Disconnect** on the top. Click the checkbox in the header to select all the users.

Click the **Refresh** button to see the latest list of connections.

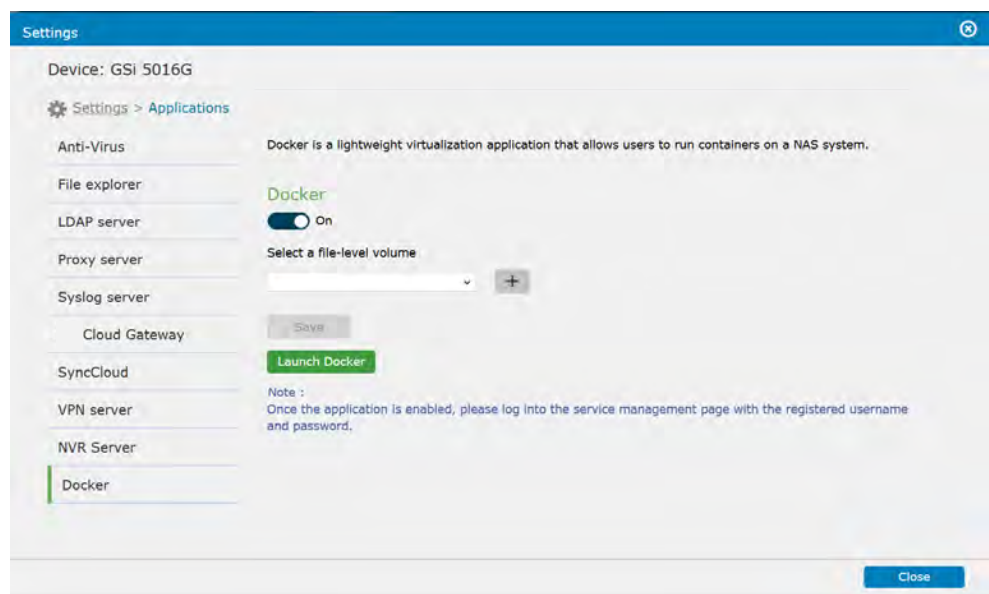


## Docker

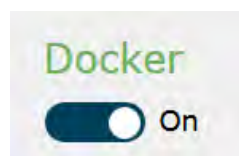
Docker is a lightweight virtualization application that allows you to run and test other applications in independent containers.

Go to **Settings > Applications > Docker**

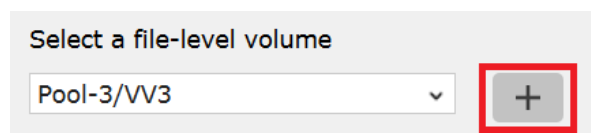
### Setup



1. Turn on Docker with the toggle.



2. Select a file-level volume to run Docker. When you switch to another volume, this action terminates services running on the previous volume.



To create a volume for use, click on the plus icon and follow the onscreen instructions.

Note: You can only create and mount a volume for Docker here.

3. Click **Save** to keep the Settings.

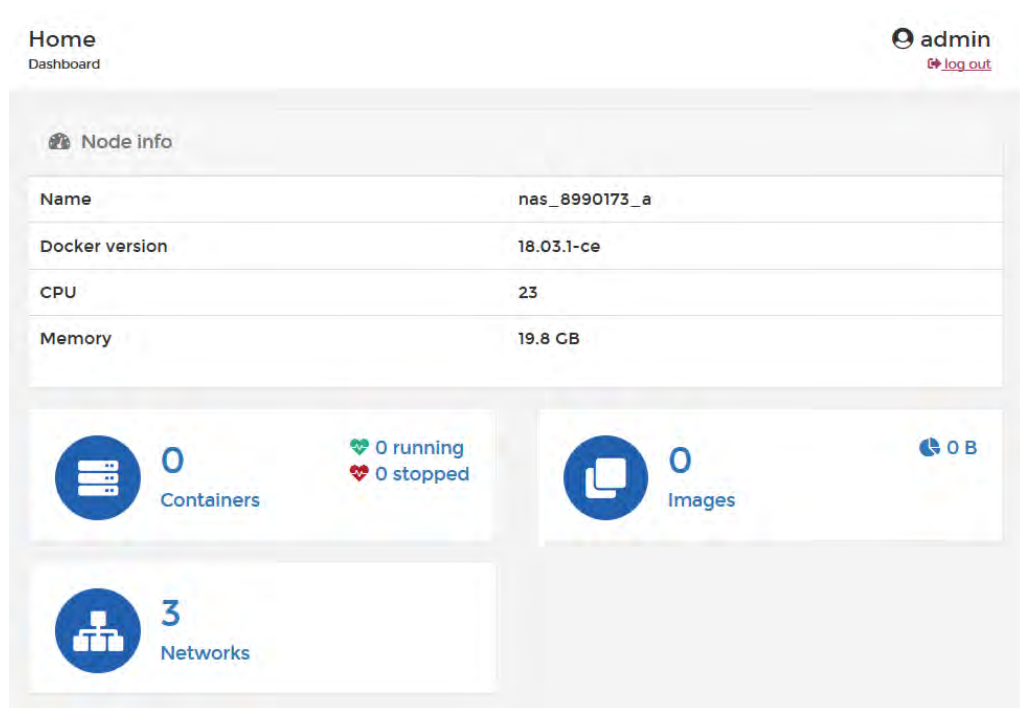


## Launch and login

1. Click **Launch Docker**, and a management site will pop up.
2. Enter your PAC Storage User Interface Firmware credentials and click **Login** to enter the site.

## Dashboard

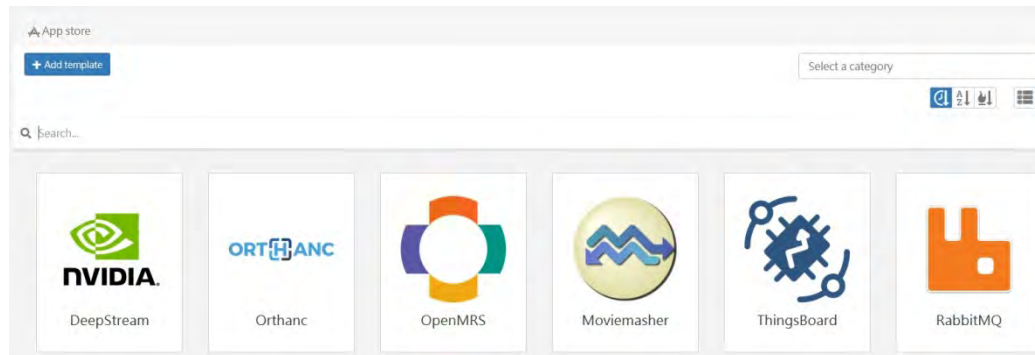
You can view information of the Docker node (i.e. your Docker-running device).



<b>Name</b>	The hostname of your storage device
<b>Docker version</b>	The version of the Docker application
<b>CPU</b>	The number of CPU cores on your storage device
<b>Memory</b>	System RAM allocated for running Docker and its containers
<b>Containers</b>	The total number of containers
<b>Networks</b>	The number of created networks
<b>Images</b>	The total number of container images and their total size

## App store

You can create a template to run a Docker image in a specific container. The system also automatically available updates for your Docker apps.



1. Click **Add template**.

2. Specify the template information:

**Title** Specify a title for the template.

**Description** Provide a description for the template.

3. Specify the advanced template information:

**Name** Assign a name to the container created by the template.

**Logo URL** Provide a link to display the template's logo image.

**Note** Specify extra information regarding the template.

**Platform** Select **Linux** or **Linux+GPU** as the running environment.

**Categories** Assign the template to a category.

4. Specify the container information:

**Image** Specify a Docker image to use the template. The image tag is required.

**Registry** Select a desired Docker registry and provide the following information to gain access to the registry.

**Account:** Enter your registry username

**Password:** Enter your registry password

**Command** Specify a custom command to run the container.

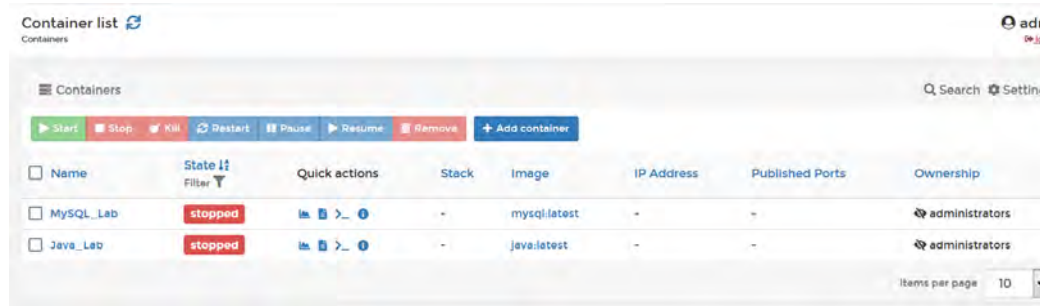
**Hostname** Assign a hostname to the container.

<b>Network</b>	<p>Select the network type.</p> <p>To prevent modification of this setting, turn on <b>Network lock</b> so that the template's users cannot change it.</p>
<b>Port mapping</b>	Map a host port (TCP/UDP) to a container port (TCP/UDP) for communication.
<b>Volume mapping</b>	<p>Bind a shared folder to the container. The folder works as a Docker volume and stores all data required and generated by the container.</p> <p><b>Required:</b> This container setting must be specified by the user.</p> <p><b>Default option of the configuration:</b> This container setting must be available in the template.</p> <p><b>Label:</b> Assign a custom name to this container setting. You can find the custom name in the template configuration.</p> <p><b>Description:</b> Provide a description of the container setting.</p>
<b>Restart policy</b>	Specify when to restart the container: <b>Always</b> , <b>Unless stopped</b> , <b>On failure</b> , or <b>None</b> .
<b>Privileged mode</b>	Enable this option to run the container in the privileged mode. This mode allows the user to run commands that require high permission in the container.
<b>Interactive mode</b>	Enable this option to run the container in the foreground so that the user can run commands in the container.
<b>Memory reservation</b>	Reserve a custom amount of system memory to run the container.
<b>Memory limit</b>	Set an upper limit on the container's memory usage.
<b>CPU limit</b>	Set an upper limit on the container's CPU usage.

- Specify the environment variables by providing their names and default values.
- Click **Create the template**.
- The created template shows up in the app store page. To run the container, click the template and click **Deploy the container**. To create another template based on the template Settings, click **Save as**.

- When Docker detects any update for your apps, click on **Update** to install the updates.

**Containers** You can view and manage containers.



- Create a container to execute a downloaded Docker image. Click **Add container** to start the setup.

**Name**

**Image configuration**

**Name**  **Registry**

**Always pull the image** ☒

**Ports configuration**

**Publish all exposed ports** ☐

**Port mapping**

<b>Name</b>	Assign a name to the container.
-------------	---------------------------------

<b>Image configuration</b>	<b>Name</b>	Enter the downloaded image's name.
----------------------------	-------------	------------------------------------

<b>Registry</b>	Choose the registry where you downloaded the image. The default registry is DockerHub.
-----------------	--

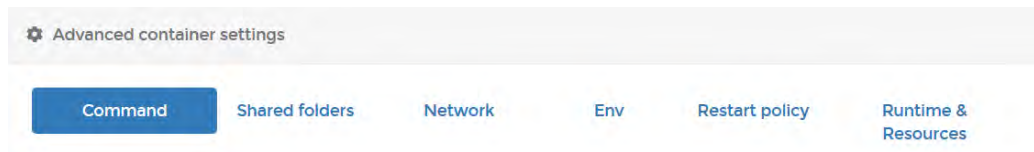
<b>Always pull the image</b>	When enabled, this option pulls the specified image when you create a container for it.
------------------------------	---

<b>Ports configuration</b>	<b>Publish all exposed ports</b>	When enabled, this option maps a random host port to ports defined in the image's Dockerfile.
----------------------------	----------------------------------	---

<b>Port mapping</b>	Click <b>map additional port</b> if you want to map another host port to the ports defined in the Dockerfile.
---------------------	---

<b>Actions</b>	Click <b>Deploy the container</b> to execute the image in the container.
----------------	--

- Go to the page bottom and configure the advanced Settings on each tab.

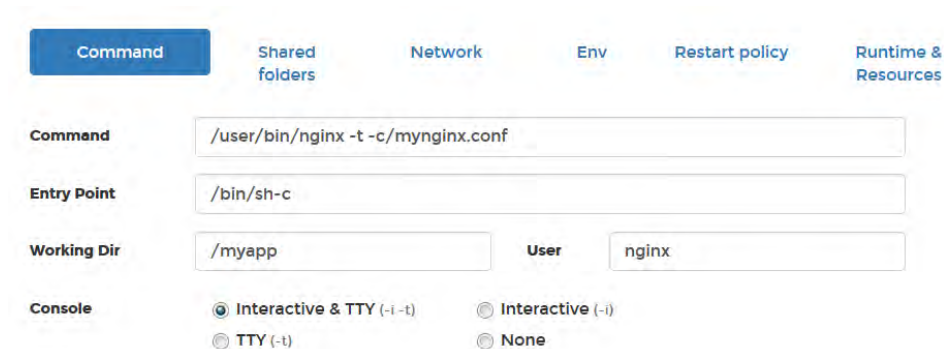


Advanced container settings

Command Shared folders Network Env Restart policy Runtime & Resources

- On the **Command** tab, you can specify the following Settings of the Dockerfile, the core file that records instructions for building an image.

To know more about the Dockerfile, check the official Docker Documentation.



Command Shared folders Network Env Restart policy Runtime & Resources

Command /user/bin/nginx -t -c/mynginx.conf

Entry Point /bin/sh-c

Working Dir /myapp User nginx

Console ☒ Interactive & TTY (-i -t) ☐ Interactive (-i)  
☐ TTY (-t) ☐ None

<b>Command</b>	Specify the default command to execute when running an image.
<b>Entry Point</b>	Specify the command to run when the container starts up.
<b>Working Dir</b>	Specify a default directory for Docker to run its commands.
<b>Console</b>	Choose a desired set of console for accessing the container.

- On the **Volumes** tab, you can choose a container to store generated data:

<b>Volume</b>	Select a volume within the Docker volume to store data.
<b>Shared folder</b>	Select a shared folder on the PAC Storage storage to store

data.

<b>Bind</b>	Select a file or a folder inside a shared folder to store data.
<b>Writable/Read-only</b>	Determine the access permission to the container.
<b>add more volume</b>	Add more containers.

5. On the **Network** tab, you can configure the network to be used by the container.

<b>Network</b>	Select a network driver to determine the network type.
<b>Hostname</b>	Specify a hostname to the container.
<b>Domain Name</b>	Specify a domain name for the Docker network.
<b>Mac Address</b>	Assign a MAC address to the container.
<b>IPv4 Address</b>	Assign an IPv4 address to the container.
<b>IPv6 Address</b>	Assign an IPv6 address to the container.
<b>Hosts file entries</b>	Click <b>add additional entry</b> to create a host file entry. The entry works as a DNS record that maps the hostname with the IP address for name resolution.

6. On the **Env** tab, you can assign a name and a value to an environment variable, which stores user-specific data for users that access Docker.

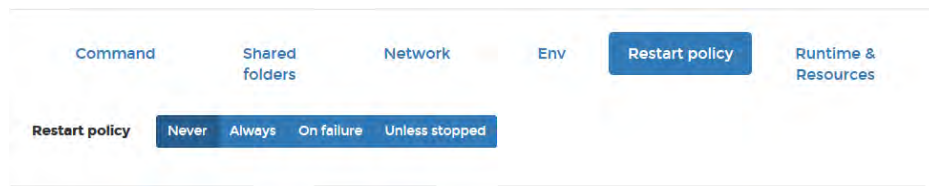
Environment variables may record configurations, encryption keys, and external address resources.

To know more about environment variables, check the official [Docker Documentation](#).

The screenshot shows the Docker container configuration interface. At the top, there are tabs for 'Command', 'Shared folders', 'Network', 'Env' (which is selected and highlighted in blue), 'Restart policy', and 'Runtime & Resources'. Below the tabs, there is a section for 'Environment variables' with a button that says 'add environment variable'. Below this button, there is a table with two columns: 'name' and 'value'. The first row has 'Foo' in the 'name' column and 'bar' in the 'value' column. To the right of the table, there is a red square icon with a white 'x' inside.

7. On the **Restart policy** tab, specify what action to take when the container is stopped.

To know more about the policies, check the official [Docker Documentation](#).



<b>Never</b>	Never automatically restart the container.
<b>Always</b>	Always restart the container when it is stopped.
<b>On failure</b>	Restart the container when it is stopped due to errors.
<b>Unless stopped</b>	Restart the container when it is not deliberately stopped and when Docker is not stopped/restarted.

8. On the **Runtime & Resources** tab, you can determine the container's runtime and allocate system resources to it.

To know more about a container's runtime privilege, check the official Docker Documentation.

To know more about a container's resource limits, check the official Docker Documentation.

Command

Shared folders

Network

Env

Restart policy

Runtime & Resources

Runtime

Privileged mode

Use GPU(s)

☒ Name

☒ nvidia0

Resources

Memory reservation

2304

19826

2304

Memory soft limit (MB)

Memory limit

7680

19826

7680

Memory limit (MB)

CPU limit

3

23

Maximum CPU usage

<b>Privileged mode</b>	When enabled, this option allows the container to access devices on your device.
<b>Use GPU(s)</b>	When enabled, this option allows you to use selected GPUs for running the container, along with the allocated CPU resources.  This option is only available to PSi models.
<b>Memory reservation</b>	Specify the minimum amount of memory that can be used by the container.
<b>Memory limit</b>	Specify the maximum amount of memory that can be used by the container.
<b>CPU limit</b>	Specify how many CPU cores to use for running the container.

9. Go back to **Containers** to view and manage containers by selection.

Start

Stop

Kill

Restart

Pause

Resume

Remove

+ Add container

<input type="checkbox"/>	Name	State	Quick actions	Stack	Image	IP Address	Published Ports	Owner
<input type="checkbox"/>	MySQL_Lab	running		-	mysql:latest	172.17.0.2	-	adm

**Start** Start the container.



<b>Stop</b>	Stop the container.
<b>Kill</b>	Delete the container when it is running.
<b>Restart</b>	Restart the container when it is stopped.
<b>Pause</b>	Pause the container when it is running.
<b>Resume</b>	Resume the container when it is paused.
<b>Remove</b>	Remove the container when it is stopped.
<b>Quick actions</b>	View the container information with the respective icons: usage statistics, logs, user interface Settings, and configuration details.

**Images** You can pull a Docker image from a hub and build a new image for use.

<b>Pull image</b>	<b>Name</b>	Enter a keyword or full name to locate a Docker image.
	<b>Registry</b>	Select a registry where you can download

		the image.
	<b>Pull the image</b>	Download the image from the registry.
<b>Images</b>	<b>Remove</b>	Remove an unused Docker image.  To remove an image being used by a container, click the arrow icon and <b>Force Remove</b> .
	<b>Build a new image</b>	Build a new Docker image with the native web editor, the uploaded tarball file or Dockerfile, or a file URL.

**Networks** You can add, remove, and monitor networks for a container.

Network list

admin
  
[log out](#)

Networks

Search

Remove
Add network

<input type="checkbox"/>	Name ↕	Stack	Scope	Driver	IPAM Driver	IPAM Subnet	IPAM Gateway	Ownership
<input type="checkbox"/>	bridge	-	local	bridge	default	172.17.0.0/16	172.17.0.1	public
<input type="checkbox"/>	host	-	local	host	default	-	-	public
<input type="checkbox"/>	none	-	local	null	default	-	-	public

Items per page
10

1. Click **Add network** to set up a new network.

<b>Name</b>	Assign a name to the network.	
<b>Network configuration</b>	<b>Subnet</b>	Enter the subnet netmask.
	<b>Gateway</b>	Enter the gateway address.
<b>Driver configuration</b>	<b>Driver</b>	Select a default driver for use. Drivers are used to create a specific type of network for your container.

		For more information about the default drivers, check the official Docker Documentation.
	<b>Driver options</b>	Create a custom network driver by assigning a name and a value to it.
<b>Advanced configuration</b>	<b>Labels</b>	Create a network label by assigning a name and a value to it.  For more information about the key and value, check the official Docker Documentation.
	<b>Restrict external access to the network</b>	When enabled, this option blocks any access from a different Docker network.
<b>Actions</b>	Click <b>Create the network</b> to complete the setup.	
2. After the setup, go back to Networks to manage and monitor existing networks.		
<b>Volumes</b>	You can create and manage volumes within the Docker volume.	
	<b>Add volume</b>	Click to add a new volume and specify the Settings:  <b>Name:</b> Specify a name for the volume  <b>Driver:</b> Select a driver to run the volume.  <b>Driver options:</b> Configure the driver by specifying its key and corresponding value. To know the keys and values available for modification, check the driver's documentation.  To add more drivers, click <b>add driver option</b> .  Then, click <b>Create the volume</b> to create a volume.
	<b>Remove</b>	Select an unwanted volume and click <b>Remove</b> to delete it.
<b>Events</b>	You can check configuration changes and container behaviors on this management site.	

Date	Category	Details
2018-08-16 16:23:05	network	Network sdsadad created

**Registries** You can manage the DockerHub credentials and add more Docker registries.

Name	URL	Actions
No registry available.		

<b>DockerHub</b>	<b>Authentication</b>	When enabled, this option allows only users with the correct credentials to pull/push Docker images.
------------------	-----------------------	--

<b>Update</b>	Sync with DockerHub.
---------------	----------------------

<b>Registries</b>	<b>Add registry</b>	You can add more Docker registries for use: Provide user credentials and other required information. Then, click <b>Add registry</b> to connect.
-------------------	---------------------	--

<b>Remove</b>	Remove a selected registry.
---------------	-----------------------------

# Update & Security

The system setting menu contains the following sub-Settings

1. Security
2. Firmware Upgrade
3. Factory Reset

## Security

**IP autoblock:** Access to PAC Storage PS/PSV from an IP address can automatically be blocked if the number of failed login attempts from the IP address reaches the specified value. The administrator can specify how long the IP address will be blocked by setting the length of period. This IP address will automatically be added to the blocked list.

**Whitelist/Blacklist:** The administrator can also create a Whitelist containing IP addresses that are granted access to the system and also a Blacklist containing IP addresses that will be rejected.

---

### Enable IP autoblock

Go to **Main menu > Settings > Update & Security > Security**

1. Switch **Enable IP block** to **ON**.

Note: The supported services for IP autoblock include HTTP(s), FTP(s), AFP, Rsync, SSH/Telnet and VPN.

**Login attempts:** specify the number of failed login attempts which, when exceeded, will make the IP address blocked. The valid range is 1 to 999 and the default value is 5.

**Within (minutes):** if the user reaches the specified login attempts within this period of time (given in minutes), the user will be blocked. The valid range is 1 to 999 and the default value is 1.

**Block for:** You can also choose to have the IP address blocked for 1 hour, 1 day, 1 week or forever(default).

2. Click **Apply** to save the Settings of IP autoblock.

**View Blocked IP Addresses:** Click on the button to see the list of blocked IP addresses.

---

Device: 1016R

Settings > Update & Security

**Security**

Firmware update

Factory reset

**IP autoblock**

Enable IP block

☒ On

If an IP address reaches the number of failed attempts within the time period entered below, it will be blocked for a certain period of time or forever.

Login attempts  
5

Within (minutes)  
1

Block for  
Forever

Apply View blocked IP addresses

**Whitelist / Blacklist**

Enable whitelist / blacklist

☐ Off

You can create a whitelist to allow IP addresses that you trust or a blacklist to reject IP addresses from

When you click **View Blocked IP Addresses**, a window will pop up. You can select one or more IP addresses and remove them from the blocked list by clicking **Remove**.

You can click **Refresh** to reload the latest list of blocked IP addresses.

<input type="checkbox"/> Select	Blocked IP Sources	Time Blocked	Expiration Time
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	2016-05-18 22:36:38
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	2016-05-18 22:36:38
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
<input type="checkbox"/>	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	2016-05-18 22:36:38

Refresh Close

In the case of a dual-controller system, there will an additional column of "Controller." The IP autoblock operations are performed individually for each controller.

## Enable Whitelist/Blacklist

Switch **Enable whitelist/blacklist** to **On**.

Note: The whitelist/blacklist mechanism is disabled by default. When it is enabled, the default activated list is the blacklist. The blacklist can be empty but the whitelist must have at least one entry when this mechanism is

enabled. If the whitelist is empty, the whitelist/blacklist mechanism will automatically be disabled. Therefore, if you want to use the blacklist function, you need to:

1. Enable the whitelist/blacklist mechanism.
2. Add IP address(es) to the whitelist because the whitelist is empty.
3. Change the activated list to the blacklist.

Click **Whitelist** and create a list of IP addresses that are allowed access to the system.

Click **Blacklist** and create a list of IP addresses that are blocked from access to the system.

### Add IP addresses to Whitelist/Blacklist

When the selection of whitelist or blacklist is made, click **Add** to include IP addresses in the whitelist or blacklist. A dialog box will pop up.

You can specify a single IP address or specify multiple IP addresses by their netmask, IP range or the region.

Click **OK** to enable the Settings.

Add IP sources

☒ Single host  
IP address:

☐ IP addresses by specifying netmask  
IP address:   
Subnet mask:

☐ IP range  
From:   
To:

☐ Region  
Continent:   
Country:

Apply Cancel

## Remove IP addresses from Whitelist/Blacklist

With the selection of whitelist or blacklist made, select one or more IP addresses you want to remove from the whitelist or blacklist, and click **Remove**.

Whitelist / Blacklist

☒ On

You can create a whitelist to allow IP addresses that you trust or a blacklist to reject IP addresses from logging in.

☒ Blacklist ☐ Whitelist

Add Remove

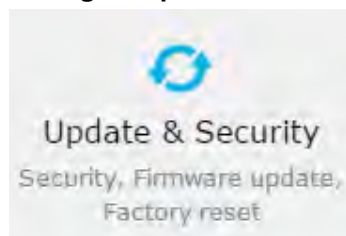
✓ Select	Blocked IP sources ^
✓	172.1.1.10



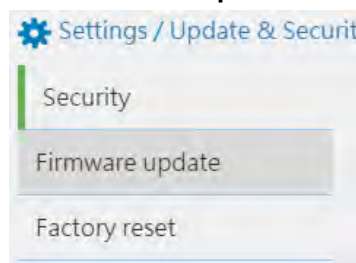
## Firmware Update

Go to

**Settings > Update & Security**



Click **Firmware update**.




---

### Update Firmware

1. Check the current firmware version and the latest available firmware version and download it from [if necessary](#).
2. Upload the firmware file by clicking the **Browse** button.
3. Click **Update Firmware**.

---

### Firmware Package

The firmware package consists of the following files.

FW30Dxyz.bin: Firmware Binary (where "xyz" refers to the firmware version)

README.TXT: Read this file first before upgrading the firmware/boot record. It contains the most up-to-date information which is very important to the firmware upgrade and usage.

These files must be unpacked prior to firmware update.

---

### Notes

Do not reset or turn off the computer or the controller while it is downloading the file. Doing so may result in an irrecoverable error that requires the service of the manufacturer.

Restoring the factory default may be required, which will erase the existing LUN mappings.

For dual-controller models, the two controllers must share the same firmware

---

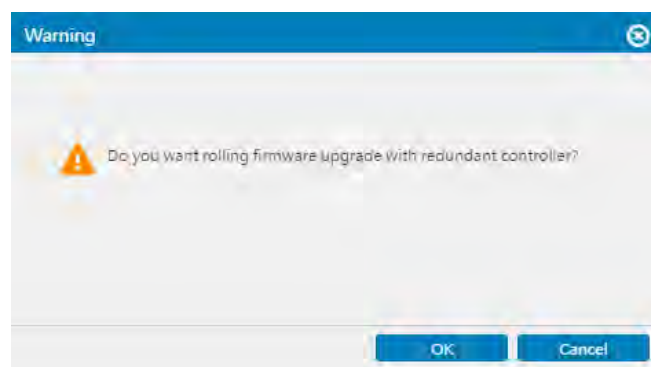
version number.

---

**Rolling firmware update**

For dual controller models, during the firmware update process, you will be prompted whether you want to reset the system.

If you choose yes, the system will ask if you want to perform rolling firmware update for the two controllers. If you choose no (i.e. you will reset the system later), the two controllers will have their firmware updated at the same time when you reset the system.



**Rolling firmware update**

For redundant controller models, “rolling firmware update” means the two controllers are individually and sequentially upgraded and restarted so that only one controller is offline at a time. During a rolling firmware update, the controller that is not actively being upgraded remains online and can continue serving clients. However, clients that are connected to a restarting controller are disconnected and reconnected. How the client connection behaves when a controller is restarted depends on several factors including the client type, client configuration (mount type, timeout Settings), IP allocation method, and how the client is connected to the system.

This approach avoids interrupting the operations the system is currently processing, but it will need double the time to upgrade the whole storage system. If you choose not to perform rolling firmware update, the two controllers will be upgraded at the same time.



## Factory Reset

Restoring to default Settings is the last resort to solving system errors as it will erase all system configurations.

---

### Pre-Restoration Works

Before you restore the default Settings, save the current configurations:

Stop all host IOs.

Export system configurations.

Make a list of host ID/LUN mapping information.

---

### Go to

**Settings >Update >Factory Reset**

---

### Factory Reset Menu

Click **Reset Settings** to carry out Factory Reset. The PAC Storage PS/PSV will be reset to the original status.

All system settings will be restored to default including channel settings, LUN mapping, etc.

Reset



# Cloud Gateway

Cloud Gateway is an enterprise-level hybrid cloud solution that integrates PAC Storage storage with mainstream cloud services, providing you with flexible and efficient data deployment. With a hybrid cloud infrastructure, you can freely transfer data between the connected cloud services and your local storage, keep important data on the cloud, speed up cloud access, and retrieve them in case of any unexpected system disruptions.

Through Cloud Gateway, you can quickly connect multiple local shared folders and local volumes to the cloud and manage connections with detailed, intuitive Settings.

Note:

- Supported cloud services: Aliyun, Amazon S3, KT ucloud, Microsoft Azure, OpenStack Swift, Tencent Cloud, Baidu Cloud, Google Cloud, Wasabi Cloud, Yandex.Cloud, and hicloud.
- Before connecting a local shared folder to the cloud, make sure it belongs to a WAN-connected controller.
- Before connecting a local volume to the cloud, make sure the primary controller is connected to WAN.
- For dual-controller models, both controllers should work properly to allow failover.
- An Cloud Gateway license is installed on your PAC Storage storage device by default. To know more about the default license's capabilities and license upgrade, go to <https://www.PACStorage.com/global/solutions/Cloud#lanchor>
- Before using Cloud Gateway, ensure that you have correctly configured system time in **Settings > System > Time**.



## Quick Setup

Cloud Gateway provides five quick setup methods to connect your local shared folders and local volumes to the cloud.

Five setup methods are available:

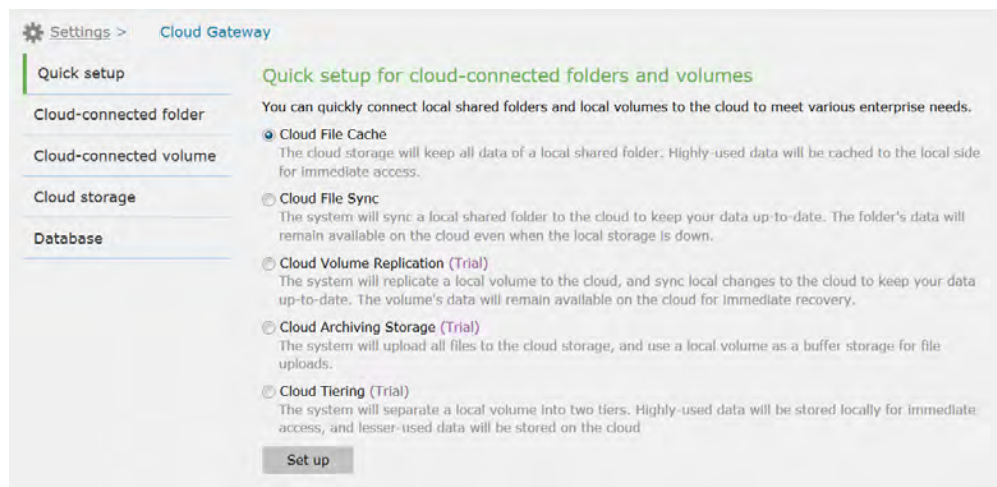
- **Cloud File Cache:** The system uploads a local shared folder's data to the cloud for secure preservation. On the local storage, the system caches the shared folder's highly-used data to allow immediate access.
- **Cloud File Sync:** The system syncs a local shared folder to the cloud to keep your data up-to-date. The folder's data remain available on the cloud even when the local storage is down.
- **Cloud Volume Replication:** The system replicates a local volume to the cloud, and syncs local changes to the cloud to keep your data up-to-date. The volume's data remain available on the cloud for immediate recovery.
- **Cloud Archiving Storage:** The system uploads all files to the cloud for secure preservation, and uses a local volume as a buffer storage for file uploads.
- **Cloud Tiering:** The system separates a local volume into two tiers according to data usage frequency: highly-used data are stored on the local storage for immediate access, while lesser-used data are securely preserved on the cloud.

## Cloud File Cache

In a Cloud File Cache task, the system uploads a local shared folder's data to the cloud for secure preservation. On the local storage, the system caches the shared folder's highly-used data to allow immediate access.

---

**Go to**                      **Settings > Cloud Gateway > Quick setup**



---

### Steps

1. Select **Cloud File Cache** and click **Set up**.
  2. Select a cloud storage to connect, or add one by clicking **+** (See [Cloud Storage](#)). Then, click **Next**.
  3. Select a cloud storage folder to connect.
  4. Select a local shared folder to connect, or add one by clicking **+**. Then, click **Next**.
  5. Set **Local cache capacity** to reserve local space for caching highly-used data. Then, click **Next**.
  6. Check the task Settings. Then, confirm them by clicking **Create**.
  7. The task is now listed at **Cloud Gateway > Cloud-connected folder**. For further managements, click on the task entry and proceed.
-

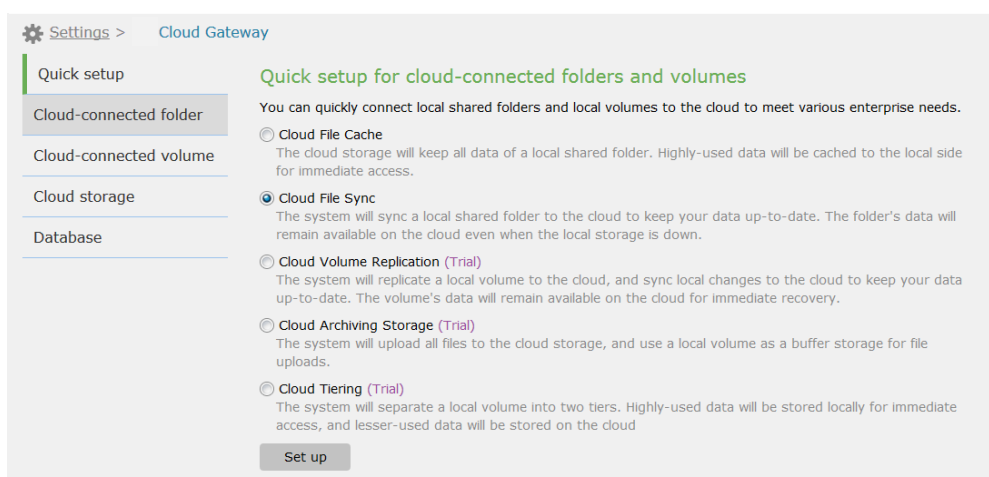


## Cloud File Sync

In a Cloud File Sync task, the system syncs a local shared folder to the cloud to keep your data up-to-date. The folder's data remain available on the cloud even when the local storage is down.

---

**Go to**                      **Settings > Cloud Gateway > Quick setup**



- 
- Steps**
1. Select **Cloud File Sync** and click **Set up**.
  2. Select a cloud storage to connect, or add one by clicking **+** (See [Cloud Storage](#)). Then, click **Next**.
  3. Select a cloud storage folder to connect.
  4. Select a local shared folder to connect, or add one by clicking **+**. Then, click **Next**.
  5. Check the task Settings. Then, confirm them by clicking **Create**.
  6. The task is now listed at **Cloud Gateway > Cloud-connected folder**. For further managements, click on the task entry and proceed.
-



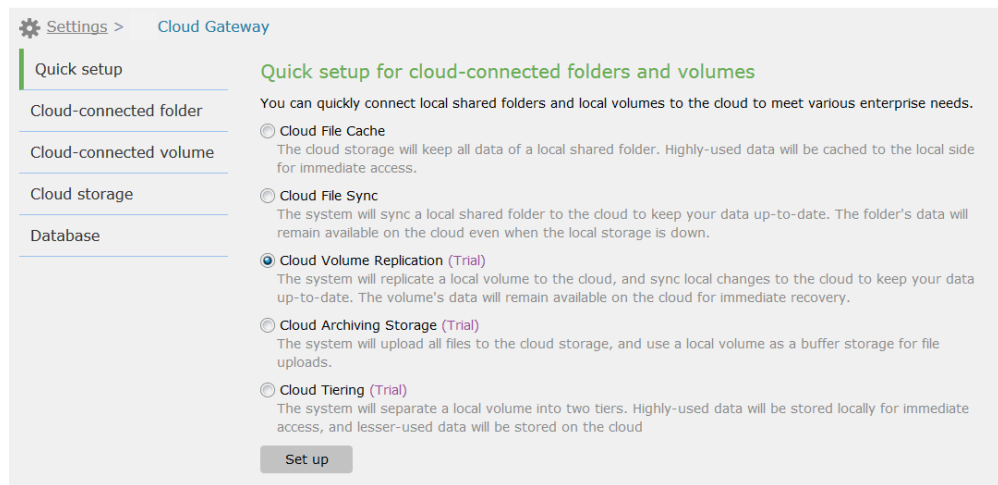


## Cloud Volume Replication

In a Cloud Volume Replication task, the system replicates a local volume to the cloud, and syncs local changes to the cloud to keep your data up-to-date. The volume's data remain available on the cloud for immediate recovery.

---

**Go to**                      **Settings > Cloud Gateway > Quick setup**

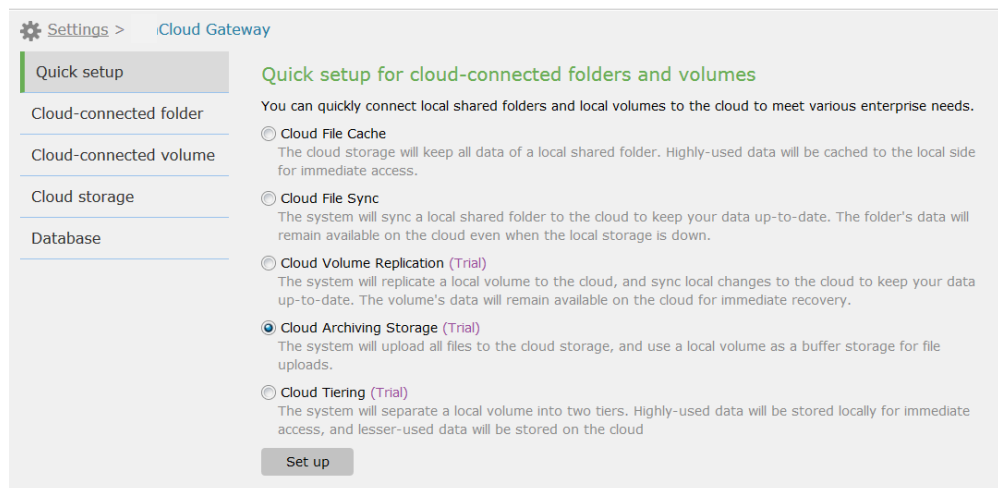


- Steps**
1. Select **Cloud Volume Replication** and click **Set up**.
  2. Select a cloud storage to connect, or add one by clicking **+** (See [Cloud Storage](#)). Then, click **Next**.
  3. Select a local volume to connect to the cloud storage, or add one by clicking **+**. Then, click **Next**.
  4. Check the task Settings. Then, confirm them by clicking **Create**.
  5. The task is now listed at **Cloud Gateway > Cloud-connected volume**. For further managements, click on the task entry and proceed.
-

## Cloud Archiving Storage

In a Cloud Archiving Storage task, the system uploads all files to the cloud for secure preservation, and uses a local volume as a buffer storage for file uploads.

**Go to**                      **Settings > Cloud Gateway > Quick setup**



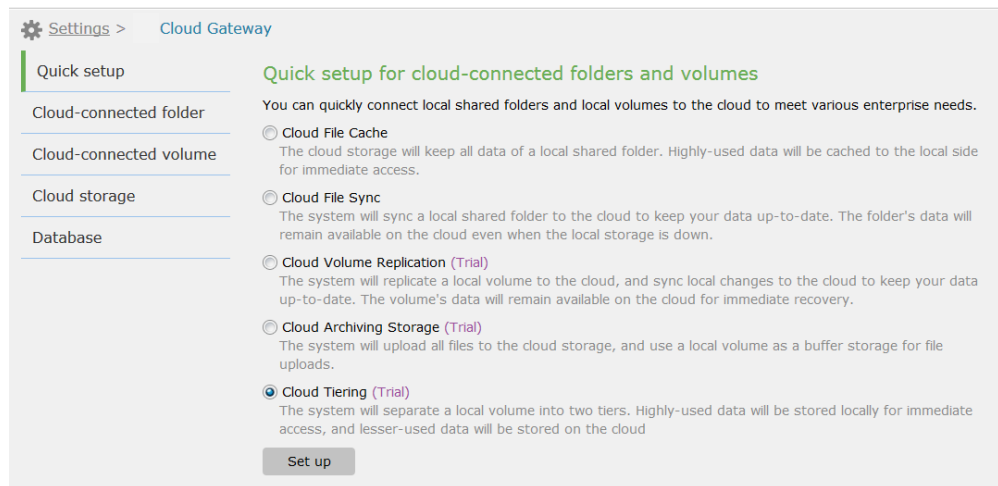
- Steps**
1. Select **Cloud Archiving Storage** and click **Set up**.
  2. Select a cloud storage to connect, or add one by clicking **+** (See [Cloud Storage](#)). Then, click **Next**.
  3. Select a local volume to connect to the cloud storage, or add one by clicking **+**.
  4. Set **Local cache capacity** to reserve local space as a buffer storage before uploading files to the cloud. Then, click **Next**.
  5. Check the task Settings. Then, confirm them by clicking **Create**.
  6. The task is now listed at **Cloud Gateway > Cloud-connected volume**. For further managements, click on the task entry and proceed.

## Cloud Tiering

In a Cloud Tiering task, the system separates a local volume into two tiers according to data usage frequency: highly-used data are stored on the local storage for immediate access, while lesser-used data are securely preserved on the cloud.

Note: For data integrity and recovery, also set up a scheduled snapshot task for the local volume at **SettnPS > Scheduling & Backup > Snapshot > Snapshot Schedule**.

Go to **Settings > Cloud Gateway > Quick setup**



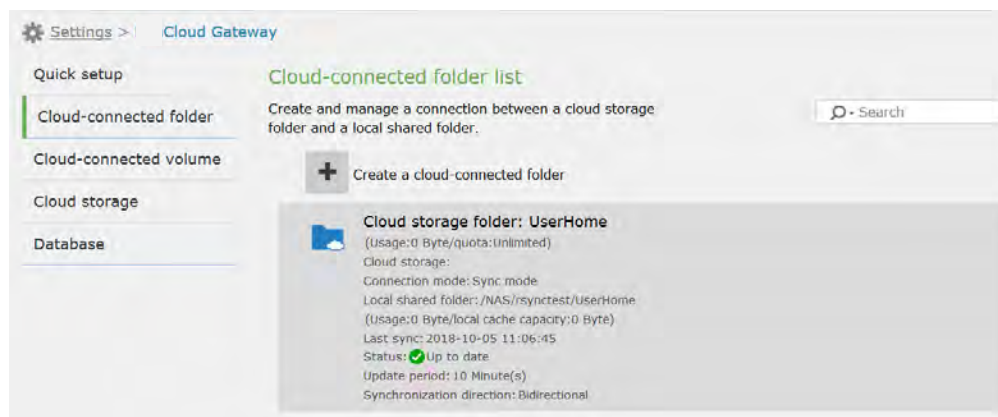
### Steps

1. Select **Cloud Tiering** and click **Set up**.
2. Select a cloud storage to connect, or add one by clicking **+** (See [Cloud Storage](#)). Then, click **Next**.
3. Select a local volume to connect to the cloud storage, or add one by clicking **+**.
4. Set **Local tier capacity** to reserve local space for storing highly-used data. Then, click **Next**.
5. Check the task Settings. Then, confirm them by clicking **Create**.
6. The task is now listed at **Cloud Gateway > Cloud-connected volume**. For further managements, click on the task entry and proceed.

## Cloud-connected Folder

Cloud Gateway provides detailed setup to create tasks that connect local shared folders with cloud storages.

**Go to**      **Settings > Cloud Gateway > Cloud-connected folder**



- Steps**
1. Click **Create a cloud-connected folder** to set up a task.
  2. On the pop-up, select a cloud storage to connect, or add one by clicking **+** (See Cloud Storage).
  3. Choose a connection mode:

<b>Cache mode</b>	The system will upload all data in the local shared folder to the cloud for preservation. Highly-used data will be cached to the local storage for immediate access.
-------------------	--

<b>Sync mode</b>	The system will sync data between the local shared folder and the cloud.
------------------	--

**Cloud-connected folder settings**

**Connection mode**

☐ Cache mode  
Highly-accessed data will be cached to a local shared folder to allow immediate access.

☒ Sync mode

Sync direction  
Two-way sync

Sync interval  
The system will regularly sync the local side and the cloud at the specified interval.  
10 Minute(s)

☐ ACL syncing  
When transferring files between the local side and the cloud, the system will sync the files' ACL settings to the cloud for preservation.

Local shared folder  
/NAS/rsynctest/UserHome

Cloud storage folder  
/UserHome Browse

4. To fine-tune the task, enable Settings specific to the chosen connection mode:

<b>ACL syncing</b>	The system will copy files' ACL Settings to the cloud for preservation.
<b>Instant cache update</b>	When locally cached data are accessed, the system will immediately check the cloud and update the local cache.
<b>Periodic cache update</b>	The system will check the cloud to update the local cache at a specified interval.
<b>Mark non-cached files by icon</b>	When users browse files in the local shared folder via File Explorer or SMB, the system marks non-cached files with a different icon.
<b>Cloud upload frequency</b>	<p>Determine how often the system uploads new local data to the cloud.</p> <p><b>Continuous:</b> The system uploads new local data to the cloud at all times.</p> <p><b>By schedule:</b> The system uploads new data to the cloud according to the set schedule. To create an upload schedule, click <b>Schedule Settings</b>.</p>

---

<b>Local cache capacity</b>	Set the maximum local capacity reserved for caching highly-used data.
-----------------------------	---

---

<b>Sync direction</b>	<p>Decide how to update changes between the local shared folder and the cloud:</p> <p><b>Two-way sync:</b> The system will update all changes on the local shared folder or on the cloud to the other side.</p> <p><b>Sync to the local side:</b> The system will update all changes on the cloud to the local shared folder.</p> <p><b>Sync to the cloud:</b> The system will update all changes on the local shared folder to the cloud.</p>
-----------------------	--

---

<b>Sync interval</b>	Decide how often the system syncs changes between the local shared folder and the cloud.
----------------------	--

- Select a local shared folder to connect, or add one by clicking **+**.
- Select a cloud storage folder to connect.
- To fine-tune cache behavior of Cloud File Cache tasks, click **Advanced cache Settings**. On the pop-up, click **Add** to create a cache policy:

<b>Expression</b>	<p>Use a glob expression to specify files and folders that the cache policy will apply to.</p> <p>Use the wildcard "*" for multiple characters and "?" for a single character.</p> <p>You can enter up to 256 UTF-8 characters.</p>
-------------------	---

---

<b>Action</b>	<p>Select a cache action to apply to files and folders specified in the glob expression:</p> <p><b>Default:</b> The system will first clear caches of any files/folders that are unused for the longest time. This action applies globally to all files and folders regardless of the provided expression.</p> <p><b>High Priority:</b> The system will assign the highest retention priority to caches of specified files/folders, and will clear</p>
---------------	--

---

them last when the local cache capacity is full.

**Local Only:** The system will keep newly written data on the local storage and will not upload them to the cloud. If you change this action to another, the system will upload the locally kept data to the cloud.

**Low Priority:** The system will assign the lowest retention priority to caches of specified files/folders, and will clear them first when the local cache capacity is full.

**Not Applicable:** The system will not allow any user to create files that match the expression, and will deny access to existing files that match.

**Uncacheable for read:** For any read access to specified files/folders, the system will not cache them locally.

**Uncacheable for write:** For any write access to specified files/folders, the system will upload newly written data to the cloud and will not cache them locally.

### Prepopulate

The system will preload specified files and folders to the local storage to speed up access.

To prepopulate new files that match the expression, click **Rescan** above the cache policy list.

### Sequentially pre-allocate

The system will reserve sequential disk space on the local storage to store specified files and folders and to speed up access.

Expression

\*cloud.xml

Action

Default (Trial)

☐ Prepopulate (Trial)
 ☐ Sequentially pre-allocate (Trial)



8. You can reset policy priority by moving cache policies up or down. Cache policies at a higher position have higher priority than lower ones.
9. Click **OK** to finish the setup. The task is now listed at **Cloud Gateway Cloud connected folder**.

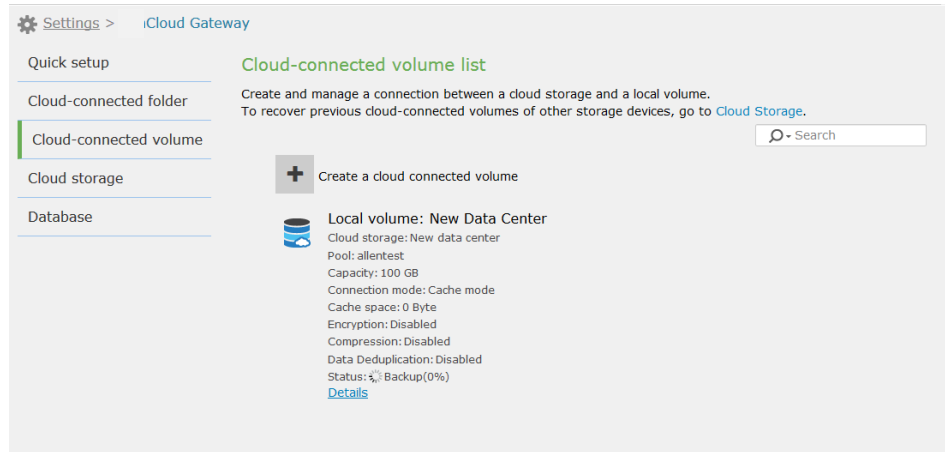


## Cloud-connected Volume

Cloud Gateway provides detailed setup to create tasks that connect local volumes with cloud storages.

Go to

**Settings > Cloud Gateway > Cloud-connected volume**



### Steps

1. Click **Create a cloud connected volume** to set up a task.
2. On the pop-up, select a cloud storage to connect, or add one by clicking **+** (See Cloud Storage).
3. Select a local volume to connect, or add one by clicking **+**.
4. Enable suitable data processing options:

#### **Deduplicate the volume's data before uploading to the cloud**

The system will deduplicate volume data before uploading them to the cloud to reduce cloud usage.

#### **Encrypt the volume's data on the cloud**

After uploading the volume's data to the cloud, the system will encrypt them with AES-256 to avoid data leaks.

#### **Compress the volume's data on the cloud**

The system will compress uploaded volume data to reduce cloud usage.

### Cloud-connected volume settings

**Cloud storage**  
Choose a cloud storage or add one by clicking "+".

User data center
+

**Local volume**  
Choose a local volume or add one by clicking "+". You should enable thin provisioning and disable WORM for the selected local volume.

Areal Revenue
+

☐ Deduplicate the volume's data before uploading to the cloud

☐ Encrypt the volume's data on the cloud

☐ Compress the volume's data on the cloud

5. Choose a connection mode:

<b>Cache mode</b>	The system will upload all data in the local volume to the cloud for preservation. Highly-used data will be cached to the local storage for immediate access.
-------------------	---

<b>Backup mode</b>	The system will back up the volume's data to the cloud.
--------------------	---

<b>Tiering mode</b>	The system will reserve highly-used volume data locally for immediate access, while lesser-used volume data are reserved on the cloud.
---------------------	--

**Connection mode**  
Select a mode to connect the cloud storage with the local volume.

☒ **Cache mode**  
All the volume's data will be uploaded to the cloud. Highly-used data will be cached to the local side for immediate access.  
Cloud upload frequency  
☒ Continuous  
☐ By interval  
Local cache capacity  

103
GB

☐ **Backup mode**  
All the volume's data will be backed up to the cloud for preservation.

☐ **Tiering mode**  
Highly-used data will be stored on the local side, while lesser-used data will be moved to the cloud.

6. To fine-tune the task, set further Settings under the connection mode:

**Cloud upload  
frequency**

Determine how often the system uploads new local data to the cloud.

**Continuous:** The system uploads new local data to the cloud at all times.

**By interval:** The system uploads new local data at the specified interval.

**By schedule:** The system uploads new data to the cloud according to the set schedule. To create an upload schedule, click **Schedule Settings**.

---

**Local cache  
capacity/Local  
tier capacity**

Determine how much local space is reserved for storing or caching highly-used data.

7. Click **OK** to finish the setup. The task is now listed at **Cloud Gateway > Cloud-connected volume**.
-

## Cloud Storage

You can create a list of available cloud storages that are ready to connect to your local storage.

<b>Go to</b>	<b>Settings &gt; Cloud Gateway &gt; Cloud storage</b>
<b>Steps</b>	<ol style="list-style-type: none"> <li>1. Click <b>Create a cloud storage</b>.</li> <li>2. On the pop-up, select a desired cloud service provider: <b>Aliyun, Amazon S3, KT ucloud, Microsoft Azure, OpenStack Swift, Tencent Cloud, Baidu Cloud, Google Cloud, Wasabi Cloud, Yandex Cloud, or hicloud</b>.</li> <li>3. Provide authentication credentials for login to the cloud service. Required information varies with cloud service providers.</li> </ol>
<b>Service IP/Port</b>	Provide the OpenStack Swift server's IP and access port.
<b>Access key</b> <b>Authentication code</b>	Provide the first access key or authentication code acquired from the cloud service provider.
<b>Key</b> <b>Secret key</b> <b>Client secret</b>	Provide the second access key acquired from the cloud service provider.
<b>Project ID</b> <b>Domain ID</b> <b>App ID</b> <b>Client ID</b>	Provide the ID acquired from the cloud service provider.
<b>Endpoint</b>	<p>Select how to set up a communication channel with the cloud storage: <b>Auto, Manual, and Customize</b>.</p> <p>Then, fill in the fields with required information.</p>
<b>Region</b>	Select the desired region that hosts the cloud storage.

---

**Node name** Select or provide the hostname of the access node.

4. To protect data transfers with the cloud storage, select **Secure data transfers over SSL**.

5. Select the connection type: **File-level** (for connection with local shared folders only) or **Block-level** (for connection with local volumes only).

A cloud storage entry allows data transmission via only one type of connection (e.g. block-level connection); to use the same cloud service with the other type of connection (e.g. file-level connection), you must create another cloud storage entry.

6. Click **Connect** to connect your storage device to the cloud service.

7. When connected to the cloud service, choose a cloud storage bucket to store your data.

8. Click **Next**.

9. Provide identifying information for the connected cloud storage:

---

**Name** Assign a name to the cloud storage.

---

**Description** Provide a description for the cloud storage.

---

**Enable password protection** Enable this option to protect this cloud storage with a password: only authorized users can access and manage this cloud storage.

Then, provide a password and confirm it.

---

**Email address** Provide an email address to receive a new password in case you forget the original one.

Then, click **Send Test Email** to check if the email address is correct.

10. Click **Create** to finish the setup. The cloud storage is now listed at **Cloud Gateway > Cloud storage**.

11. For further managements, click on the cloud storage entry and proceed.

---



## Access Control Management

After you connect different storage devices to the same cloud storage bucket, you can enable access control management to avoid access conflicts.

Note: Access control management is only available to file-level cloud storages.

---

<b>Go to</b>	<b>Settings &gt; Cloud Gateway &gt; Cloud storage</b>
--------------	---

---

- |              |   |
|--------------|---|
| <b>Steps</b> | <ol style="list-style-type: none"><li>1. Click on a cloud storage that is connected with local shared folders on different storage devices.</li><li>2. Click <b>Edit</b>.</li><li>3. On the pop-up, select <b>Enable access control management</b> and click <b>Save</b>.</li></ol> |
|--------------|---|

**Access control management (Trial)**  
We recommend you enable the option because other storage devices are accessing this cloud storage.

☒ **Enable access control management**  
Set access privileges for cloud storage folders to avoid file conflicts when multiple Infortrend storage devices are accessing the folders at the same time.  
[Access privilege settings](#)

Save

**Connected storage devices**  
Manage all Infortrend storage devices that are connected to this cloud storage.

+ Add a storage device

Storage device: F03(0)  
[Access privilege list](#)

Delete

4. Click **Access privilege Settings** to determine the access privilege between a connected storage device and a cloud storage folder.
5. Click **Add access privilege pair** and provide needed information:

<b>Storage device</b>	Select a connected storage device.
-----------------------	------------------------------------

---

<b>Cloud storage folder</b>	Click <b>Browse</b> to select a cloud storage folder.
-----------------------------	---

---

<b>Access privilege</b>	Select an access privilege to apply:
-------------------------	--------------------------------------

---

**Read/write:** The storage device can have read and write access to the cloud storage folder.

**Read-only:** The storage device can only have read access to the cloud storage folder.

The screenshot shows a configuration window with a light gray background. It contains three main sections: 'Storage device:' with a dropdown menu showing 'F03(0)'; 'Cloud storage folder:' with a text input field and a 'Browse' button to its right; and 'Access privilege:' with a dropdown menu showing 'Read/write'.

6. Click **OK** to finish the setup.
  7. In the **Connected storage devices** section, you can view storage devices connected to the cloud storage. To join more storage devices, click **Add a storage device** and proceed.
  8. To view each storage device's access privileges, click **Access privilege list**.
-



## Connection History

The system logs data transfers between the local storage and the cloud storage for monitoring.

Go to	Settings > Cloud Gateway > Cloud storage
Steps	<ol style="list-style-type: none"><li>Click on a cloud storage entry and click <b>Edit</b>.</li><li>Go to the <b>Connection history</b> section.</li><li>Select how long the system should retain connection records: <b>Retain history for 1 week</b>, <b>Retain history for 1 month</b>, or <b>Retain history for 6 months</b>.</li></ol> <div data-bbox="402 804 1353 1122"><p><b>Connection history</b></p><p>You can check this cloud storage's data transfer records and restrict the retention time. The system can retain up to one million records.</p><p><input checked="" type="radio"/> Retain history for 1 week</p><p><input type="radio"/> Retain history for 1 month</p><p><input type="radio"/> Retain history for 6 months</p><p><a href="#">Save</a></p><p><a href="#">Show connection history</a></p></div> <ol style="list-style-type: none"><li>Click <b>Save</b> to finish the setup.</li><li>To view existing connection records, click <b>Show connection history</b>. To export the connection history, click <b>Export</b> on the connection history page.</li></ol>

## Status Management

You can pause or restart the connection between the local storage and the cloud storage.

Note: This feature is only available to file-level connections with local shared folders.

Go to	Settings > Cloud Gateway > Cloud storage
Steps	<ol style="list-style-type: none"><li>Click on a cloud storage entry and click <b>Edit</b>.</li><li>Go to the <b>Status management</b> section.</li><li>Click <b>Pause</b> to pause the connection; to reconnect the local storage with the cloud storage, click <b>Restart</b>.</li></ol>



**Status management**

You can pause this connection and its data transfers.

Pause

Reconnect with this cloud storage if unexpected errors occur

Restart

## Database

Cloud Gateway requires a local shared folder as its database to store all relevant configurations and records. You must set the database before you connect the local storage to the cloud.

---

<b>Go to</b>	<b>Settings &gt; Cloud Gateway &gt; Database &gt; Database</b>
--------------	--

---

- |              |   |
|--------------|---|
| <b>Steps</b> | <ol style="list-style-type: none"><li>1. Select an available local shared folder, or click <b>+</b> to create one.</li><li>2. Click <b>Save</b> to finish the setup.</li><li>3. To delete the database from the local shared folder, click <b>Delete database</b>. All data in the deleted database can never be recovered.</li></ol> |
|--------------|---|
- 

## SyncCloud and Cloud Gateway

SyncCloud and Cloud Gateway are legacy versions of Cloud Gateway. You can retain the two legacy versions or upgrade them to Cloud Gateway.

---

<b>Go to</b>	<b>Settings &gt; Cloud Gateway &gt; Database &gt; SyncCloud and Cloud Gateway</b>
--------------	---

---

- |              |  |
|--------------|--|
| <b>Steps</b> | <ol style="list-style-type: none"><li>1. Select <b>Retain SyncCloud and Cloud Gateway</b>.</li><li>2. Click <b>Save</b> to finish the setup.</li></ol> |
|--------------|--|
-

