STORANDER

User Manual

EonStor GS/GSa/GSc/GSe/GSe Pro/GSi

EonOne Web-Based User Interface

Version 5.6 (January 2024)

Legal Information

All STORANDER products, including the product customers have purchased from ANDRA will be subject to the latest Standard Warranty Policy available on the STORANDER website: https://www.storander.com

STORANDER may from time to time modify, update or upgrade the software, firmware or any accompanying user documentation without any prior notice. STORANDER will provide access to these new software, firmware or documentation releases from certain download sections of our website or through our service partners. Customer will be responsible for maintaining updated version of the software, firmware or other documentation by downloading or obtaining from STORANDER and installing designated updated code, including but not limited to firmware, microcode, basic input/out system code, utility programs, device drivers, and diagnostics delivered with STORANDER product. Before installing any software, applications or components provided by a third party, customer should ensure that they are compatible and interoperable with STORANDER product by checking in advance with STORANDER Customer is solely responsible for ensuring the compatibility and interoperability of the third party's products with STORANDER product. Customer is further solely responsible for ensuring its systems, software, and data are adequately backed up as a precaution against possible failures, alternation, or loss.

For any questions of hardware/ software compatibility, and the update/ upgrade code, customer should contact STORANDER sales representative or technical support for assistance.

To the extent permitted by applicable laws, ANDRA will NOT be responsible for any interoperability or compatibility issues that may arise when (1) products, software, or options not certified and supported by STORANDER are used; (2) configurations not certified and supported by STORANDER are used; (3) parts intended for one system are installed in another system of different make or model.

Trademarks

Infortrend, the Infortrend logo, EonOne and EonStor are registered trademarks of Infortrend Technology, Inc. Other names prefixed with "IFT", "GS" and "GSe" are trademarks of Infortrend Technology, Inc.

STORANDER, ANDRA are trademarks and/or registered trademarks of ANDRA LLC.

All other names, brands, products or services are trademarks or registered trademarks of their respective owners.

Contact Information

Customer Support	Contact your system vendor or visit STORANDER's website https://storander.com

About This Manual

This manual introduces how to access and use the browser-based interface version of the EonOne software suite for EonStor GS series.

For the following subjects, consult other resources for more information:

- For components that are not user-serviceable, contact our support staff or visit our support sites.
- Regarding hardware operations, see Hardware Manual.

Version 5.6	Updated contents

Table of Contents

Introduction

Installation

Accessing the Firmware

Initial Setup Wizard

Calibration Wizard

Navigating User Interface

Service Manager

Certification

System

Access

Appliance

Privilege

Storage

Data Protection

Applications

Update & Security

EonCloud Gateway

Cluster

HA Service

Appendix

Introduction

EonOne is the proprietary software suite for managing single or multiple EonStor GS storage systems. EonOne is accessible through a web browser if both the computer running EonOne 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 EonStor GS/GSe storage system has an embedded copy of EonOne pre-installed in the firmware for management of the individual device. The EonOne software suite (Central EonOne) being referred to in this manual can be installed on different servers to manage multiple EonStor GS/GSe storage systems. The graphic user interfaces are similar with only slight differences.

Connecting EonOne to Storage Subsystems

EonOne, 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). EonOne is web-based and therefore is accessible from anywhere on the network. The flexible connection schemes allow the user to manage EonOne 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

Storage Subsystems

A storage subsystem refers to a hard drive array (storage subsystems + expansion enclosures).

Host Computer

The host computer refers to the computer to which the storage subsystem's host links are connected.

Remote Computer

The remote computer refers to a computer on the network to which the host computer is connected via LAN.

In-Band Connection

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.

Out-of-Band Connection

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.

Computer Requirements

Computer Requirements

- **Hardware**

Broadband access

- **Operating System**

Follow the steps to find out the operating systems compatible with your STORANDER storage device:

1. Go to STORANDER’s official website: https//www.storander.com
2. Click on selected **Products**

- **Browser**
  - Microsoft Edge 91 or later
  - Firefox 74 or later
  - Google Chrome 80 or later

Installation

The following sections provide an introduction on how to install, uninstall and upgrade EonOne.

Enabling Access Ports

Enable the following ports in Inbound Rules for access so that the EonOne system can connect to the EonStor GS/GSe:

TCP ports: 6100, 6101, 58630, 58632

UDP ports: 58640, 58641

Initiating EonOne Installation

Initially, methods and tools to launch EonOne installation vary depending on the operating system (OS) you are using, but they are basically helping you install Java 7 and launch the EonOne Installation Wizard.

For Windows

Go to Infortrend Support (https://www.infortrend.com/global/products/service). Select your model, and go to **Download** > **Software** to download **Central EonOne**.

Choose EonOne GUI Software Installation from the navigation menu that appears, and select Windows Platform under EonOne Management Tool. Proceed to the next section.

For macOS, Linux, and Solaris

Note: If you want to install the data host only instead of the GUI-based EonOne, skip to the next section directly.

Go to Infortrend Support (https://www.infortrend.com/global/products/service). Select your model, and go to **Download** > **Software** to download **Central EonOne**.

Open the command line utility of your OS (such as Terminal for Linux), and log into the command line shell as root.

For Linux users, locate the " EonOne" folder copied to your computer and then browse its contents to make sure the "linux.sh" script is in the folder. If you are using Solaris, make sure "unix.sh" is in the folder.

```
 [root@localhost ~]# cd <computer_path>/EonOne/
 [root@localhost <computer_path>/EonOne]# ls -l
...
-rw-r--r--. 1 root root      4279 Jun 23 19:55 linux.sh
...
-rw-r--r--. 1 root root      2037 Jun 23 19:55 unix.sh
```

If you are using Linux, make "linux.sh" executable, and then execute it.

```
[root@localhost <computer_path>/EonOne]# chmod +x linux.sh
[root@localhost <computer_path>/EonOne]# ./linux.sh
```

If you are using macOS or Solaris, do the same to "unix.sh."

```
[root@localhost <computer_path>/EonOne]# chmod +x unix.sh
[root@localhost <computer_path>/EonOne]# ./unix.sh
```

The first two sections of the script will take you through Java installation. If you already have Java 7 or higher installed on your computer, you can skip Java installation by typing “no” and pressing Enter. Otherwise, keep typing "yes" (shown below) and pressing Enter until Java is installed on your computer.

```
  **********************************************************
           Java-based GUI RAID Manager Installation Procedure
  **********************************************************
  SECTION I : JRE <version> Installation
...
Would you like to install JRE <version> now?
Please type yes or no.
yes
...
Done.
...
Install JRE <version> finished!
------------------------------------------------------------
SECTION II : Java Plug-in <version> Installation
...
Would you like to install Java Plug-in <version> now?
Please type yes or no.
yes
...
          Java(TM) Plug-in <version> Pre-Release
            Binary Code Evaluation License
...
Do you agree to the above license terms?
If you do not agree to the terms, installation cannot proceed
   Please type yes or no.
yes
```

The final section of the script will ask you whether you want to install EonOne. Type "yes" and press Enter to proceed to the next section.

```
------------------------------------------------------------
SECTION III : Java-based GUI RAID Manager Installation
*NOTE: To install and configure Java-based GUI RAID Manager
successfully,
      We highly recommend you refer to INSTALLATION GUIDE first.
Would you like to install Java-based GUI RAID Manager now?
Please type yes or no.
yes
```

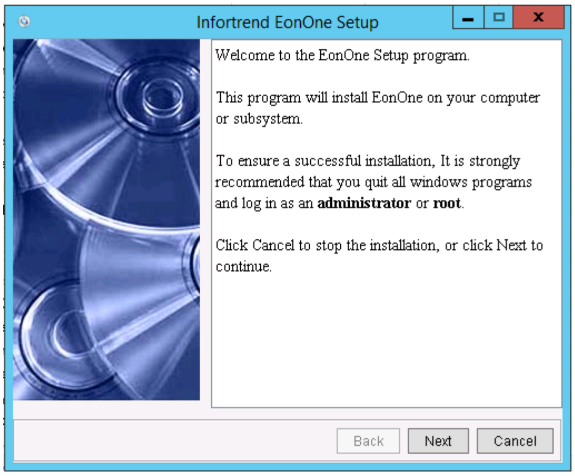
Installing EonOne

This section introduces how to install the whole GUI-based EonOne on various OS platforms.

For the Linux platform, you can install the data host agent only to save system resources.

Installing GUI-based EonOne

1. After installation is initiated, you will be guided to the EonOne Setup wizard. Click Next to continue.



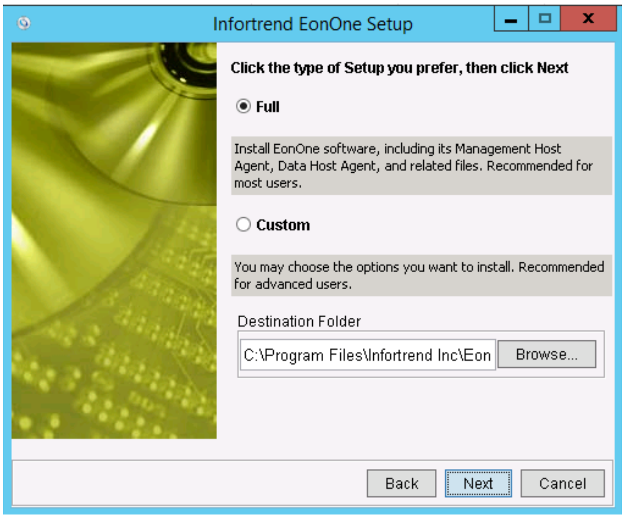
Welcome to the EonOne Setup program.

This program will install EonOne on your computer or subsystem.

To ensure a successful installation, It is strongly recommended that you quit all windows programs and log in as an **administrator** or **root**.

Click Cancel to stop the installation, or click Next to continue.

2. The installation program asks for Full or Custom installation. You can also select the installation folder here.
Choose Full installation if you intend to manage EonOne directly from the host computer. Skip to Step 4.



Click the type of Setup you prefer, then click Next

● **Full**

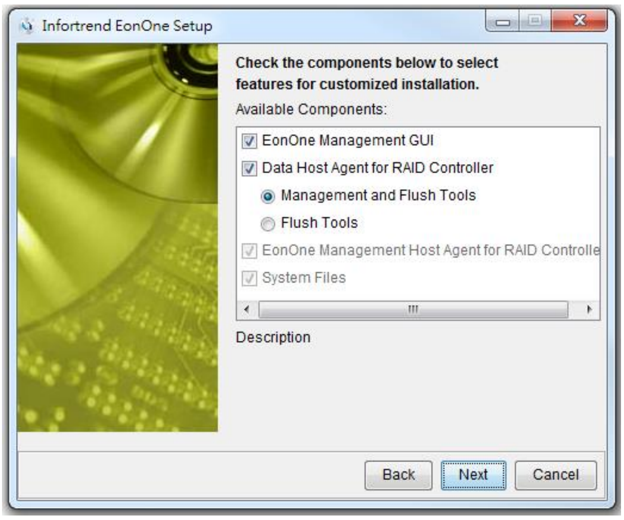
Install EonOne software, including its Management Host Agent, Data Host Agent, and related files. Recommended for most users.

○ **Custom**

You may choose the options you want to install. Recommended for advanced users.

Destination Folder: C:\Program Files\Infortrend Inc\Eon

3. Otherwise, choose **Custom** installation. In the component list, select the module(s) you need based on the computer on which you are installing EonOne.



Infortrend EonOne Setup

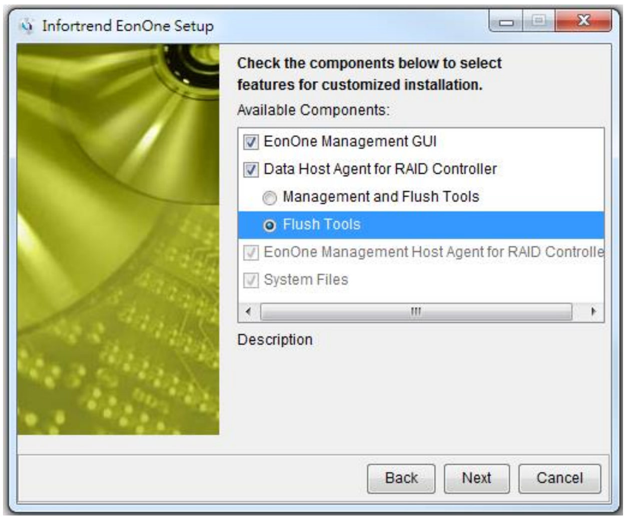
Check the components below to select features for customized installation.

Available Components:

- ☑ EonOne Management GUI
- ☑ Data Host Agent for RAID Controller
  - ● Management and Flush Tools
  - ○ Flush Tools
- ☑ EonOne Management Host Agent for RAID Controlle
- ☑ System Files

Description

If you are using DB Flush Agent for taking snapshot images with database applications, select **Flush Tools**. Click Next to continue.



Infortrend EonOne Setup

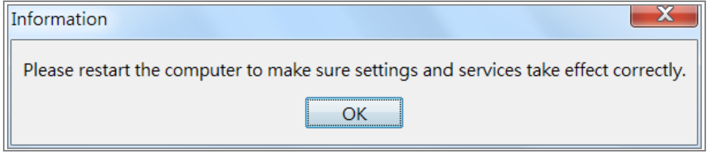
Check the components below to select features for customized installation.

Available Components:

- ☑ EonOne Management GUI
- ☑ Data Host Agent for RAID Controller
  - ○ Management and Flush Tools
  - ● Flush Tools
- ☑ EonOne Management Host Agent for RAID Controlle
- ☑ System Files

Description

4. When the installation is completed, restart the computer.



Information

Please restart the computer to make sure settings and services take effect correctly.

Installing data host agent only (Linux command line)

1. Extract the EonOne installation package using the following command:
   `unzip EonOne_[x.0.x.xx].zip`

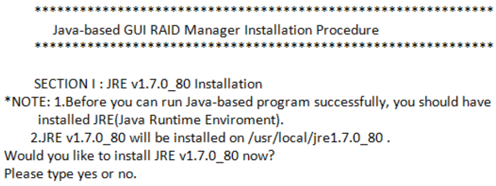
2. Navigate to the EonOne directory:
   `cd EonOne-[x.0.x.xx]`

3. Change the access permission of the executable file:
   `chmod 755 linuxCmd.sh`

4. Run linuxCmd.sh:
   `./linuxCmd.sh`

5. Type in yes when you are prompted with the question "Would you like to

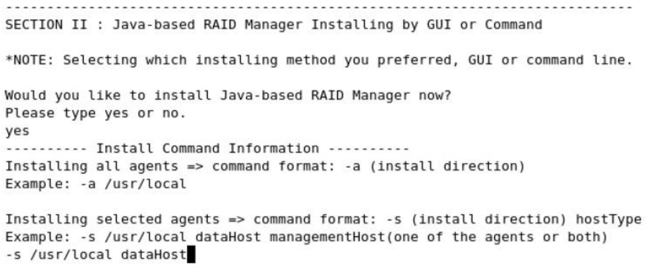
install Java-based RAID Manager now?"



```
    *************************************************************
       Java-based GUI RAID Manager Installation Procedure
    *************************************************************

    SECTION I : JRE v1.7.0_80 Installation
*NOTE: 1.Before you can run Java-based program successfully, you should have
       installed JRE(Java Runtime Enviroment).
      2.JRE v1.7.0_80 will be installed on /usr/local/jre1.7.0_80 .
Would you like to install JRE v1.7.0_80 now?
Please type yes or no.
```

6. When you are asked whether to install all agents or selected agents only, use the "**`-s /usr/local dataHost`**" command to install the data host agent:



```
----------------------------------------------------------------------------
SECTION II : Java-based RAID Manager Installing by GUI or Command

*NOTE: Selecting which installing method you preferred, GUI or command line.

Would you like to install Java-based RAID Manager now?
Please type yes or no.
yes
---------- Install Command Information ----------
Installing all agents => command format: -a (install direction)
Example: -a /usr/local

Installing selected agents => command format: -s (install direction) hostType
Example: -s /usr/local dataHost managementHost(one of the agents or both)
-s /usr/local dataHost
```

The data host agent is now installed successfully. It will be activated automatically during system startup, saving you the trouble of having to manually start the service.

Uninstalling/Upgrading EonOne

Uninstalling EonOne

Uninstall EonOne just as you would with any other application. For example in Windows, go to Start > All Programs > Infortrend Inc > Uninstall EonOne.

Upgrading EonOne

In order to upgrade EonOne to a new version, you need to uninstall the current version and then install the new version. Visit the Support site for the latest version of EonOne.

Accessing the Firmware

In this manual, the term “firmware” refers to the tool that enables access to functionalities of the EonStor GS/GSe without having to install software in a computer.

Firmware Interface

Tool	Description	Interface
EonOne	You will access the firmware online with a GUI interface similar to that of the Central EonOne.	LAN

List of Available Configurations

In addition to the firmware tool, you can configure your subsystem through the GUI-based EonOne.

Tool	System Configuration	Drive Configuration	Event Notification	Data Replication*	Centralized Management
EonOne	Yes	Yes	Yes	Yes	No
Central EonOne	Yes	Yes	Yes	Yes	Yes

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

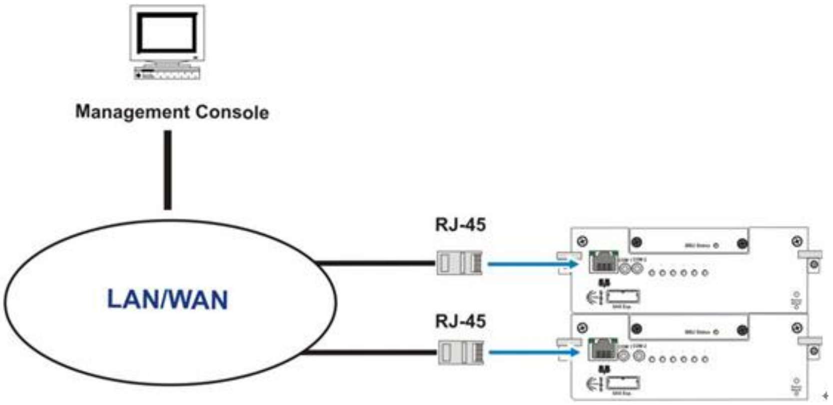
*Remote replication and disk roaming cannot be executed between EonStor DS and EonStor GS.

Establishing LAN Connection

Cabling

Before using the EonOne (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 EonStor GS/GSe 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 EonStor GS/GSe 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

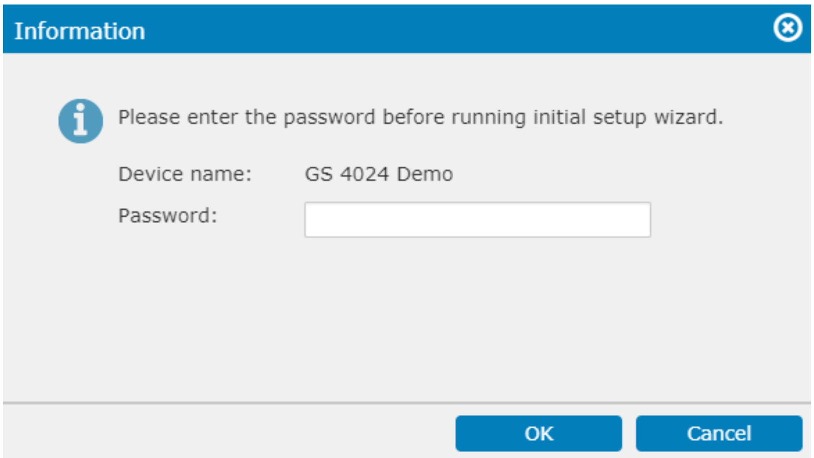
The firmware can be configured with a text user interface and can be accessed through a terminal emulator application such as PuTTY.

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 EonOne installation, during the first-time login, EonOne will automatically start the Initial Setup Wizard. It guides you through the process of configuring an EonStor GS/GSe 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 EonOne software and STORANDER 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.



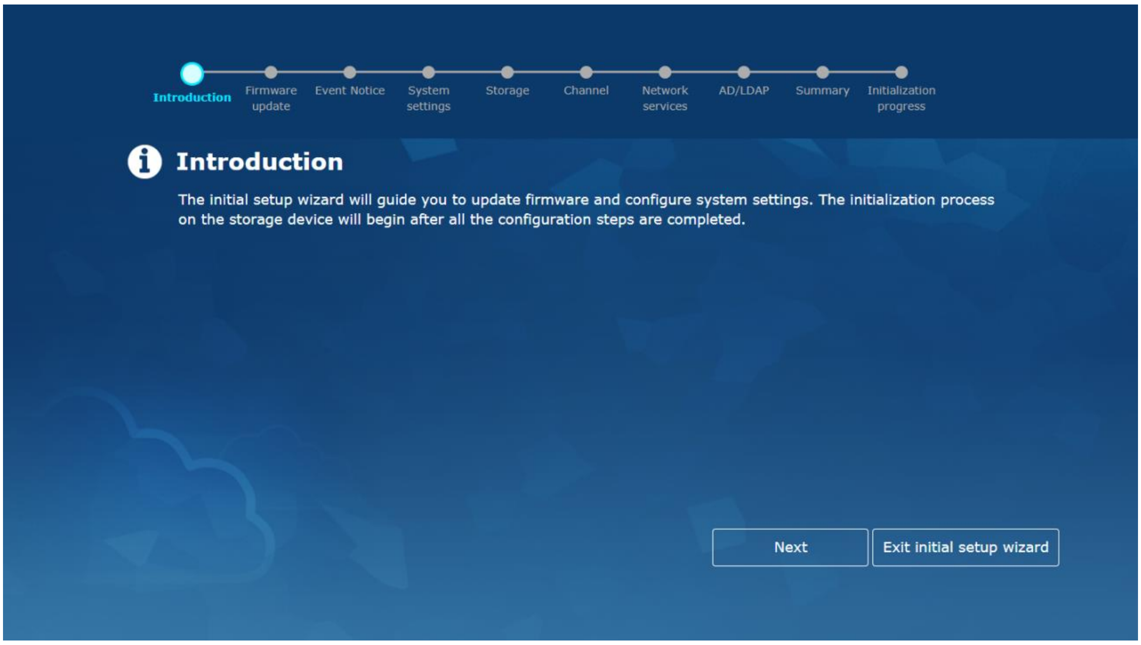
Information

Please enter the password before running initial setup wizard.

Device name: GS 4024 Demo

Password:

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



Introduction

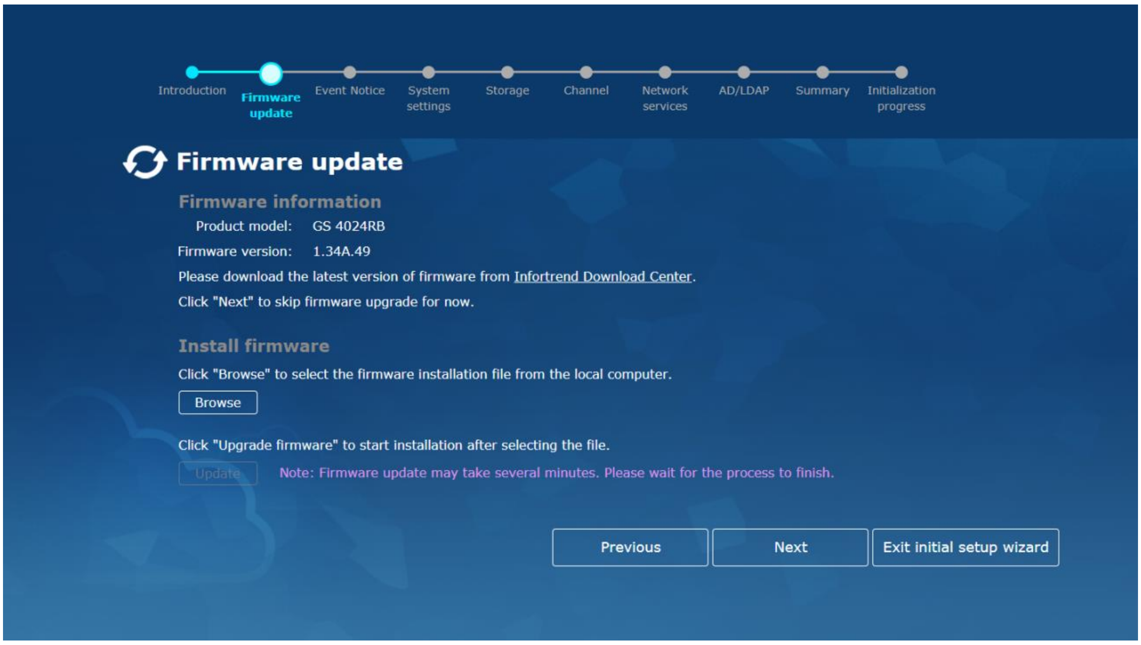
The initial setup wizard will guide you to update firmware and configure system settings. The initialization process on the storage device will begin after all the configuration steps are completed.

Step 1 - Firmware Update

To check or obtain the latest version of firmware, please go to Infortrend Download 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.



Firmware update

Firmware information

Product model: GS 4024RB

Firmware version: 1.34A.49

Please download the latest version of firmware from Infortrend Download Center.

Click "Next" to skip firmware upgrade for now.

Install firmware

Click "Browse" to select the firmware installation file from the local computer.

Click "Upgrade firmware" to start installation after selecting the file.

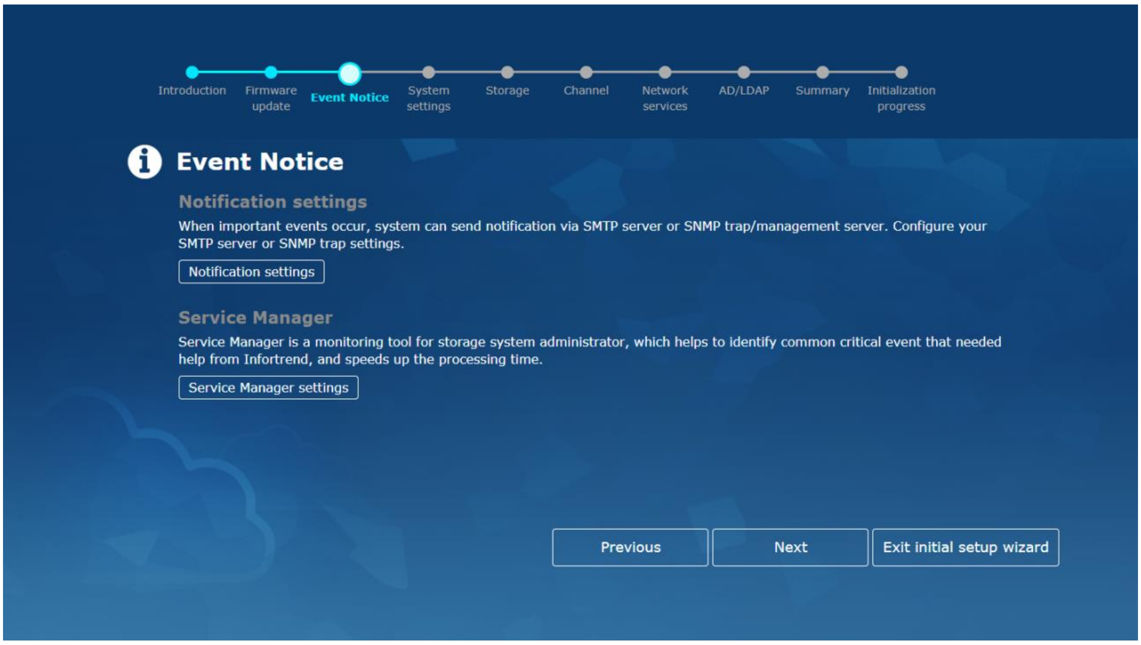
Note: Firmware update may take several minutes. Please wait for the process to finish.

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.



Event Notice

Notification settings

When important events occur, system can send notification via SMTP server or SNMP trap/management server. Configure your SMTP server or SNMP trap settings.

Service Manager

Service Manager is a monitoring tool for storage system administrator, which helps to identify common critical event that needed help from Infortrend, and speeds up the processing time.

Step 3 - System Settings

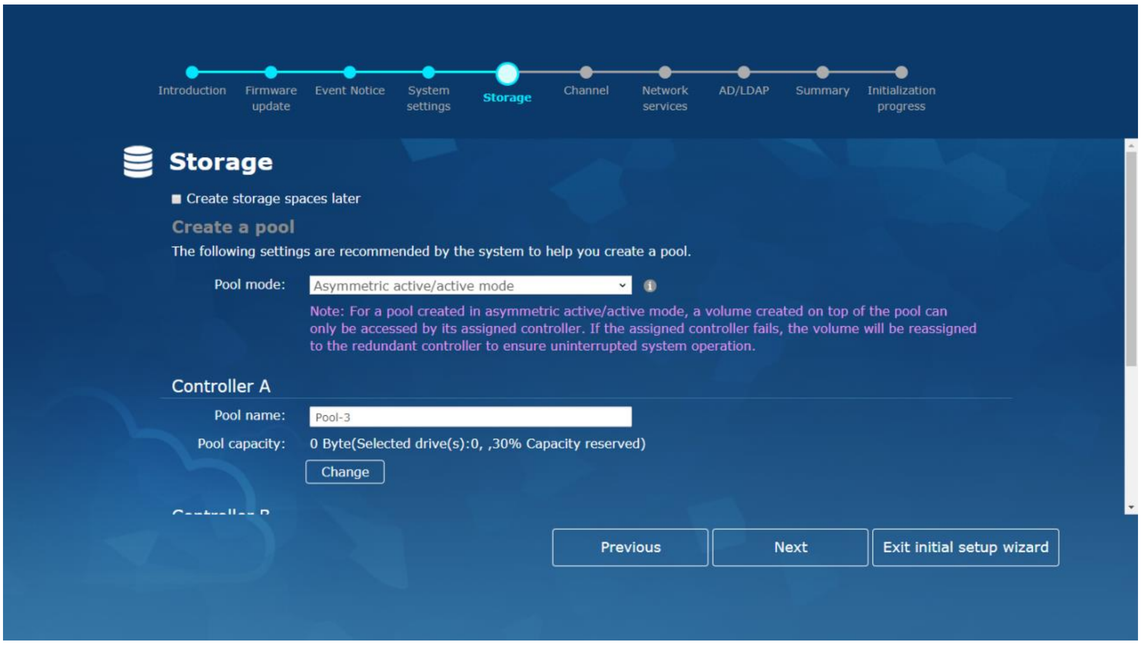
Set the system name, password for administrator, time and time zone for the device, configure DNS server(s), and specify how to optimize system performance.

You can improve storage capacity and performance by integrating several storage appliances into one file cluster. To create the scale-out cluster of one or more appliances, you can enable scale-out cluster and specify an identify name for the cluster. You can also enable file cluster to manage file-level data services in the cluster. When the file cluster is enabled, the system performance optimization will be set to **Better performance for file access service** by default.

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).

If the scale-out cluster is enabled in previous step, you can create the cluster pool as well as one or more cluster volumes in this step. If file cluster function is also enabled in previous step, you can configure the root shared folder here.



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)

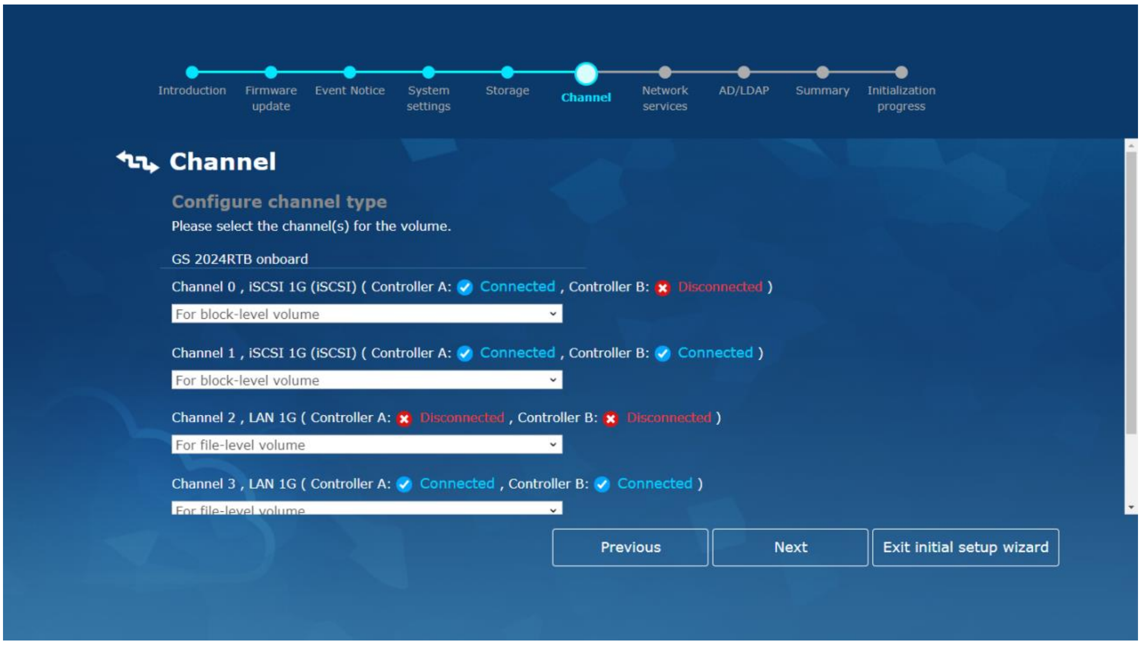
Controller B

Step 5 - Channel

EonOne currently manages EonStor GS/GSe systems via management ports. You should configure the data ports in the storage system in order to access the volumes. Since EonStor GS/GSe 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 EonOne, such as file explorer, proxy server, syslog server and VPN server, are accessible only through the data ports, not the management ports.



Channel

Configure channel type

Please select the channel(s) for the volume.

GS 2024RTB onboard

Channel 0 , iSCSI 1G (iSCSI) (Controller A: ✓ Connected , Controller B: ✗ Disconnected)

For block-level volume

Channel 1 , iSCSI 1G (iSCSI) (Controller A: ✓ Connected , Controller B: ✓ Connected)

For block-level volume

Channel 2 , LAN 1G (Controller A: ✗ Disconnected , Controller B: ✗ Disconnected)

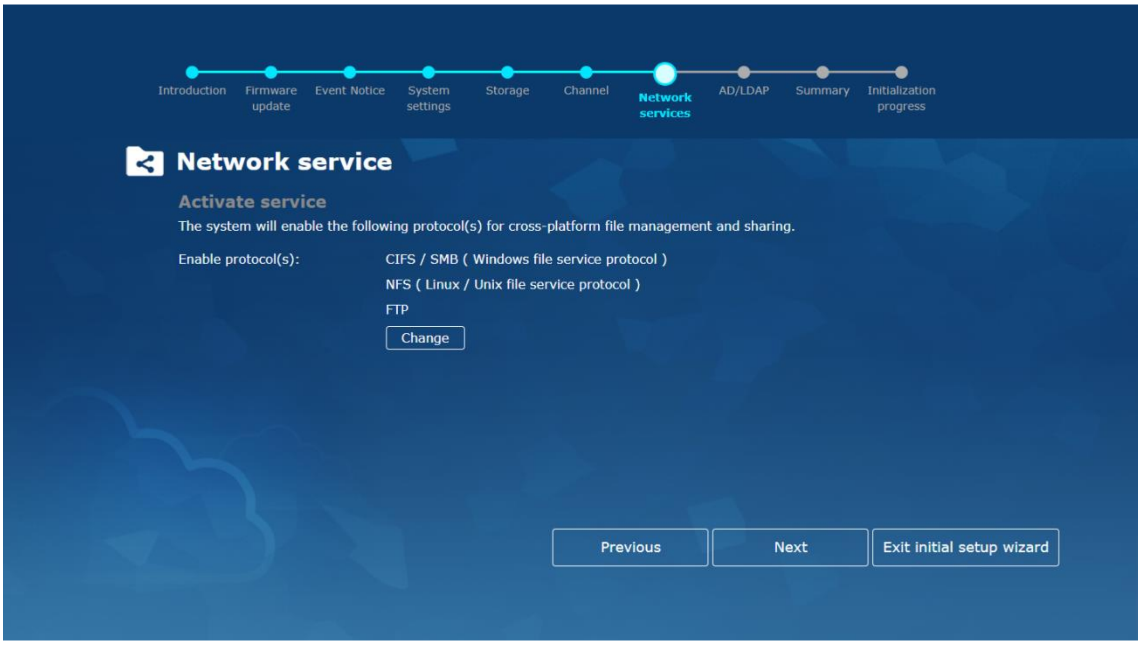
For file-level volume

Channel 3 , LAN 1G (Controller A: ✓ Connected , Controller B: ✓ Connected)

For file-level volume

Step 6 - Network Services

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



Network service

Activate service

The system will enable the following protocol(s) for cross-platform file management and sharing.

Enable protocol(s): CIFS / SMB (Windows file service protocol)
NFS (Linux / Unix file service protocol)
FTP

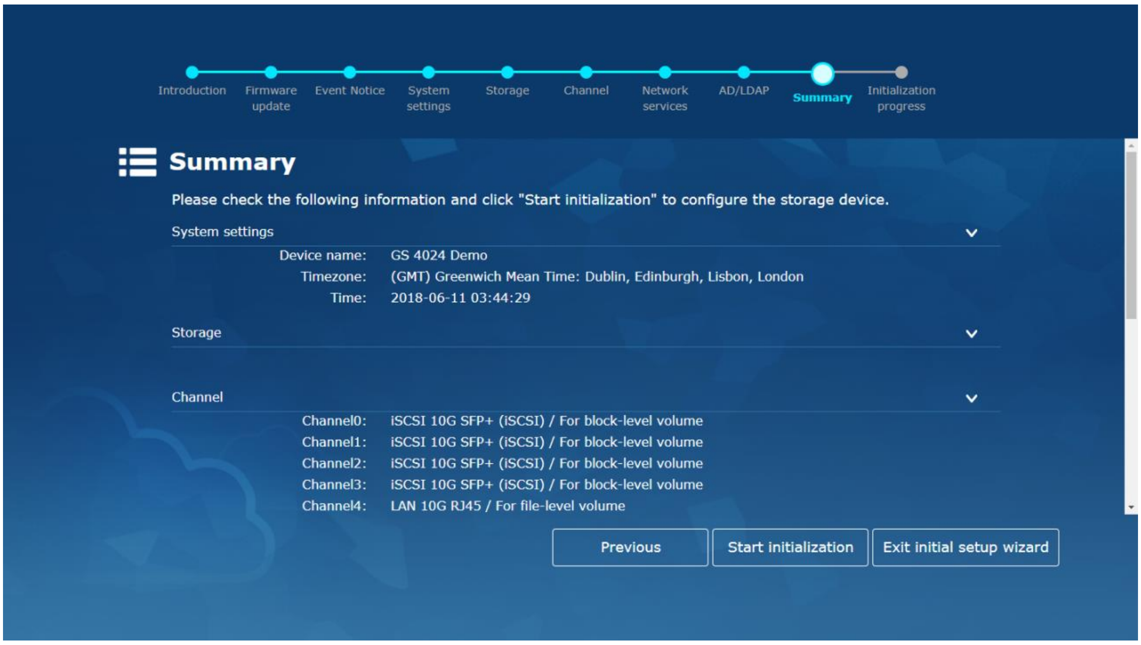
Step 7 - AD/LDAP

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.



Summary

Please check the following information and click "Start initialization" to configure the storage device.

System settings

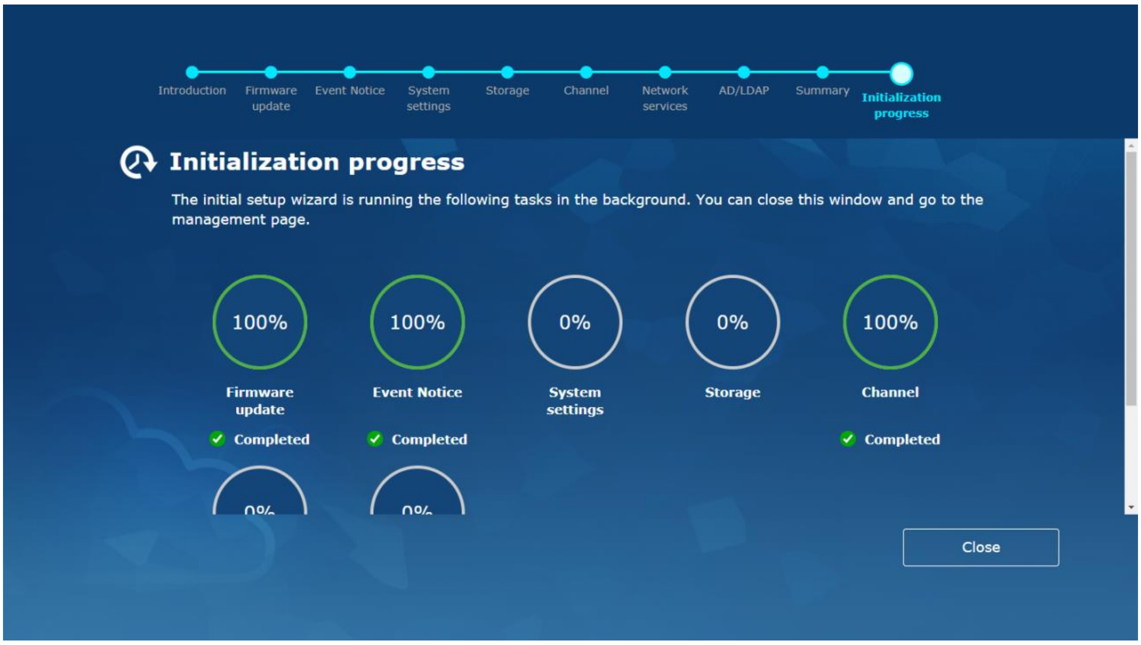
Device name: GS 4024 Demo
Timezone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Time: 2018-06-11 03:44:29

Storage

Channel

Channel0: iSCSI 10G SFP+ (iSCSI) / For block-level volume
Channel1: iSCSI 10G SFP+ (iSCSI) / For block-level volume
Channel2: iSCSI 10G SFP+ (iSCSI) / For block-level volume
Channel3: iSCSI 10G SFP+ (iSCSI) / For block-level volume
Channel4: LAN 10G RJ45 / For file-level volume

The progress of each task is displayed. You can close the window and continue to configure another - EonStor GS/GSe device or go to the EonOne management page.



Initialization progress

The initial setup wizard is running the following tasks in the background. You can close this window and go to the management page.

100% Firmware update ✓ Completed
100% Event Notice ✓ Completed
0% System settings
0% Storage
100% Channel ✓ Completed
0%
0%

Calibration Wizard

Overview

If you exit the initial setup wizard without completing all the settings, the calibration wizard guides you through the rest of the settings to ensure optimal system performance.

1. When the wizard appears, click **Next** to calibrate one or both system settings:

   Default route:

Choose a network channel	Choose a network channel from the menu as the default route. The system uses the default route to communicate data with external systems. To keep the system for internal access only, select **None**.
Edit	Click to change the selected network channel’s configurations.
Refresh	Click to refresh the menu.

   System time:

Time zone	Choose a time zone from the menu for the system. To update information of the chosen time zone via the Internet, select **Automatically update time zone information (Internet connection required)**.
Adjust daylight saving time	Turn on this function to allow the system to automatically update daylight saving time. Click **Edit** to choose an update policy: **Automatically adjust daylight saving time**: The system updates the daylight saving time automatically. **Customize**: Specify the start time and end time to apply daylight saving time. Then, choose the time offset.

2. Click **OK** to save the settings.
3. Click **Next** and then **Close** to finish the calibration.

Navigating User Interface

Overview

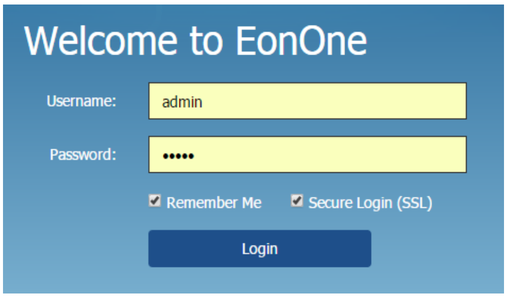
In this section, you can learn about the basic GUI elements of the EonOne management suite.

Logging into/Logging out of EonOne UI

To open the EonOne software in the browser, double click the EonOne 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.)



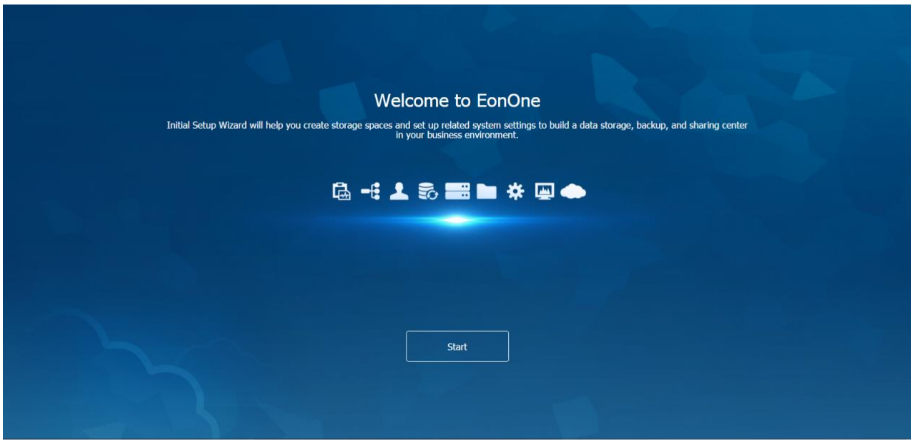
Welcome to EonOne

Username: admin

Password: •••••

☑ Remember Me ☑ Secure Login (SSL)

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

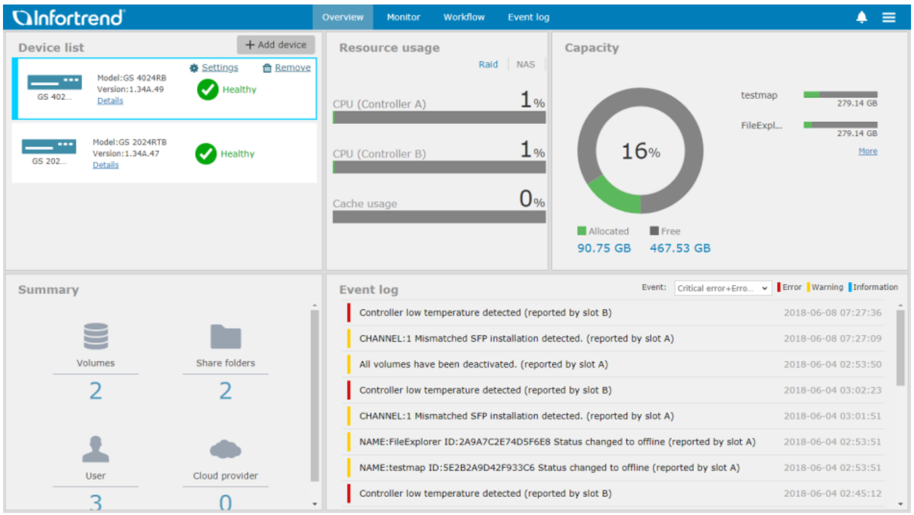


Welcome to EonOne

Initial Setup Wizard will help you create storage spaces and set up related system settings to build a data storage, backup, and sharing center in your business environment.

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.



```
Controller low temperature detected (reported by slot B)                                2018-06-08 07:27:36
CHANNEL:1 Mismatched SFP installation detected. (reported by slot A)                    2018-06-08 07:27:09
All volumes have been deactivated. (reported by slot A)                                 2018-06-04 02:53:50
Controller low temperature detected (reported by slot B)                                2018-06-04 03:02:23
CHANNEL:1 Mismatched SFP installation detected. (reported by slot A)                    2018-06-04 03:01:51
NAME:FileExplorer ID:2A9A7C2E74D5F6E8 Status changed to offline (reported by slot A)    2018-06-04 02:53:51
NAME:testmap ID:5E2B2A9D42F933C6 Status changed to offline (reported by slot A)         2018-06-04 02:53:51
Controller low temperature detected (reported by slot B)                                2018-06-04 02:45:12
```

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

Changing EonOne Login Password via EonOne

You can change the EonOne login password or set a new password for storage subsystems.

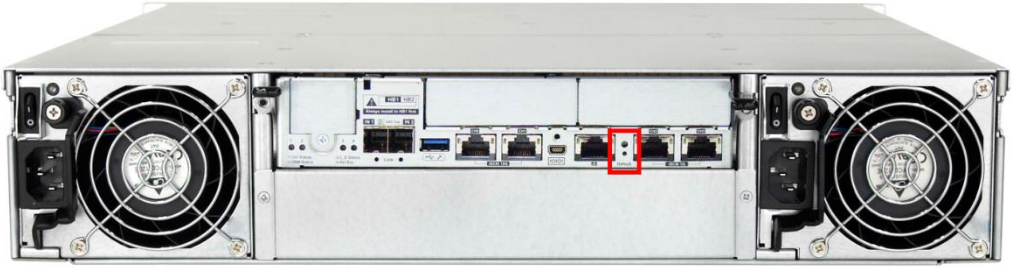
Go to	**Menu Icon > Admin > Change the password**
Changing EonOne Login Password	Enter the old password and new password (twice for confirmation) in the pop-up window. The default login password is “**admin**”. For an embedded system, the login password and the system’s storage device password (in **Settings** > **System** > **General** > **Storage device password**) share the same value.

Changing EonOne Login Password via Default Button

You can change the EonOne 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 EonOne Login Password

The EonOne and the terminal login password will be reset. Their default login passwords are both “**admin**”.

User Interface

Display Elements	Description
Top Menu Bar > Navigation	Switch between the **Overview**, **Monitor**, and **Event Log** pages by clicking the navigation buttons on the top menu bar.
Top Menu Bar > System Setting	☰ The system settings include: **administrator (admin)**, **Language**, **Service Manager**, **Certification**, **Help**, **Logout**. ● **Admin** Select the administrator setting button to change the display language and the EonOne login password. ● **Language** Choose the display language that you prefer. ● **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 EonOne software) via the Help button. ● **Logout** Log out of the EonOne software and go back to the login page.
Top Menu Bar > Notification	🔔 The notification setting button allows users to set their notification rule and information.
Top Menu Bar > Settings	⚙ The device settings contains links that enable users to set detailed configurations for EonStor GS/GSe devices, including System Settings, Data

Access Configurations, Account Privilege Settings, Storage Provisioning, Data Protection, Applications, Update & Security, EonCloud Gateway, Initial Setup Wizard, Cluster, and HA service.

Scale-out cluster device list

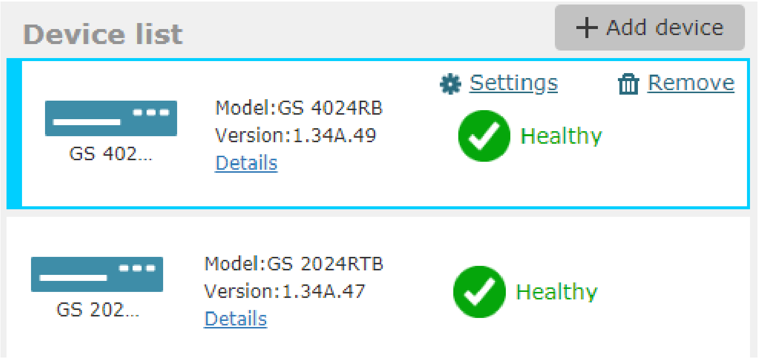
When the scale-out cluster is enabled, you can click the drop-down menu to switch the overviews between the cluster and a specific appliance in the cluster.

When HA service is enabled, you can click the drop-down menu to switch from one storage device to the other to view and manage the two devices.

Device information

Device list shows the EonStor GS/GSes that currently have connection with the EonOne. You can add a new EonStor GS/GSe by clicking **Add Device**, or you can configure the device setting for already added EonStor GS/GSe.

The **Add Device** button is only available on Central EonOne.



Model:GS 4024RB
Version:1.34A.49

Model:GS 2024RTB
Version:1.34A.47

Cluster settings
When the scale-out cluster is enabled, the button contains links that enable users to set detailed configurations for the scale-out cluster, including System Settings, Appliance, Account Privilege Settings, Storage Provisioning, Scheduling & Backup, and Update.

Device Management
When the scale-out cluster is enabled, there will be one or more columns to indicate the status of each appliance in the cluster. The device settings button **Device Management** will be displayed in the columns for users to access detailed configurations as **Settings** does.

Performance Quick Monitor

Performance Quick Monitor shows the usage of CPU, memory and SSD cache for a connected EonStor GS/GSe.

Capacity Usage Quick Monitor

Capacity Usage Quick Monitor shows a brief summary of capacity usage rate of a connected EonStor GS/GSe.

Storage Summary	Storage Summary shows a brief summary of configured volumes, shared folders, and cloud spaces.
Application status	Some add-on applications support to display an overview here. You can click **Details** to learn more information respectively.
Events Quick View	Events Quick View shows the current warnings, errors, and information of a connected device.

Setting up EonOne with Multi-factor Authentication (MFA)

With MFA, you add an extra layer of protection to your account. After completing the setup of MFA, you will log into your account in two steps using your password and your mobile device / email / backup code.

Before enabling the function, install an authenticator app on your mobile device first. The following apps are supported: Google Authenticator, Microsoft Authenticator, FreeOTP Authenticator, and Twilio Authy.

Note:

- If the scale-out cluster is enabled, MFA settings are only available on the master appliance. After enabling MFA, it requires two steps to log into all appliances in the cluster.
- Central EonOne is not supported using email to receive verification codes. On Embedded EonOne, you must set up SMTP server so that you can receive verification codes via email. To set up SMTP server, refer to “Email notification” in Notification.
- The backup code will be displayed after the setup is completed. Record the backup code and keep it in a safe place.
- When you use the backup code to log into your account, after logging in, MFA will be disabled.

Go to	**Menu Icon > Admin > Multi-factor authentication**
Setup	1. Turn on this function with the toggle. 2. The account and its security key will be then displayed along with a QR code. Scan the QR code with an authenticator app, or enter the account information into the app. After scanning or specifying the information on the app, a verification code will be displayed on the app. 3. On Embedded EonOne, specify an email address. This enables you to receive a verification code via email when you cannot receive the code via an app. Click **Send**. Later, you can check if a mail is sent to the email address you specified. 4. Enter the verification code and click **Verify**. 5. If the verification is successful, the backup code will be displayed below. You must record the backup code and keep it in a safe place. When you cannot receive the verification code via an app or email, you can verify yourself by entering the backup code. 6. Click **Apply** to complete the settings.
Changing the email	If needed, on Embedded EonOne, you can change the email address.

address	1. Specify another email address. 2. Click **Send**. Later, you can check if a mail is sent to the email address you specified. 3. Click **Apply** to complete the settings.

Logging into EonOne with MFA

In addition to your username and password, after MFA is enabled, you must log into EonOne with verification codes or the backup code.

Note: No matter you receive the verification code from the authenticator app or the email, the verification code will expire after a certain time period. It is recommended that you always enter the latest one to verify yourself.

Using a verification code with the authenticator app

1. Log into EonOne with your username and password. Click **Login**.
1. The multi-factor authentication page will be displayed. On your mobile device, tap the icon to open the authenticator app. Check the verification code displayed along with your account.
2. On the multi-factor authentication page, enter the verification code.
3. Click **Verify**.

Using a verification code with your email

1. Log into EonOne with your username and password. Click **Login**.
2. The multi-factor authentication page will be displayed. Click **Send me the verification code by mail**. A code will be sent to the email address that is specified on the setting page. Check the inbox for the code.
3. On the multi-factor authentication page, enter the verification code.
4. Click **Verify**.

Using the backup code

1. Log into EonOne with your username and password. Click **Login**.
2. The multi-factor authentication page will be displayed. Click **Verify with the backup code**.
3. Enter the backup code.
4. Click **Verify**.

Administrator Privilege

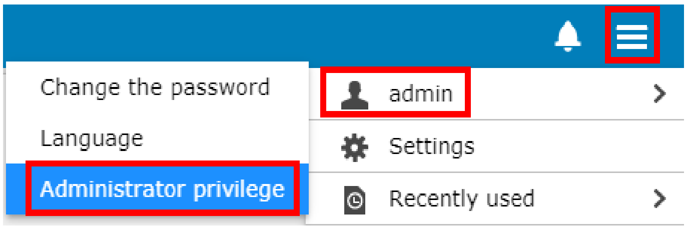
Three types of administrator accounts with different privileges are available, including super administrator, power administrator, and general administrator. Refer to the following table for their limit numbers and authorized actions.

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 EonOne**.

Go to

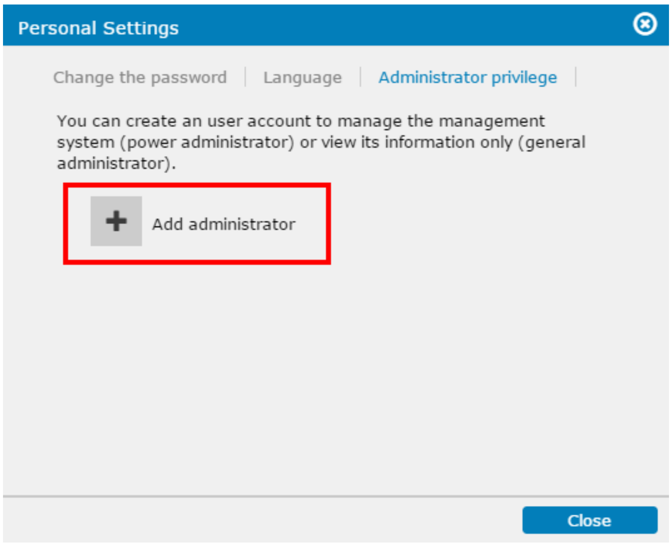
Menu Icon > Admin > Administrator privilege



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

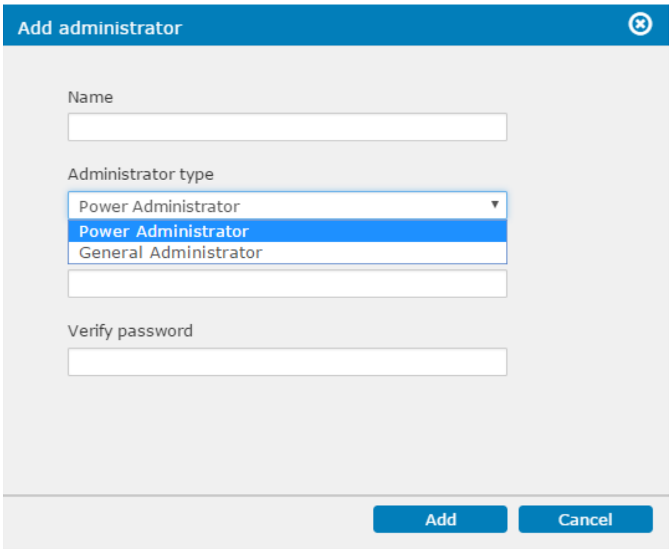
Add an administrator

After clicking **Administrator privilege**, you will see the following window. Click **Add administrator** to add an administrator account on EonOne.



You can create an user account to manage the management system (power administrator) or view its information only (general administrator).

Then, you will see the following window.



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.

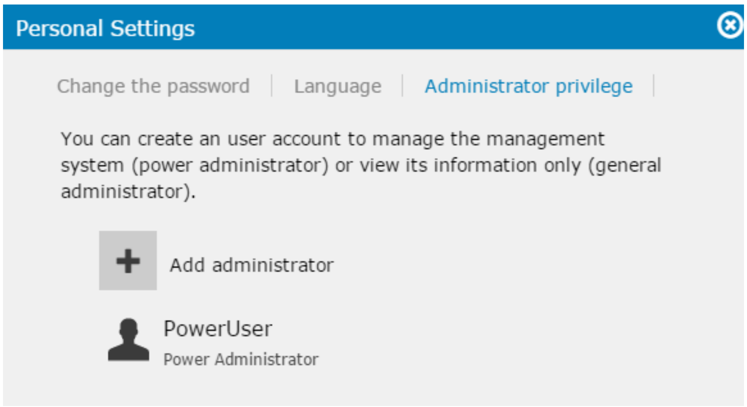
Note:

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 EonOne.
2. A general administrator only has permission to view the settings on the EonOne 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.



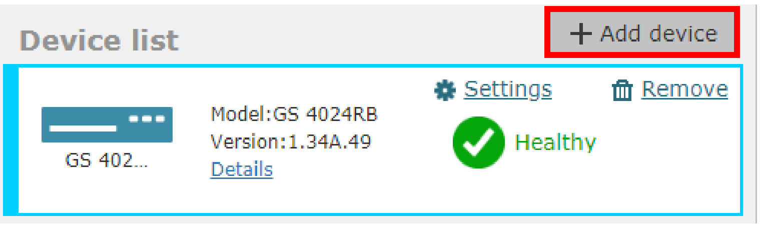
Personal Settings

You can create an user account to manage the management system (power administrator) or view its information only (general administrator).

Adding/Logging into/Removing a Device

Go to

Device List > Add Device



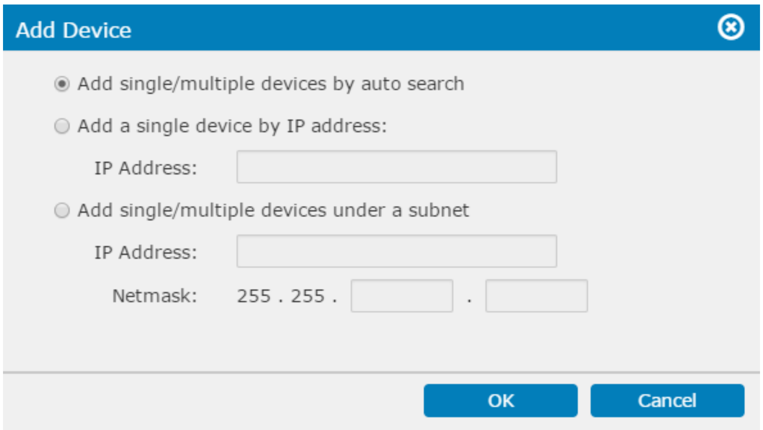
Device list

GS 402...

Model:GS 4024RB
Version:1.34A.49

Healthy

Add a device



Add Device

● Add single/multiple devices by auto search

○ Add a single device by IP address:

IP Address:

○ Add single/multiple devices under a subnet

IP Address:

Netmask: 255 . 255 . .

1. Choose a method to connect to a EonStor GS/GSe

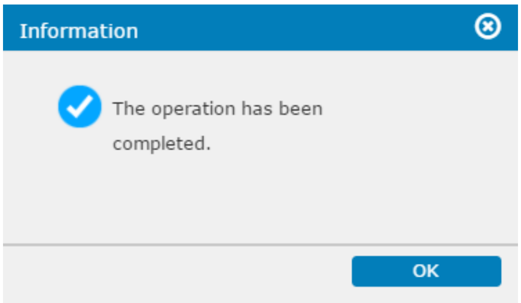
   a) Add single/multiple devices by auto search – the system will automatically search for connected device(s).

   b) Add a single device by IP address – enter the IP address of the EonStor GS/GSe.

   c) Add single/multiple devices under a subnet – enter the starting IP address and Netmask to automatically connect all EonStor GS/GSes within a subnet.

2. Click **OK**.

3. If all information is correct, the pop-up message below will be displayed.

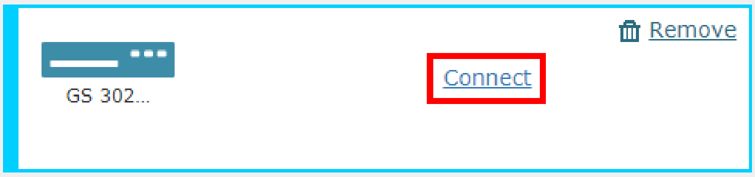


Information

The operation has been completed.

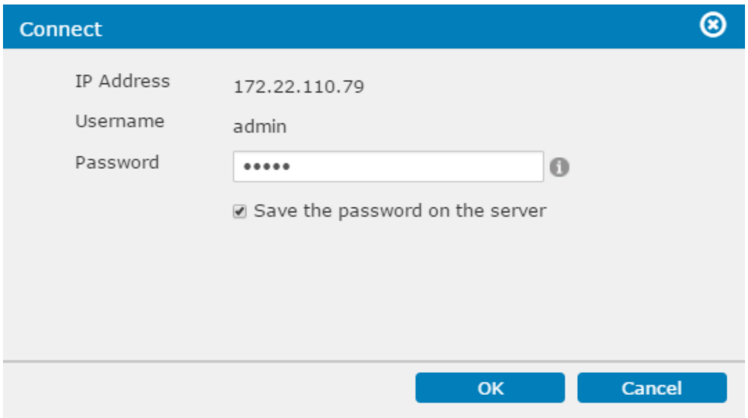
Connect to a device

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.


Connect

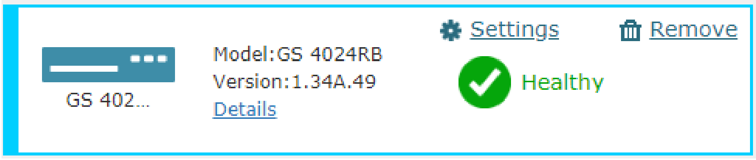
IP Address 172.22.110.79

Username admin

Password •••••

☑ Save the password on the server

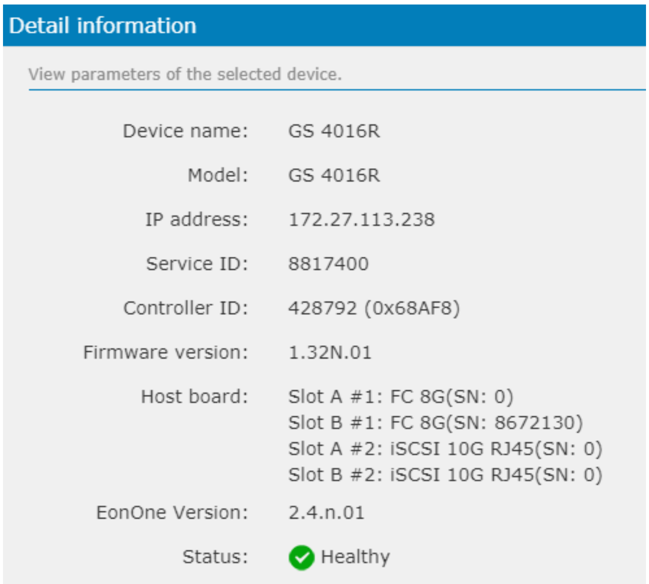
2. The device status will appear, including the model name, firmware version and the working status.


GS 402...

Model:GS 4024RB

Version:1.34A.49

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

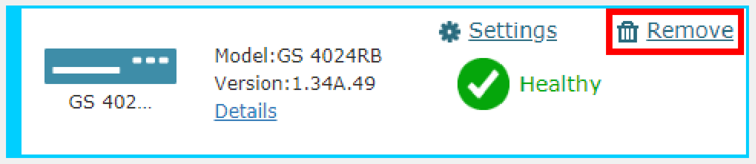

Detail information

View parameters of the selected device.

Device name:	GS 4016R
Model:	GS 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

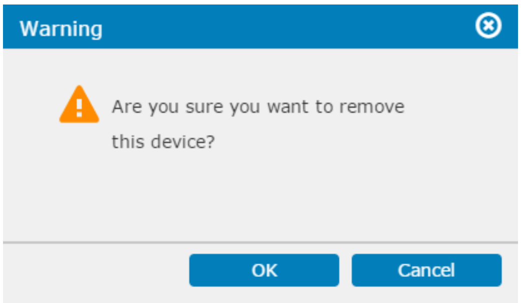
Remove a device

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



Model:GS 4024RB
Version:1.34A.49
Details

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



Are you sure you want to remove this device?

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.

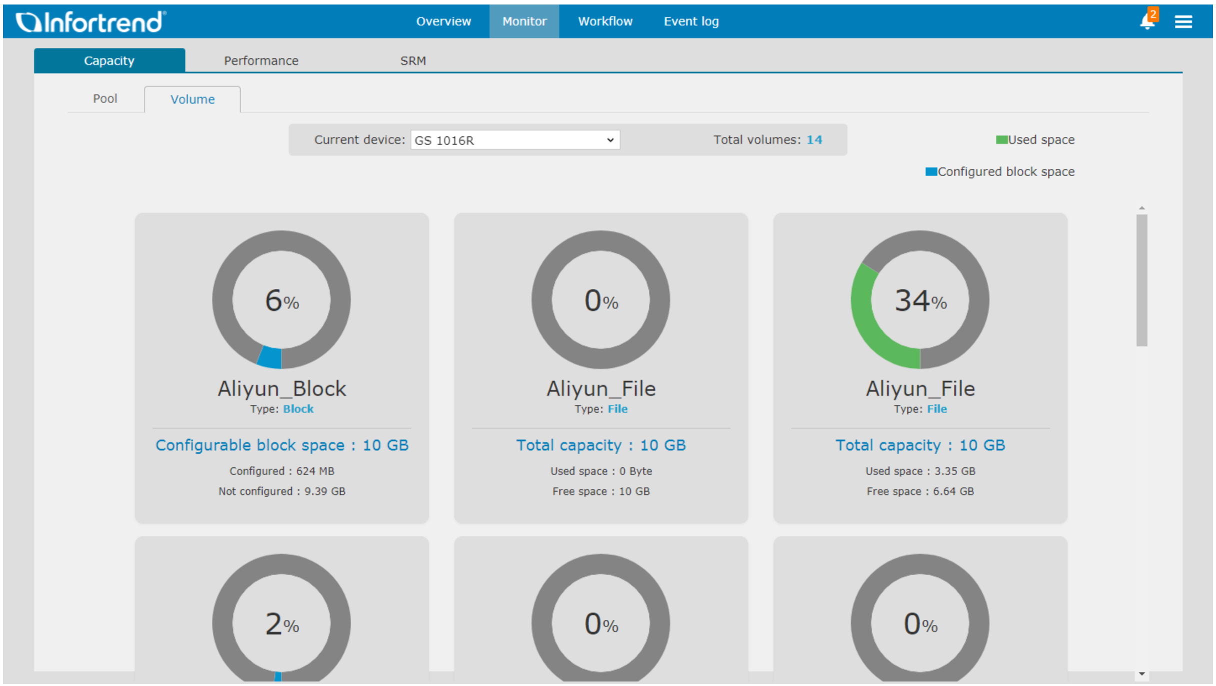
Steps

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 EonStor GS/GSe devices.



Current device: GS 1016R

Total volumes: 14

🟩Used space

🟦Configured block space

6%
Aliyun_Block
Type: Block
Configurable block space : 10 GB
Configured : 624 MB
Not configured : 9.39 GB

0%
Aliyun_File
Type: File
Total capacity : 10 GB
Used space : 0 Byte
Free space : 10 GB

34%
Aliyun_File
Type: File
Total capacity : 10 GB
Used space : 3.35 GB
Free space : 6.64 GB

2%

0%

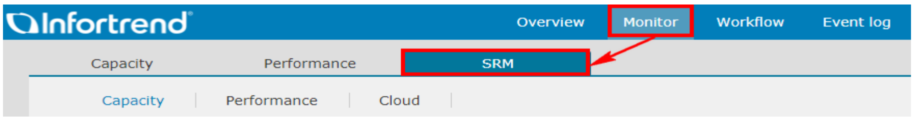
0%

Storage Resource Management (SRM)

The main purpose of SRM is to allow users to monitor the usage of STORANDER 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 EonOne.

Go to

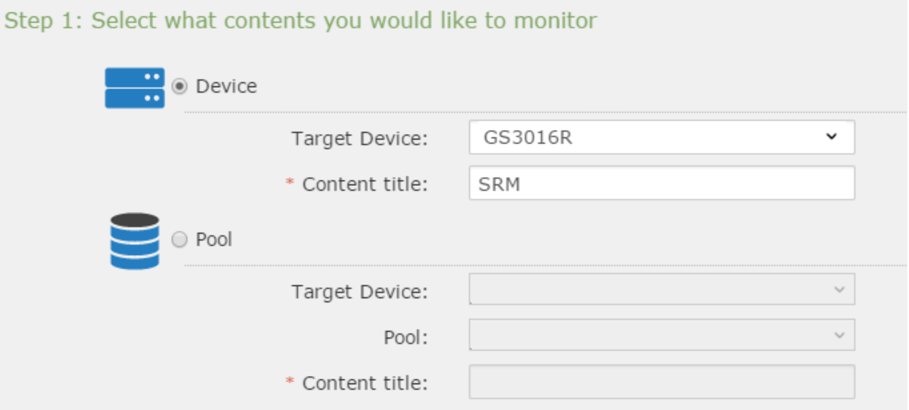
Monitor > SRM



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: GS3016R

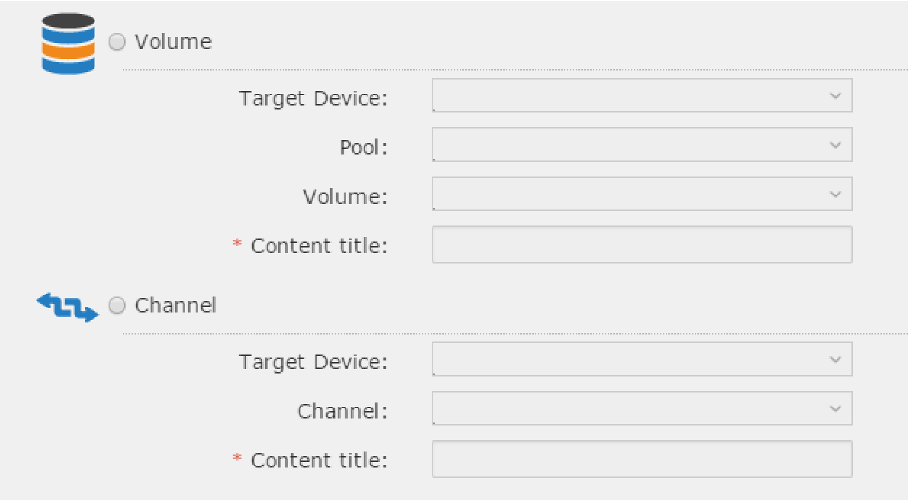
* Content title: SRM

○ Pool

Target Device:

Pool:

* Content title:



○ Volume

Target Device:

Pool:

Volume:

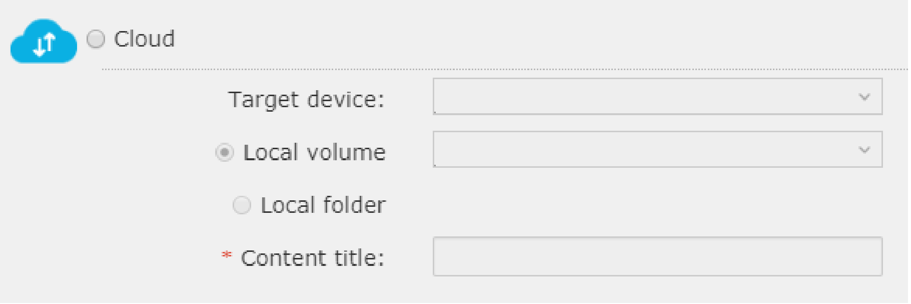
* Content title:

○ Channel

Target Device:

Channel:

* Content title:



○ Cloud

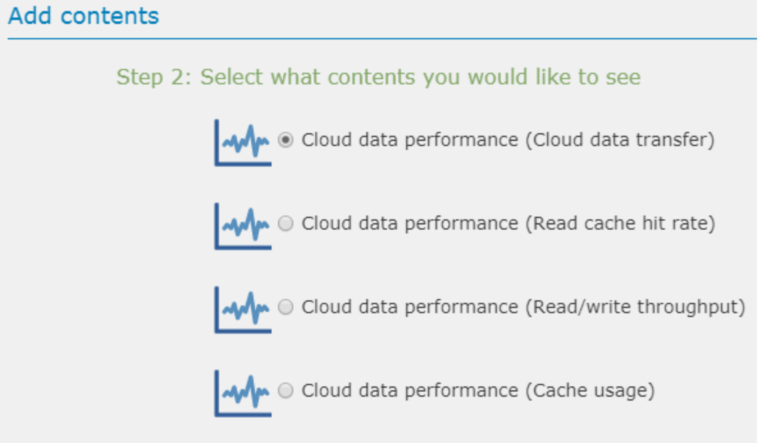
Target device:

● 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

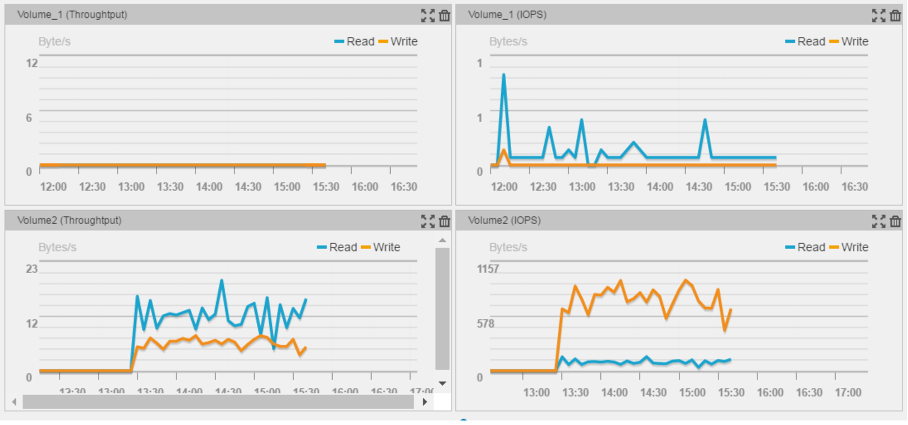
● Cloud data performance (Cloud data transfer)

○ Cloud data performance (Read cache hit rate)

○ Cloud data performance (Read/write throughput)

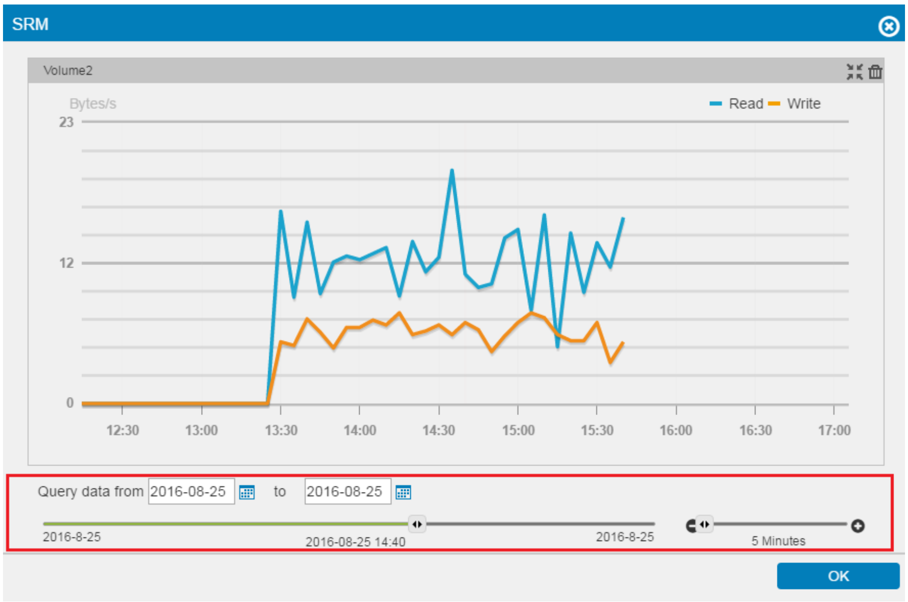
○ Cloud data performance (Cache usage)

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



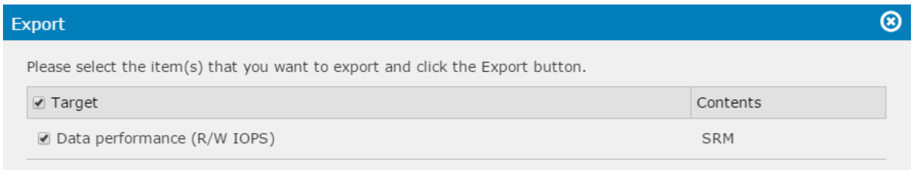
Configure an SRM diagram

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



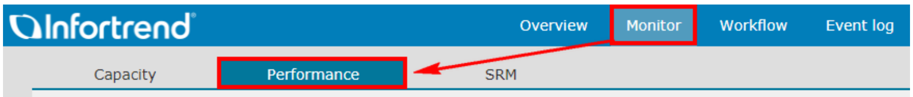
Please select the item(s) that you want to export and click the Export button.

☑ Target	Contents
☑ Data performance (R/W IOPS)	SRM

Monitoring Storage Performance

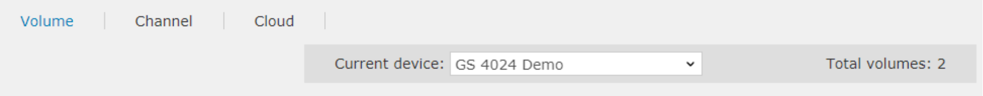
Go to

Monitor > Performance



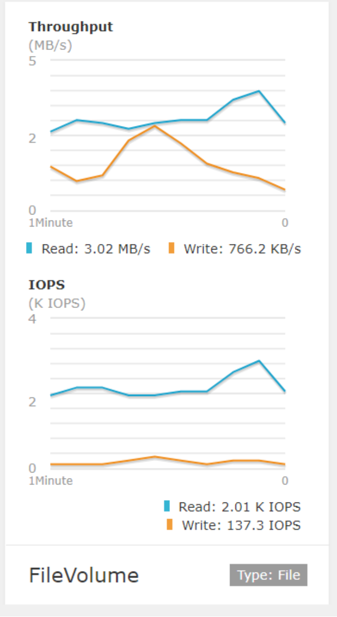
Monitor storage performance (Volume)

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



Current device: GS 4024 Demo

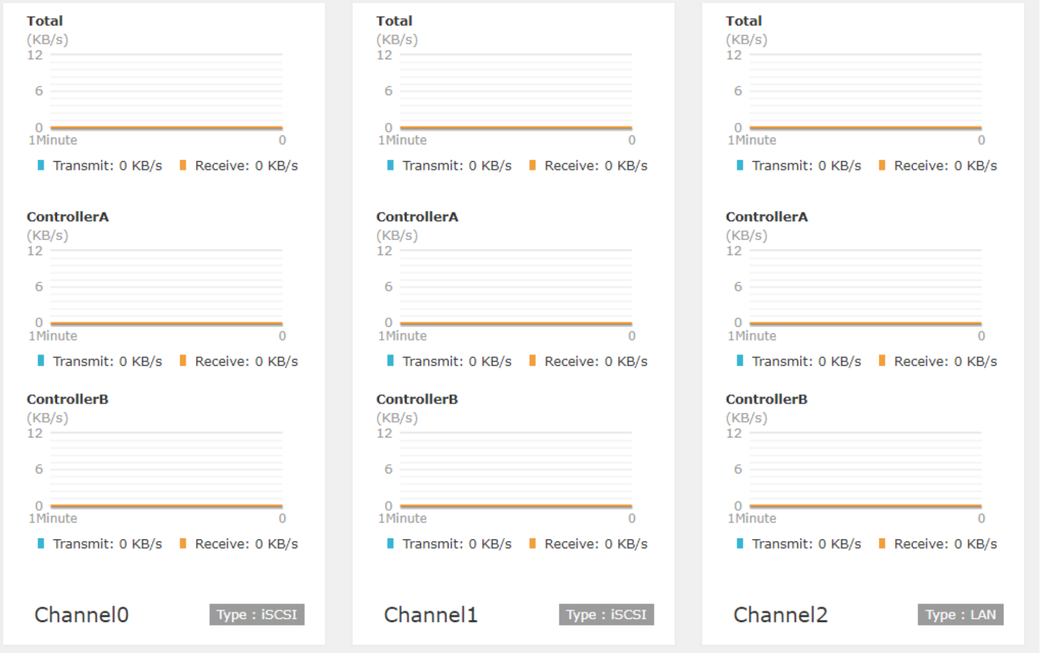
Total volumes: 2



Monitor storage performance (Channel)

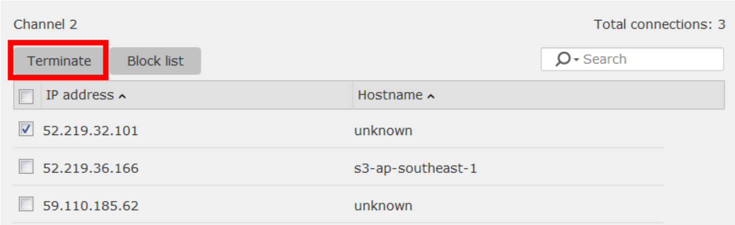
Click the **Channel** tab and select the device. Each channel's data transfer status is displayed in charts.

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**.

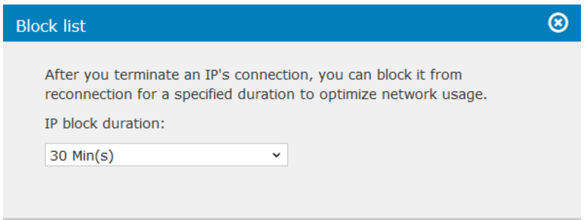


Channel 2

Total connections: 3

	IP address ▴	Hostname ▴
☑	52.219.32.101	unknown
□	52.219.36.166	s3-ap-southeast-1
□	59.110.185.62	unknown

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.



Block list

After you terminate an IP's connection, you can block it from reconnection for a specified duration to optimize network usage.

IP block duration: 30 Min(s)

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

Monitor drive performance

1. Go to **Filters** to set filters to show desired performance data:

   Device: Choose which device with controllers to sample its performance data.

   Enclosure: Choose the desired type of devices to sample their performance data. You may choose **Enclosure**, **Expansion enclosure**, or **All**.

   Type: Choose the type of data to display on the diagrams. You may choose **Latency**,

Rate, or **All**.

2. Go to **Sample settings** to define the sampling and diagram settings:

   Interval: Choose how often to sample the devices' performance data. You may choose **1 second**, **2 seconds**, **4 seconds**, or **8 seconds**.

   Display range: Define the maximum length of time for the diagrams. You may choose **30 seconds**, **60 seconds**, **90 seconds**, **120 seconds**, or **150 seconds**.

3. Click **Log settings** to specify the performance logging settings:

   Start time: Specify when to start the performance logging.

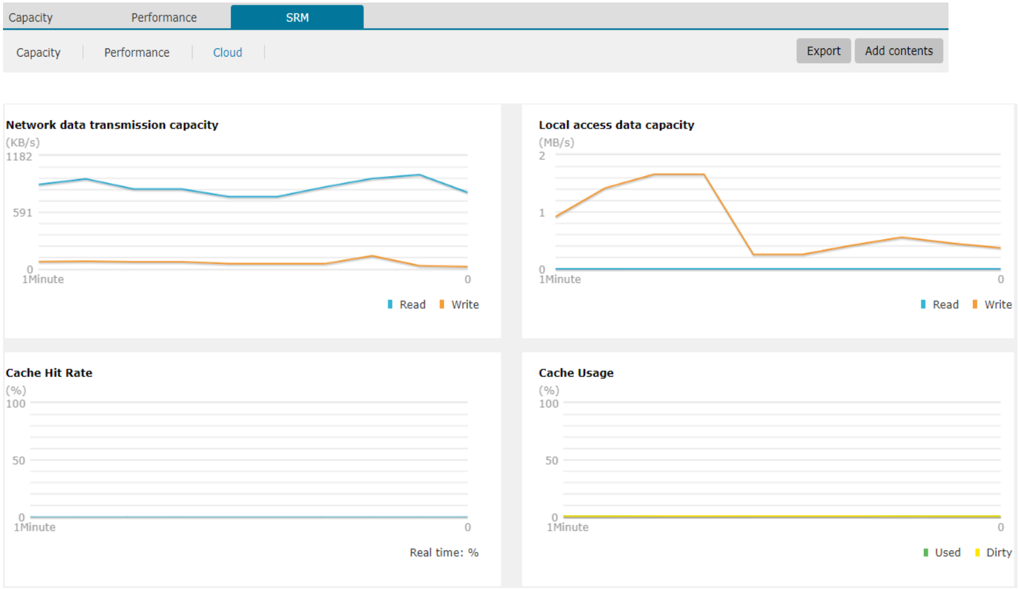
   End time: Specify when to end the performance logging.

   Log update: Specify how often to log the performance data.

   Click **OK** to activate performance logging. Then, you can export the logs by clicking **Export logs**. To stop logging, click **Stop logging**.

Monitor storage performance (Cloud Cache)

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.



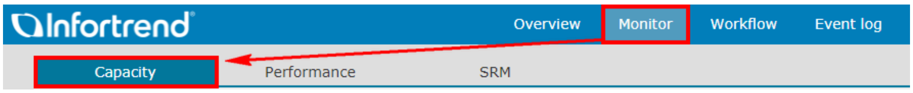
Monitor storage performance (HA storage)

After HA service is enabled, click **HA Volume** tab. The read/write throughput and IOPS of each HA volume will be displayed instantly in charts.

Monitoring Storage Capacity

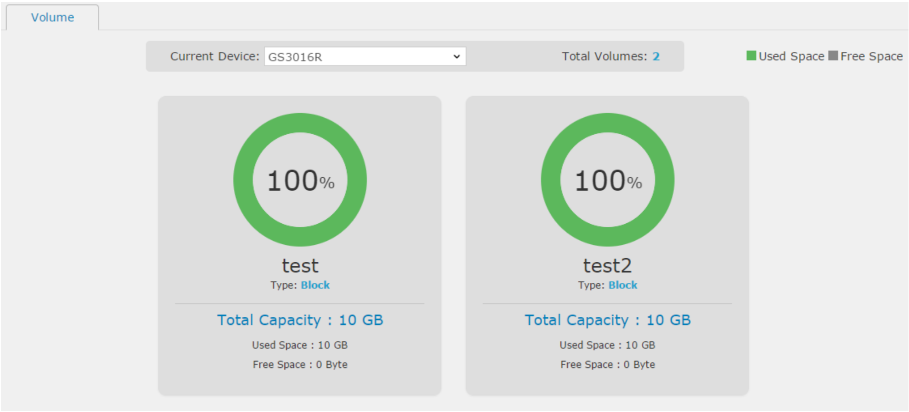
Go to

Monitor > Capacity



Monitor storage capacity

Volumes in your EonStor GS/GSe devices will be listed with their usage of capacity and type of volume shared.



Current Device: GS3016R

Total Volumes: 2

test
Type: Block
Total Capacity : 10 GB
Used Space : 10 GB
Free Space : 0 Byte

test2
Type: Block
Total Capacity : 10 GB
Used Space : 10 GB
Free Space : 0 Byte

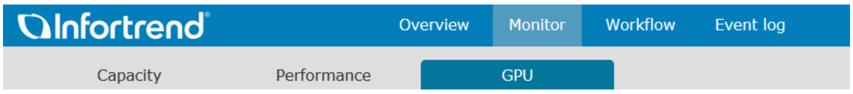
Monitor HA storage capacity

After HA service is enabled, the usage of capacity of each HA volume will be displayed.

Monitoring GPU Status

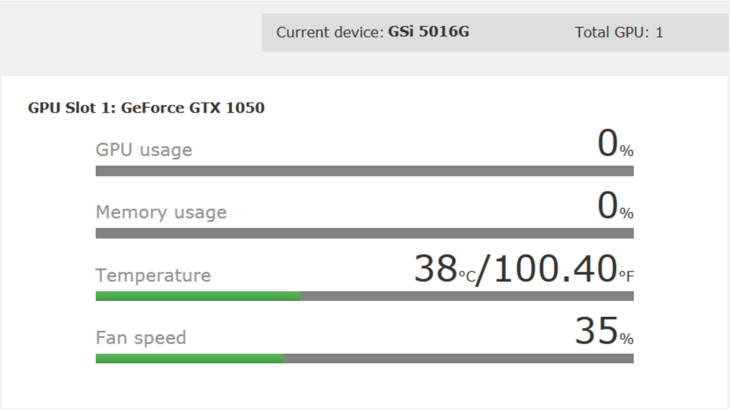
Go to

Monitor > GPU



Monitor GPU Status

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



Current device: **GSi 5016G** Total GPU: 1

GPU Slot 1: GeForce GTX 1050

GPU usage 0%

Memory usage 0%

Temperature 38°C/100.40°F

Fan speed 35%

Note

This function is only supported on the GSi series.

Monitoring Client Connections

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

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.

Monitoring Application Status

You can have an overview when some add-on applications are enabled. These applications include Antivirus, Backup server, Syslog server, and VPN server.

Click the application tab to gain an overview respectively.

Event Log

The EonOne 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

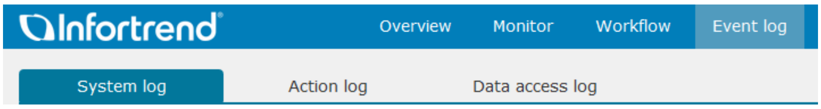
Events can be categorized by (1) their scope and (2) their severity. For the detailed list of events and their descriptions, see the Troubleshooting Guide. Contact Support to obtain the guide.

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.

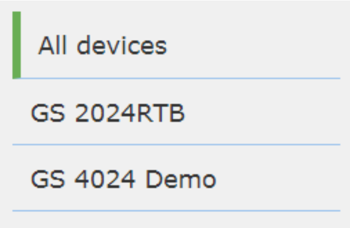
System Log

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

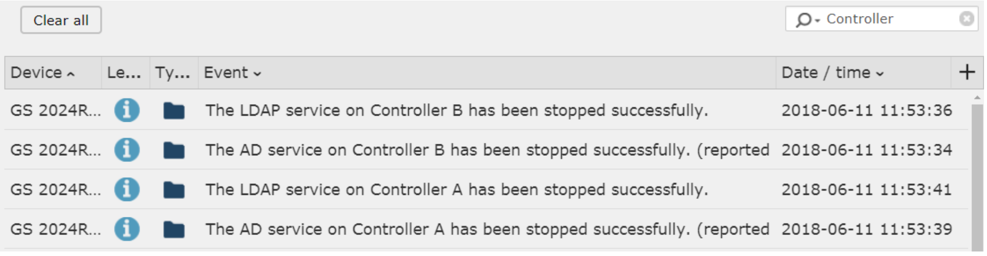


System log

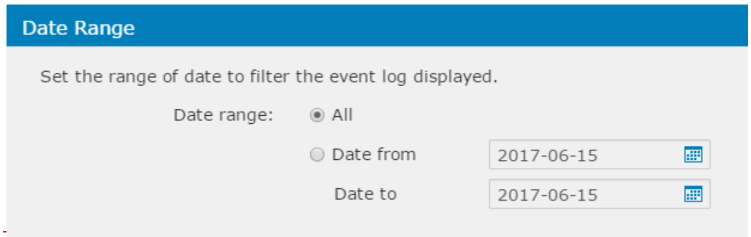
1. Select a specific device or all devices by default.



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



Device	Le...	Ty...	Event	Date / time
GS 2024R...	ℹ	▬	The LDAP service on Controller B has been stopped successfully.	2018-06-11 11:53:36
GS 2024R...	ℹ	▬	The AD service on Controller B has been stopped successfully. (reported	2018-06-11 11:53:34
GS 2024R...	ℹ	▬	The LDAP service on Controller A has been stopped successfully.	2018-06-11 11:53:41
GS 2024R...	ℹ	▬	The AD service on Controller A has been stopped successfully. (reported	2018-06-11 11:53:39


Date Range

Set the range of date to filter the event log displayed.

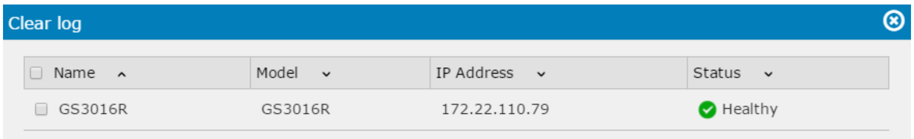
Date range: ● All

○ Date from 2017-06-15

Date to 2017-06-15

Clear system log

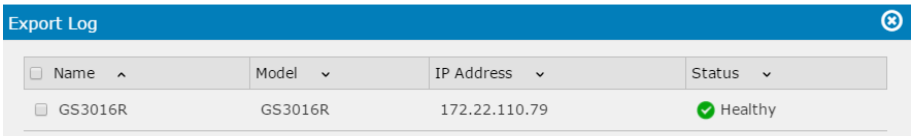
Click the **Clear all** button, select the device(s), and click **OK**. The system log of the device(s) will be cleared.


Clear log

□ Name	Model	IP Address	Status
□ GS3016R	GS3016R	172.22.110.79	✓ Healthy

Download system log

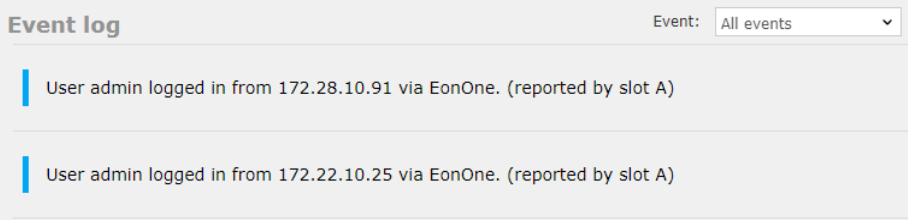
Click the **Download** button, select a device and click **OK**. The EonOne will start downloading the system log of the device as a .zip file.


Export Log

□ Name	Model	IP Address	Status
□ GS3016R	GS3016R	172.22.110.79	✓ Healthy

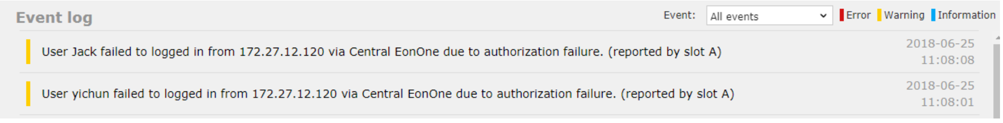
Event Login Log

When user log into EonOne, the Event log will show the history of the user login:



```
User admin logged in from 172.28.10.91 via EonOne. (reported by slot A)
User admin logged in from 172.22.10.25 via EonOne. (reported by slot A)
```

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



```
User Jack failed to logged in from 172.27.12.120 via Central EonOne due to authorization failure. (reported by slot A)      2018-06-25
                                                                                                                          11:08:08
User yichun failed to logged in from 172.27.12.120 via Central EonOne due to authorization failure. (reported by slot A)    2018-06-25
                                                                                                                          11:08:01
```

Forward system logs

The system can forward its system logs to a remote syslog server for backup purposes.

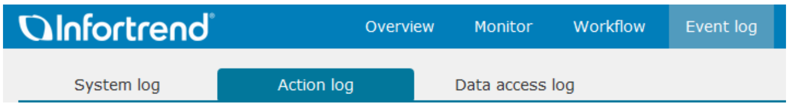
1. Click **Forward**.
2. Select **Enable log forwarding** and specify the settings

Server	Specify the IP address of the remote syslog server.
Transfer protocol	Choose a protocol for transferring system logs: **UDP**.
Port	Specify the port on the remote syslog server for receiving logs.
Log format	Choose a log format accepted by the remote syslog server: **RFC3164** or **RFC5424**.
Severity level	Choose the types of system logs by severity level to forward to the remote syslog server.

3. Click **Send test log** to see if the above settings are correct.
4. Click **OK** to save the settings.

Action Log

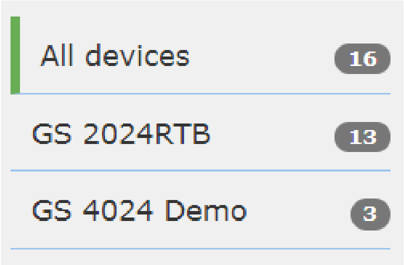
Go to **Top menu bar > Event Log > Action Log**



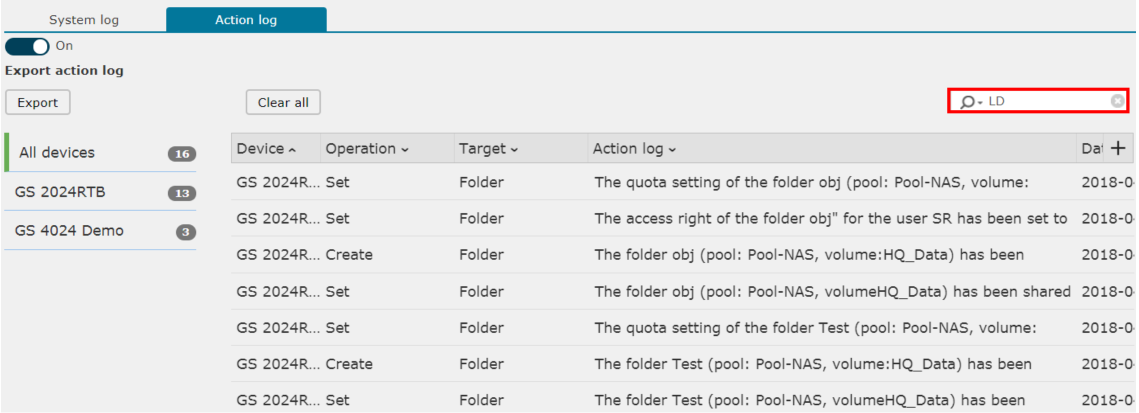
Action log

1. Turn on the switch on the upper left corner

2. Select a specific device or all devices by default.



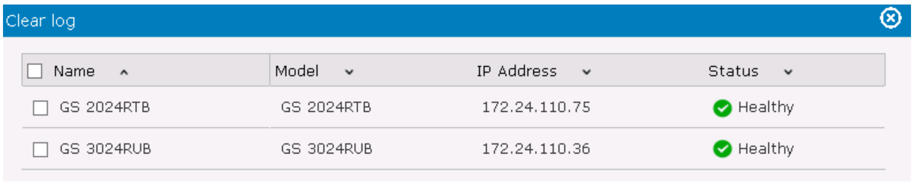
3. You can use the search bar to display certain events.



Device	Operation	Target	Action log	Dat
GS 2024R...	Set	Folder	The quota setting of the folder obj (pool: Pool-NAS, volume:	2018-0
GS 2024R...	Set	Folder	The access right of the folder obj" for the user SR has been set to	2018-0
GS 2024R...	Create	Folder	The folder obj (pool: Pool-NAS, volume:HQ_Data) has been	2018-0
GS 2024R...	Set	Folder	The folder obj (pool: Pool-NAS, volumeHQ_Data) has been shared	2018-0
GS 2024R...	Set	Folder	The quota setting of the folder Test (pool: Pool-NAS, volume:	2018-0
GS 2024R...	Create	Folder	The folder Test (pool: Pool-NAS, volume:HQ_Data) has been	2018-0
GS 2024R...	Set	Folder	The folder Test (pool: Pool-NAS, volumeHQ_Data) has been	2018-0

Clear action log

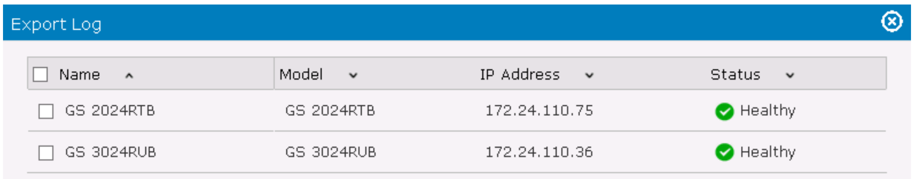
Click the **Clear all** button, select the device(s), and click **OK**. The action log of the device(s) will be cleared.



□ Name	Model	IP Address	Status
□ GS 2024RTB	GS 2024RTB	172.24.110.75	✓ Healthy
□ GS 3024RUB	GS 3024RUB	172.24.110.36	✓ Healthy

Export action log

Click the **Export** button Export , select a device and click **OK**. EonOne will start downloading the action log of the device as a .zip file.



□ Name ▴	Model ▾	IP Address ▾	Status ▾
□ GS 2024RTB	GS 2024RTB	172.24.110.75	✓ Healthy
□ GS 3024RUB	GS 3024RUB	172.24.110.36	✓ Healthy

Data Access Log

Note:

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

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:

File protocol	The file protocol used for accessing file data
Time	The time when the access event occurs
IP address	The accessing user’s IP address
Username	The accessing user’s EonOne username
Action	The file operation performed on file data
File path	The location of accessed file data

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

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

Service Manager

Service Manager provides proactive technical support for your storage system. It automatically creates a monitoring connection with STORANDER Service Center so that the center can check system health in real time. When the connection is lost or a critical event occurs on EonStor GS/GSe, Service Manager can automatically send a service request to STORANDER Service Center with related system information for diagnosis. STORANDER 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 STORANDER Service Center may include contact information, product information, system logs and configurations, as well as core dumps.

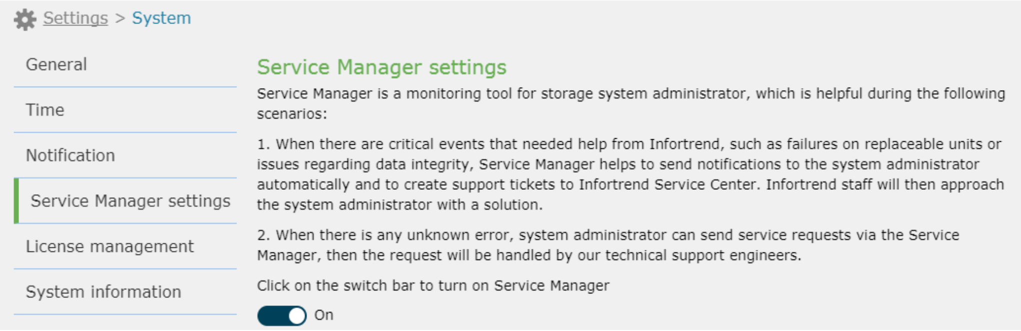
You will need to configure Service Manager in the Initial Setup Wizard when you log in to EonOne for the first time.

Configure Service Manager

Go to

Settings > System > Service Manager settings

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



Service Manager settings

Service Manager is a monitoring tool for storage system administrator, which is helpful during the following scenarios:

1. When there are critical events that needed help from Infortrend, such as failures on replaceable units or issues regarding data integrity, Service Manager helps to send notifications to the system administrator automatically and to create support tickets to Infortrend Service Center. Infortrend staff will then approach the system administrator with a solution.

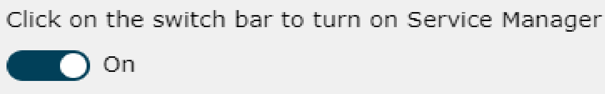
2. When there is any unknown error, system administrator can send service requests via the Service Manager, then the request will be handled by our technical support engineers.

Click on the switch bar to turn on Service Manager

On

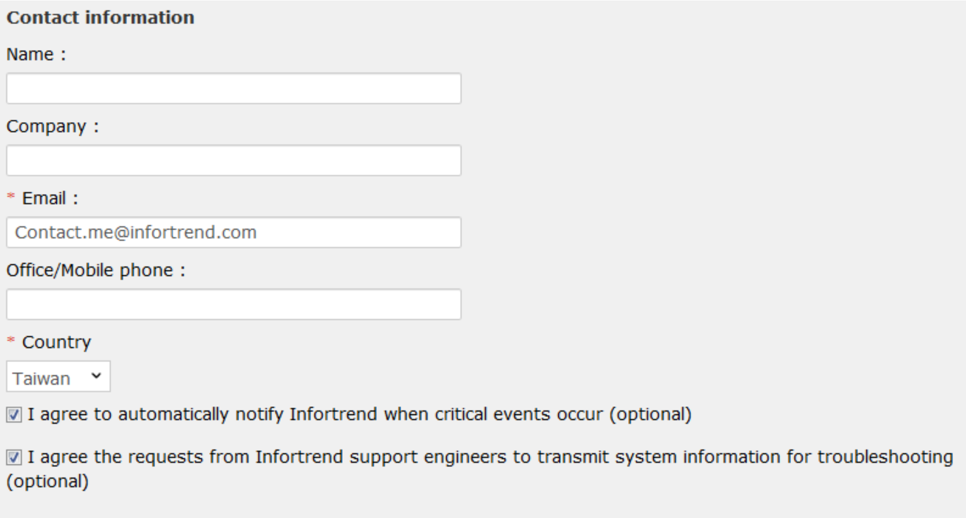
Configure Service Manager settings

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


Click on the switch bar to turn on Service Manager

On

Fill in your contact information.(Refer to parameters below for details)


Contact information

Name :

Company :

* Email :

Contact.me@infortrend.com

Office/Mobile phone :

* Country

Taiwan

☑ I agree to automatically notify Infortrend when critical events occur (optional)

☑ I agree the requests from Infortrend support engineers to transmit system information for troubleshooting (optional)

2. We recommend you enable the option **I agree to automatically notify Infortrend when critical events occur**. The system will automatically create a support ticket to STORANDER Service Center when any critical errors occur.

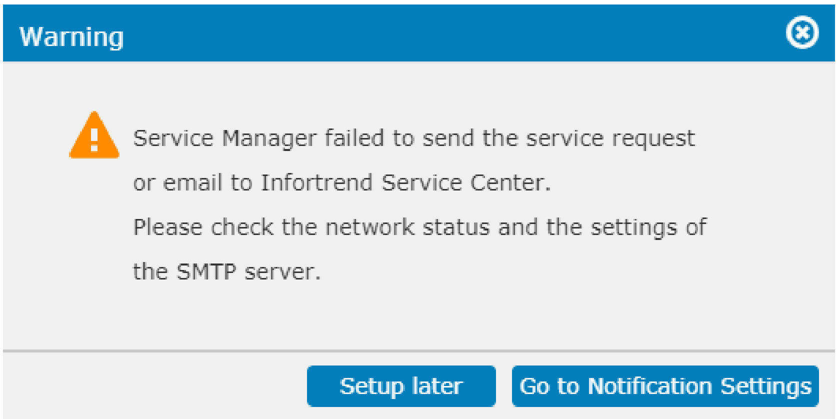
3. We also recommend you enable the option **I agree the requests from Infortrend support engineers to transmit system information for troubleshooting**. Upon request, the system will send out relevant information (i.e., logs, system configurations, and core dumps) for diagnosis to Infortrend/STORANDER 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 EonStor GS/GSe storage system.

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

If a warning window pops up with the following message:



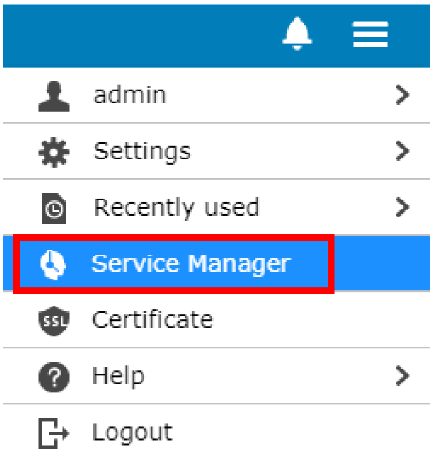
Service Manager failed to send the service request or email to Infortrend Service Center.
Please check the network status and the settings of the SMTP server.

It means SMTP server connection failure, Please check network status and SMTP server setting by clicking "Go to Notification Settings" button.

Service Manager Status

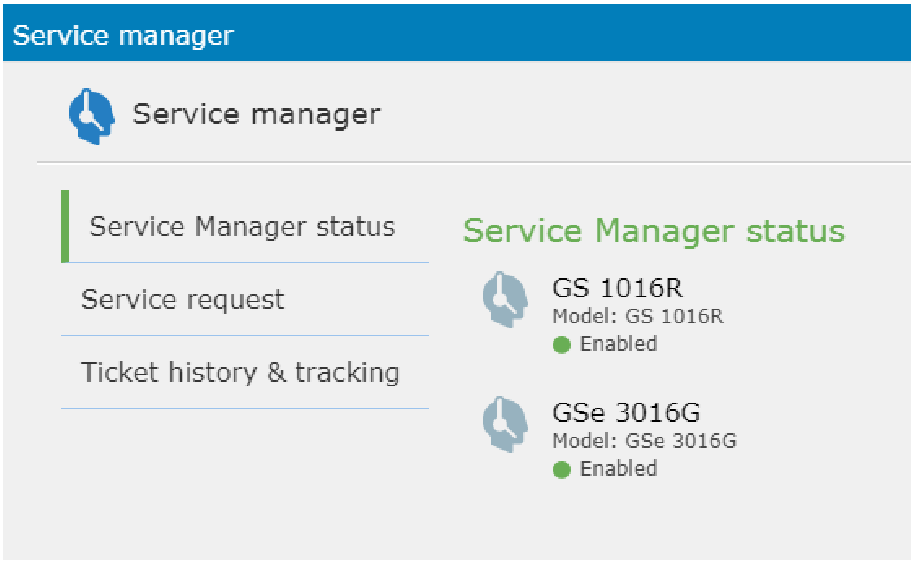
After configuring Service Manager setting, you can access Service Manager from the EonOne main menu. From here you can send service request and track your ticket easily directly via Service Manager.

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 EonOne, you may only see the status of the storage model that you are using; for the Central EonOne, 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 EonOne.

Service Manager Status	**Status Color**	**Action to Critical Events**
Enabled	Green	If a critical event is encountered, you will be notified by the Service Manager, a ticket will be automatically sent to STORANDER 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 STORANDER 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 STORANDER 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 STORANDER 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 STORANDER Service Center for instant help from our technical support engineers. Since Service Manger will not notify STORANDER automatically, therefore the Ticket history & Tracking function is unavailable.
Enabled, but no connection to STORANDER Service Center	Red	Service Manager is unable to connect to STORANDER Service Center, please check your SMTP server settings.
Disabled	Grey	Enable Service Manager at Settings > System > Service Manager settings

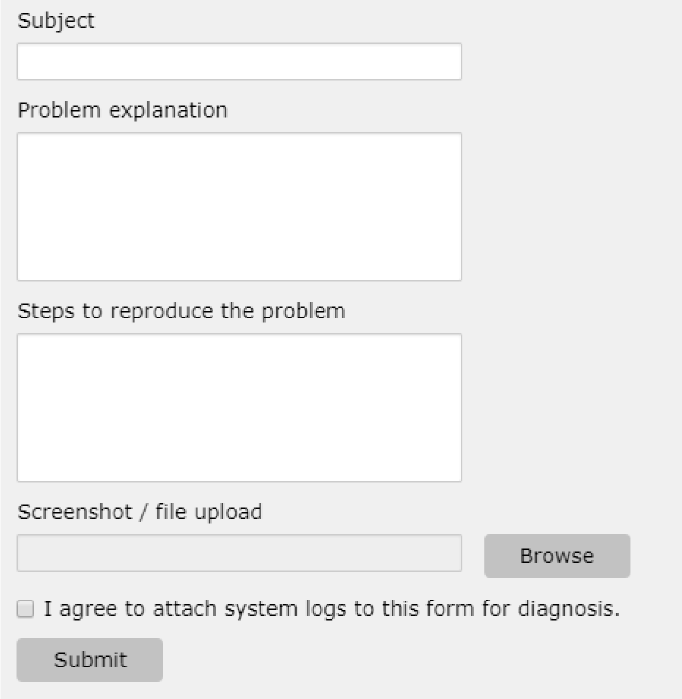
Service Request

Here you can manually submit a service request or issue ticket to STORANDER 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.


Subject
Problem explanation
Steps to reproduce the problem
Screenshot / file upload
Browse
□ I agree to attach system logs to this form for diagnosis.
Submit

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 STORANDER 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.

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

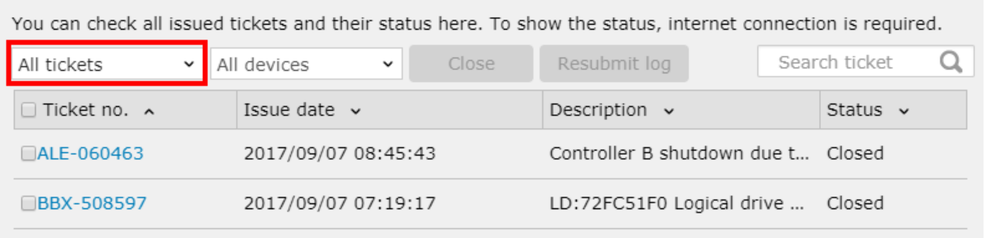
Ticket History & Tracking

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)

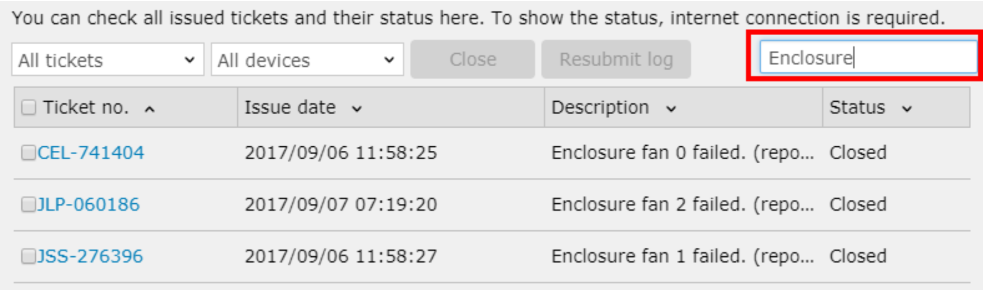
You can click the drop-down menu above the Ticket No. column to choose to display all tickets, active tickets or closed tickets.



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

□ Ticket no.	Issue date	Description	Status
□ALE-060463	2017/09/07 08:45:43	Controller B shutdown due t...	Closed
□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.

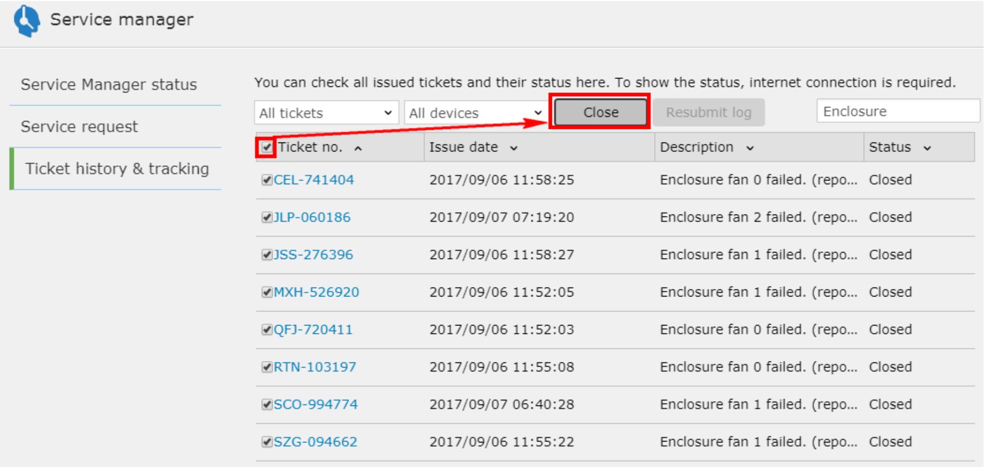


You can check all issued tickets and their status here. To show the status, internet connection is required.

□ Ticket no.	Issue date	Description	Status
□CEL-741404	2017/09/06 11:58:25	Enclosure fan 0 failed. (repo...	Closed
□JLP-060186	2017/09/07 07:19:20	Enclosure fan 2 failed. (repo...	Closed
□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).



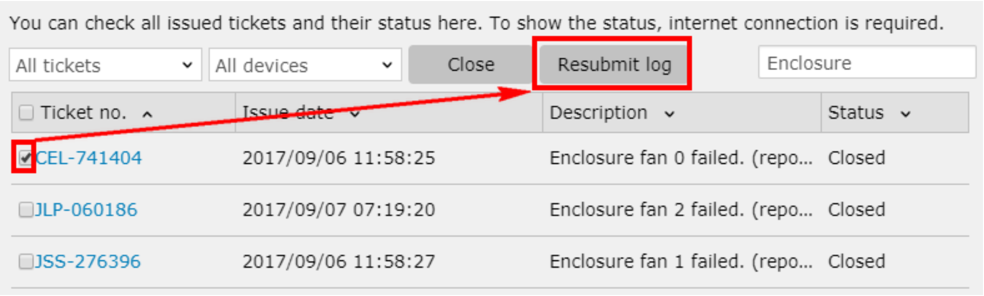
You can check all issued tickets and their status here. To show the status, internet connection is required.

☑ Ticket no.	Issue date	Description	Status
☑CEL-741404	2017/09/06 11:58:25	Enclosure fan 0 failed. (repo...	Closed
☑JLP-060186	2017/09/07 07:19:20	Enclosure fan 2 failed. (repo...	Closed
☑JSS-276396	2017/09/06 11:58:27	Enclosure fan 1 failed. (repo...	Closed
☑MXH-526920	2017/09/06 11:52:05	Enclosure fan 1 failed. (repo...	Closed
☑QFJ-720411	2017/09/06 11:52:03	Enclosure fan 0 failed. (repo...	Closed
☑RTN-103197	2017/09/06 11:55:08	Enclosure fan 0 failed. (repo...	Closed
☑SCO-994774	2017/09/07 06:40:28	Enclosure fan 1 failed. (repo...	Closed
☑SZG-094662	2017/09/06 11:55:22	Enclosure fan 1 failed. (repo...	Closed

Note: When the user closes a ticket, the status will be synchronized to STORANDER 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 STORANDER Service Center for a specified ticket. Select the ticket and click **Resubmit log**.



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

□ Ticket no.	Issue date	Description	Status
☑ CEL-741404	2017/09/06 11:58:25	Enclosure fan 0 failed. (repo...	Closed
□ JLP-060186	2017/09/07 07:19:20	Enclosure fan 2 failed. (repo...	Closed
□ JSS-276396	2017/09/06 11:58:27	Enclosure fan 1 failed. (repo...	Closed

Ticket Status

Each ticket can have one of the four statuses:

- **New**: STORANDER Service Center has received the request.
- **Opened**: STORANDER Service Center has accepted the request and is currently processing it.
- **Wait for customer**: The replacement unit is being sent to the customer. STORANDER 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.

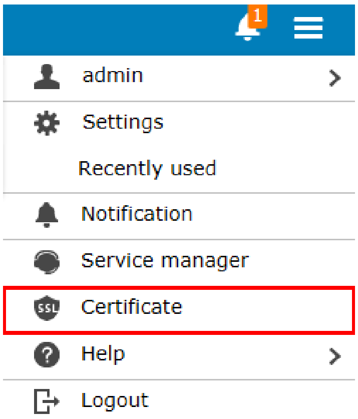
Certification

To protect and enhance the security data transmission, the EonStor GS/GSe storage systems can now transmit data through HTTP communication protocol. Before any access through HTTP protocol, the user must apply for a valid certification signing request (CSR). After applying for a CSR and once approved by the third party organization, you need to import the certificate into EonOne system, then you can access EonOne, File Explorer, and SyncCloud via HTTP communication.

Configure Web Certification

Go to

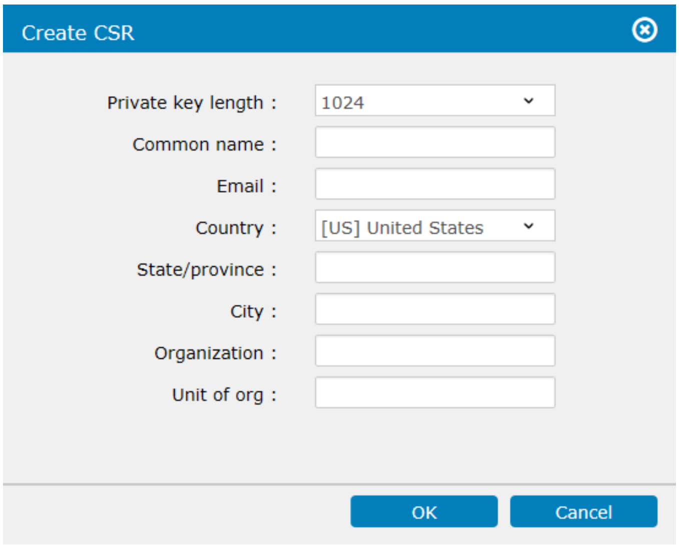
Main menu > Certificate



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.



Private key length : 1024

Common name :

Email :

Country : [US] United States

State/province :

City :

Organization :

Unit of org :

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)

Click **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.

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

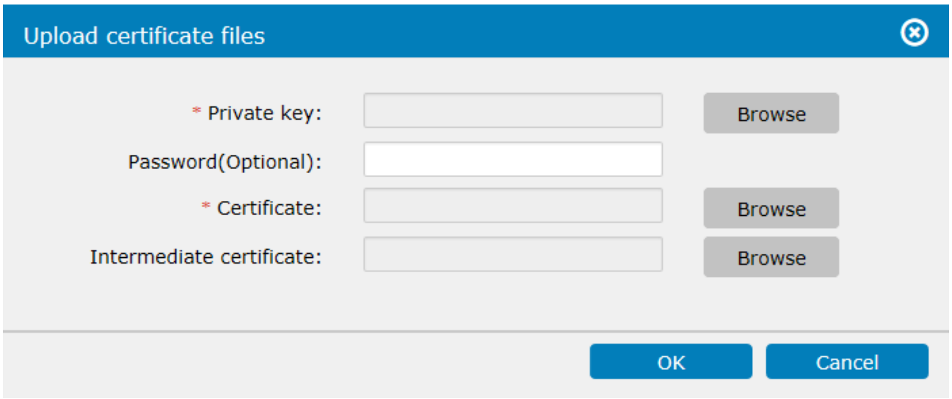
After submitting the CSR, you will see:

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

Click **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

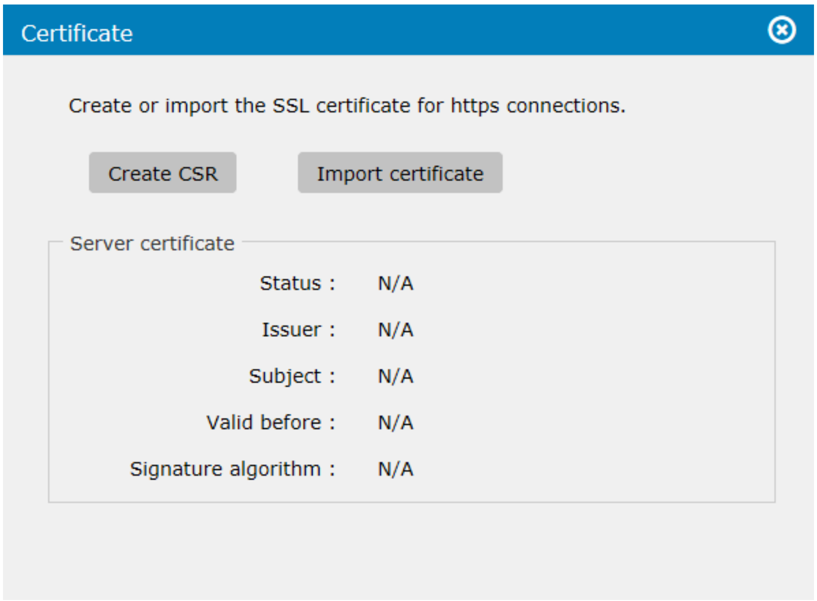
Once uploading the certificate onto your GS model, a window will be displayed with the information: "**The existing certificate will be replaced by the one below. Are you sure to import this certificate?**"

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.



Certificate

Create or import the SSL certificate for https connections.

Server certificate

Status : N/A

Issuer : N/A

Subject : N/A

Valid before : N/A

Signature algorithm : N/A

System

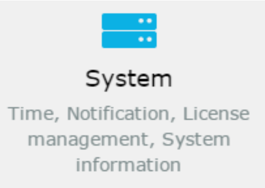
The System setting menu contains the following sub-settings.

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

For cluster settings, the System setting menu contains the following sub-settings.

1. General
2. Time
3. File Cluster
4. Maintenance

Go to **Settings / Device management > System**



System

Time, Notification, License management, System information

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

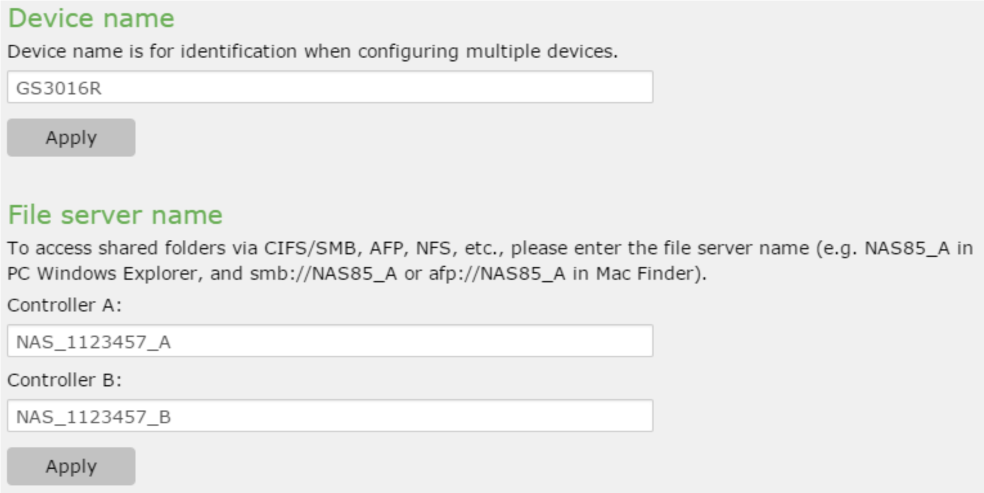
Go to **Settings / Device management > System > General**

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.

GS3016R

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

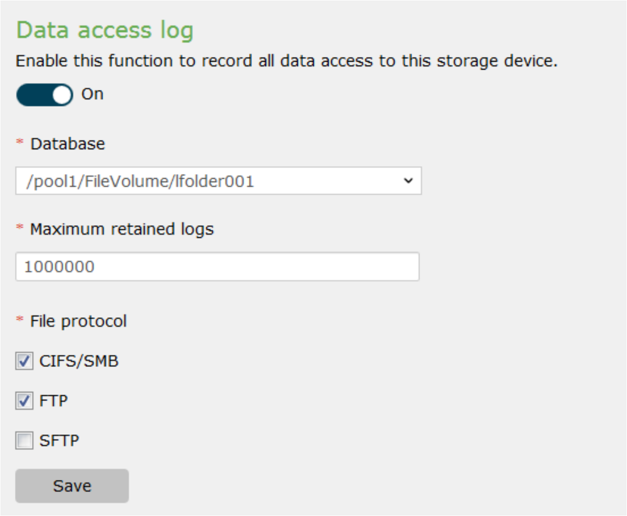
Apply

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**.



Data access log

Enable this function to record all data access to this storage device.

On

* Database

/pool1/FileVolume/lfolder001

* Maximum retained logs

1000000

* File protocol

☑ CIFS/SMB

☑ FTP

□ SFTP

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, you can include letters in lowercase or uppercase, numbers, and hyphens (-) in the file server name. Besides, the first character of the name must be a letter.

Super user

The super user can access all shared folder on the system via the CIFS/SMB and FTP protocols.

To log in as the super user, enter the current EonOne login credentials on dedicated client software.

HTTP redirection

Enable this function to disallow HTTP and HTTPS access to the management interface via their default ports (80 and 443).

You can only access the management interface via port 8816 (for HTTP access) and port 8817 (for HTTPS access).

TLS

Specify the required TLS version for securely connecting to the management interface.

Note: When HA service is enabled, the settings are synced between the two devices in the HA storage.

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.

Local management interface

You can boost the storage device's access performance by switching off the top switch for the local management interface.

You can open more network ports for data access via the data ports by switching on the bottom switch.

Password Change

Click the **Change the Password** button and input the old and the new passwords to modify the login password for accessing the EonStor GS/GSe through the Central EonOne.

Performance Optimization

Allocate more system resource to a specific data service to optimize its read and write access. Select an option:

- **Better performance for file access service**

  This option enhances resources for NAS services.

- **Better performance for block data access**

  This option enhances resources for SAN services.

- **Maximum block data access and stop NAS service**

  This option cancels file-level data services on the device to maximize resources for SAN services.

Go to **Cluster settings > System > General**

After the scale-out cluster is enabled, you can view the cluster name, its capacity, number of appliances in this cluster, and status of total drives.

Time Settings

Go to	**Settings / Device management / Cluster settings > System > Time**

Steps

1. Go to the **Current time** section.

2. To change the system time, go to **Change date and time** and click **Change**:

Customize	Select this option to manually set the system time.
Automatically sync with NTP server	You can let the cluster sync its system time with an NTP server. You can specify at most two NTP servers for use. A. Select an NTP server to sync with from the **Internet time server** menu. To sync with a custom NTP server, select **Customize** and specify the server’s URL. B. Click **Update now** to sync time with the NTP server. C. Set **Polling interval** in hours. The system checks and calibrates the system time with the NTP server at the specified interval.

3. Go to **Time zone** to choose an appropriate time zone and specify the settings:

Update time zone information	Click on this option to immediately update the system’s built-in time zone information.
Automatically update time zone information (Internet connection required)	Select this option to let the system automatically update time zone information.

4. Go to **Adjust daylight saving time** and turn on the function. Then, click **Edit** to specify the settings:

Automatically adjust daylight saving time	Click **Update daylight saving time information** to immediately update the daylight saving time settings. Select **Automatically update time zone information (Internet connection required)** to let the system auto-update the time zone settings.

Customize	**Start time**: Specify when to start applying daylight saving time. **End time**: Specify when to stop apply daylight saving time. **Offset (minutes)**: Specify the time offset of daylight saving time.

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

Notification

Using the remote event notification feature, you can receive event notifications even when not accessing the subsystem through the User Interface.

About Severity Settings

Three event severity levels are available: Notification, Warning and Critical. The Notification level includes all types of events while Warning and Critical levels are for events that may cause harm to the system or people. A higher severity level includes all events of a lower severity level.

- Notification: all events, including Warning and Critical events.
- Warning: includes Warning and Critical events.
- Critical: includes only Critical events.

Severity Settings in the Sender and the Receiver side

The severity level settings have to be consistent between the sender and the receiver. If the severity level settings on both sides are different, the following situations will occur.

- If the sender's severity level is Critical but the receiver’s is set to Notification, the receiver will only receive events of the Critical level.
- If the sender's severity level is Notification and the receiver’s is also set to Notification, the receiver will receive all events.
- If the sender's severity level is Notification but the receiver’s is set to Critical, the receiver will only receive events of the Critical level.

If you have multiple receivers and each has different settings, the overall severity control depends on the sender’s setting. That is, if the sender’s severity level is set to Notification, all receivers will receive Notification level events.

Go to

Settings / Device management > System > Notification

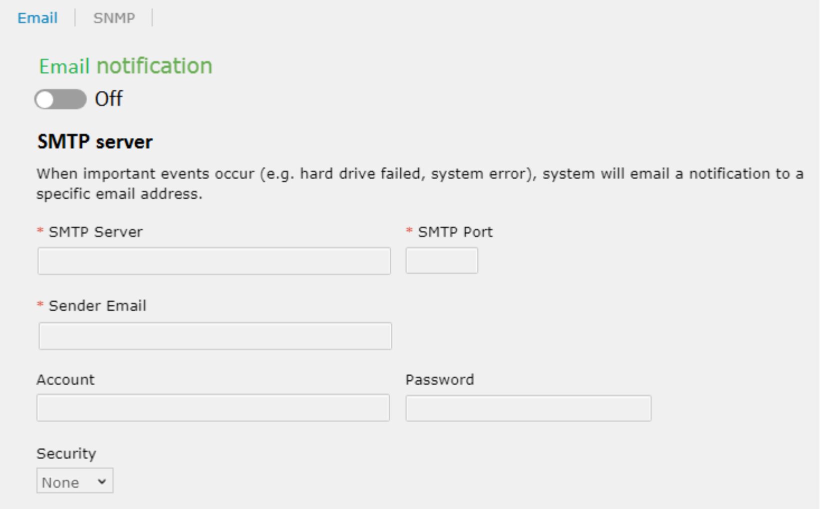
Email Notification

1. Turn on email notification with the toggle.
2. Configure the SMTP server settings. Please note that you must to fill in the information for **SMTP server** and **Sender email** to complete email notification. (Make sure your Sender email address is correctly entered with the correct email address format).

   Account and **password** indicate the account and password information of the sender’s SMTP server. These fields are optional since some of the SMTP servers may not have the authentication mechanism. You can also set the **security** level of the SMTP server.

   Note: You do not have to enter domain name for the Account name filed e.g.

Username, instead of Username@infortrend.com



Email notification

Off

SMTP server

When important events occur (e.g. hard drive failed, system error), system will email a notification to a specific email address.

* SMTP Server

* SMTP Port

* Sender Email

Account

Password

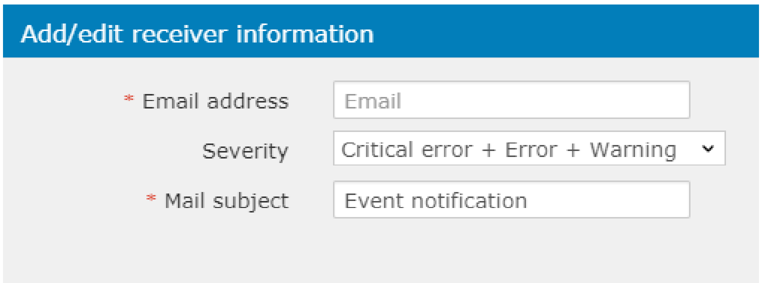
Security

None

Note: The SMTP port number is usually set to 25. If you want to use a secure over SSL, set it to 465; for secure over TLS, set to 587.

SMTP port number	Description
25	Transmission without authentication (may contain span mails)
465	SSL encryption enabled
587	TLS encryption enabled

3. Add Email Receivers by clicking the **Add Receiver** button at the bottom of the page. Note that at least an email receiver is required for the email notification.



Add/edit receiver information

* Email address: Email

Severity: Critical error + Error + Warning

* Mail subject: Event notification

To configure the receiver information, please enter the receiver's Email address and select the notification **severity level** listed in the previous paragraph in the pop-up window. You must also name your **mail subject** to identify your notification email.

After saving SMTP settings, click on each email receiver and then click **Send test email** to see if the intended receiver gets a test message.

4. For status change notification, select this option if you want to be notified when the status of scheduled task is changed. The notification will be sent via

email.

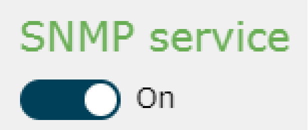
5. Click **Save** to save the settings.

SNMP Settings

Go to **Settings / Device management > System > Notification > SNMP**

SNMP Notification

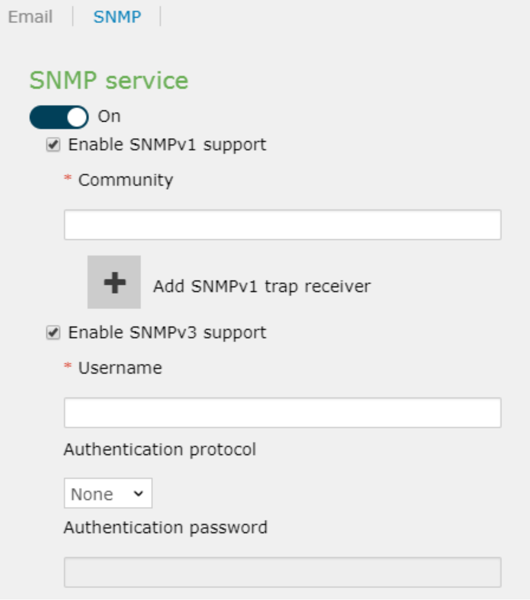
1. Enable SNMP notification by clicking the switch button. (You must first turn on SNMP service for any further SNMP settings)



SNMP service

On

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



SNMP service

On

☑ Enable SNMPv1 support

* Community

☑ Enable SNMPv3 support

* Username

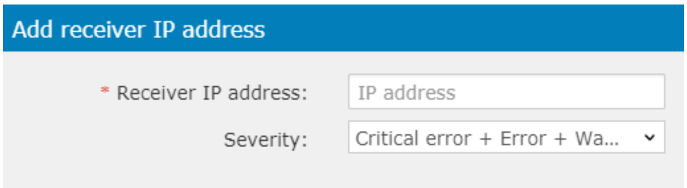
Authentication protocol

None

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.



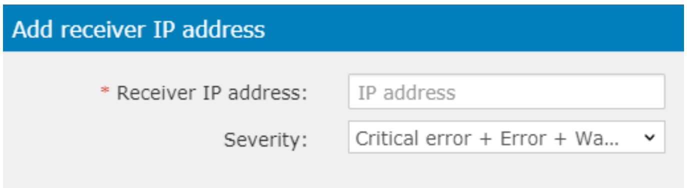
Add receiver IP address

* Receiver IP address: IP address

Severity: 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.

Parameters	**Community**	The password of the SNMP.

		Minimum / Maximum length of the community name: 1 / 31 digits. Note that the name must not contain any punctuation marks such as quotation mark, vertical bar and comma.
Enable SNMPv3 support	1. Click the **Enable SNMPv3 support** check box to activate the SNMPv3. 2. Enter the **Username** of the SNMPv3 server. 3. Select the authentication protocol of the SNMPv3 and the password. 4. Select the privacy protocol of the authentication if needed. 5. Click **Add SNMPv3 trap receiver** to add a trap server. 6. Enter the **Receiver IP address** and select the **severity** level to complete the settings.  Add receiver IP address * Receiver IP address: IP address Severity: Critical error + Error + Wa... 7. 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.	
Parameters	**Username**	The username for authentication. Maximum length: 31 digits.
	Authentication Protocol	Currently, the EonStor GS/GSe supports the **MD5** and **SHA-1** authentication. You can select the protocol in the drop-down list.
	Authentication Password	Enter the authentication password in the field. The minimum / maximum length is 8 / 16 digits.
	Privacy Protocol & **Privacy Password**	Select the privacy protocol in the drop-down list, which includes the **DES** and **AES-128**, and enter the privacy password. The privacy protocol field is enabled according to the **Authentication Protocol** and its minimum / maximum password length is 8 / 16 digits.

Service Manager Settings

For Service Manager settings details, please refer to Service Manager section.

License Management

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

Go to	**Settings / Device management > System > License management**
License Types	You will need to apply for or download a license key to use the following features in the EonStor GS/GSe series. A Standard License is provided for free for all users and is preloaded in your EonStor GS/GSe 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
EonCloud Gateway	Standard/Enterprise/Ultimate License

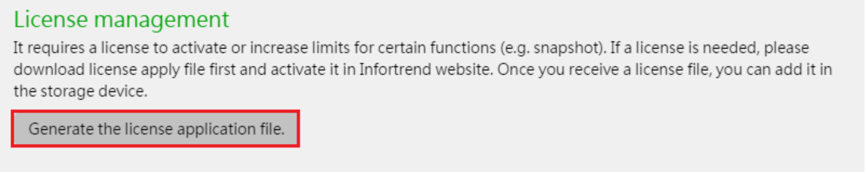
Notes

- 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 EonStor GS/GSe 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 EonStor GS/GSe via EonOne.

Before starting any EonStor GS/GSe license process, please make sure Infortrend's EonOne management suite shipped together with the EonStor GS/GSe storage system has been properly installed.

Go to	**Settings / Device management > System > License management**
Steps	In the License Key window, click **Generate License Application File**.  License management It requires a license to activate or increase limits for certain functions (e.g. snapshot). If a license is needed, please download license apply file first and activate it in Infortrend website. Once you receive a license file, you can add it in the storage device. Generate the license application file. Download will start immediately and the file will be saved automatically in your computer.

Generating an Advanced License

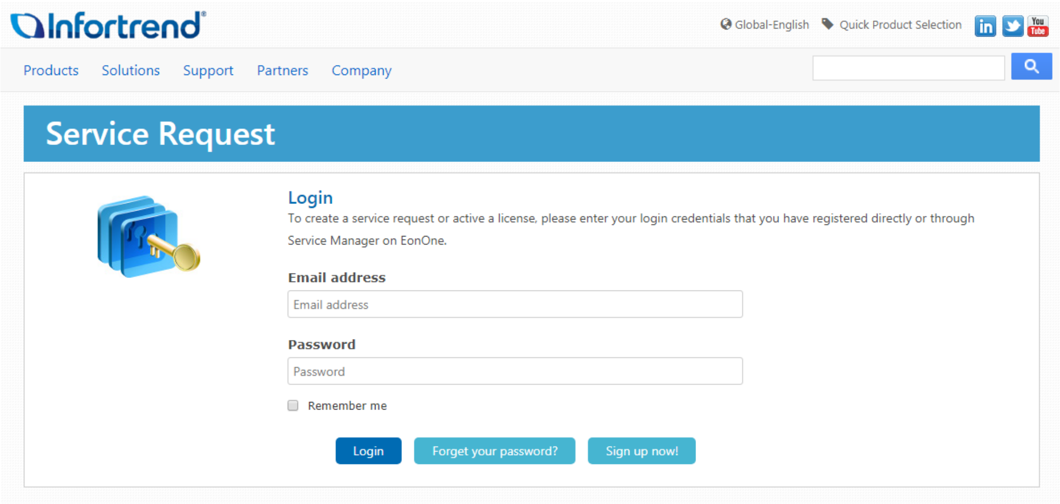
An advanced License is required to access the following features:

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

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

Steps

1. Visit Infortrend's EonStor GS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Sign up now** to register for one.



Login

To create a service request or active a license, please enter your login credentials that you have registered directly or through Service Manager on EonOne.

Email address

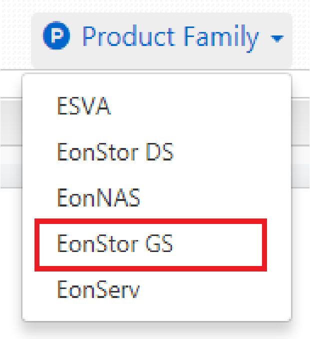
Email address

Password

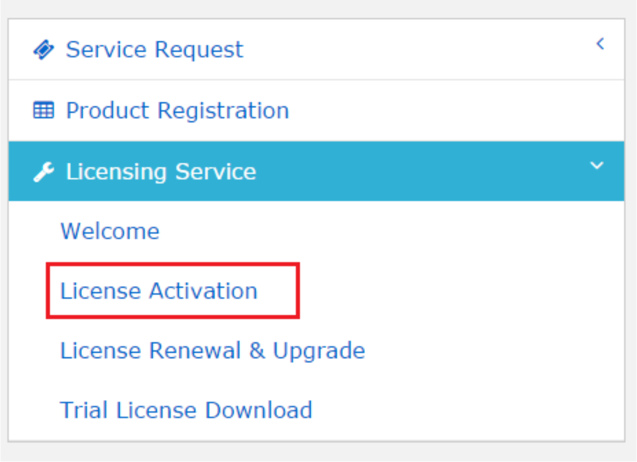
Password

□ Remember me

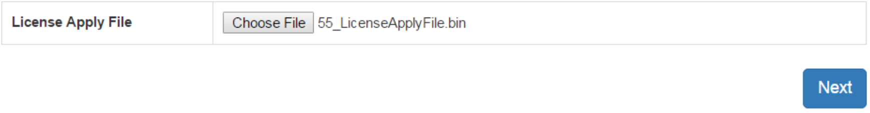
2. At the **Product Family** drop-down menu located at the top right corner, select EonStor GS.



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

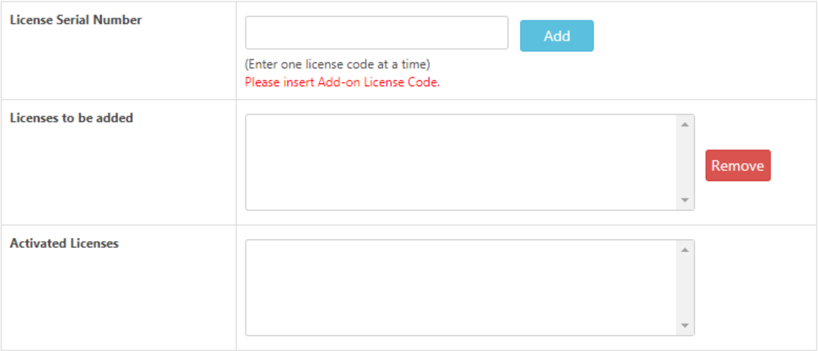


4. Upload the License Application File you obtained through EonOne and click **Next**.



License Apply File: Choose File 55_LicenseApplyFile.bin

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.

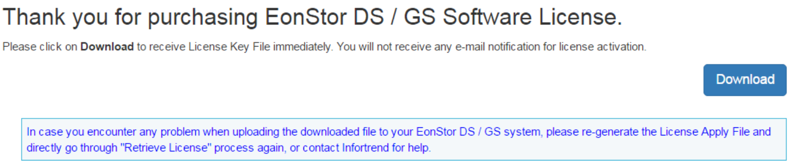


License Serial Number

(Enter one license code at a time)

Please insert Add-on License Code.

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



Thank you for purchasing EonStor DS / GS Software License.

Please click on **Download** to receive License Key File immediately. You will not receive any e-mail notification for license activation.

In case you encounter any problem when uploading the downloaded file to your EonStor DS / GS system, please re-generate the License Apply File and directly go through "Retrieve License" process again, or contact Infortrend for help.

Save the License Key File at a preferred location and upload it to EonOne.

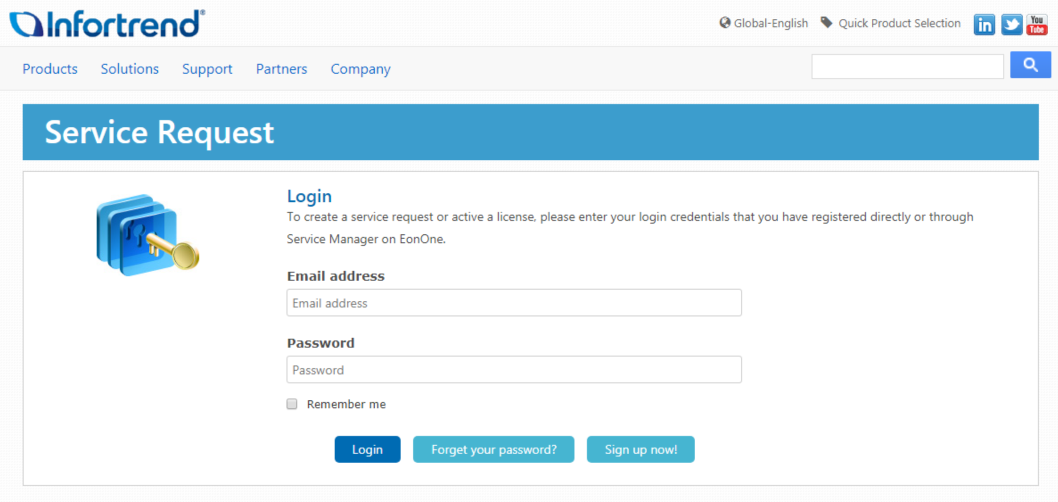
Please note it is required to reset the system for the license to take effect after it is installed.

Upgrading Standard License to Advanced License

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

Steps

1. Visit Infortrend's EonStor GS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Sign up now** to register for one.



Service Request

Login

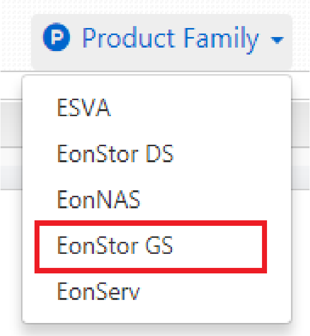
To create a service request or active a license, please enter your login credentials that you have registered directly or through Service Manager on EonOne.

Email address: Email address

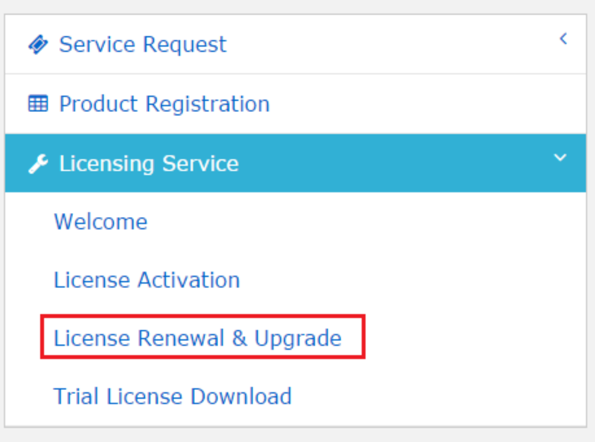
Password: Password

□ Remember me

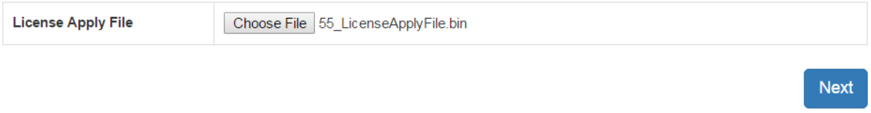
2. At the **Product Family** drop-down menu located at the top right corner, select EonStor GS.



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

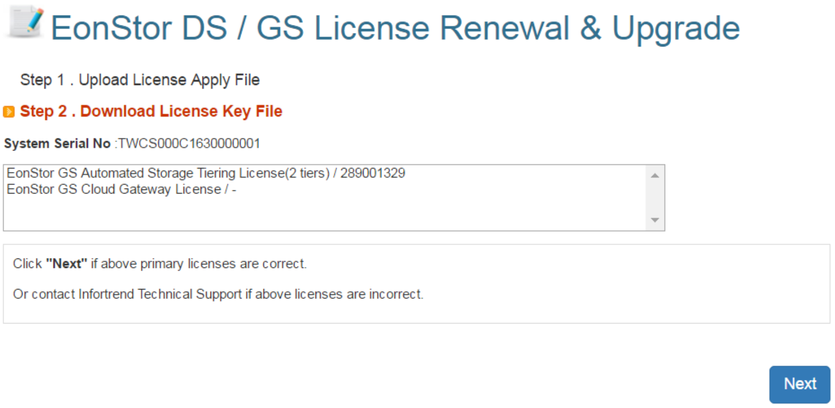


4. Upload the License Application File generated through EonOne and click **Next**.



License Apply File: Choose File 55_LicenseApplyFile.bin

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



EonStor DS / GS License Renewal & Upgrade

Step 1 . Upload License Apply File

Step 2 . Download License Key File

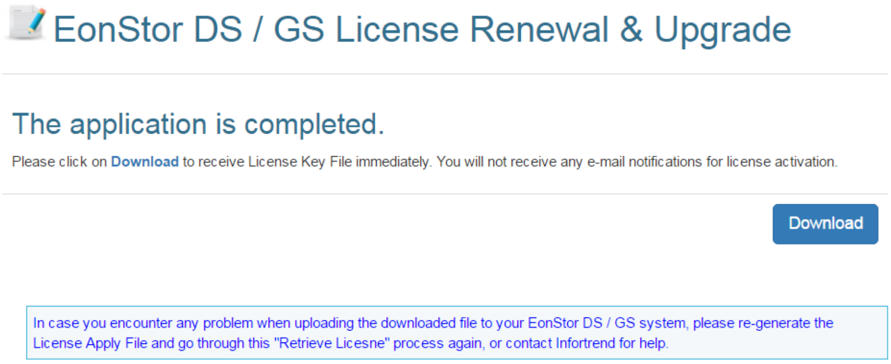
System Serial No :TWCS000C1630000001

EonStor GS Automated Storage Tiering License(2 tiers) / 289001329
EonStor GS Cloud Gateway License / -

Click **"Next"** if above primary licenses are correct.

Or contact Infortrend Technical Support if above licenses are incorrect.

6. Click **Download** to receive the License Key File and save the License Key File at a preferred location and upload it to EonOne.

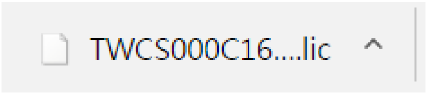


EonStor DS / GS License Renewal & Upgrade

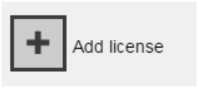
The application is completed.

Please click on Download to receive License Key File immediately. You will not receive any e-mail notifications for license activation.

In case you encounter any problem when uploading the downloaded file to your EonStor DS / GS system, please re-generate the License Apply File and go through this "Retrieve Licesne" process again, or contact Infortrend for help.



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



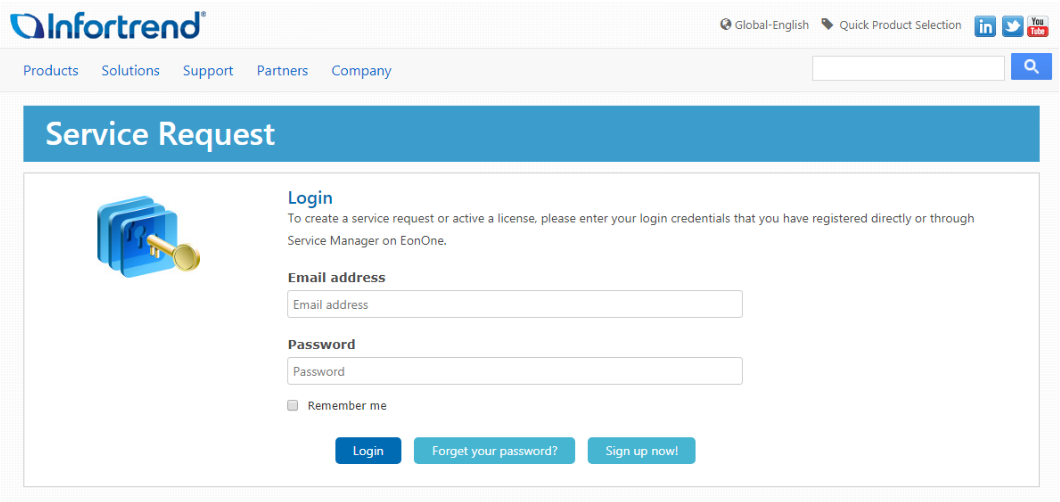
Please note it is required to reset the system for the license to take effect after it is installed.

Renewing License

If you have lost a previously generated License Key File, you can regenerate it through the license website.

Steps

1. Visit Infortrend's EonStor GS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Sign up now** to register for one.



Service Request

Login

To create a service request or active a license, please enter your login credentials that you have registered directly or through Service Manager on EonOne.

Email address

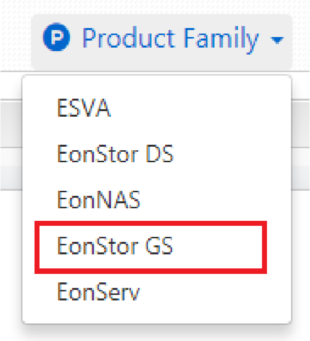
Email address

Password

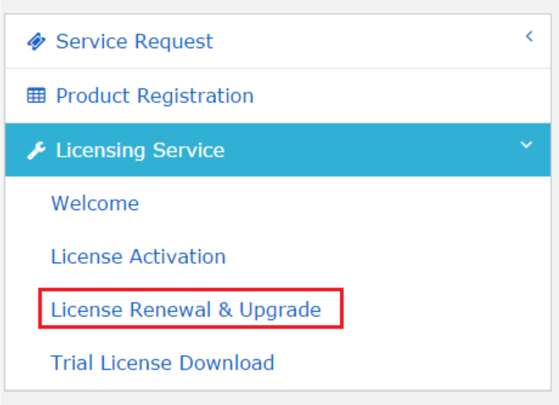
Password

□ Remember me

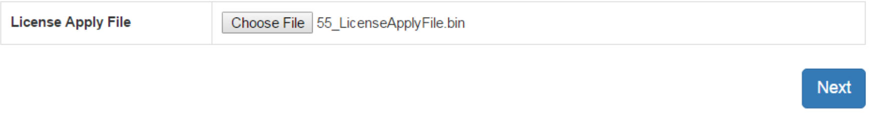
2. At the **Product Family** drop-down menu located at the top right corner, select EonStor GS.



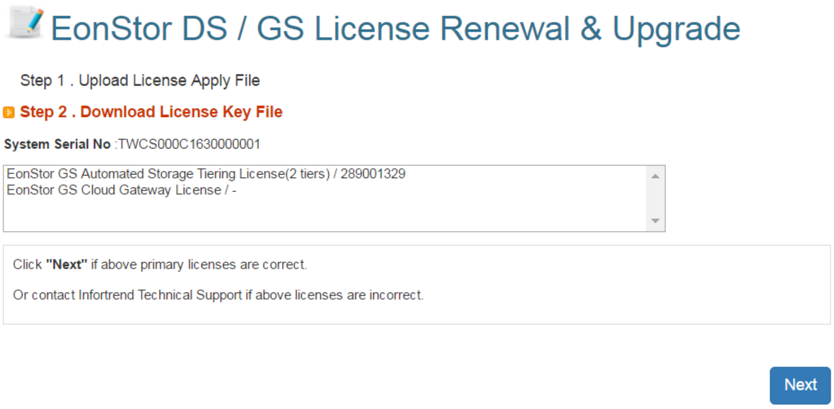
3. Click on **License Renewal & Upgrade** under **Licensing Service** at the left column.



4. Upload the License Application File generated through EonOne and click **Next**.


License Apply File | Choose File 55_LicenseApplyFile.bin

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


EonStor DS / GS License Renewal & Upgrade

Step 1 . Upload License Apply File

Step 2 . Download License Key File

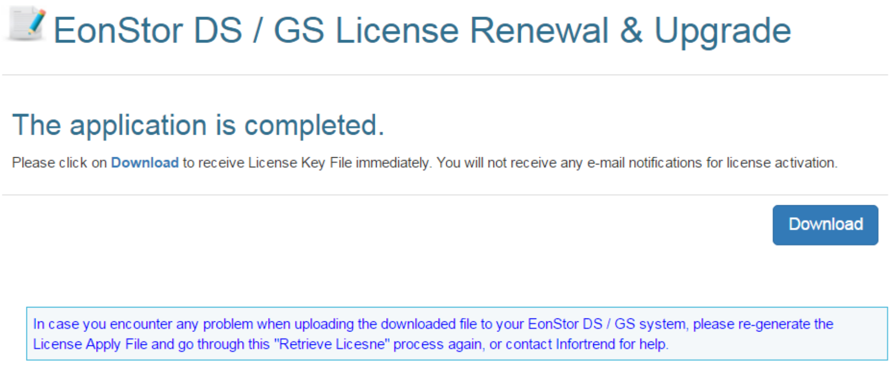
System Serial No :TWCS000C1630000001

EonStor GS Automated Storage Tiering License(2 tiers) / 289001329
EonStor GS Cloud Gateway License / -

Click **"Next"** if above primary licenses are correct.

Or contact Infortrend Technical Support if above licenses are incorrect.

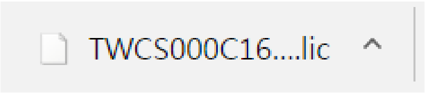
6. Click **Download** to receive the License Key File and save the License Key File at a preferred location and upload it to EonOne.


EonStor DS / GS License Renewal & Upgrade

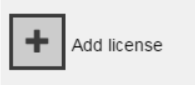
The application is completed.

Please click on Download to receive License Key File immediately. You will not receive any e-mail notifications for license activation.

In case you encounter any problem when uploading the downloaded file to your EonStor DS / GS system, please re-generate the License Apply File and go through this "Retrieve Licesne" process again, or contact Infortrend for help.



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



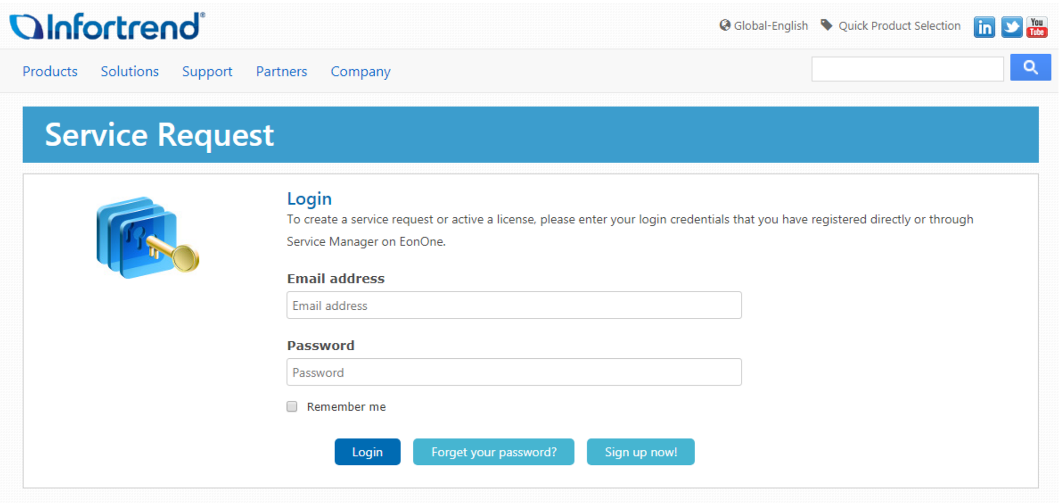
Please note it is required to reset the system for the license to take effect after it is installed.

Downloading Trial License

If you want to try out the advanced license features before making a purchase decision, you can use the trial license. All features requiring the advanced license will be effective for 30 days.

Steps

1. Visit Infortrend's EonStor GS Software License website: http://support.infortrend.com/ and log in. If you don't have an account, please click **Sign up now** to register for one.



Login

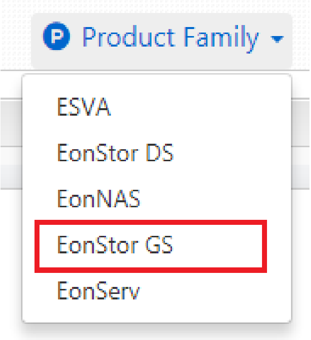
To create a service request or active a license, please enter your login credentials that you have registered directly or through Service Manager on EonOne.

Email address: Email address

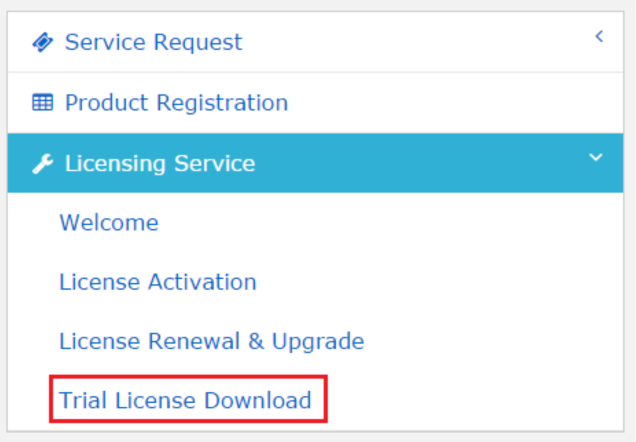
Password: Password

□ Remember me

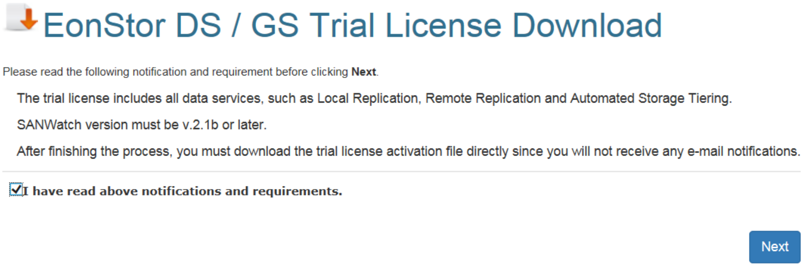
2. At the **Product Family** drop-down menu located at the top right corner, select EonStor GS.



3. Click **Trial License Download** under **Licensing Service** at the left column.



4. Carefully read the information, tick the checkbox, and click **Next**.



EonStor DS / GS Trial License Download

Please read the following notification and requirement before clicking **Next**.

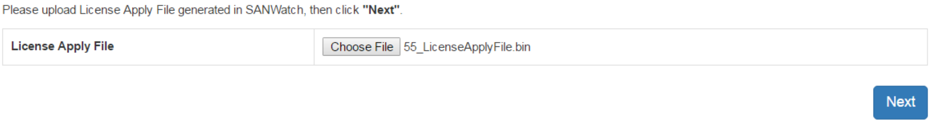
The trial license includes all data services, such as Local Replication, Remote Replication and Automated Storage Tiering.

SANWatch version must be v.2.1b or later.

After finishing the process, you must download the trial license activation file directly since you will not receive any e-mail notifications.

☑ **I have read above notifications and requirements.**

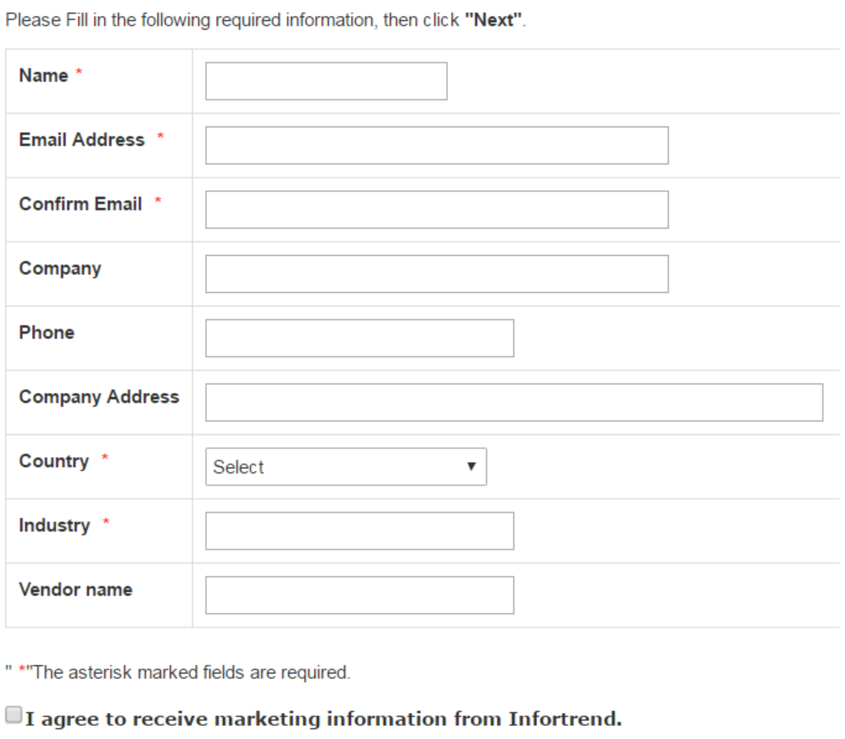
5. Upload the License Application File generated through EonOne and click **Next**.



Please upload License Apply File generated in SANWatch, then click **"Next"**.

License Apply File	Choose File 55_LicenseApplyFile.bin

6. Fill in the required information and click **Next.**



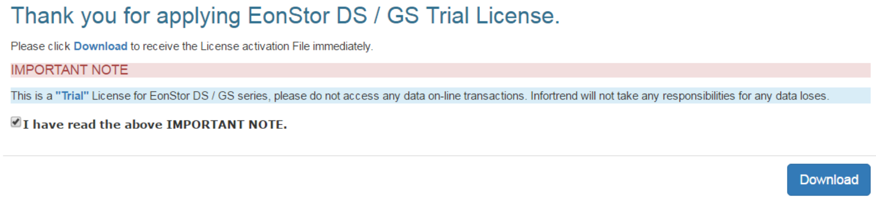
Please Fill in the following required information, then click **"Next"**.

Name *	
Email Address *	
Confirm Email *	
Company	
Phone	
Company Address	
Country *	Select ▾
Industry *	
Vendor name	

" *"The asterisk marked fields are required.

□ **I agree to receive marketing information from Infortrend.**

7. Click **Download** to receive the License Key File immediately.



Thank you for applying EonStor DS / GS Trial License.

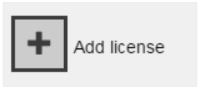
Please click **Download** to receive the License activation File immediately.

IMPORTANT NOTE

This is a **"Trial"** License for EonStor DS / GS series, please do not access any data on-line transactions. Infortrend will not take any responsibilities for any data loses.

☑ **I have read the above IMPORTANT NOTE.**

Save the License Key File at a preferred location and upload it to EonOne.



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

System Information

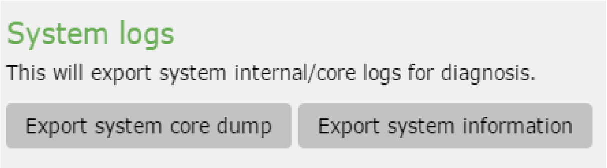
Go to **Settings / Device management > System > System Information**

System Information

This page shows the information of the EonStor GS/GSe, 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**.

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.



System logs

This will export system internal/core logs for diagnosis.

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:

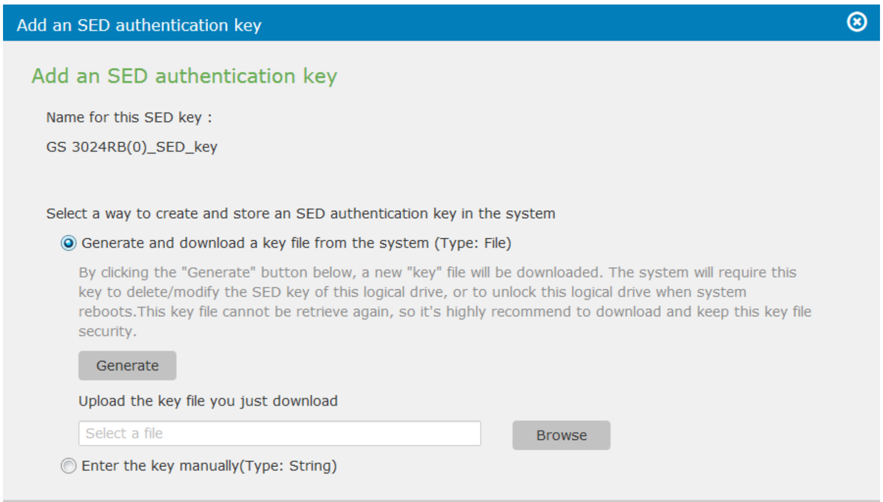
- The system can only hold one global encryption key.
- Global encryption is unlocked after system reboot. To re-enable it, provide the global key file or enter the password again.
- If you disable encryption for a specific SED logical drive after setting up global encryption, previously-set global encryption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

Go to	**Settings / Device management > System > SED key management**

Steps

1. Click on **Add an SED authentication key in the system**.
2. Select how to generate an SED authentication key:

Generate and download a key file from the system	Click **Generate** to create a .key file that contains the SED authentication key. Then, upload the key file for confirmation by clicking **Browse**. You must keep this key in a secure place. This key cannot be recovered once lost.
Enter the key manually	Enter a custom key and confirm it. This key cannot be recovered once forgotten.



Add an SED authentication key

Add an SED authentication key

Name for this SED key :

GS 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.

Generate

Upload the key file you just download

Select a file

Browse

○ Enter the key manually(Type: String)

	3. Click **OK** to finish the setup.
Delete the Global SED Authentication Key	1. Click on the key in **Settings** > **System** > **SED key management**. 2. Click **Delete** > **OK**. 3. Provide the key for confirmation and click **OK** to delete the key.

File cluster

Enabling the File Cluster

After the scale-out cluster is enabled, you can enable file cluster to manage file-level data service on all appliances in the cluster.

Go to	**Cluster settings > System > File cluster**

Steps

1. Turn on the file cluster function.
2. Specify the file cluster settings:

Root shared folder name	Specify an identifying name for the cluster's root shared folder. The root folder is responsible for storing mappings between cluster volumes and appliances.
Cluster root volume	Choose a volume as the cluster's root volume from the list. Only qualified file volumes appear in the list: ● A volume in a RAID1, RAID5, or RAID6 storage pool ● A volume that is not used to run Docker ● A volume that is not set as a WORM volume

3. CIFS/SMB will be pre-selected.

   If needed, change the following file protocol settings:

File protocols	Choose how to encrypt the CIFS/SMB connection from the menu: **Allow only unencrypted connections**, **No restriction**, or **Allow only encrypted connections**. You can enable other functions to suit your needs: **Enable access-based enumeration**: This option hides folders or resources that the user is not allowed access to. **Enhance SMB compatibility with macOS and iOS clients**: This option increases compatibility of an SMB client running on the macOS system.

	Transfer files in asynchronous mode: This option allows the system to transfer files asynchronously to minimize file transfer wait time and avoid transfer bottlenecks.
NFS	Select to enable the NFS protocol.

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

5. After enabling, go to **Data ports** section to find the IP addresses that you can use to access the file cluster.

6. If needed, enable File explorer. See File explorer for more details.

   After File explorer is enabled, you can click **File explorer** to access local shared folders and attached USB storage devices with a web browser.

Maintenance

Exporting/Importing 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

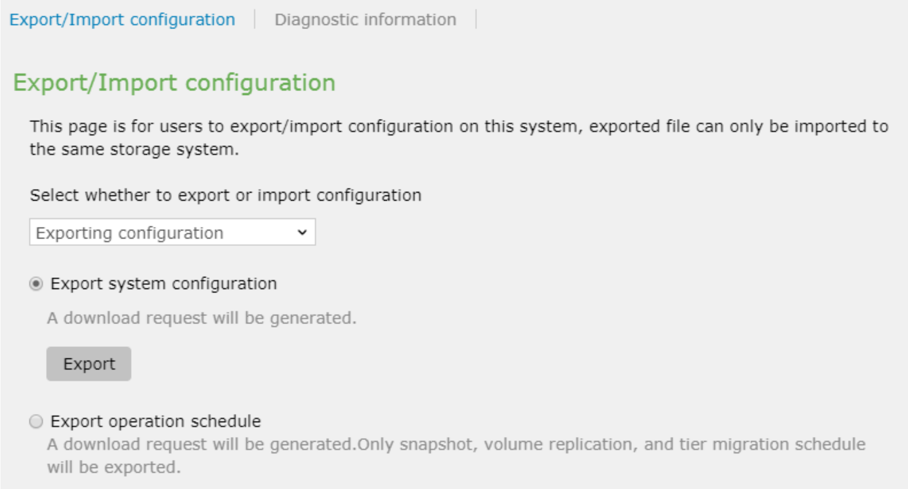
When to import system configuration

- 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 / Device management > System > Maintenance



Export/Import configuration

This page is for users to export/import configuration on this system, exported file can only be imported to the same storage system.

Select whether to export or import configuration

Exporting configuration

● Export system configuration

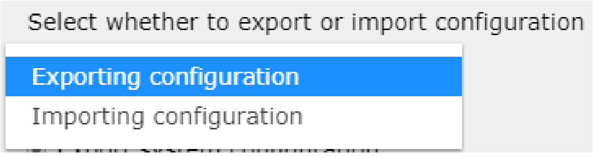
A download request will be generated.

○ Export operation schedule

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

Export/Import configuration

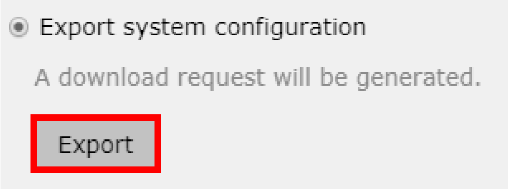
Click the **Export/Import configuration** tab. Select whether to export or import configuration from the drop down list.


Select whether to export or import 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.

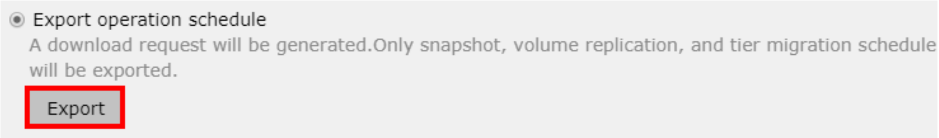


◉ Export system configuration

A download request will be generated.

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

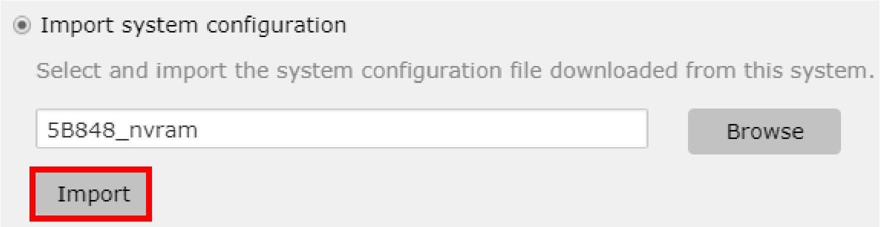
A download request will be generated.Only snapshot, volume replication, and tier migration schedule will be exported.

[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

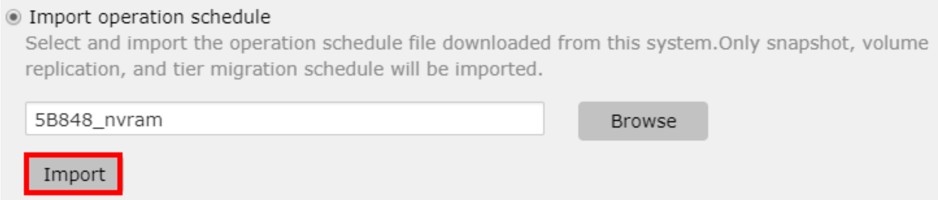
Select and import the system configuration file downloaded from this system.

5B848_nvram

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.



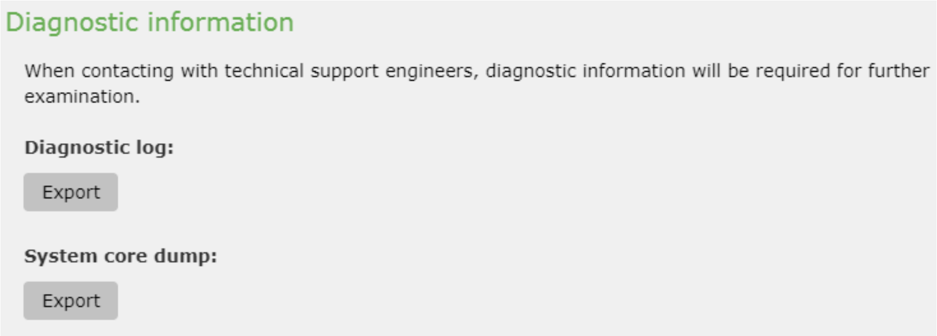
◉ Import operation schedule

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 / Device management > System > Maintenance > Diagnostic information tab**
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:

Backing up and Exporting the Cluster Configurations

Go to **Cluster settings > System > Maintenance**

Steps

1. Go to the **Last backup time** section. You can check when the last time the cluster ran a backup.
2. Click **Back up now** to back up the cluster's configurations
3. If needed, you can configure the backup schedule at **Every week** or **Every month**.
4. Go to the **Export cluster configurations** section. Click **Export** to export current cluster configurations for system recovery.

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 EonStor GS/GSe 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.

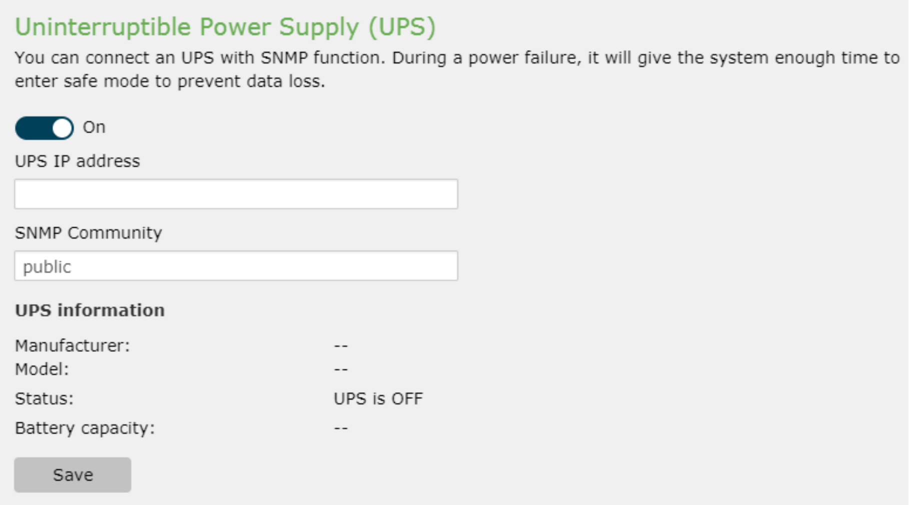
The administrator can establish a connection between the EonStor GS/GSe and SNMP UPS through the EonOne. When power supply is interrupted, the system can enter into a safe mode when the remaining power on the UPS has reached a certain threshold. The system will also keep a log on the events for tracking purposes.

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

Go to **Settings / Device management > 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:	--

Parameter

UPS IP Address: The destination for the EonStor GS/GSe to send SNMP requests.

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

SNMP Community: The default setting is “public.”

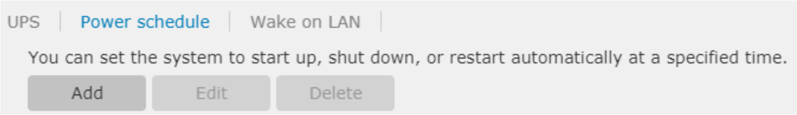
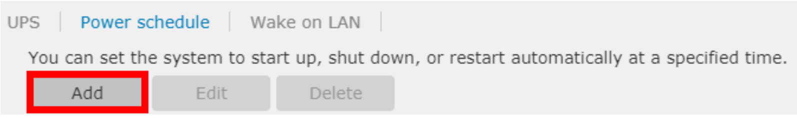
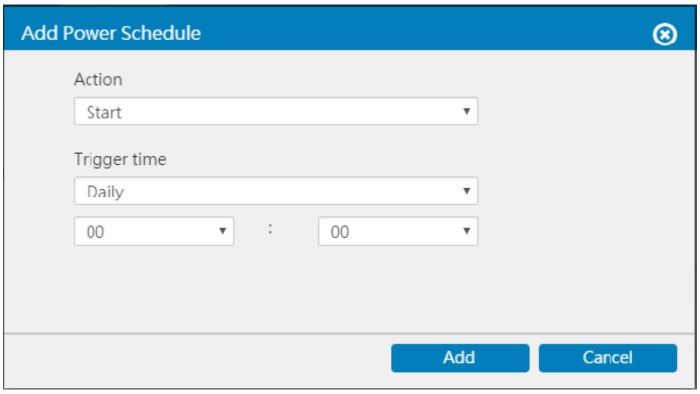
Note: When in safe mode, the EonStor GS/GSe will unmount file-level volumes. For block-level volumes, the write policy will change from write-back to write-through to prevent data loss during power failure.

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.

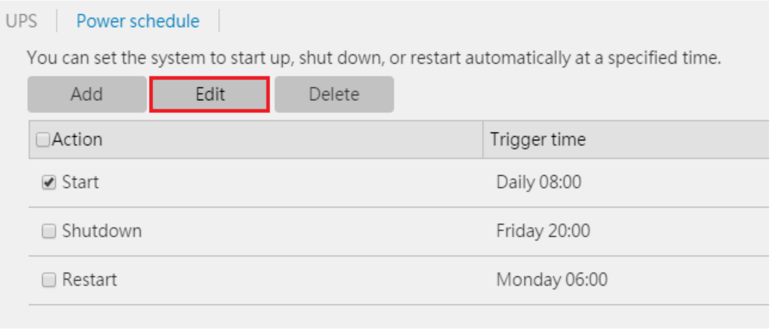
Note:

- This function is available only on GSe Pro 100 and 200 series.
- 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 / Device management > System > Power**
Power Schedule	Select the **Power schedule** tab.  You can set the system to start up, shut down, or restart automatically at a specified time.
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.  You can set the system to start up, shut down, or restart automatically at a specified time. 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.  Add Power Schedule Action: Start Trigger time: Daily 00 : 00 **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.

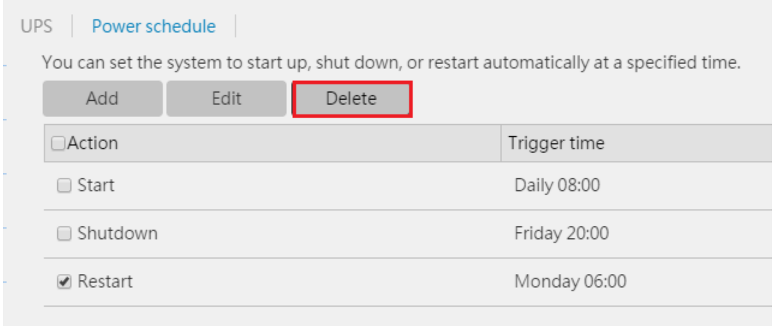


You can set the system to start up, shut down, or restart automatically at a specified time.

□Action	Trigger time
☑ Start	Daily 08:00
□ Shutdown	Friday 20:00
□ Restart	Monday 06:00

Delete a scheduled task

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



You can set the system to start up, shut down, or restart automatically at a specified time.

□Action	Trigger time
□ Start	Daily 08:00
□ Shutdown	Friday 20:00
☑ 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.

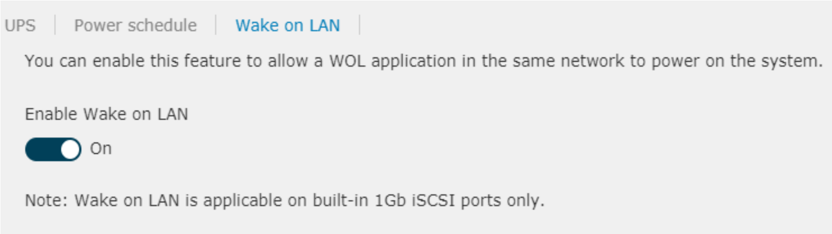
Note:

- WoL is available only to GSe Pro 100 and 200 series.
- Only the built-in 1Gb iSCSI ports (for both block & file level) support WoL.
- 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.



You can enable this feature to allow a WOL application in the same network to power on the system.

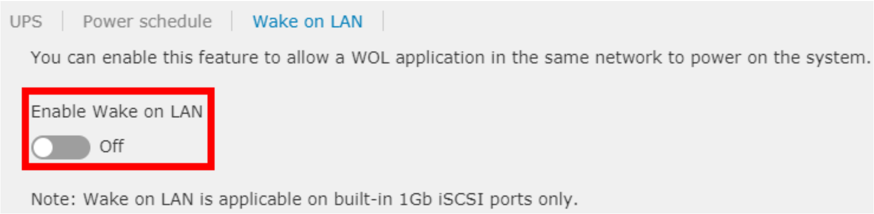
Enable Wake on LAN

On

Note: Wake on LAN is applicable on built-in 1Gb iSCSI ports only.

Enable/Disable Wake on LAN

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



You can enable this feature to allow a WOL application in the same network to power on the system.

Enable Wake on LAN

Off

Note: Wake on LAN is applicable on built-in 1Gb iSCSI ports only.

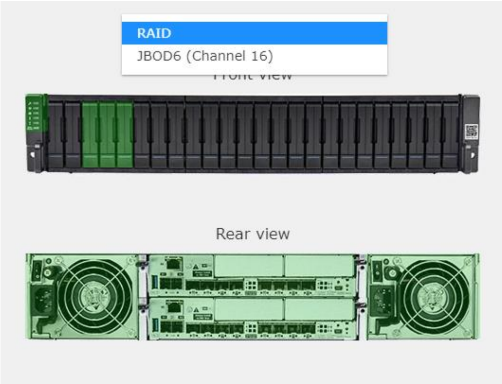
Verify the feature

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 EonOne.
4. Send the magic packets via a free Wake on LAN tool. The system will be powered on.

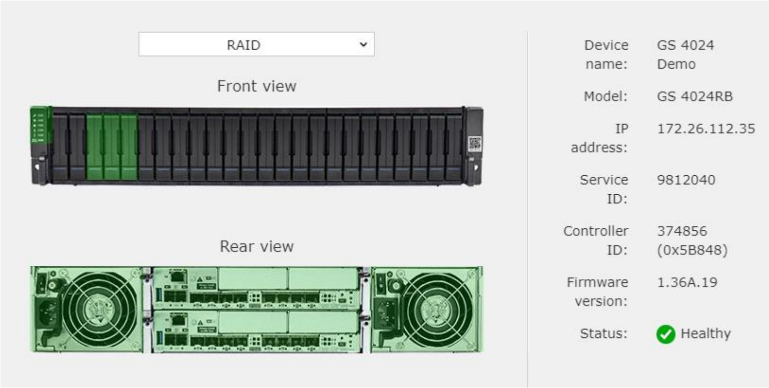
Enclosure View

Go to **Settings / Device management > 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:

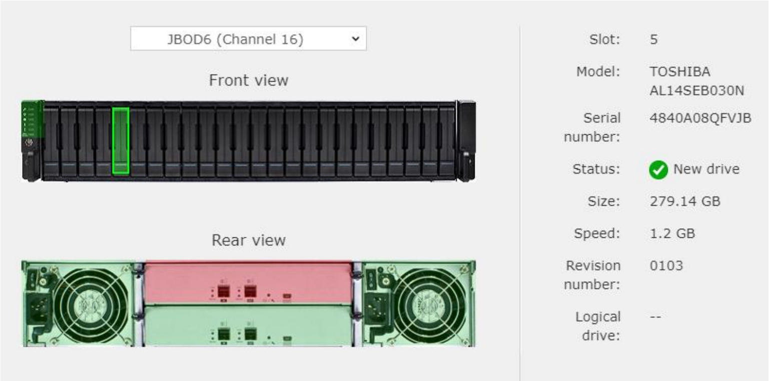


✓ RAID view:



Device name:	GS 4024 Demo
Model:	GS 4024RB
IP address:	172.26.112.35
Service ID:	9812040
Controller ID:	374856 (0x5B848)
Firmware version:	1.36A.19
Status:	✓ Healthy

✓ JBOD view:

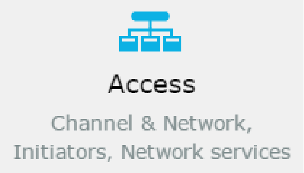


Slot:	5
Model:	TOSHIBA AL14SEB030N
Serial number:	4840A08QFVJB
Status:	✓ New drive
Size:	279.14 GB
Speed:	1.2 GB
Revision number:	0103
Logical drive:	--

Access

The Data Access menu contains the following sub-settings

1. Channel and network settings
2. Initiators
3. Network services
4. VLAN
5. VMware
6. Traffic control

Go to	**Settings / Device management > Access**  Access Channel & Network, Initiators, Network services
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

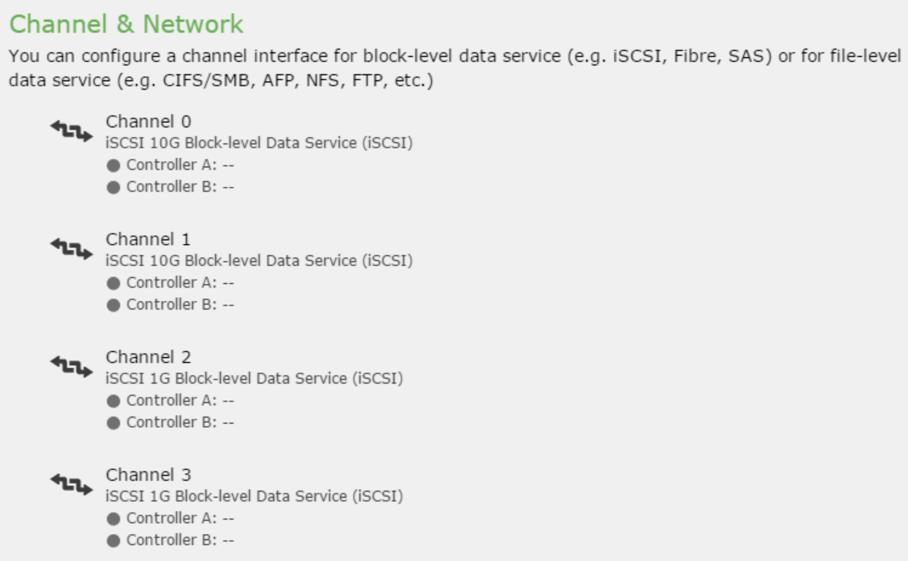
The Channel and Network setting allows users to modify the settings of host channels, management ports, and trunk groups.

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 / Device management > 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.

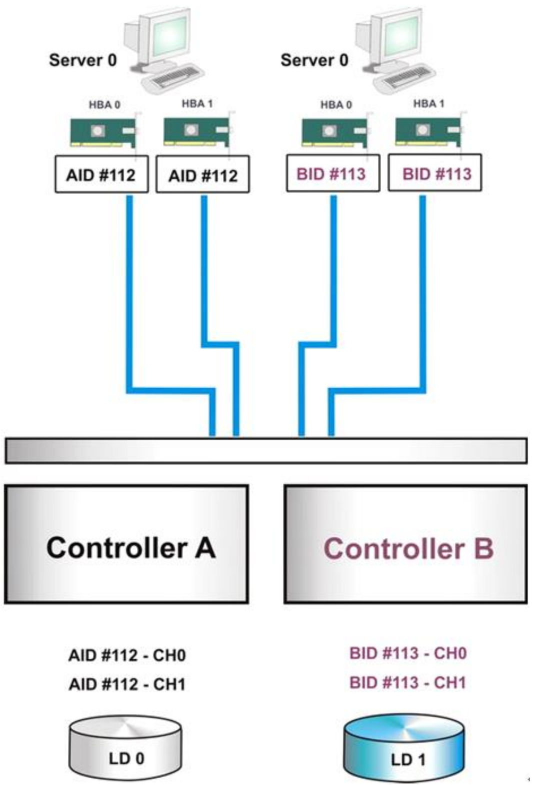
In a dual-active controller configuration, you need to manually create more Slot A or Slot B Channel IDs to distribute the workload between partner controllers.

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 host board, both of its channels can only be set to either file-level or block-level.
- To enable RDMA, make sure you have installed at least 24 GB memory. For dual-controller models, you must install at least 24 GB memory per controller.

Go to	**Settings / Device management > 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.
	RDMA	For onboard ports and host board ports that support RDMA (RoCE), the relevant port is displayed. For iSCSI channels whose type is set to block-level, you can configure as **RoCE** or **iWARP**.
	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:

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

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

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

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

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

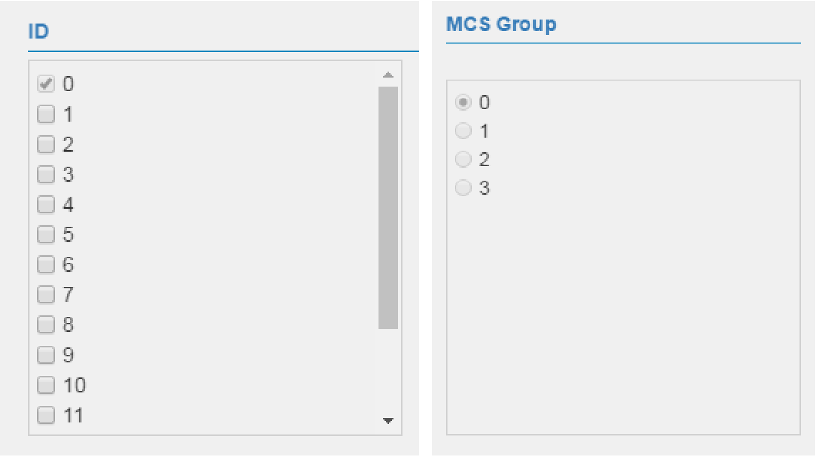
FF05:0:0:0:0:0:0:2

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.

Advanced Parameters

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



ID

☑ 0
□ 1
□ 2
□ 3
□ 4
□ 5
□ 6
□ 7
□ 8
□ 9
□ 10
□ 11

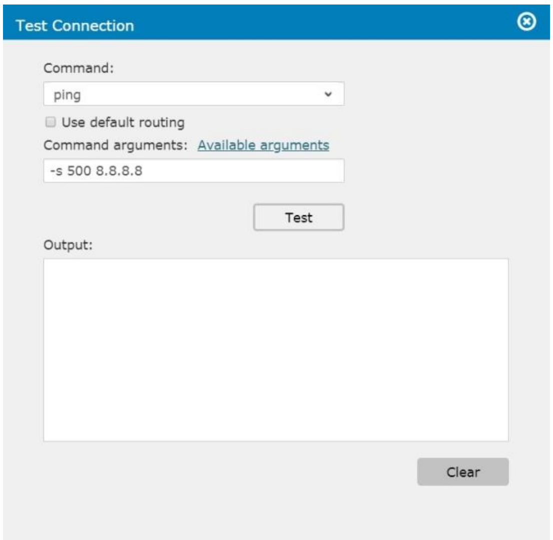
MCS Group

● 0
○ 1
○ 2
○ 3

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.

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



-s 500 8.8.8.8

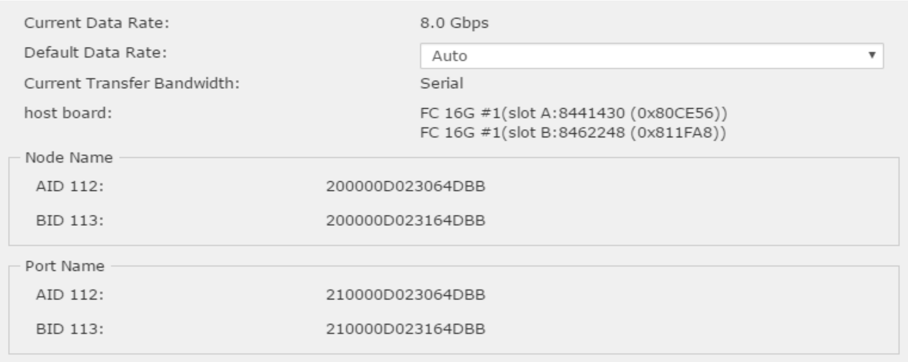
1. Select the desired command in the **Command** drop-down menu:

ping	Check network connection and data transmission speed.
traceroute	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.
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

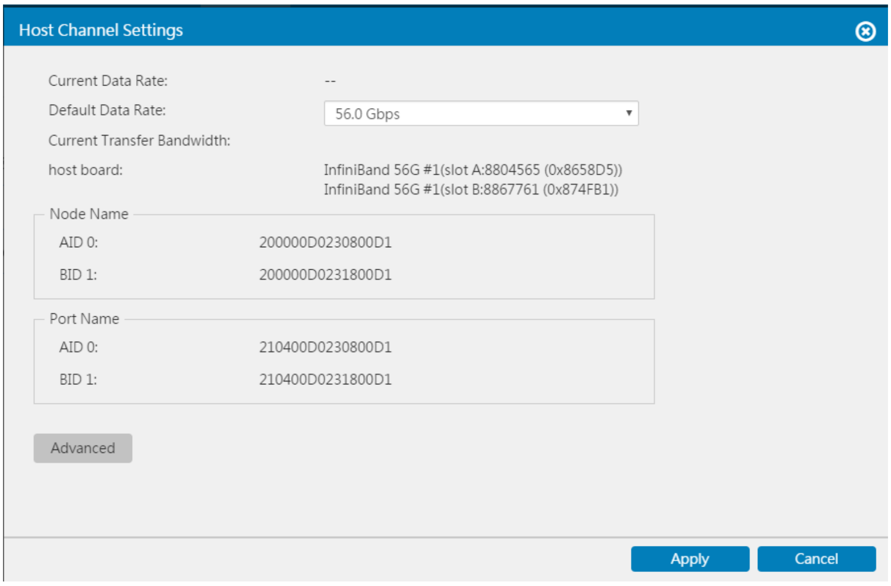
AID 112: 210000D023064DBB

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

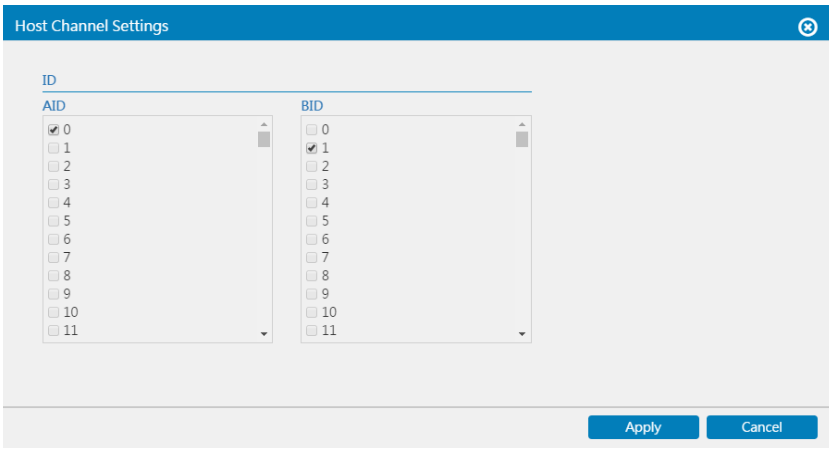
BID 1: 200000D0231800D1

Port Name

AID 0: 210400D0230800D1

BID 1: 210400D0231800D1

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



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

Note:

- If you have two InfiniBand 56Gb/s host boards on one controller, the controller must have at least 16GB of memory.
- 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.

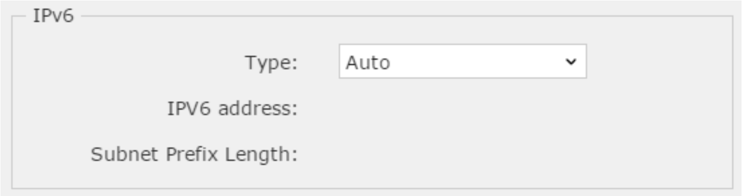
Go to	**Settings / Device management > Access > Channel & Network**	
Steps	1. Scroll the page to the bottom, finding the Management port section and click the **Edit** button. 2. Select the IP address type: **DHCP**, **Static** 3. If you select **Static**, enter the IP address, subnet mask, and the gateway address.	
Notes	You are not allowed to assign any of the following system reserved IP addresses to your subsystem: 127.x.x.x 128.0.x.x 191.255.x.x 192.0.x.x 223.255.255.x	
Parameters	**(IP) Address**	Specifies the IP address of the subsystem. To use DHCP, select **DHCP** from the drop down list. Example: 192.168.4.246, DHCP
	Subnet mask	Specifies the subnet mask for the IP address. When using DHCP, leave this parameter blank.
	Default gateway	Specifies the IP address of the network gateway. When using DHCP, leave this parameter blank.
Note on Using DHCP	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. With DHCP, the IP address may change when cable disconnection or other network errors occur. If you are accessing the subsystem from the EonOne suite, you will have to re-connect with the subsystem with the new IP address.	

Configuring IP Address (IPV6) of Management Port

Go to **Settings / Device management > 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



IPv6

Type: Auto

IPV6 address:

Subnet Prefix Length:

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 are properly configured.
- The maximum jumbo frame size can be 8K or 9K, depending on the firmware version.
- To use 8K jumbo frames, the system must be installed with 8Gb RAM ; to use 9K jumbo frames, the system must be installed with 32Gb RAM.

Go to	**Settings > Access > Channel &Network**
Steps	1. Go to the **Jumbo frames** section. **2.** Turn on jumbo frames. **3.** Choose a desired jumbo frame size: **Disable**, **8K** or **9K** (bytes). If you choose **Disable**, the jumbo frame size is set to 1.5K. **4.** Then, click **OK** to apply the change.

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 and NAS 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.
- For HA storage:
  - If you want to use a trunk group in HA storage, the trunk group must be created before enabling of HA service.
  - If a trunk group is in use by HA storage, the trunk group cannot be deleted.

Go to **Settings / Device management > 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	The system assigns client traffic to different channels

Dynamic Link Aggregation (LACP)	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:

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

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.

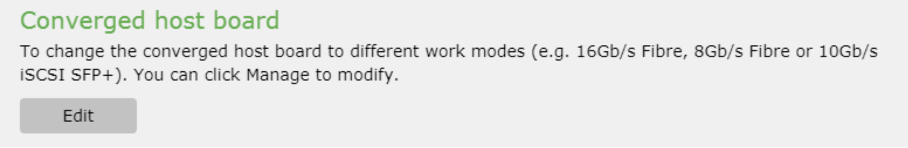
Currently the following channel types supported by the converged host board includes:

- 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**.



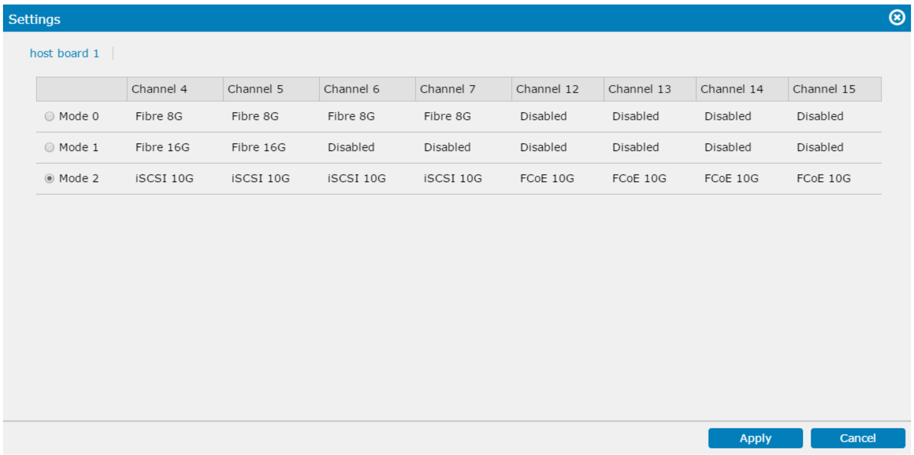
Converged host board

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.

(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
● 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

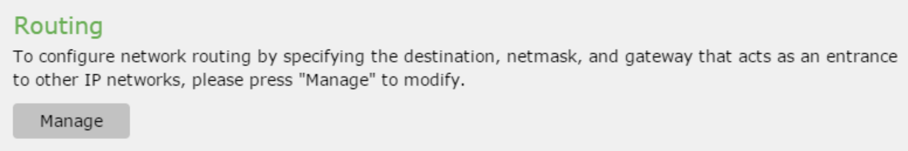
You can configure network routing by specifying the destination, netmask and gateway that acts as an entrance to other IP networks.

Note:

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

Go to **Settings / Device management > Access > Channel & Network**

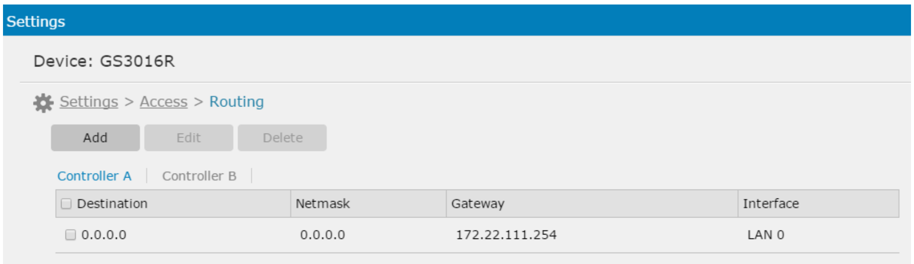
Scroll the page to the bottom and click the **Manage** button under **Routing**.



Routing

To configure network routing by specifying the destination, netmask, and gateway that acts as an entrance to other IP networks, please press "Manage" to modify.

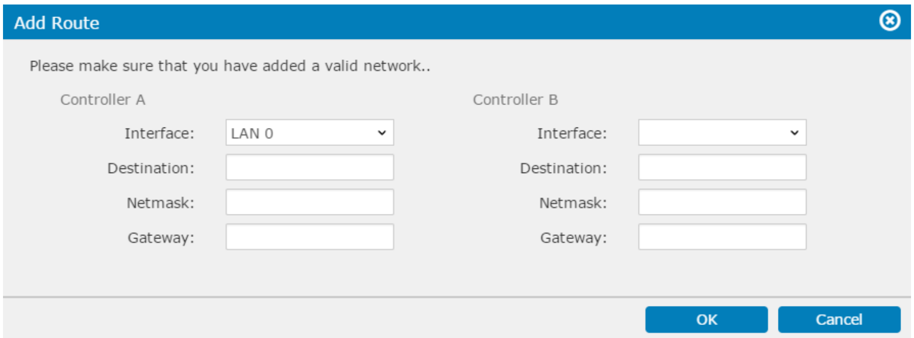
Then, click **Add** to add network routing information.



Device: GS3016R

□ Destination	Netmask	Gateway	Interface
□ 0.0.0.0	0.0.0.0	172.22.111.254	LAN 0

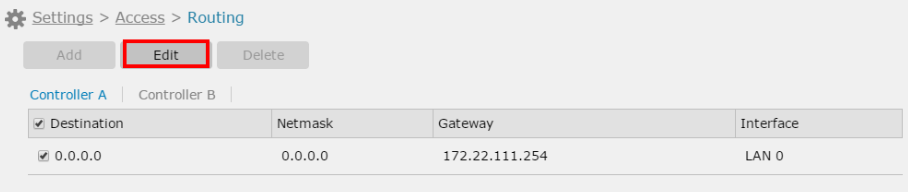
Enter the routing information and click **OK** to apply and save the settings.



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

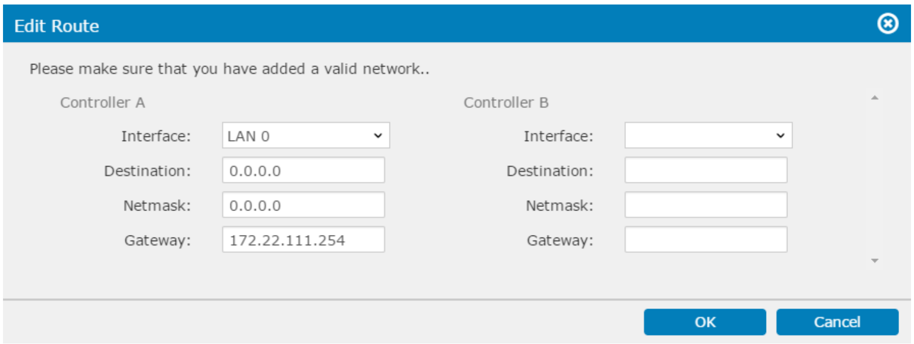
Controller A		Controller B	
Interface:	LAN 0	Interface:	
Destination:		Destination:	
Netmask:		Netmask:	
Gateway:		Gateway:	

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



☑ Destination	Netmask	Gateway	Interface
☑ 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: LAN 0

Destination: 0.0.0.0

Netmask: 0.0.0.0

Gateway: 172.22.111.254

Controller B

Interface:

Destination:

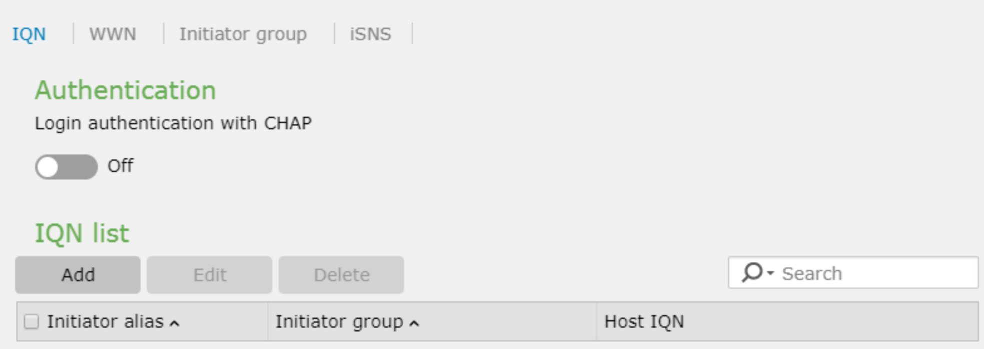
Netmask:

Gateway:

Initiators

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

Go to **Settings / Device management > Access > Initiators**



Authentication

Login authentication with CHAP

Off

IQN list

□ Initiator alias ⌃	Initiator group ⌃	Host IQN

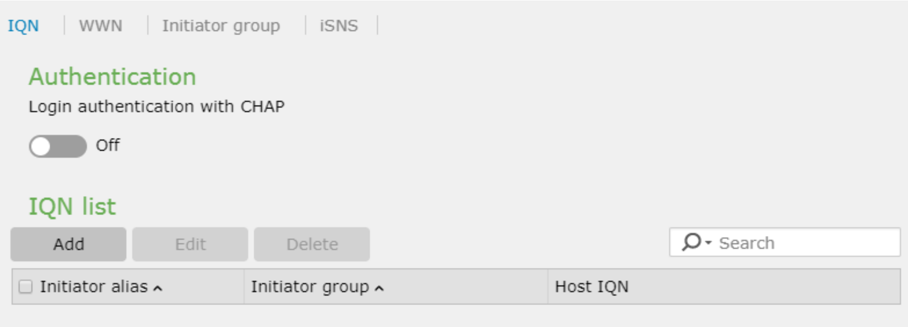
Configuring Alias for iSCSI Initiators

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

Go to

Setting / Device management > Access > Initiators

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

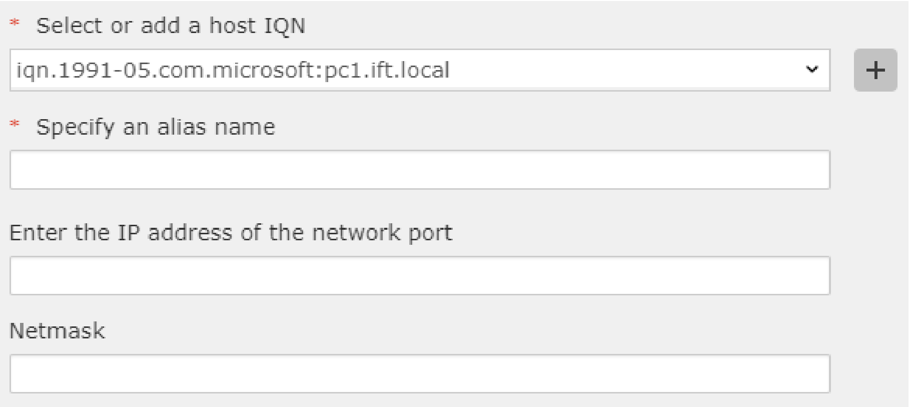


Login authentication with CHAP

Off

Add an Alias (for a iSCSI initiator)

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



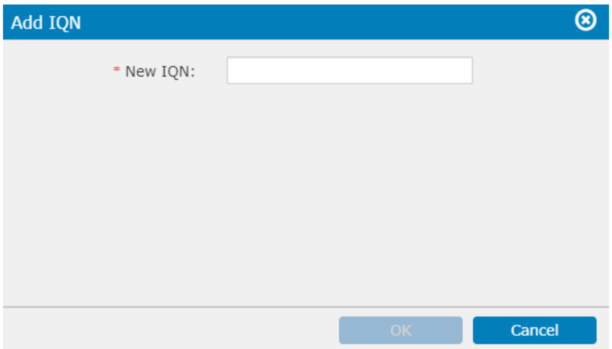
* Select or add a host IQN: iqn.1991-05.com.microsoft:pc1.ift.local

* Specify an alias name

Enter the IP address of the network port

Netmask

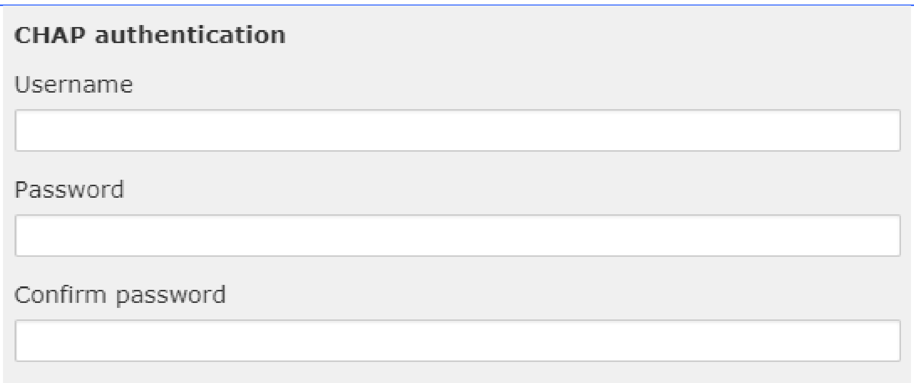
Host IQN: Select one of the pre-defined host IQN or click the **Add** button and type in a new host IQN.



* New 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.



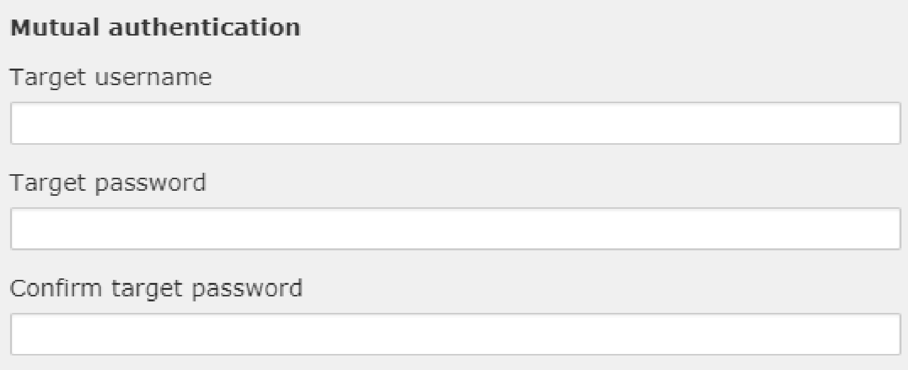
CHAP authentication

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

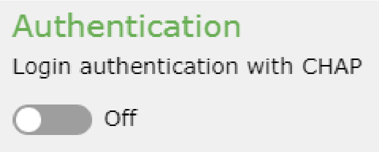
Target password

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

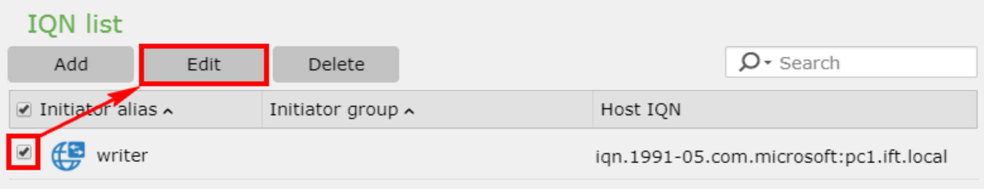
Login authentication with CHAP

○ Off

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

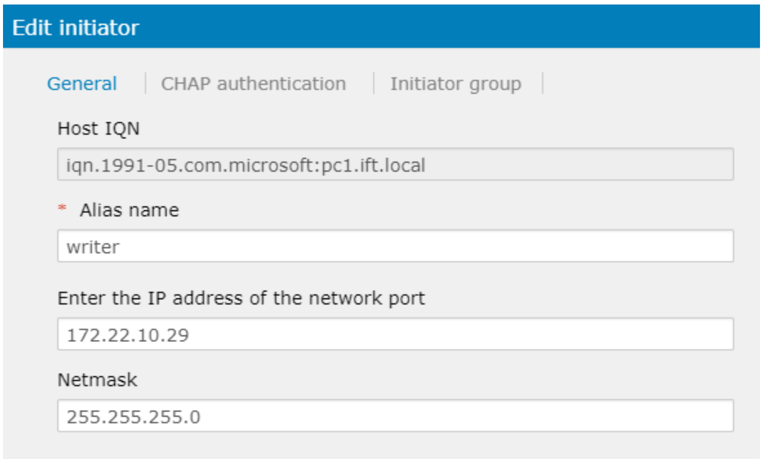
Edit an iSCSI Initiator Alias

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



☑ Initiator alias ⌃	Initiator group ⌃	Host IQN
☑ writer		iqn.1991-05.com.microsoft:pc1.ift.local

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



Host IQN
iqn.1991-05.com.microsoft:pc1.ift.local

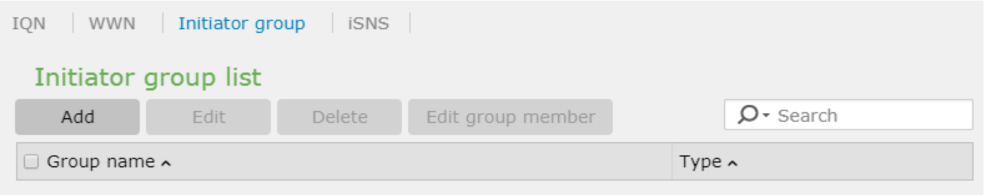
* Alias name
writer

Enter the IP address of the network port
172.22.10.29

Netmask
255.255.255.0

Initiator Group

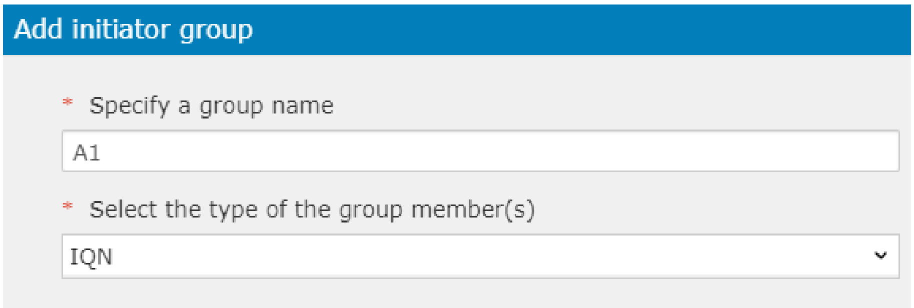
1. Click in the **Initiator** tab to switch to the Initiator group page.



□ Group name ⌃	Type ⌃

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.



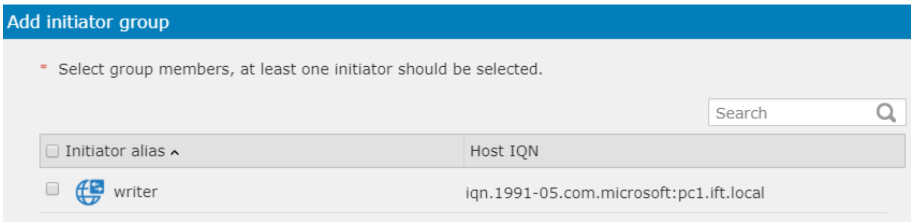
* Specify a group name
A1

* Select the type of the group member(s)
IQN

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

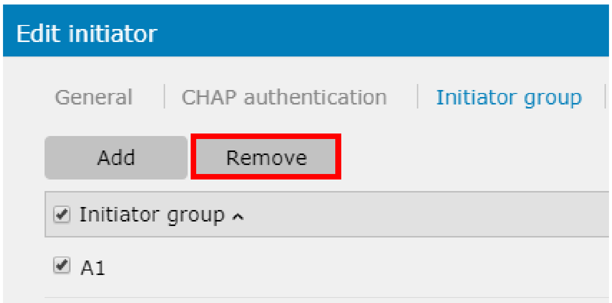
* Select group members, at least one initiator should be selected.

□ Initiator alias ^	Host IQN
□ writer	iqn.1991-05.com.microsoft:pc1.ift.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**.

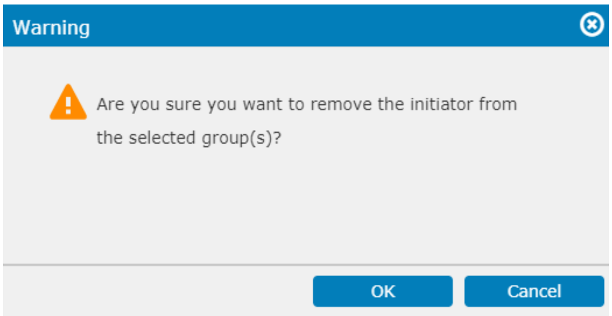
Unassign Group

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

☑ 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)?

Configuring iSNS Server in Storage Subsystems

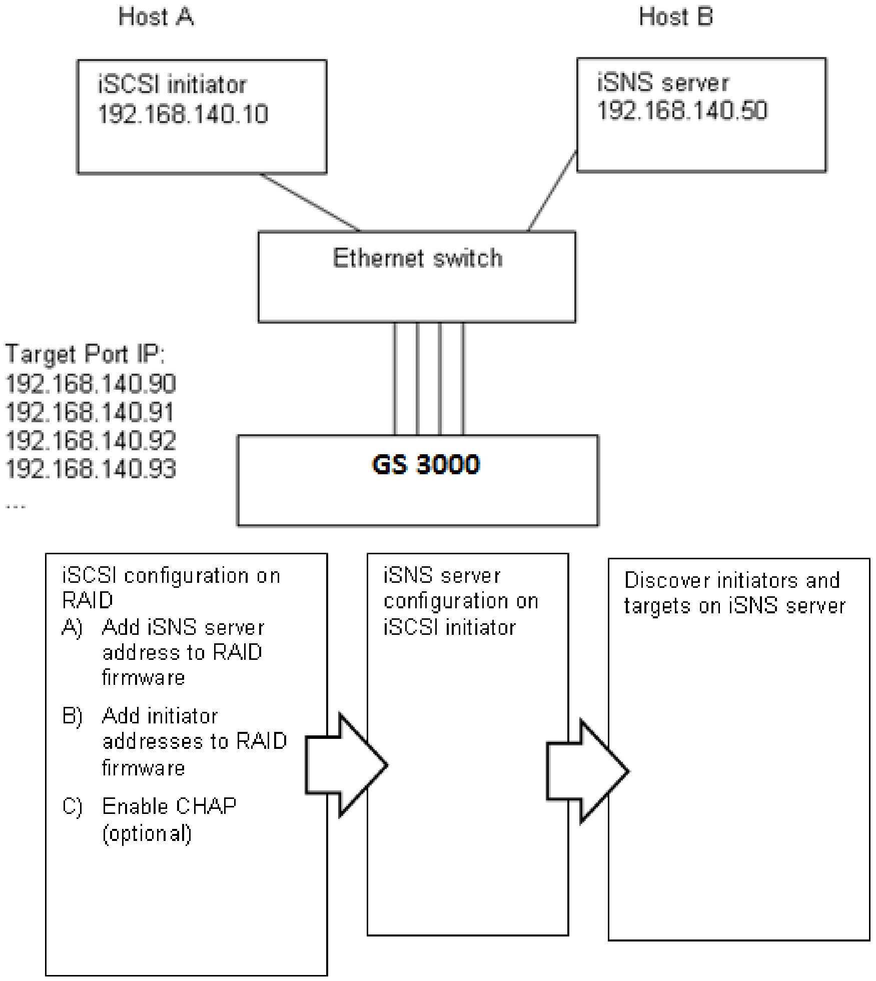
iSNS(Internet Storage Name Service) is a common discovery, naming and resource management service for all IP storage protocols. Infortrend's iSNS implementation complies with RFC 4171 standards. iSNS discovers iSCSI initiators and targets within a domain and their related information. Windows iSNS server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

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.

Limitation Setting up iSNS is available only for iSCSI host models.

Example

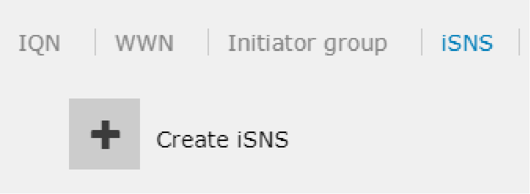

Host A
Host B
iSCSI initiator
192.168.140.10
iSNS server
192.168.140.50
Ethernet switch
Target Port IP:
192.168.140.90
192.168.140.91
192.168.140.92
192.168.140.93
...
GS 3000
iSCSI configuration on RAID
A) Add iSNS server address to RAID firmware
B) Add initiator addresses to RAID firmware
C) Enable CHAP (optional)
iSNS server configuration on iSCSI initiator
Discover initiators and targets on iSNS server

Go to **Settings / Device management > Access > Initiators**

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.

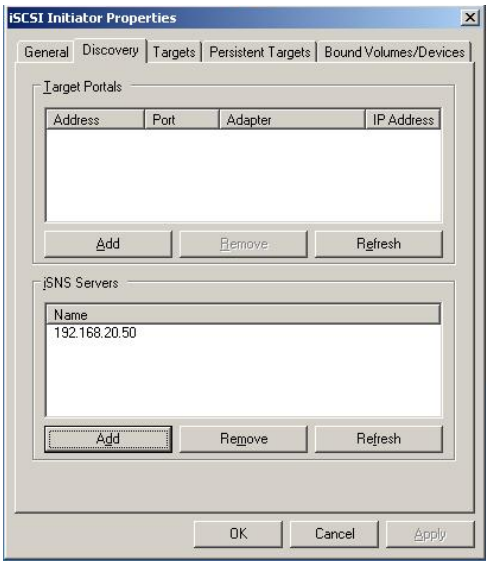
iSNS Settings	**Add:** Click **Create ISNS** and enter the iSNS server IP address. **Edit:** Select an iSNS server and click the **Edit** button to modify the IP address. **Delete:** Select an iSNS server and click the **Delete** button. The iSNS server will be deleted from the list.

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.



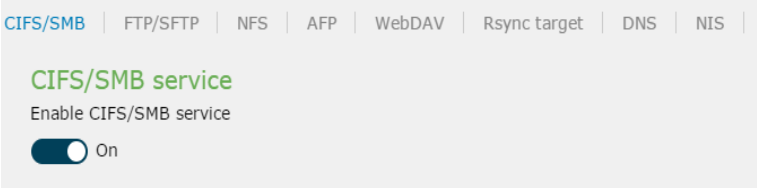
192.168.20.50

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 / Device management > Access > Network Services**
Networking Services	 CIFS/SMB FTP/SFTP NFS AFP WebDAV Rsync target DNS NIS CIFS/SMB service Enable CIFS/SMB service On

Configuring CIFS/SMB Service

CIFS (Common Internet File System) is a protocol developed by Microsoft to enable access to files stored on fileservers 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 / Device management > Access > Network services > CIFS/SMB**

Steps

1. Turn on the CIFS/SMB service.
2. Specify the following settings:

Windows domain name	It displays the name of the Windows Active Directory domain that the system joins in **Settings** > **Privilege** > **AD/LDAP.**
Windows workgroup name	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.
Maximum SMB protocol	Select the latest SMB version allowed when clients access the cluster via CIFS/SMB.
Minimum SMB protocol	Select the oldest SMB version allowed when clients access the cluster via CIFS/SMB. The minimum SMB protocol version should be equal to or less than the maximum SMB protocol version.
WINS Server	Specify the primary and secondary WINS servers' IP addresses.

3. Specify the advanced settings to suit your needs:

Inoperative client checking period	Specify how often the system checks if a CIFS/SMB client is not operative. The value must be between **10** to **864000**.
Support creating multiple connections over SMB	Select this option to allow the system to create multiple SMB connections to improve throughput and network fault tolerance.
Enable opportunistic lock	Select this option to allow clients to cache files locally. The system supports level 2 oplock which allows

(oplock)	client read caching instead of write caching. This can reduce network traffic and improve performance. If the environment is unreliable, disable this option.
Maximum block size (read/write)	Choose the maximum block size that reads/writes through SMB.

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 / Device management > Access > Network services > FTP/SFTP**

Steps

1. Turn on the FTP service.
2. Specify the FTP settings:

Listen port	Specify a port for FTP transfers (default port: 21)
Maximum number of failed login attempts	Specify how many failed login attempts are allowed from an FTP client. The number **0** means no limit. When the specified number is reached, the FTP client is banned from connecting to the system.
Login directory	Choose which directory the client is allowed to access upon login: **User's home directory**: The client can access only the personal directory. **Root directory**: The client can access the root directory. **Customize**: You can customize the login directory for each client. Then, click **Manage** to add a mapping between a client and the login directory.
Enable anonymous FTP	Select this option to allow a client to access files via FTP without unique user credentials.
Enable FTP over SSL/TLS support (FTPS)	Select this option to enable SSL/TLS-encrypted FTP. Enable the auxiliary functions when necessary. ● **Allow explicit FTP over TLS**: After connecting to the system, an FTP client can initiate a secure FTP connection by send this explicit command: `AUTH TLS` To force all clients to use secure connections, select **Disallow plain unencrypted FTP**. ● **Force PROT P to encrypt file transfers in SSL/TLS mode**: Enforce the `PROT P` 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.

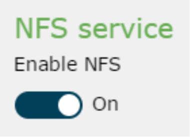
3. Click **Save** to save the settings.
4. To protect FTP connections with SSH, turn on the SFTP service.

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

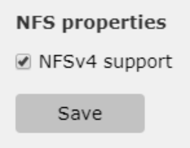
1. Click on the **NFS** tab to switch to the NFS setting page.
2. Click on the switch bar to enable the NFS service.



NFS service

Enable NFS

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**.



NFS properties

☑ NFSv4 support

NLM Support

STORANDER GS/GSe 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.

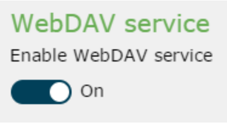
Note: The Network Lock Manager is used only for NFS Version 2 and NFS Version 3 installations.

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

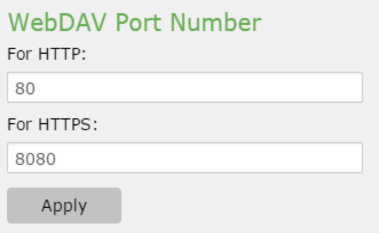
1. Click on the **WebDAV** tab to switch to the WebDAV setting page.
2. Click on the switch bar to enable the WebDAV service.
3. Press **Apply** to save the settings.



WebDAV service

Enable WebDAV service

On



WebDAV Port Number

For HTTP: 80

For HTTPS: 8080

Port for HTTP	WebDAV uses TCP ports 80 by default.
Port for HTTPS	Port 8080 is default port for many web servers.

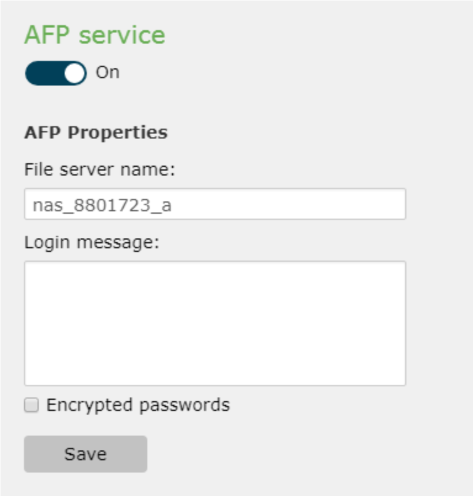
Note: If WebDAV is enabled, when you connect to your EonStor GS/GSe via a web browser, please enter **http://NAS IP:8816** in the web browser**.** If WebDAV is not enabled, you only have to enter **http://NAS IP** and it will automatically redirect to port 8816 (port 8817 for SSL connection).

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

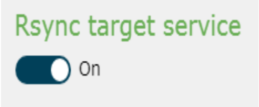
File Server Name	Specifies the server name (the default setting is the name of your system).
Login Message	Specifies a custom message that appears at login.

Configuring Rsync Target Service

Before setting up a EonStor GS/GSe as the Rsync Target (of third party), you need to configure the Rsync Target service first.

Parameters

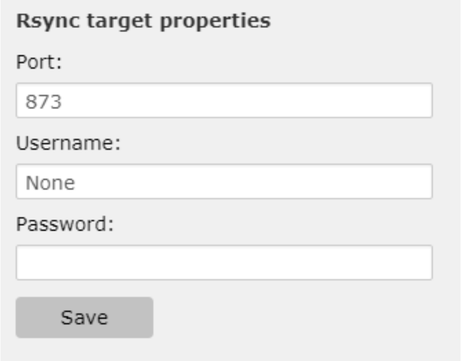
1. Click on the switch bar to enable the Rsync Target service.



Rsync target service

On

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**.



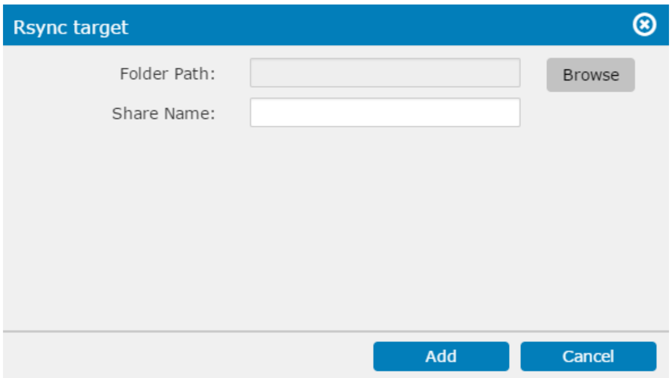
Rsync target properties

Port: 873

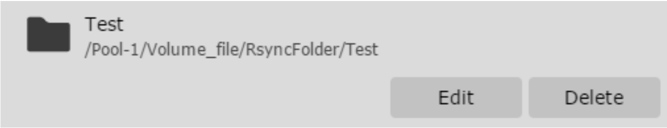
Username: None

Password:

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



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



Test

/Pool-1/Volume_file/RsyncFolder/Test

Rsync Target Information for this case:

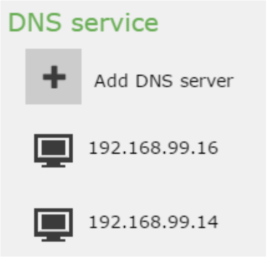
- **Share Name**: Test
- **Directory**: /Pool-1/Volume_file/RsyncFolder/Test

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 service

192.168.99.16

192.168.99.14

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 Object Storage

Go to	**Settings > Access > Network services**

Steps

1. Click the **Object storage** tab to switch to the setting page.
2. Turn on this function by clicking the toggle switch.
3. Select a volume, or create one to run object storage. If you have created a volume before, the one will be available for you to choose. Click the drop-down menu to select it.

   To create one, click **+** and go to Create volume page. Specify the following settings, and click **OK** to keep the settings:

Pool	Choose a pool where the volume resides.
Volume type	The type is pre-selected as **file-level volume for NAS**.
Volume name	Specify an identifying name for the volume.
File system	The file system is pre-selected as **XFS**.
Volume size	Specifies the size and unit of the volume. The minimum size of a volume is 10GB.

4. Click **Save**.

Using Object Storage

To store the data, you can create a bucket via EonOne or the 3rd party software. To access the data, you must create access keys on EonOne to grant access permission to users. Besides, the object lock option is available for you to keep the data immutable. This feature ensures the data will not be overwritten or deleted during a certain period of time.

Go to	**Settings > Access > Network services > Object storage**	
Bucket management	You can create or delete a bucket when needed. On the list of installed apps, find the app and click **Open**.	
	Adding a bucket	1. Click **Add**. 2. Specify the following settings: **Bucket name**: Specify an identifying name for the bucket. **Object lock**: You can only enable this function during bucket creation. To enable it, select the checkbox. 3. Click **OK** to save the settings. A new bucket will be displayed in the list.
	Deleting a bucket	Before deleting a bucket, make sure the bucket is empty. To delete a bucket: 1. Select the desired bucket. 2. Click **Delete**. Click **Yes** to confirm the action and delete it.
Key management	Each user must be granted with access permission to view or store data in the object storage. You can add, edit, regenerate, or delete a key for each user. On the list of installed apps, find the app and click **Open**.	
	Adding a key	1. Click **Add**. 2. Specify the following settings: **Users**: Select **Local users** or **Domain users**. Relevant users will be displayed in the list. Choose the desired user. **Permission**: Select **Read only** or **Read/write** to grant the permission to the user. 3. Click **OK** to save the settings. All users who have access permission will be displayed in the list.
	Change a user's	1. Choose the desired user. Click **Edit**.

	permission type	2. Select **Read only** or **Read/write** to change the permission. 3. Click **OK** to save the settings.
	Regenerating a key	1. Choose and select the desired user. Click **Regenerate**. 2. Click **Yes** to confirm the action and new keys for the user will be generated. Old keys will be replaced.
	Deleting keys	1. Choose one or more desired users. Click **Delete**. 2. Click **Yes** to confirm the action. The one or more users without keys will disappear from the list.
Viewing information & settings	On the list of installed apps, find the app and click **Settings**. To view all service endpoints of the object storage service, click **All service endpoints**.	

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.
- IPv6 is not supported.

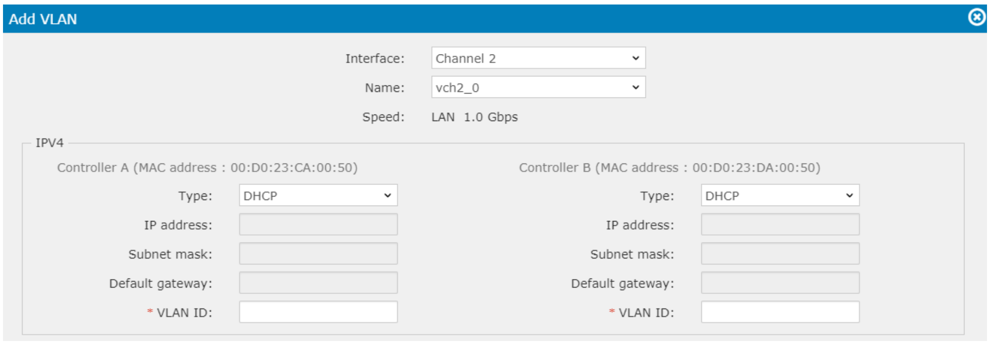
Go to	**Settings / Device management > Access > VLAN**

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.

Create VLAN

Configure VLAN

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



Add VLAN

Interface: Channel 2

Name: vch2_0

Speed: LAN 1.0 Gbps

IPV4

Controller A (MAC address : 00:D0:23:CA:00:50)

Type: DHCP

IP address:

Subnet mask:

Default gateway:

* VLAN ID:

Controller B (MAC address : 00:D0:23:DA:00:50)

Type: DHCP

IP address:

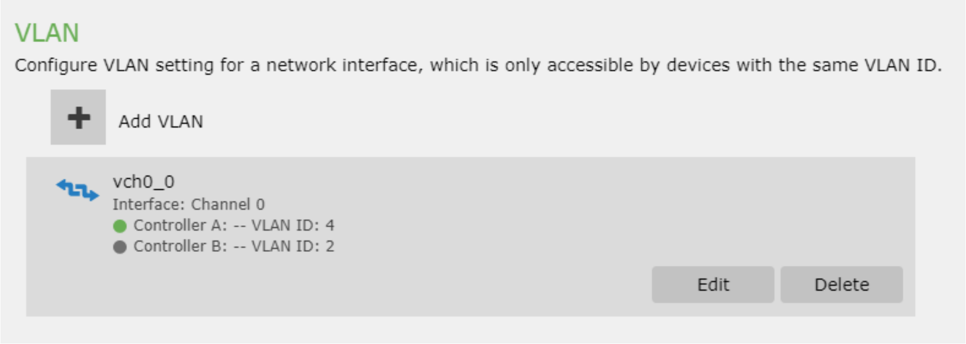
Subnet mask:

Default gateway:

* VLAN ID:

Interface	From the scroll down list, the system only displays the file-level channels.
Name	From the scroll down list, select the VLAN name. The VLAN name are automatically generated following the VLAN Naming Rule
IPv4	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.
VLAN ID	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:



VLAN

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

vch0_0

Interface: Channel 0

● Controller A: -- VLAN ID: 4

● Controller B: -- VLAN ID: 2

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.

VMware

To set up your VMware vSphere environment, you have to connect the storage device with desired vCenters and ESXi hosts so that they can access and manage virtual volumes on the storage.

Add vCenters

vCenter is a vSphere client application for managing virtual machines. When you add a vCenter host to the storage device, it can access and manage virtual volumes on the storage.

Go to **Settings / Device management > Access > VMware**

Steps

1. Click **Add** above the vCenter list.
2. In the pop-up, enter the IP address or hostname of the desired vCenter server.
3. Provide the username and password for login.
4. Click **Find ESXi host**. The system will list all ESXi hosts associated with the vCenter. You can check information of the ESXi hosts:

Host domain	It shows the hostname and domain of an associated ESXi host.
ESXi IP	It shows the IP address of an associated ESXi host.
Version	It shows the ESXi version running on an associated ESXi host.
Status	It shows whether an associated ESXi host can be imported into the vCenter.

5. Select from the available ESXi hosts. The imported ESXi hosts will be imported to the vCenter and run virtual machines.
6. Select **Register VASA Provider**. Then, provide needed information to connect the vCenter with the host running VASA Provider:

VASA Provider IP/hostname	Enter the IP address/hostname of the VASA Provider host.
Username	Enter the VASA Provider username.
Password	Enter the VASA Provider password.

7. Click **OK** to save the settings. The system will display the added vCenter and the selected ESXi hosts at **Settings** > **Access** > **VMware**.

Manage vCenters and ESXi Hosts

You can manage added vCenters and imported ESXi hosts.

vCenter list

IP/hostname: The vCenter host’s IP address/hostname

Version: The version of vCenter running on the host

VASA Provider: Whether the vCenter has a registered VASA Provider host

Status: Whether the vCenter host is connected with the storage device

ESXi host list

IP/hostname: The ESXi host’s IP address/hostname

vCenter IP: The associated vCenter’s IP address

Version: The version of ESXi running on the host

Status: Whether the ESXi host is connected with the storage device

VASA Provider

VASA Provider is a dedicated application that communicates data and commands between virtual machines in vSphere and virtual volumes on your storage devices.

Note: We recommend installing VASA Provider on an independent host running Windows Server 2016 or newer.

Steps

1. Go to Infortrend’s official website and specify your model at **Support** > **Materials Download**.
2. Download the compatible version of VASA Provider and install it on a host computer.
3. Open VASA Provider.
4. Click **Generate SSL certificate** and provide needed information on the pop-up:

The VASA Provider’s IP address	Enter the IP address or FQDN of the host running VASA Provider, as provided in the vCenter. You can provide up to 255 characters.
Your full name (CN)	Enter the system administrator’s full name. You can provide up to 128 UTF-8 characters.
Your organization unit (OU)	Enter the name of your organization unit or company division/department. You can provide up to 128 UTF-8 characters.
Your organization (O)	Enter the name of your organization/company. You can provide up to 128 UTF-8 characters.
Your city/area (L)	Enter the city/area where the host computer is located. You can provide up to 128 UTF-8 characters.
Your state/province/region (ST)	Enter the state/province/region where the host computer is located. You can provide up to 128 UTF-8 characters.
Your country (2-letter code) (E)	Enter the 2-letter code of the country where the host computer is located. You can provide up to 2 alphabetic characters.

5. Click **OK** to generate an SSL certificate using the provided information.

6. Set the login username for VASA Provider.

   You can provide up to 80 case-sensitive alphanumeric characters.

7. Set the login password for VASA Provider.

   You can provide up to 255 case-sensitive alphanumeric characters or special characters:

   ! # $ % & ' ( ) * + - . = @ ^ _ | \

8. Click **Save** to remember the login credentials.

9. Go to **Storage devices**, and click on the fields to check/modify information of storage devices connected with VASA Provider:

IP	The storage device’s IP address
Password	The storage device’s login password
Status	Whether VASA Provider is connected with the storage device
Model	The storage device’s model name

10. Click **Save** to remember the storage devices.

11. Check **VASA Provider status** and click **Run** or **Stop** as needed.

Traffic Control

For file-level channels, you can create and manage the traffic control rules and QoS (Quality of Service) settings to control download traffic running in the network. Besides, you can prioritize the rules by putting them in a particular order.

Note: Before creating a traffic control rule, make sure there is at least a file-level channel in the system. For more details about configuring channel type, refer to Host Channel Parameters.

Adding a Traffic Control Rule

Go to **Settings / Device management > Access > Traffic control**

Steps

1. Select the channel.
2. Click **Add**.
3. Go to Add traffic rule page. Choose which ports to apply the rule.

All	The rule will be applied to all ports.
Select by Application	Select one or more applications. The rule will be applied to the ports which are in use by the selected applications.
Customize	The rule will be applied to the specified ports as well as the selected protocols according to its selected port type. **Type**: Choose the port type as **Source port** or **Destination port**. **Protocol**: Select **All**, **TCP**, **UDP**, **GRE**, or **ESP**. **Port**: Specify certain ports or port ranges. Separate the ports and/or port ranges by commas with no spaces.

4. Specify the following bandwidths:

Guaranteed bandwidth	The outgoing traffic is guaranteed to be served, and it must not exceed 1250000 KB/s.
Maximum bandwidth	The maximum outgoing traffic that can be used, and it must not exceed 1250000 KB/s. To put no limitation on the maximum bandwidth, enter 0 in this field.

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

Editing a Traffic Control Rule

Go to **Settings / Device management > Access > Traffic control**

Steps

1. Select the rule from the list.
2. Click **Edit**.
3. Modify the settings that you want to change.
4. Click **OK** to save the settings.

Prioritizing of the Traffic Control Rules

You can put the traffic control rules in a particular order to prioritize them. The higher a rule is in the list, the higher its priority.

Go to **Settings / Device management > Access > Traffic control**

Steps

1. Click **Prioritize**.
2. Go to Prioritize rules page. Select the rule.
3. Click **Up** or **Down** to adjust the order. You can also click **Top** or **Bottom** to move the rule to the top or bottom of the list.

   If needed, you can also check if the rule is enabled or disabled at the end column of the rule list. To enable or disable specific rules, refer to Enabling/Disabling a Traffic Control Rule.
4. Click **OK** to save the settings.

Enabling/Disabling a Traffic Control Rule

Go to	**Settings / Device management > Access > Traffic control**
Steps	1. Find the rule that you want to enable/disable in the list. 2. Click the toggle switch at the end column of the rule to change its status.

Deleting a Traffic Control Rule

Go to	**Settings / Device management > Access > Traffic control**
Steps	1. Select the rule from the list. 2. Click **Delete**. Click **Yes** to confirm the action.

File Explorer

Note:

- Only GSe Pro and GSi models support access to attached USB storage devices via File Explorer.
- Compatible USB file systems are EXT3, EXT4, exFAT, FAT32, HFS+, and NTFS.
- Make sure there is a channel configured for file-level service.

Enabling and Opening File Explorer

Go to **Settings > Access > File explorer**

Steps

1. Click the toggle switch to enable File explorer.
2. You can open File Explorer through EonOne or your browser:
   - To open File Explorer through EonOne or your browser, click **Open Controller A** or **Open Controller B**. EonOne will connect to the file system via the data port of the controller.
   - To open File Explorer through your browser:
     - ■ Entry point: **http://device_ip:port/**
     - ■ Port number: **8989**

     Note: The port number is not configurable.
3. Enter your username and password. Click **Login**.

Note:

- The login user has to have the application privilege to access File Explorer.
- The user login authentication will include both NAS local account authentication and domain (AD/LDAP) authentication.
- The account “admin” is used for system management only.

4. After logging in, you will see the folders under volume ID/ volume name.

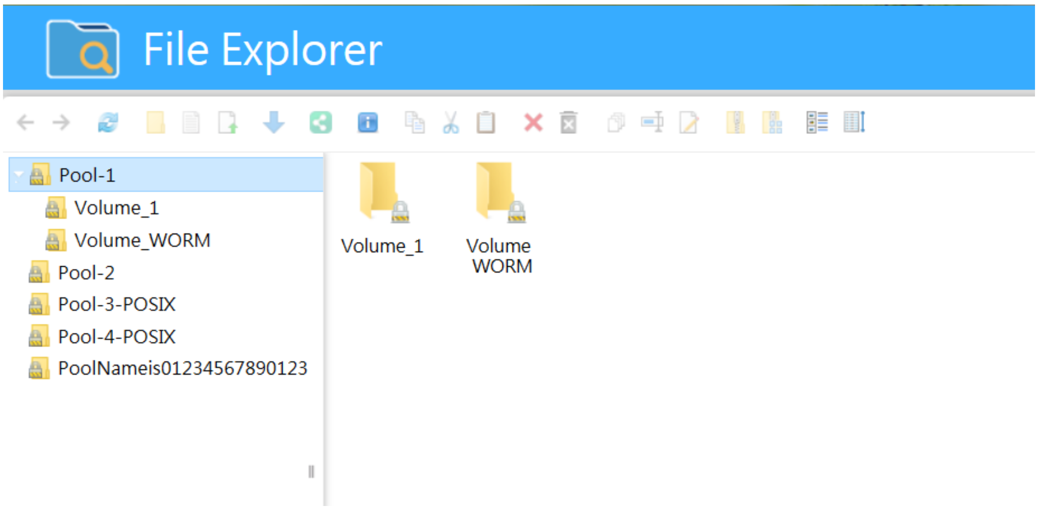
Viewing and Managing Files in File Explorer

In the File explorer, you can do the following to manage your files and folders:

- Create a folder
- Work with a text file
- Upload files
- Work with zip files
- Search for files
- Sort files/folders

Go to **Settings > Access > File explorer**

Overview 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.

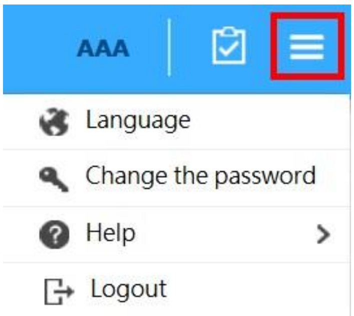
Reload: reload the page.

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.

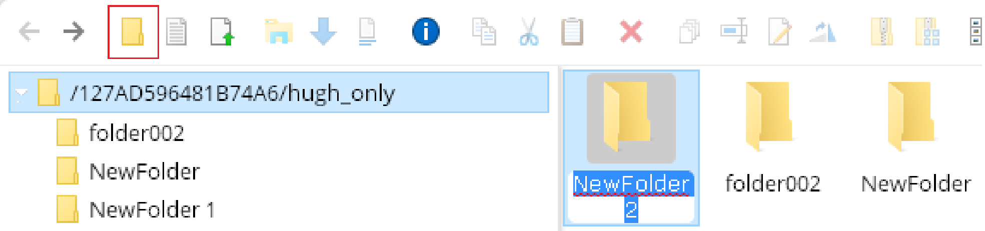
	Download: download the highlighted file/folder. Share: share a folder. Get info: show the information about the selected file. When multiple files are selected, only the total number selected will be displayed. Copy: copy a highlighted file/folder. Cut: cut a highlighted file/folder. Paste: paste a copied/cut 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 EonOne > Settings > Privilege > Users > More > Password policy > Allow local users to change their passwords. Then, log in to File Explorer again as a local user.

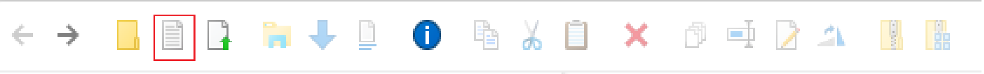
Create a new folder

Click the icon 📁 to create a new folder under the folder highlighted in the left pane.



Work with a text file

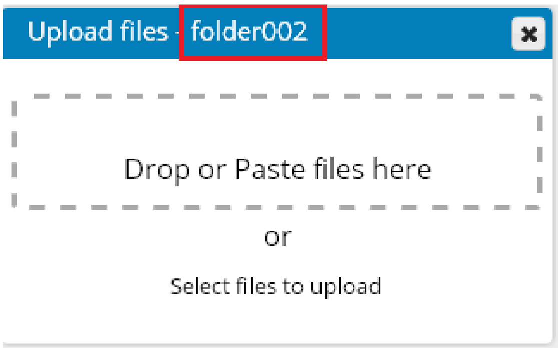
Click the icon 📄 to create a new text file under the folder highlighted in the left pane.



Select a text file and click the icon 📝 to edit it.

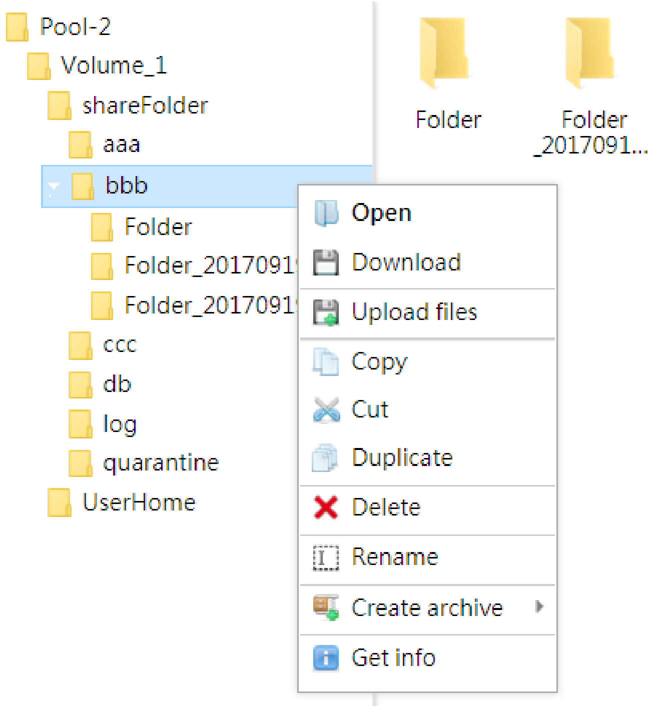
Upload files

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		You can create/extract a zip file and specify its file name.
	Create a zip file	Select one or more files to compress and click . A popup menu will appear for you to select the zip file type as **TAR archive**, **TGZ archive**, **XZ archive**, or **ZIP archive**.
	Specify a zip file name	Click the file name and edit it.
	Extract a zip file	Select one or multiple zip files to extract and click . A popup menu will appear for you to place the extracted files in a **New folder** or **Here**.
Search for files		Click the search bar at the top-right corner. Here are basic search and advanced search: ● **Basic search**: Enter keywords in the 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 the downward arrow icon on the search bar and provide relevant information.
Sort files/folders		Click to sort the files/folder. A popup menu will show the available sorting options: **by name**, **by size**, **by kind**, or **by date**. You can also check to sort them as **Folders first**.
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 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 ☒ and then the red trash can icon.

Changing the Ownership of a Shared folder and its Subfolder

Note: Only the system administrator can change the subfolder owner.

Go to **Settings > Access > File explorer**

Steps

1. Right-click on a shared folder or a subfolder. A pop-up menu will display the available operations for the shared folder/subfolder.

2. 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.

3. Go to the **General** tab. Click **Set**.

4. On the pop-up menu, select a user from listed local users or domain users.

5. 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**.

Changing Permission to Access a 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.
- 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.
- 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**.

Go to **Settings > Access > File explorer**

Steps

1. Go to the **Permission tab**.
2. To add extra permission settings, click **Add**. 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. Click **Apply** to complete the seetings.
3. 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**.

Sharing Subfolders

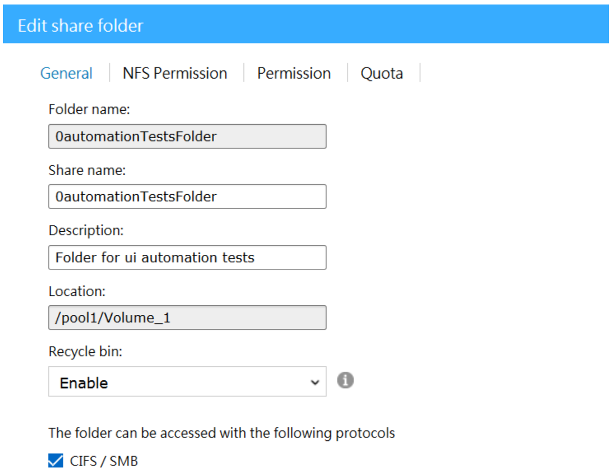
You can share subfolders in a shared folder via common file transferring protocols. To share a folder, right-click a desired one, select **Share**, and complete the following settings.

Note: This function is not supported on the GSi family models.

Go to **Settings > Access > File explorer**

General

1. Specify basic information of the shared subfolder.



Edit share folder

Folder name: 0automationTestsFolder

Share name: 0automationTestsFolder

Description: Folder for ui automation tests

Location: /pool1/Volume_1

Recycle bin: Enable

The folder can be accessed with the following protocols

☑ CIFS / SMB

Folder name	The shared subfolder’s name is displayed.
Share name	Set an identifying name to this shared subfolder. When other users are accessing it, they identify it with this name.
Description	Specify additional identifying information.
Location	The shared subfolder’s location is displayed.
Recycle bin	Enable or disable a recycle bin for this shared folder. This option is only available when **CIFS/SMB** is selected.

2. Select the protocols for accessing the shared subfolder: **CIFS/SMB**, **FTP**, **SFTP**, **NFS**, **AFP**, **WebDAV**, and **Object**.

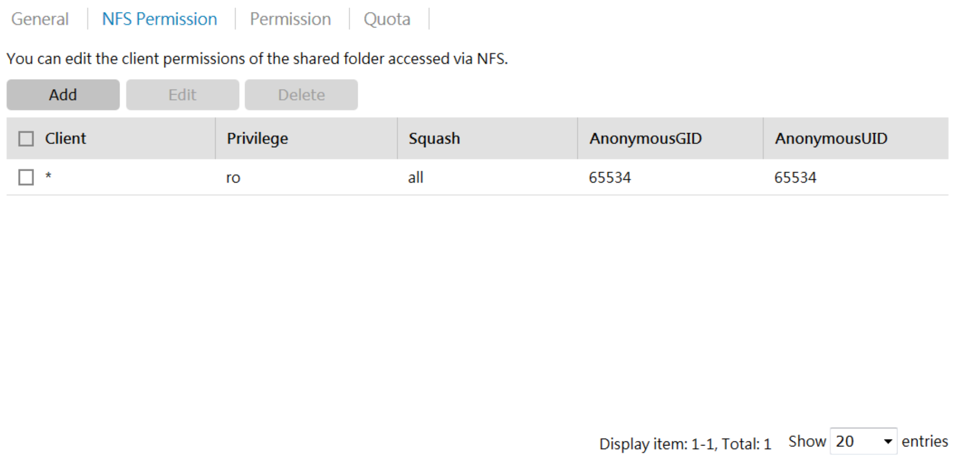
   When you select the CIFS/SMB protocol, you can apply further options:

Enable access-based enumeration	Let users only see files and folders that they have read access to.
SMB encryption	Encrypt data transfers over SMB connections.
Enhance SMB compatibility with macOS and iOS clients	Increase compatibility with an SMB client running on the macOS system.

	(Not supported for EonCloud)	
	Transfer files in asynchronous mode	This option allows the system to transfer files asynchronously to minimize file transfer wait time and avoid transfer bottlenecks.

NFS Permission

When you select the NFS protocol in the **General** tab, you can click **Add** to create an access privilege entry.



You can edit the client permissions of the shared folder accessed via NFS.

□ Client	Privilege	Squash	AnonymousGID	AnonymousUID
□ *	ro	all	65534	65534

Display item: 1-1, Total: 1

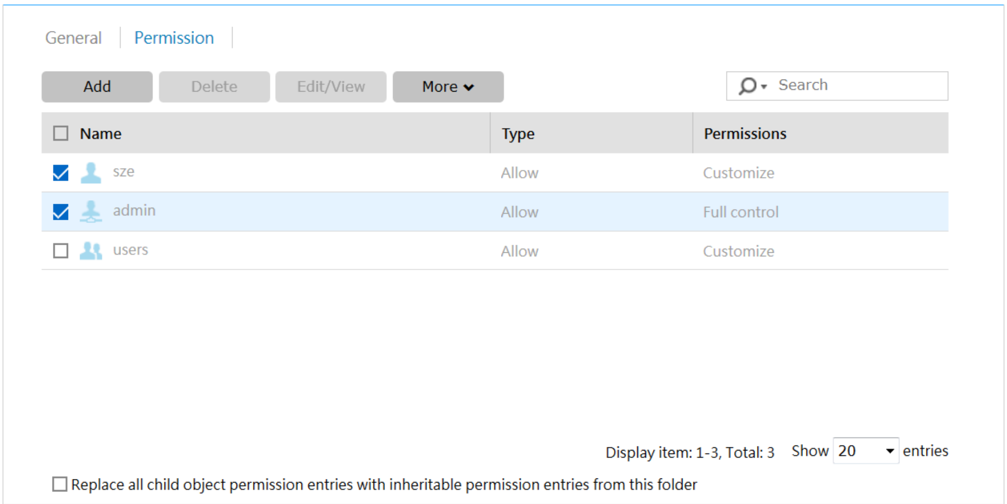
IP / Hostname	Specify the IP address or hostname of a privileged user.	
Access rights	Specify the user’s access privilege: **Read only** or **Read/Write**.	
Squash	Specify the access privileges for remotely accessing users:	
	All Squash	All remote users are identified as anonymous users (i.e. non-administrator 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

Add | Delete | Edit/View | More

Search

□ Name	Type	Permissions
☑ sze	Allow	Customize
☑ admin	Allow	Full control
□ users	Allow	Customize

Display item: 1-3, Total: 3 Show 20 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.
	Change	Change access permissions of this

	permission	shared subfolder.
	Take ownership	Have the ability to be the owner of this shared subfolder.
Read	Assign the read privileges to the user/group:	
	All	Assign all read privileges.
	Traverse folders / execute files	Enter and exit child folders and execute child files.
	List folders / read data	List child folders and read child files.
	Read attributes	Read attributes of child files and folders.
	Read extended attributes	Read extended attributes of child files and folders.
	Read permissions	Read access permissions of child files and folders.
Write	Assign the write privileges to the user/group:	
	All	Assign all write privileges.
	Create files / write data	Create files in child folders, and write data into child files.
	Create folders / append data	Create folders in child folders, and write data into child files with the original data unchanged.
	Write attributes	Change attributes of child files and folders.
	Write extended attributes	Change extended attributes of child files and folders.
	Delete subfolders and files	Delete child folders and 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**.

Appliance

You can improve storage capacity and performance by integrating several storage devices into one file cluster.

The appliance menu contains the following sub-settings.

1. Member appliances

Member Appliances

View the status and details of all member appliances in the cluster.

Adding an Appliance

Go to	**Cluster settings > Appliance > Member appliances**

Steps

1. Click **Add an appliance**.
2. Choose an appliance from the list to join the cluster. Then, click **Next** to continue. If needed, click **Rescan** to reload all available appliances.
3. Go to cluster member settings section. Specify the device name. Configure the management interface IP and the file server name. Click **Next**.
4. Go to channel section. If needed, select one of the channels and click **Edit** to edit it. Click **Next**.
5. Go to storage section:

Pool	For a used model, you can click **View existing pools** before creating a new one. You can select **skip** to create a new pool later, or select **Create a pool now**. If you are going to create a pool now, specify an identifying name for the new pool. You can click **Change** to check and edit the configuration of the pool. For a new model, create a new pool and specify the pool name. Only applied models need to select the pool mode as **Asymmetric Active/Active** or **Symmetric Active/Active mode.** For those models with dual controllers, create and specify the pool name under each controller.
Block-level volume for SAN	For a used model, you can click **View existing block-level volumes** before creating a new one. To create a block-level volume for SAN, specify the volume name and the volume size. If needed, select **Use thin provisioning**. For a new model, specify the volume name and the volume size to create a new volume. If needed, select **Use thin provisioning**.
File-level volume	**Note:** File-level volumes cannot be configured on a

for NAS	pool in Symmetric Active/Active mode. For a used model: You can click **View existing file-level volumes** before creating a new one. Specify the volume name. Choose **XFS** or **Btrfs** as the file system. When you choose XFS, you can select **Enable case-insensitive file and folder names** to suit your needs. When you choose Btrfs, if needed, select **Enable deduplication**. You can choose its data compression policy as **LZO**, **ZSTD**, or **ZLIB** to suit your needs. Specify how much storage space to allocate to the volume. For a new model: Specify the volume name. Choose **XFS** or **Btrfs** as the file system. When you choose XFS, you can select **Enable case-insensitive file and folder names** to suit your needs. When you choose Btrfs, if needed, select **Enable deduplication**. You can choose its data compression policy as **LZO**, **ZSTD**, or **ZLIB** to suit your needs. Specify how much storage space to allocate to the volume.

6. Go to summary section to view all settings that have been done in previous steps.

7. Click **Start initialization** to save the settings.

Privilege

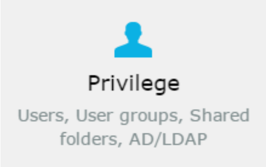
The Privilege setting menu contains the following sub-settings.

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

For cluster settings, the Privilege setting menu contains the following sub-settings.

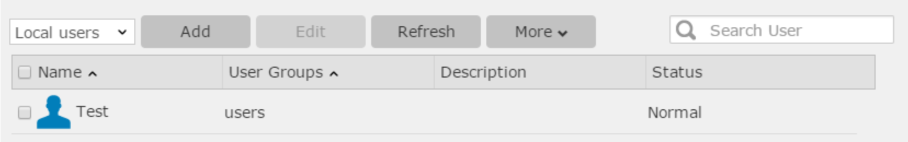
1. Users Settings
2. User Group Settings
3. AD/LDAP Settings
4. NIS

Go to **Settings / Device management / Cluster 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.



□ Name	User Groups	Description	Status
□ Test	users		Normal

Users

Adding a User Account

User accounts can be created to allow access to shared files with unique usernames and passwords. You can create a user and set a volume usage limit on the user.

Note:

- Quota settings are only available on XFS volumes.
- When the specified capacity limit for a user is reached, write operations by the user to the volume will fail.

Go to	**Settings / Device management > Privilege > Users**	
General	1. Click **Add** to create a new user. 2. The Add User window will appear. In the **General** tab, specify the following information:	
	Username	Specifies the new user name. No spaces are allowed.
	UID	Assign a unique UID to this user for system's identification. The UID can only be a number between 100001 and 999999.
	Password	Enter the password for this user account. (default password policy requires at least 8 characters; you can change the setting by clicking Password Policy.)
	Description	Shows a description for this user.
	Group	Specifies the group which this user belongs.
	Home Directory	Creates a home directory (volume) for this user. When you check the box, the home directory path will automatically appear.
	Password	Specifies the validity period of the user password. The

<table>
<tr><td></td><td>
<table>
<tr><td><b>Expiration</b></td><td>user has to change the password when it expires.</td></tr>
</table>
6. If needed, you can set the usage quota for the user. Click the <b>Quota</b> tab. If not, click <b>OK</b> to save the settings.
</td></tr>
<tr><td><b>Quota</b></td><td>
1. In the <b>Quota</b> tab, choose a volume and click <b>Edit</b>.
2. Choose a volume quota limit for the user:
<table>
<tr><td><b>No limit</b></td><td>The user does not have any volume quota limit.</td></tr>
<tr><td><b>Custom</b></td><td>Specify a volume quota limit on the user.</td></tr>
<tr><td><b>Same as the group quota limit</b></td><td>Apply the group quota limit to the user.
If the user belongs to multiple user groups, only the highest group quota limit applies to the user.
To set a group quota limit and learn more details about group quota limit, see the “Group quota limit management” in Creating a User Group.</td></tr>
</table>
3. Click <b>OK</b> to save the settings.
</td></tr>
</table>

Importing User Accounts in Batch

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

Prerequisite

Prepare a user list file in the .csv format in UTF-8 character encoding.

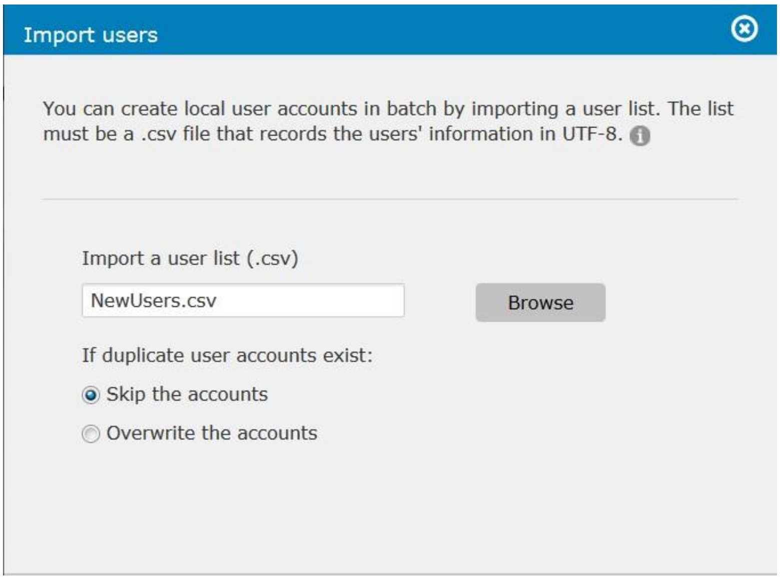
For each user, provide the following types of information from left to right in the same row, and separate each type with a comma (,):

Username (leftmost)	Specify a username. To avoid import errors, do not include any comma (,).
UID	Specify a UID. The UID must be between 100001 and 1000000.
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: **30** (30 days), **60** (60 days), **90** (90 days), or **N** (no validity limit).
Notification days before expiration	Specify when to notify a user before the password is expired: **7** (7 days), **14** (14 days), or **N** (no validity limit).
User home directory	Specify whether to enable a user home directory: **Y** (enable) or **N** (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: **MB**, **GB**, **TB**, or **PB**.

Go to **Settings / Device management > Privilege > Privilege > Users**

Steps

1. Click **More** and select the **Import users** option.
2. Click **Browse** to select the user list file to import.



You can create local user accounts in batch by importing a user list. The list must be a .csv file that records the users' information in UTF-8.

Import a user list (.csv)

NewUsers.csv

If duplicate user accounts exist:

● Skip the accounts

○ Overwrite the accounts

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

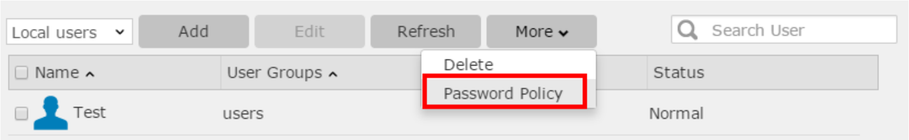
Skip the accounts	The system skips duplicate accounts while importing the user list.
Overwrite the accounts	The system overwrites existing duplicate accounts with information imported from the user list.

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

Setting Password Policies

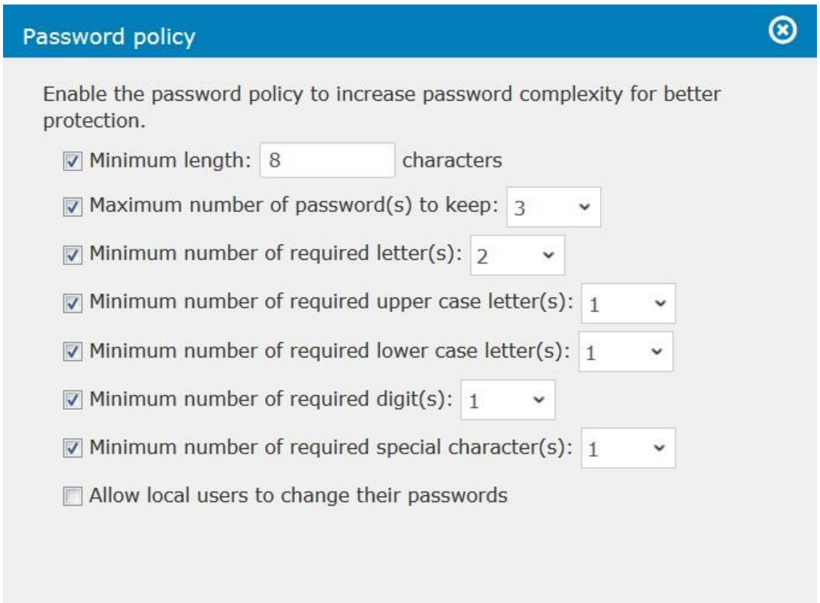
Set user password policies to allow EonOne and File Explorer users to manage their passwords.

Go to **Settings / Device management > 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.
Minimum number of required lower case letter(s)	Specify the least number of lowercase characters allowed for a password.

Minimum number of required digit(s)	Specify the least number of numeric characters allowed for a password.
Minimum number of required special character(s)	Specify the least number of special characters allowed for a password. Accepted special characters are those available on the keyboard (including the space character).
Allow local users to change their passwords	Select to allow local users to modify their own passwords without the system administrator’s assistance.

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

Editing a User Account

Go to	**Settings / Device management > Privilege > Users**

Steps

1. Choose a user to edit the user’s settings.
2. Click **Edit**.
3. Change the desired settings.
   - To change the user account information, click the **General** tab. When you change the user’s home directory by choosing **Use existing home directory**, click **Take ownership** to ensure that the user has full access rights to the selected folder.
   - To change the user quota limit, click the **Quota** tab. For more information about quota settings, see Adding a User Account.
4. Click **OK** to save the changes.

Deleting a User Account

Go to **Settings / Device management > Privilege > Users**

Steps

1. Choose one or more of users.
2. Click **Delete**.
3. Choose to **Delete the home directory** or **Keep the home directory for further use**.
4. Click **Delete User**.

Object Access Keys

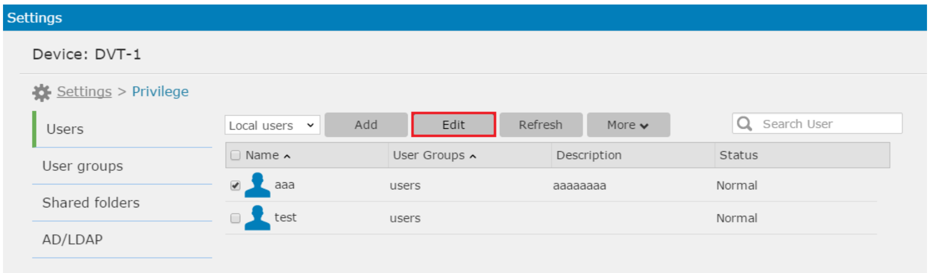
The administrator can create/delete object access keys for users.

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

Go to

Settings / Device management > Privilege > Users

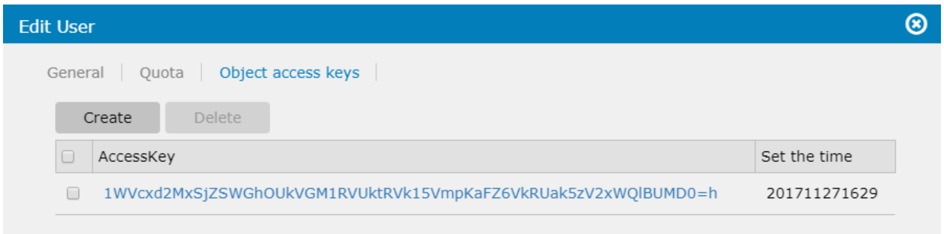
Select a user and click the **Edit** button.



	Name	User Groups	Description	Status
☑	aaa	users	aaaaaaaa	Normal
□	test	users		Normal

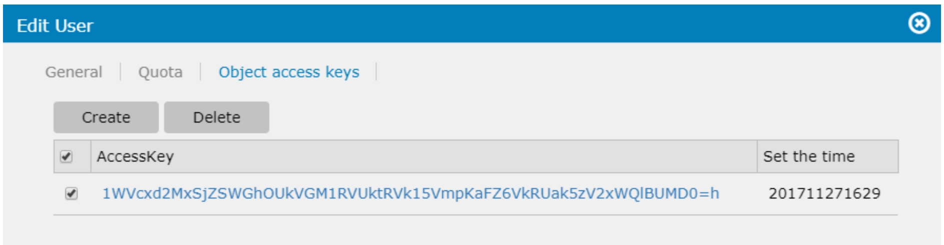
Steps

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.



□	AccessKey	Set the time
□	1WVcxd2MxSjZSWGhOUkVGM1RVUktRVk15VmpKaFZ6VkRUak5zV2xWQlBUMD0=h	201711271629

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



☑	AccessKey	Set the time
☑	1WVcxd2MxSjZSWGhOUkVGM1RVUktRVk15VmpKaFZ6VkRUak5zV2xWQlBUMD0=h	201711271629

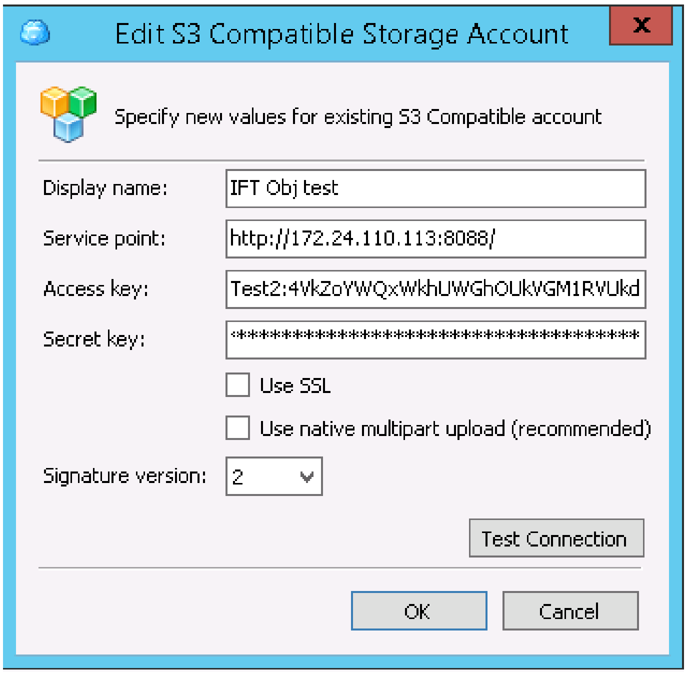
Access Object Storage

You can access the object storage via 3rd 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 EonStor GS/GSe 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.



Edit S3 Compatible Storage Account

Specify new values for existing S3 Compatible account

Display name: IFT Obj test

Service point: http://172.24.110.113:8088/

Access key: Test2:4VkZoYWQxWkhUWGhOUkVGM1RVUkd

Secret key: **

□ Use SSL

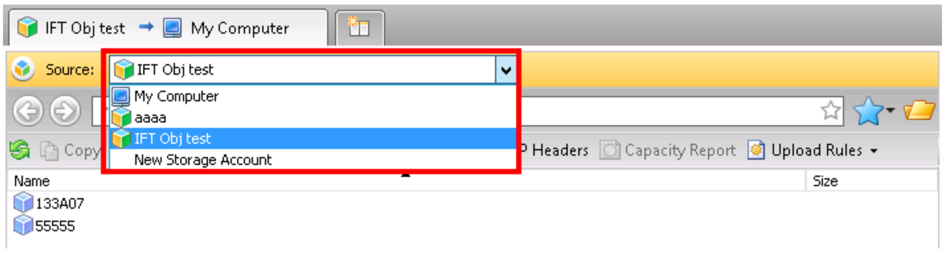
□ Use native multipart upload (recommended)

Signature version: 2

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.



Source: IFT Obj test

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

User Group

You can create a user group and manage its settings.

Creating a User Group

You can add users to a user group and set a volume usage limit on all group members.

Group Quota Limit Management

All users belongs to the user group “users”. When a user belongs to multiple groups and sets its quota limit to “Same as the group quota limit” on a specific volume, the highest group quota limit among these groups applies to the user.

For example, on Volume 1, the following users set their quota limits to “Same as the group quota limit”. According to the one or more groups that they respectively belong to, the actual quota limits to each user are listed as below:

User account	Belonging groups and group quota	Actual user quota on Volume 1
User_a	users: 25 GB	25 GB
User_b	users: 25 GB group_1: No limit	No limit
User_c	users: 25 GB group_2: 10 GB	25 GB

- User_a only belongs to the group “users”. The group limit is 25 GB. As a result, User_a’s quota limit is 25 GB on Volume 1.
- User_b belongs to two groups, users and group_1. The highest group quota limit is No limit from group_1. Therefore, User_b’s quota limit is “No limit” and does not have any quota limit on Volume 1.
- User_c belongs to two groups, users and group_2. The highest group quota limit is 25 GB from users. Therefore, User_c’s quota limit is 25 GB.

Note:

- Quota settings are only available on XFS volumes.
- When the specified capacity limit for a user is reached, write operations by the user to the volume will fail.

Go to	Settings / Device management > Privilege > User groups

General

1. Click **Add**.
2. The Add group window is displayed. In the **General** tab, specify the following information:

Group name	Specify a name for this user group.
GID	The GID (group identifier) is assigned by the system. Do not change it unless necessary.
Description	Specify a description for this user group.
Group members	Choose one or more users to add to this user group.

3. If needed, you can set the usage quota for the user group. Click the **Quota** tab.
   If not, click **OK** to save the settings.

Quota

1. In the **Quota** tab, Choose a volume and click **Edit**.
2. Choose a volume quota limit for the group:

No limit	The system does not set a volume usage limit on the group members.
Custom	Set a custom volume usage limit on the group members.

3. Click **OK** to save the settings. The quota limit applies to the group members who set their quota limit to **Same as the group quota limit**.

   Note: When a member belongs to more than one group, the highest limit among these groups will be applied to the member. For more details, see the **Group Quota Limit Management** section above.

   To set quota limit to a specific user, see Adding a User Account.

Editing a User Group

Go to	**Settings / Device management > Privilege > User Groups**
Change the group name / description	1. Choose a user group. 2. Click **Edit**. 3. In the **General** tab, change the group name / description.
Add a user into this group	1. Choose a user group. 2. Click **Edit**. 3. In the **General** tab, go to the list of **Group members**. 4. Choose the user that you want to add. 5. Click **OK** to save the changes.
Change the group quota	1. Choose a user group. 2. Click **Edit**. 3. Click the **Quota** tab. In this tab, choose a volume and click **Edit**. 4. Change the volume quota limit for the group. 5. Click **OK** to save the changes.

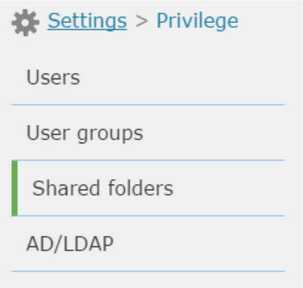
Deleting a User Group

Go to	**Settings / Device management > Privilege > User Groups**
Steps	1. Choose one or more user groups. 2. Click **Delete**. 3. A warning will pop up. Click **OK** to delete the user group.

Shared Folders

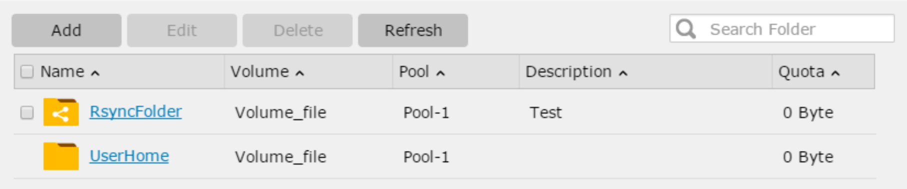
Go to

Settings / Device management > Privilege > Shared Folders



View

The shared folder status will appear.



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

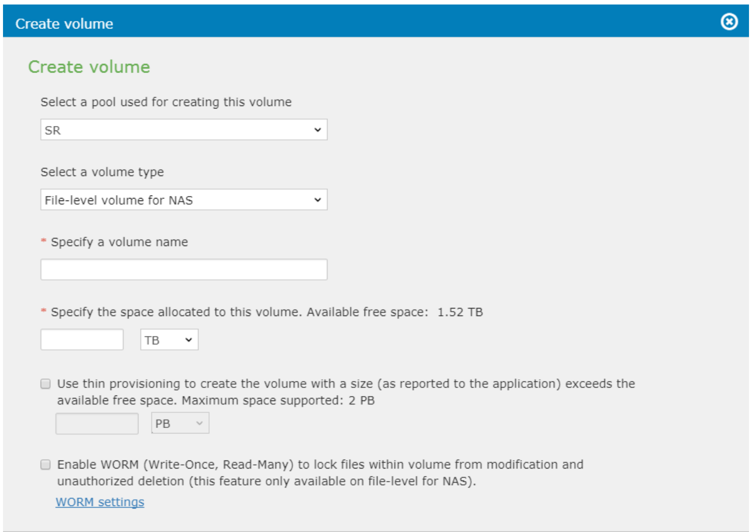
Parameters

Name	The name of the shared folder
Volume	The source volume that contains the shared folder
Pool	The source pool that contains the shared folder
Description	The description for the shared folder
Quota	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.



Create volume ⊗

Create volume

Select a pool used for creating this volume

SR

Select a volume type

File-level volume for NAS

* Specify a volume name

* Specify the space allocated to this volume. Available free space: 1.52 TB

TB

□ 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).

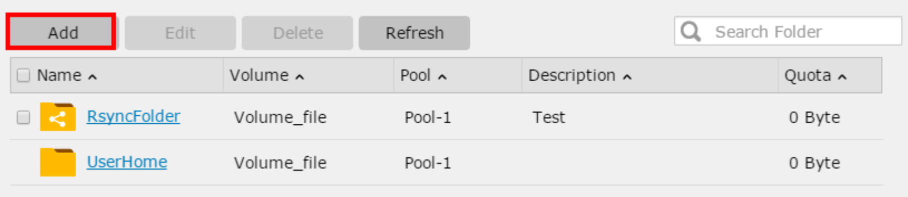
WORM settings

Go to

Settings / Device management > Privilege > Shared Folders

Create/Edit a Folder

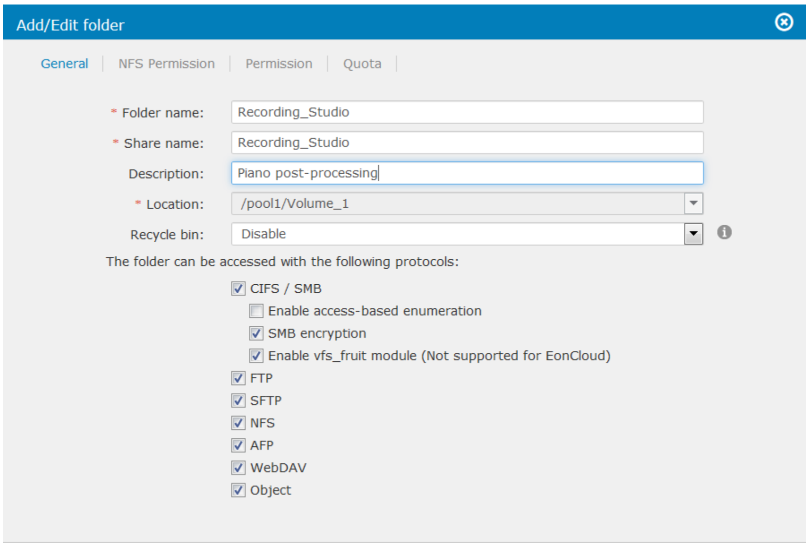
To create a folder, click the **Add** button. The folder configuration page will pop up.



□ 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:



Add/Edit folder ⊗

* Folder name: Recording_Studio

* Share name: Recording_Studio

Description: Piano post-processing

* Location: /pool1/Volume_1

Recycle bin: Disable

The folder can be accessed with the following protocols:

☑ CIFS / SMB
- □ Enable access-based enumeration
- ☑ SMB encryption
- ☑ Enable vfs_fruit module (Not supported for EonCloud)

☑ FTP

☑ SFTP

☑ NFS

☑ AFP

☑ WebDAV

☑ Object

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, WebDAV, or FTP 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.

Enhance SMB compatibility with macOS and iOS clients (Not supported for EonCloud): 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.

Transfer files in asynchronous mode: This option allows the system to transfer files asynchronously to minimize file transfer wait time and avoid transfer bottlenecks.

FTP

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

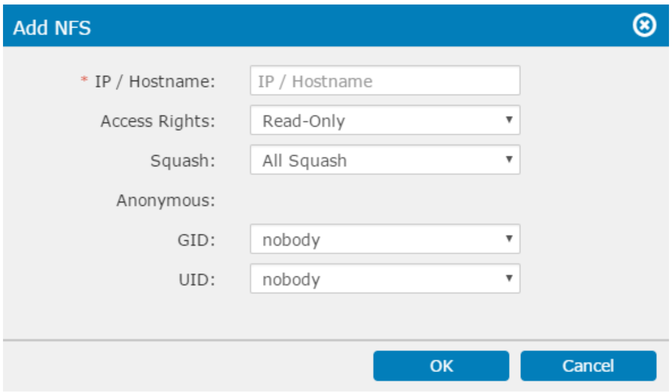
SFTP

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**:



Add NFS

* IP / Hostname: IP / Hostname

Access Rights: Read-Only

Squash: All Squash

Anonymous:

GID: nobody

UID: nobody

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.

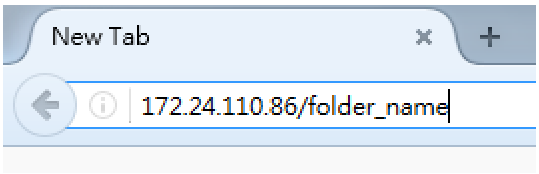
AFP

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.



172.24.110.86/folder_name

Object

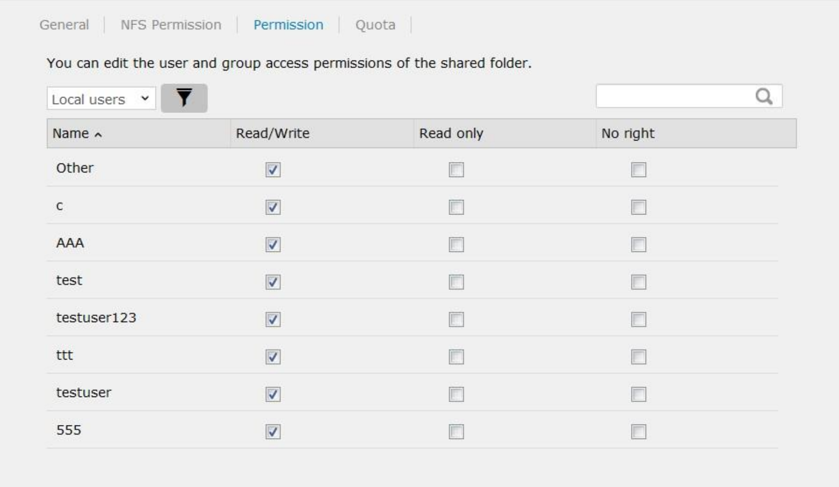
This data protocol allows your storage device to transfer small-chunk data (i.e. objects) with storage devices running OpenStack Swift or other object storage protocols.

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.



You can edit the user and group access permissions of the shared folder.

Local users

Name	Read/Write	Read only	No right
Other	☑	□	□
c	☑	□	□
AAA	☑	□	□
test	☑	□	□
testuser123	☑	□	□
ttt	☑	□	□
testuser	☑	□	□
555	☑	□	□

Note:

- 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.
- 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**.

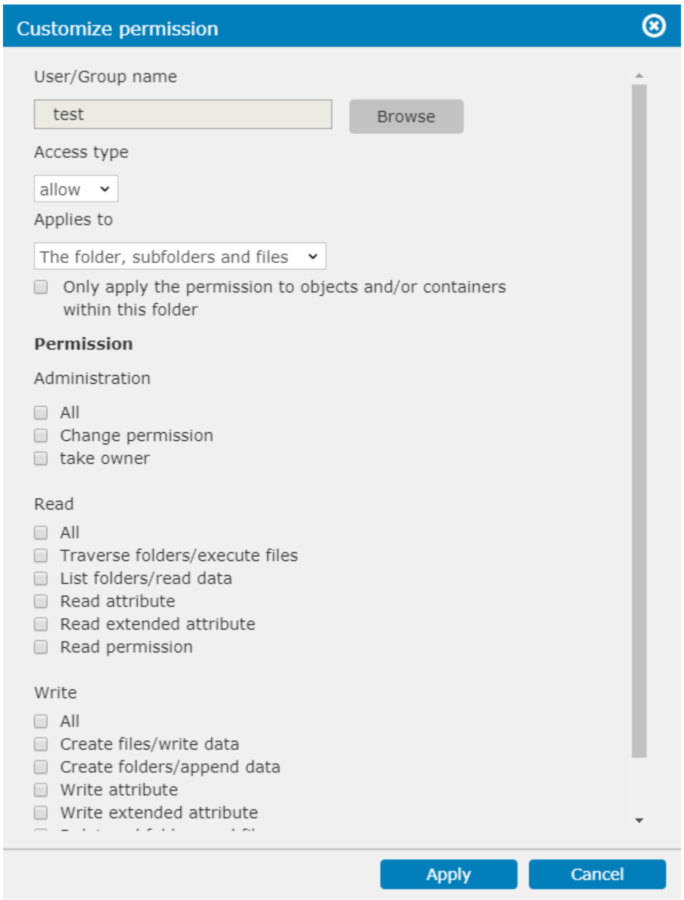
Customize permission

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.



Customize permission

User/Group name: test

Access type: allow

Applies to: The folder, subfolders and files

□ Only apply the permission to objects and/or containers within this folder

Permission

Administration
□ All
□ Change permission
□ take owner

Read
□ All
□ Traverse folders/execute files
□ List folders/read data
□ Read attribute
□ Read extended attribute
□ Read permission

Write
□ All
□ Create files/write data
□ Create folders/append data
□ Write attribute
□ Write extended attribute

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.

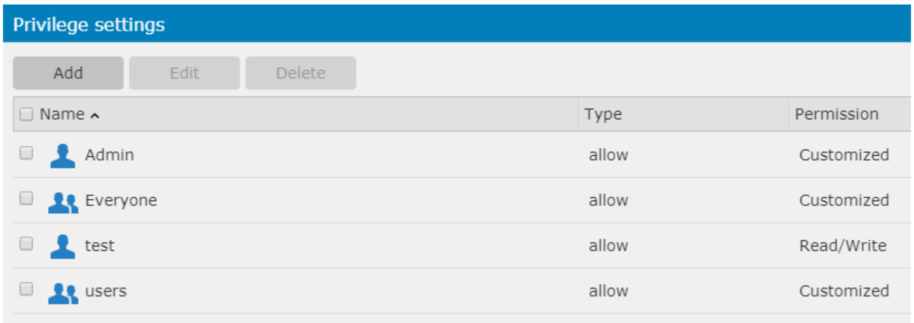
Write attribute: Allow the user to modify attributes (i.e. read-only, hidden, etc.) of the file or folder.

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.

5. 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.



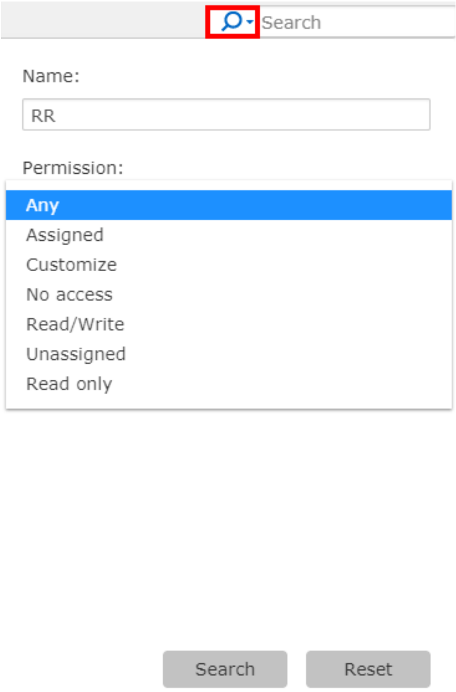
Privilege settings

□ Name	Type	Permission
□ Admin	allow	Customized
□ Everyone	allow	Customized
□ test	allow	Read/Write
□ users	allow	Customized

6. 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.



Name: RR

Permission:

- Any
- Assigned
- Customize
- No access
- Read/Write
- Unassigned
- Read only

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.

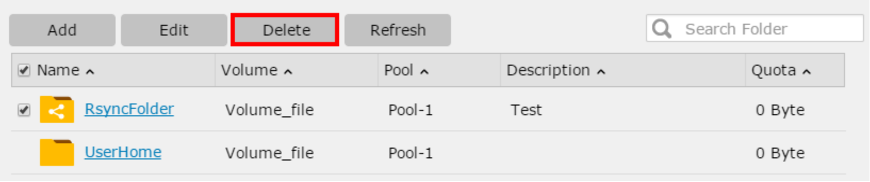
Assigned: all users with configured access rights.

Deleting a Folder

Go to **Settings / Device management > Privilege > Shared Folders**

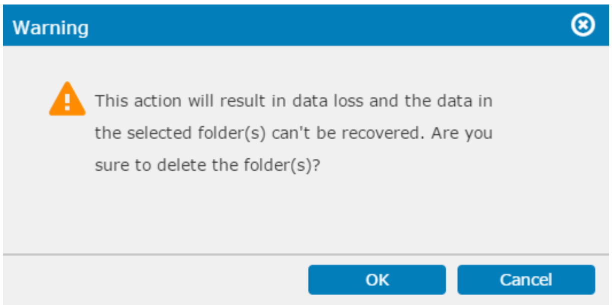
Steps

1. Select a folder and click the **Delete** button.



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

2. A warning message will appear. Click **Yes** to confirm.



This action will result in data loss and the data in the selected folder(s) can't be recovered. Are you sure to delete the folder(s)?

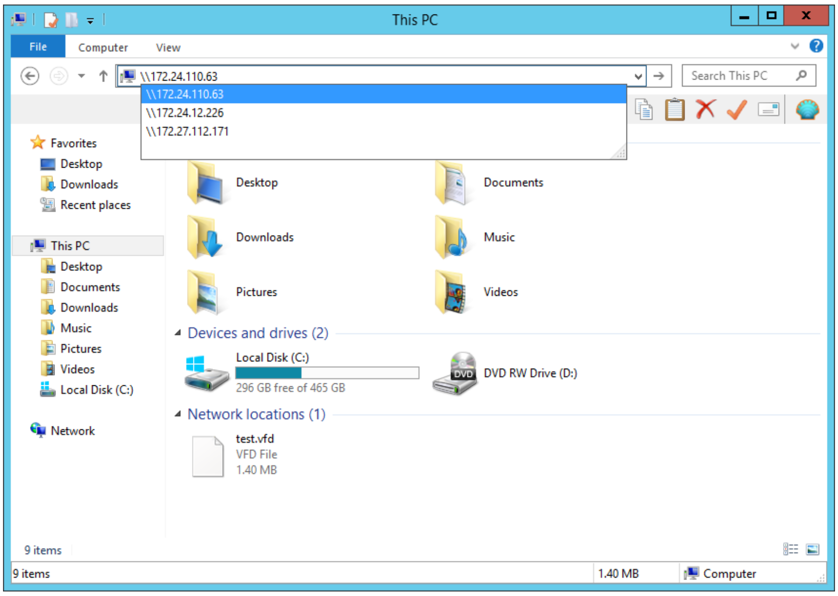
Accessing a Folder

After sharing folders, users can access the sharing folder via folder browser.

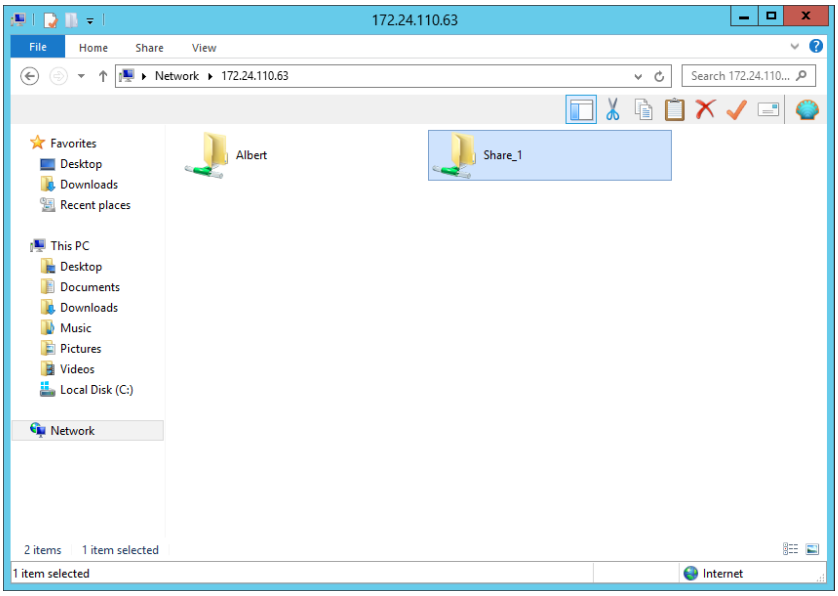
Steps

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.

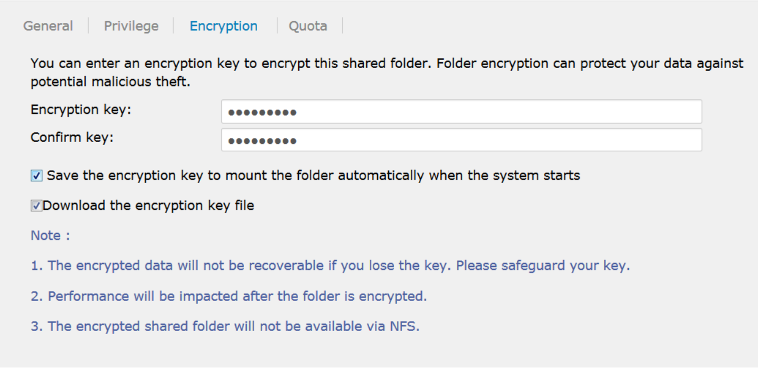


Encrypting a Folder

Folder Encryption provides data protection in the case of malicious attacks on the system or theft of hard disks. The EonOne 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 EonStor GS/GSe, 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



You can enter an encryption key to encrypt this shared folder. Folder encryption can protect your data against potential malicious theft.

Encryption key: ●●●●●●●●●

Confirm key: ●●●●●●●●●

☑ Save the encryption key to mount the folder automatically when the system starts

☑Download the encryption key file

Note :

1. The encrypted data will not be recoverable if you lose the key. Please safeguard your key.
2. Performance will be impacted after the folder is encrypted.
3. The encrypted shared folder will not be available via NFS.

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.

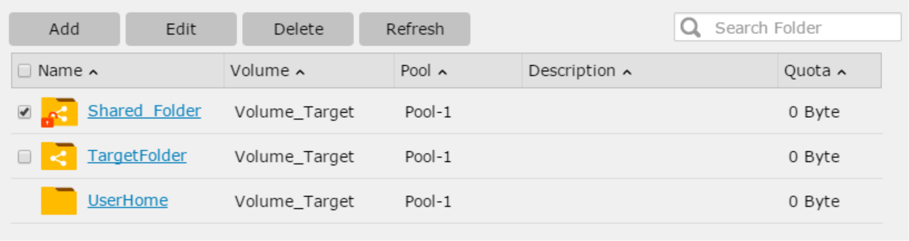
Note:

- Please safeguard the encryption key. The encrypted data will not be recoverable if you lose the key.
- The encryption process will slightly affect the system performance.
- The encrypted shared folder will not be accessible via NFS.

- You cannot encrypt a shared folder after it is created.

Lock a folder

1. Go to **Settings / Device management > 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
☑ Shared_Folder	Volume_Target	Pool-1		0 Byte
□ TargetFolder	Volume_Target	Pool-1		0 Byte
UserHome	Volume_Target	Pool-1		0 Byte

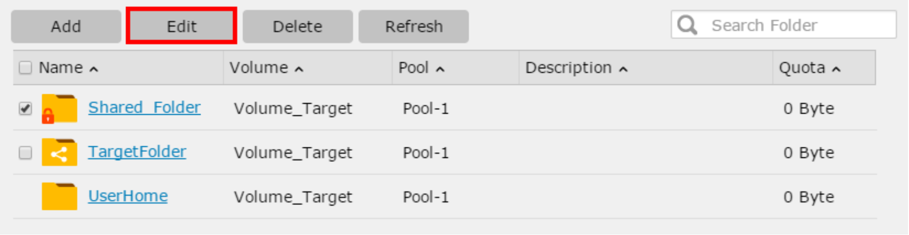
2. Select the **Encryption** tab. Check the box **Lock the folder now** to lock the shared folder. You can choose to save the key in the system for automatic mounting of the folder at system start-up. You can also download the key file to the local host for safekeeping (click on **Download Encryption Key File**).

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

Unlock a folder

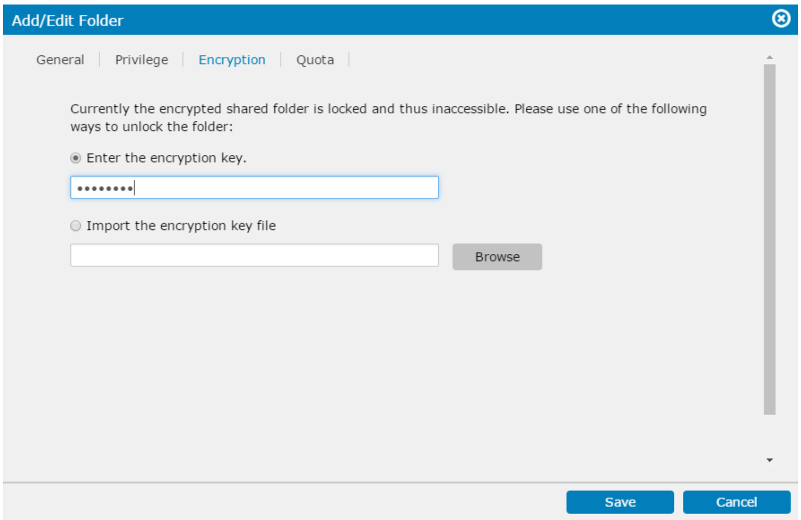
1. Go to **Settings / Device management > Privilege > Shared folders**.
   If a shared folder is locked, there will an icon with a lock next to the name.
   If a shared folder is unlocked, there will an icon with an opened lock next to the name.

2. Select the shared folder to unlock and click on the **Edit** tab. Then, click on the **Encryption** tab.



Name	Volume	Pool	Description	Quota
☑ Shared_Folder	Volume_Target	Pool-1		0 Byte
□ TargetFolder	Volume_Target	Pool-1		0 Byte
UserHome	Volume_Target	Pool-1		0 Byte

3. Enter the encryption key or import a key file. Click **Save** to enable the settings.



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.

••••••••

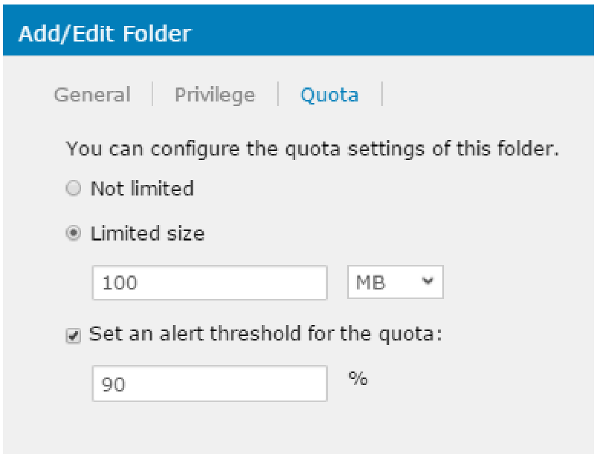
○ Import the encryption key file

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 / Device management > 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.

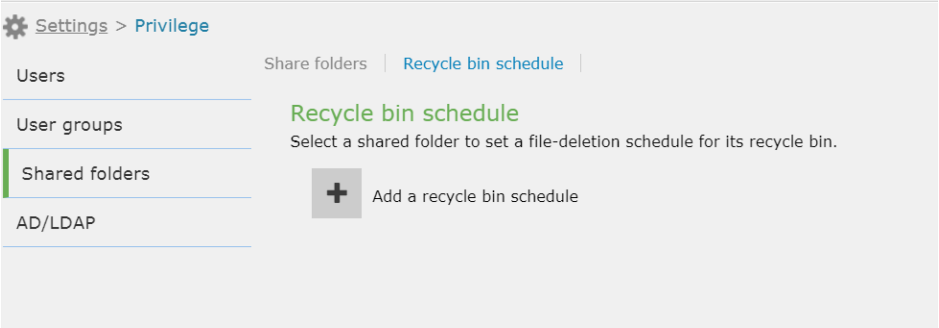
3. Click **Save** to apply the settings.

Recycle Bin Schedule

After enabling the recycle bin for a shared folder, you can set up a schedule to empty it.

Go to

Settings / Device management > Privilege > Shared folders > Recycle bin schedule



Settings > Privilege

Users

User groups

Shared folders

AD/LDAP

Share folders | Recycle bin schedule

Recycle bin schedule

Select a shared folder to set a file-deletion schedule for its recycle bin.

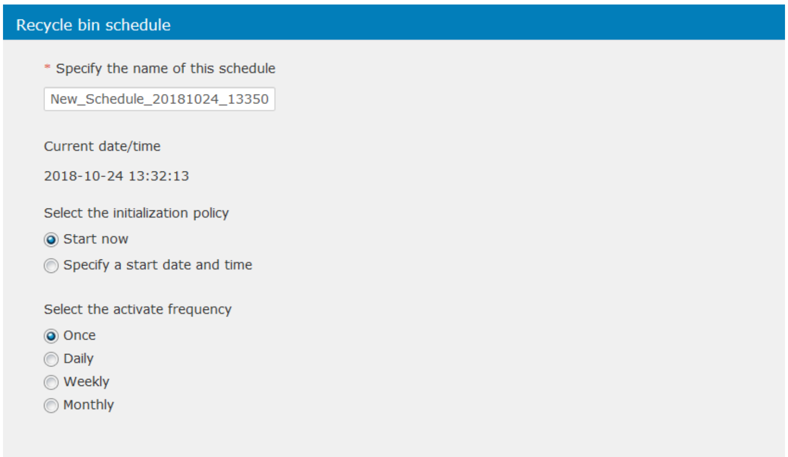
+ Add a recycle bin schedule

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:

Specify the name of the schedule	Assign a name to this recycle bin schedule.
Current date/time	Check current time.
Select the initialization policy	Select when to begin emptying the recycle bin: **Start now**: The system immediately runs the schedule and empties the recycle bin. **Specify a start date and time**: The system runs the schedule from the specified time.
Select the activate frequency	Select how often to empty the recycle bin: **Once**, **Daily**, **Weekly**, or **Monthly**.
File deletion policy	Select how to empty the recycle bin: **Delete all files**: The system deletes all files from the recycle bin. **Delete old files**: The system deletes files past the specified retention days. **Delete files when the recycle bin reaches the maximum size**: When the recycle bin exceeds the maximum size, the system deletes 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

Go to	**Settings / Device management > Privilege > AD/LDAP** Select **Windows Active Directory (AD)** from the drop down list.	
Parameters	**AD Server (IP Address)**	Specifies the IP address of the AD server.
	AD Security	Specifies how the system will communicate with the AD server. You can select none or an encrypted connection with TLS.
	Username / Password	The root username and password.
	DNS authentication	Select the option according to the DNS server's authentication requirement. **No authentication required**: Select this option if the DNS server does not require any authentication. **Same with AD server**: Select this option if the DNS server requires the same authentication information provided by the AD server. **Manual**: Select this option and provide the username and password if the DNS server requires specific authentication information.
	Number of trusted domains	**Only this AD domain**: The storage device trusts only the AD domain that it joins. **Multiple AD domains**: The storage device trusts multiple AD domains. Click **Add trusted domain** to specify the AD domains to trust.

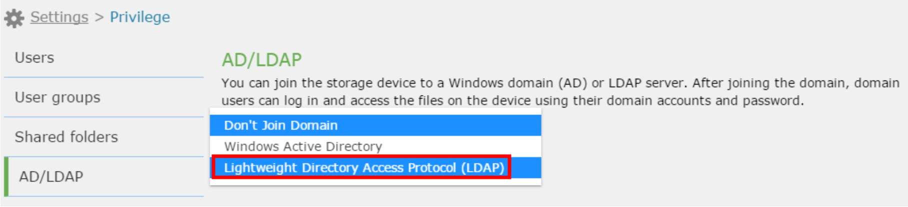
Mapping backend	Specify how to pull the domain user data from the AD server. **RID**: The system pulls the domain users from the domain server and creates a new GID and UID for each domain user. **AD**: The system pulls the domain users from the domain server. The domain users continue to use the GIDs and UIDs assigned by the domain server.
Authentication Level	Specifies the Authentication level.
Check domain	Click this button to check if all the provided domain information is valid.
Create home folder	Choose a local folder to create a home folder for the domain users. Choose **Don’t create** if you do not want to create a home folder.
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.
Update the user list	Click this button to sync updates regarding domain users and groups from the domain server.

Lightweight Directory Access Protocol Settings

Go to

Settings / Device management > Privilege > AD/LDAP

Select **Lightweight Directory Access Protocol** from the drop down list.



Settings > Privilege

Users

User groups

Shared folders

AD/LDAP

AD/LDAP

You can join the storage device to a Windows domain (AD) or LDAP server. After joining the domain, domain users can log in and access the files on the device using their domain accounts and password.

Don't Join Domain

Windows Active Directory

Lightweight Directory Access Protocol (LDAP)

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.

NIS

Configuring NIS Service

You can enable NIS service and set the properties.

Go to	**Settings / Device management > Privilege > NIS**
Parameters	1. Click on the switch bar to enable the NIS service. 2. Enter the NIS server domain and server IP address and click **Save** to save the settings. 3. If needed, click **Update user list** to update domain users.

Storage

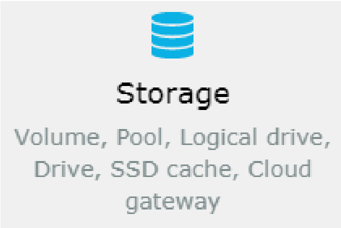
The Storage setting menu contains the following sub-settings.

1. Volumes
2. Pools
3. Drives
4. SSD cache
5. Storage Maintenance
6. VMware volume

For cluster settings, the Storage setting menu contains the following sub-settings.

1. Volumes
2. Pools
3. Folder explorer
4. Cluster folders
5. Migration
6. Auto-balancing

Go to **Settings / Device management > Storage**



Storage

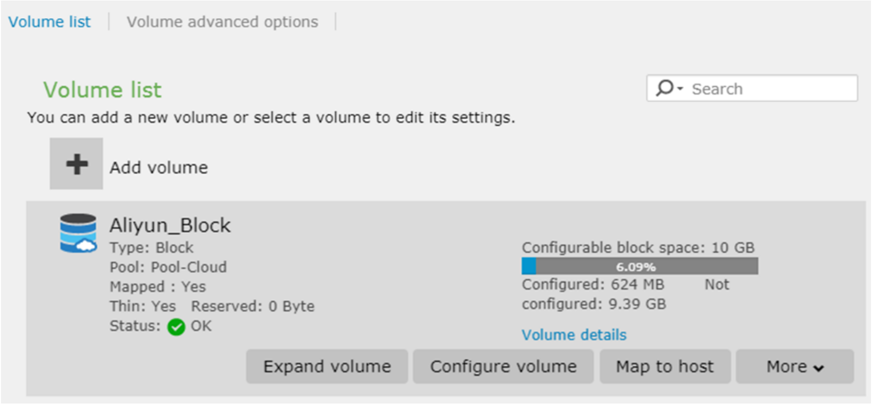
Volume, Pool, Logical drive, Drive, SSD cache, Cloud gateway

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.

Volumes

Go to **Settings / Device management > Storage > Volumes**

View You can add a volume or select a volume to edit its settings from the volume list tab.



Volume list

You can add a new volume or select a volume to edit its settings.

Aliyun_Block
Type: Block
Pool: Pool-Cloud
Mapped : Yes
Thin: Yes Reserved: 0 Byte
Status: OK

Configurable block space: 10 GB
6.09%
Configured: 624 MB Not configured: 9.39 GB

Volume details

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.
Mounted	Shows whether the file-level volume is mounted or not.
Thin-Provision	Shows whether the volume has enabled thin provisioning or not.
Status	Shows the volume status.

Click **Volume Details** to see more information.

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 / Device management > Storage > Volumes**

Adding a Volume

1. Click **Add Volume**.
2. The volume configuration table will be shown. Specify the following settings:

Pool	Select a pool for the volume to claim capacity.
Volume Type	Choose which type of volume that you want to create: **Block-level volume for SAN** or **File-level volume for NAS**.
Volume Name	Enter the name of the volume.
Enable case-insensitive file and folder names	Enable this option so that the system does not distinguish folders or files sharing the same name but in different cases. For example, folders named “xyz” and “XYZ” are treated as the same.
Volume Size	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. **Note:** The minimum size of a volume is 10GB.
Deduplication on block-level volumes	When choosing to create a block-level volume, if needed, you can enable deduplication. Select the option to enable it. When enabling this option, thin provisioning will also be enabled. Specify the capacity. To further configure deduplication, click **Deduplication settings**. You can choose whether to **Enable data compression to save more space**, **Enable background optimization**, or **Enable throughput optimization**. When throughput optimization is enabled, schedule when to perform deduplication and how long the deduplication should last.
Advanced ACL	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.

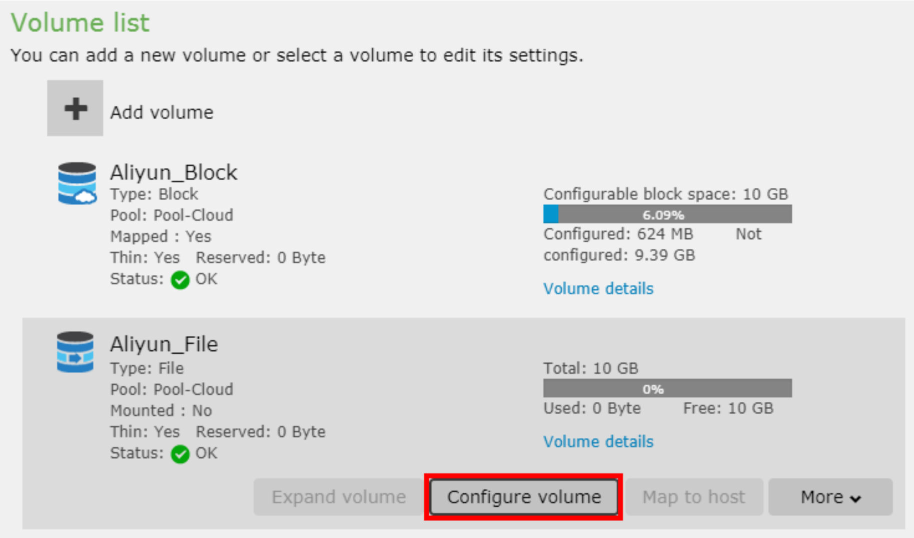
Thin Provisioning & Minimum Reserved Space	Enables thin provisioning. Enter the volume size to set the volume capacity that will be physically allocated as a safe reserve. If the reserve reaches 100%, the volume becomes fully-provisioned (all space is allocated from the pool). For more information, refer to the next section.
Enable WORM	Enable WORM (Write Once Read Many) functionalities. Refer to Creating a WORM Volume for more details.
Host LUN Mapping	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.

3. Click **OK**.

Renaming a Volume

Note: If you rename a volume where object storage resides, after the renaming, object storage service will be then disabled. You must re-enable the service and configure the object storage again. For more information about the setup, refer to Using Object Storage.

1. Select the volume and click **Configure Volume**.



Volume list

You can add a new volume or select a volume to edit its settings.

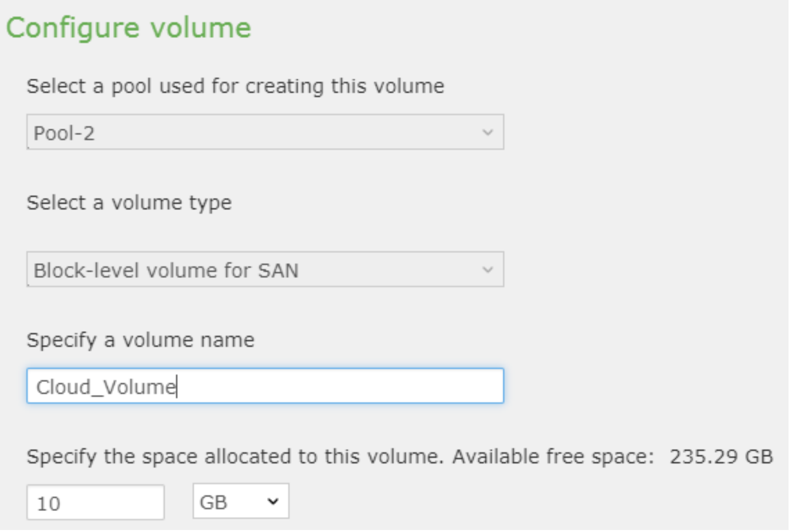
Aliyun_Block
Type: Block
Pool: Pool-Cloud
Mapped : Yes
Thin: Yes Reserved: 0 Byte
Status: ✓ OK

Configurable block space: 10 GB
6.09%
Configured: 624 MB Not configured: 9.39 GB

Aliyun_File
Type: File
Pool: Pool-Cloud
Mounted : No
Thin: Yes Reserved: 0 Byte
Status: ✓ OK

Total: 10 GB
0%
Used: 0 Byte Free: 10 GB

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

Volume advanced options

Go to	Settings / Device management > Storage > Volumes > Volume advanced options	
Parameters	**Maximum number of queued I/O**	Specifies the maximum number of I/O operations per host channel that can be accepted from servers.
	LUN per host SCSI ID	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 associated with host IDs and appears to the host as a contiguous volume. Choose the parameter for your LUN per host SCSI ID
	Tags reserved per host-LUN connections	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. Set the parameter for the tags that are reserved per host-LUN connections.
	Peripheral device type	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. Select the peripheral device type from the scroll down list.
	Peripheral device qualifier	Select the qualifier for your peripheral device to “Connected” or “Supported but not Connected” from the scroll down list.
	Host devices support removable media	Enable or Disable Host devices support removable media for searching.
	LUN applicability	Select “First Undefined LUN” or “Only Undefined LUN ’s”.
	Cylinder/Head/Sector	In Solaris, the capacity of a drive is determined by the cylinder/head/sector count. Select the valuables from the scroll down list.

Press **Save** button to complete volume advanced options, if nothing was changed in this page, the Save button will display as “**Disabled**”.

Besides, you can add a volume on this page.

Go to **Settings / Device management > Storage > Volumes > Volume advanced options**

Steps

1. Click **Add Volume**.
2. The volume configuration table will be shown. Specify the following settings:

Pool	Select a pool for the volume to claim capacity.
Volume Type	Choose which type of volume that you want to create: **Block-level volume for SAN** or **File-level volume for NAS**.
Volume Name	Enter the name of the volume.
File system	If you choose to create a file volume, choose **XFS** or **Btrfs** as the file system.
Enable case-insensitive file and folder names	Enable this option so that the system does not distinguish folders or files sharing the same name but in different cases. For example, folders named “xyz” and “XYZ” are treated as the same.
Deduplication on file-level volumes with Btrfs file system	When choosing to create a file-level volume, if needed, you can enable deduplication. This option is only available for Btrfs file system. To activate deduplication schedule, refer to Activating Deduplication on File-level Volumes (Btrfs File System).
Enable compression	When you choose Btrfs as the file system, select **LZO**, **ZSTD**, or **ZLIB** as its data compression policy to suit your needs.
Volume Size	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. **Note:** The minimum size of a volume is 10GB.
Deduplication on block-level volumes	When choosing to create a block-level volume, if needed, you can enable deduplication. Select the option to enable it. When enabling this option, thin provisioning will also be enabled. Specify the capacity. To further configure deduplication, click **Deduplication settings**. You can choose whether to **Enable data compression to save more space**, **Enable background optimization**, or **Enable throughput optimization**. When throughput optimization is enabled, schedule when to

	perform deduplication and how long the deduplication should last.
Advanced ACL	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.
Thin Provisioning & Minimum Reserved Space	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.
Enable WORM	Enable WORM (Write Once Read Many) functionalities. Refer to Creating a WORM Volume for more details.
Host LUN Mapping	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.

3. Click **OK**.

Creating a WORM Volume

EonStor GS/GSe 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 / Device management > Storage > Volumes > Add Volume**

Steps

4. Select the volume type to **File-level volume for NAS** and then check **Enable WORM**. Click the **WORM settings** button to configure the settings.

5. Select **Enable WORM** on the top and set a retention period for the WORM volume.

6. Select a WORM mode. Please refer to the parameter below.

7. Select the **file locking mode.**
   You can either manually or automatically change file property into read-only.

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

The other steps and options are the same as the creation procedures for regular volumes.

Note:

1. 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.

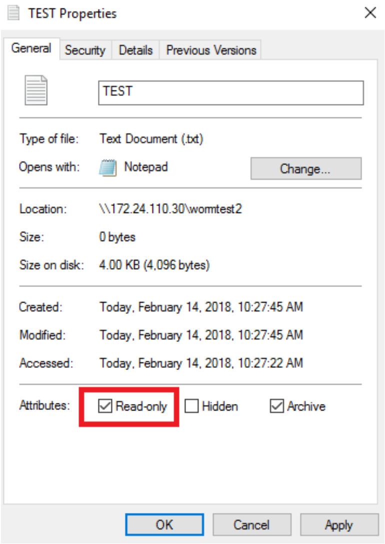
Parameter

Retention period: Specify the retention period of files in the volume. The default period is 2 years.

Mode: Choose one from the two supported modes: Enterprise or Compliance.

- **Enterprise** (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.
- **Compliance**: 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.

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.



TEST Properties

TEST

Type of file: Text Document (.txt)

Opens with: Notepad

Location: \\172.24.110.30\wormtest2

Size: 0 bytes

Size on disk: 4.00 KB (4,096 bytes)

Created: Today, February 14, 2018, 10:27:45 AM

Modified: Today, February 14, 2018, 10:27:45 AM

Accessed: Today, February 14, 2018, 10:27:22 AM

Attributes: ☑ Read-only ☐ Hidden ☑ Archive

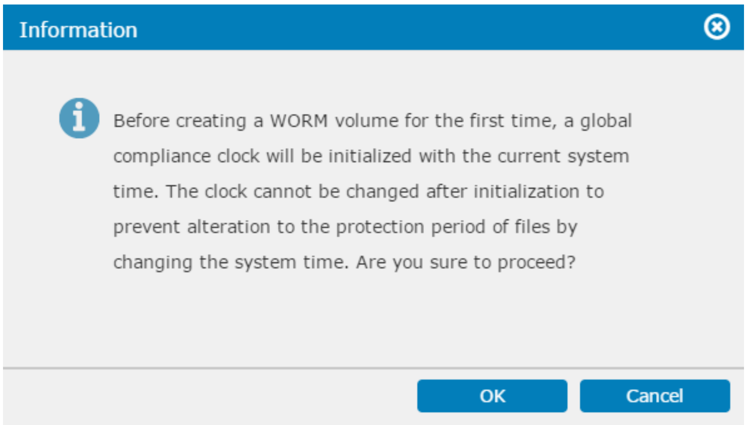
Automatic file locking: If this option is enabled, when the specified waiting time has expired after a file is created and is being written, the file will automatically go into the read-only state (i.e. locked). The default waiting time is 10 minutes.

Before the 1st WORM volume is created

Before the first WORM volume is created, a confirmation window will pop up to inform the administrator to initialize the global compliance clock first.

The global compliance clock can be initialized once only. It's not re-initialized even if there are no WORM volumes in the system.

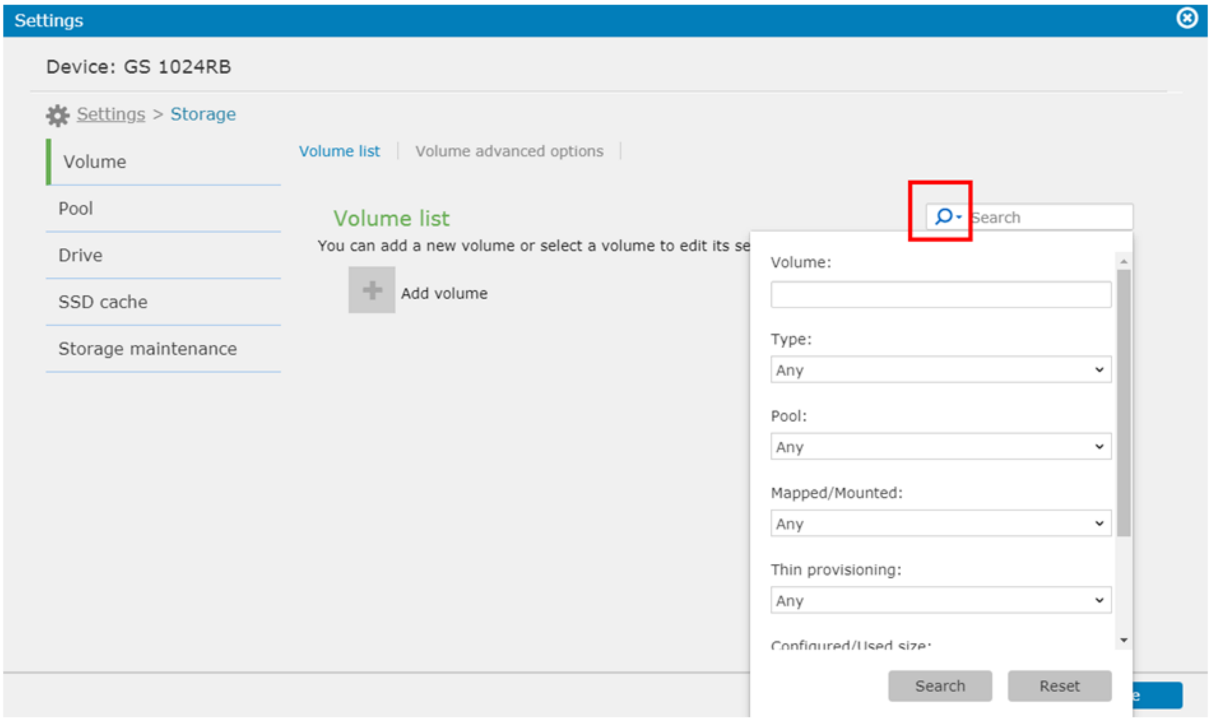
The retention time for WORM volumes will be based on the global compliance clock without being affected by system clock reset or change.



Before creating a WORM volume for the first time, a global compliance clock will be initialized with the current system time. The clock cannot be changed after initialization to prevent alteration to the protection period of files by changing the system time. Are you sure to proceed?

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:



Device: GS 1024RB

Volume list

You can add a new volume or select a volume to edit its se

Volume:

Type: Any

Pool: Any

Mapped/Mounted: Any

Thin provisioning: Any

Configured/Used size:

Parameters	**Name**	Select a pool for the volume to claim capacity.
	Type	Select a volume type.
	Pool	Enter the name of the volume.
	Mapped/Mounted	Select “Yes” or “No” whether to searched volume has mapped/mounted, “Any” is set as factory default.
	Thin provision	Select “Yes” or “No” whether the searched volume has Thin provision function, “Any” is set as factory default.
	Configured/Used size	Select “Yes” or “No” whether the searched volume has Configured/Used size. “Any” is set as factory default.
	Configurable/Total size	Select “Yes” or “No” whether the searched volume has Configured/Total size. “Any” is set as factory default.

About Thin Provisioning

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.

Note: 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.

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.

Note: 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.

Note: The reserved space cannot exceed the actual available capacity.

Creating a Volume in a Tiered Pool

In a tiered pool, you can create a volume on a specific storage tier or across different storage tiers.

Go to **Settings / Device management > Storage > Volumes**

Steps

1. Click **Add Volume**.
2. The volume configuration table will be shown. Specify the following settings:

Pool	Select a pool.
Volume Type	Choose **Block-level volume for SAN**.
Volume Name	Enter the name of the volume.
Volume Size	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. **Note:** The minimum size of a volume is 10GB.
Thin Provisioning & Minimum Reserved Space	You can choose to enables thin provisioning or not. 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).

3. Click **Next**.
4. For the space allocation policy, select **Use selected tiers by ratio calculation (recommended)**. The system will automatically allocate the volume's data to all tiers.
5. Select all tiers.
6. Click **OK** to complete the settings. After creating a volume, set up a schedule for the system to migrate data between tiers. For more details, see Creating a Tiered Data Migration Schedule.

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.

Note: You can only set thresholds for a file-level volume. If a volume is unmounted, setting a threshold is not available.

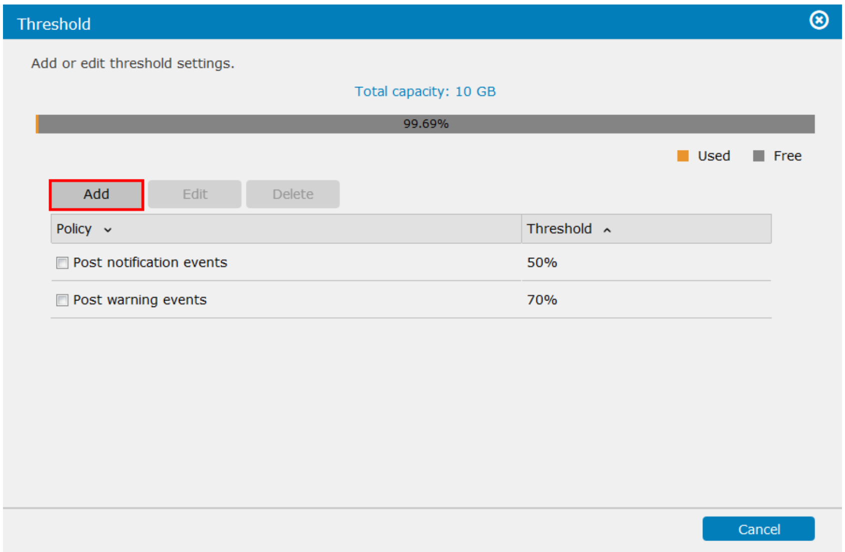
Go to

Settings / Device management > Storage > Volumes

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.



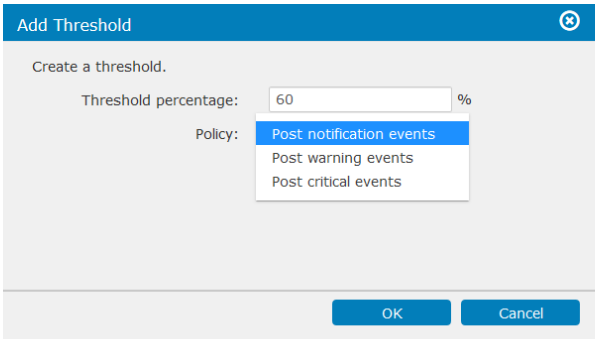
Add or edit threshold settings.

Total capacity: 10 GB

99.69%

Policy	Threshold
□ Post notification events	50%
□ Post warning events	70%

On the pop-up window, enter the threshold value (% of the volume) and choose the notification type. Click **OK** to save the threshold.



Create a threshold.

Threshold percentage: 60 %

Policy: Post notification events

Parameters

Post notification events	Create a notification event when the amount of volume usage reaches the threshold.
Post warning events	Create a warning event when the amount of volume usage reaches the threshold.
Post critical events	Create a critical event when the amount of volume usage reaches the threshold.

Deleting a Volume

Go to	**Settings / Device management > Storage > Volumes**
Steps	1. Select the volume, click the **More** button and select **Delete volume**. 2. 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

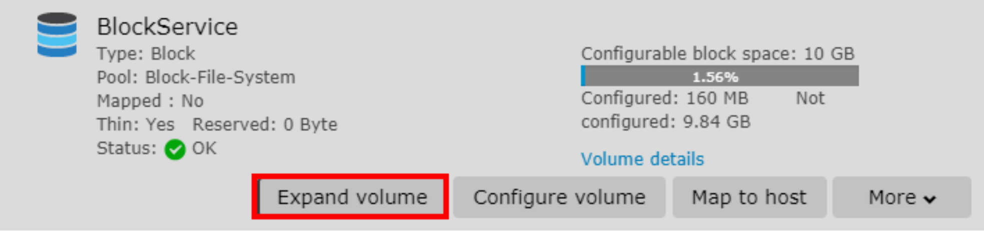
Expanding a volume's capacity is available only when there is available capacity.

Note: If a volume is unmounted, expanding is not available.

Go to

Settings / Device management > Storage > Volumes

Select the volume and click the **Expand Volume** button.

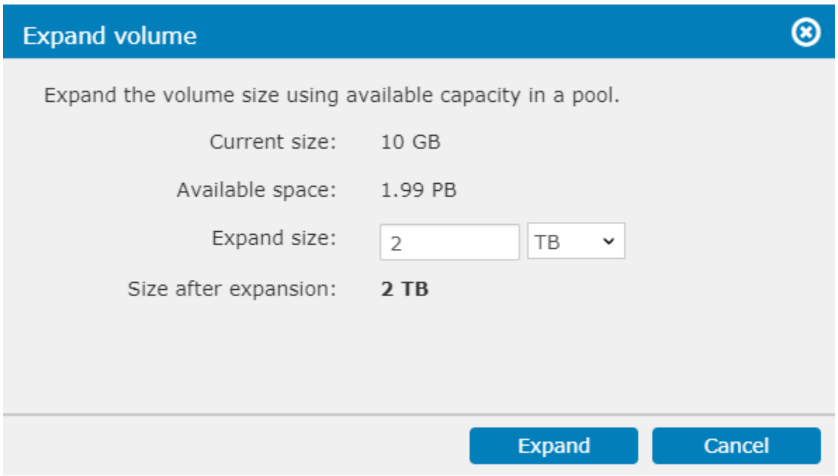


BlockService
Type: Block
Pool: Block-File-System
Mapped : No
Thin: Yes   Reserved: 0 Byte
Status: ✓ OK

Configurable block space: 10 GB
1.56%
Configured: 160 MB   Not configured: 9.84 GB

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: 2 TB
Size after expansion: **2 TB**

Expansion will begin. When it is completed, check that the size of the volume is increased by the specified amount.

Defragmenting a Volume by Schedule

Defragmentation allows file fragments on the volume to merge into contiguous fragments, therefore boosting file access and storage efficiency. You can run a defragmentation task manually or by schedule.

To run defragmentation by schedule, in addition to specifying the activate time, list one or more volumes. They system will perform defragmentation the listed volumes during the scheduled period.

To manually run defragmentation, see Defragmenting a Volume Manually.

Note:

- Only an XFS volume resides in a pool which consists of all-HDD or HDD/SSD can be defragmented. Besides, defragmentation reduces SSD lifespan.
- The system can only defragment one volume at one time. The scheduled task will be skipped if a manual task is in progress.

Go to	**Settings / Device management > Storage > Volumes > Defragmentation tab**
Activate defragmentation schedule	1. Turn on defragmentation function. 2. Click **Add** to select one or more volumes to run the defragmentation task. Click **OK** to save settings. If needed, click **Refresh** to update the list. 3. Specify a start date and time. 4. Specify the activation frequency. 5. Specify the maximum execution time for the schedule. Choose **Not limited** or **Customize**. If the schedule is customized, specify the time period. 6. Click **Save** to save the settings. 7. The Defragmentation Status section will indicate when will be the next time to run the schedule and the progress of defragmentation.
Remove a volume from the defragmentation list	1. On the volume list, select the volume that you want to remove. 2. Click **Delete**. 3. Click **Save** to save the changes.
Stop defragmentation schedule	1. Go to the Defragmentation Status section. The defragmentation is indicated as In progress. 2. Click **Stop** to stop it, and click **Yes** to confirm your action.

Defragmenting a Volume Manually

Defragmentation allows file fragments on the volume to merge into contiguous fragments, therefore boosting file access and storage efficiency. You can run a defragmentation task manually or by schedule.

To run defragmentation by schedule, see Defragmenting a Volume by Schedule.

Note:

- Only an XFS volume resides in a pool which consists of all-HDD or HDD/SSD can be defragmented. Besides, defragmentation reduces SSD lifespan.
- The system can only defragment one volume at one time. If a manual task is still in progress, you must stop the on-going task, so the new task can run.

Go to	**Settings / Device management > Storage > Volumes**
Steps	1. Select a volume. 2. Click **Volume details** to check **Fragmentation factor**. If the factor is high, you can defragment the volume to improve its access and storage efficiency. 3. Click **More** > **Defragmentation** to start defragmenting the volume.

Mounting/Unmounting a Volume

After a file-level volume is created, its default status of mounting is “Yes,” which means the volume is mounted. You can then create share folders on this volume.

If needed, you can unmount the volume. If there have been any configurations about share folders and the usage threshold for this volume, they will be removed. The status of mounting will turn into “No,” indicating that the volume is unmounted. An unmounted volume cannot be expanded or set a usage threshold.

Note: Only file-level volumes can be mounted/unmounted.

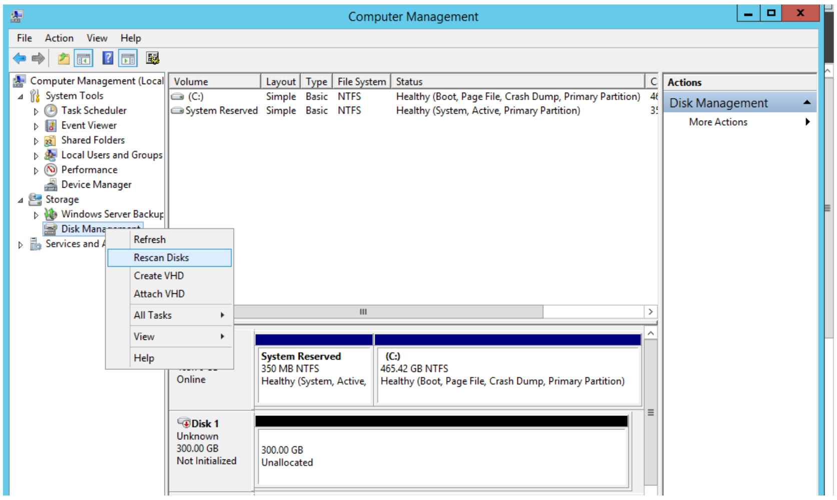
Go to	**Settings / Device management > Storage > Volumes**
Unmount a volume	1. Select the desired volume from the list. 2. Click **More** and select the **Unmount** option to unmount the volume.
Mount a volume	1. Select the desired volume from the list. 2. Click **More** and select the **Mount** option to mount the volume.

Reflecting the Expanded Volume Status in Windows Server (Windows Server 2012 R2 for example)

Steps

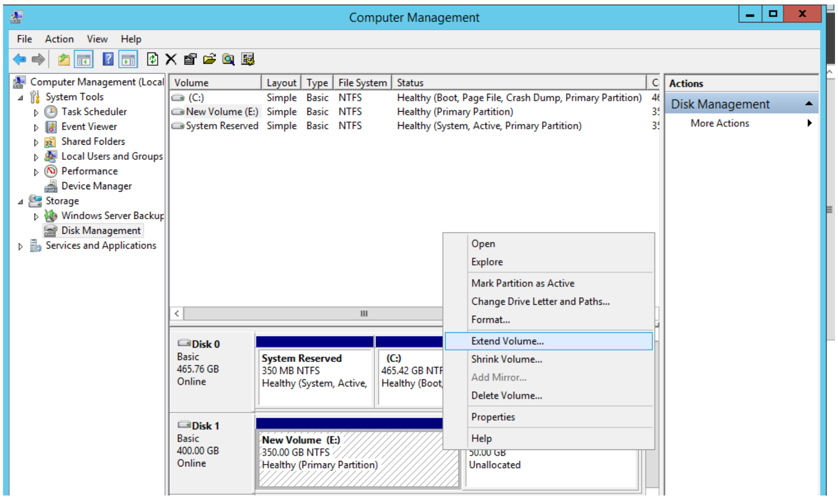
1. Open the Computer Management Utility.

2. Right-click on the Disk Management icon in the sidebar and select Rescan Disks.



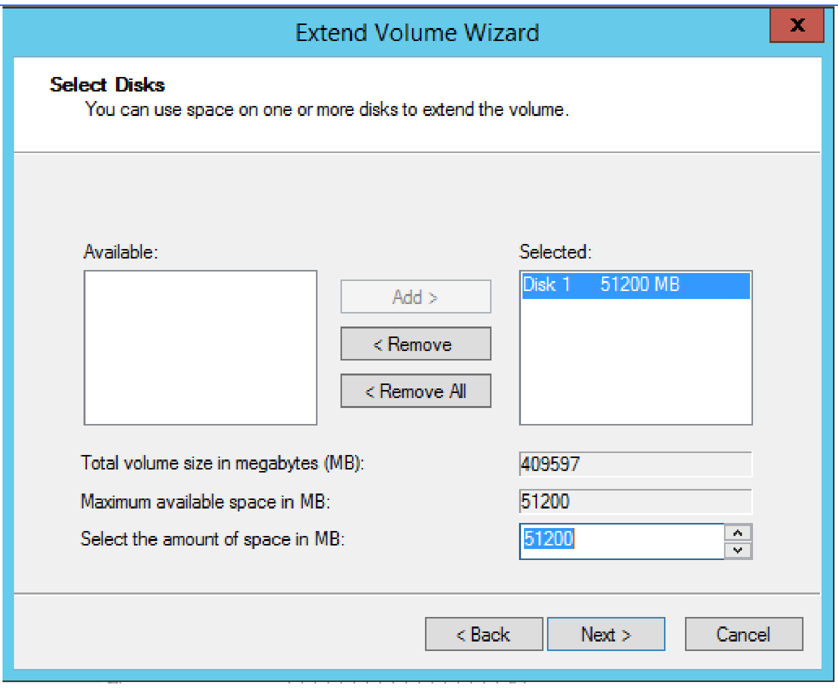
Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)

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**.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)
New Volume (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)

4. The Extend Volume Wizard will appear. Add available disk and click **Next**.



Extend Volume Wizard

Select Disks

You can use space on one or more disks to extend the volume.

Available:

Selected:

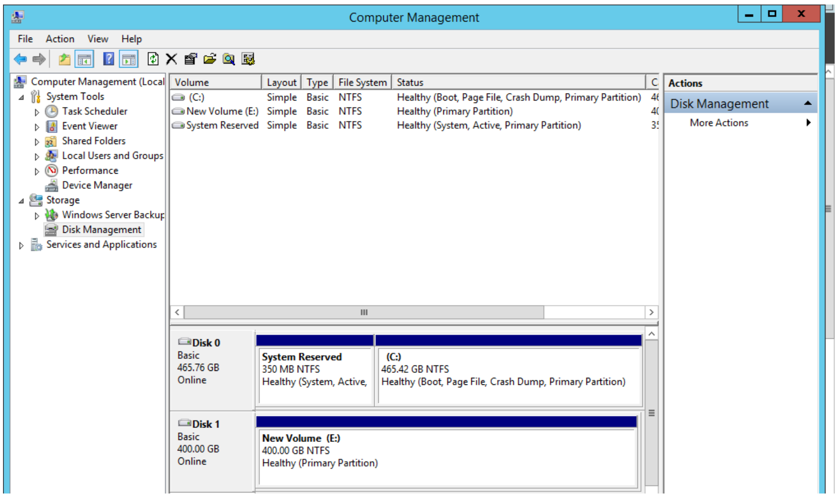
Disk 1   51200 MB

Total volume size in megabytes (MB): 409597

Maximum available space in MB: 51200

Select the amount of space in MB: 51200

5. You should be able to see the extended volume.



Computer Management

Volume	Layout	Type	File System	Status	C
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	46
New Volume (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	40
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	35

Disk 0
Basic
465.76 GB
Online

System Reserved
350 MB NTFS
Healthy (System, Active,

(C:)
465.42 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
400.00 GB
Online

New Volume (E:)
400.00 GB NTFS
Healthy (Primary Partition)

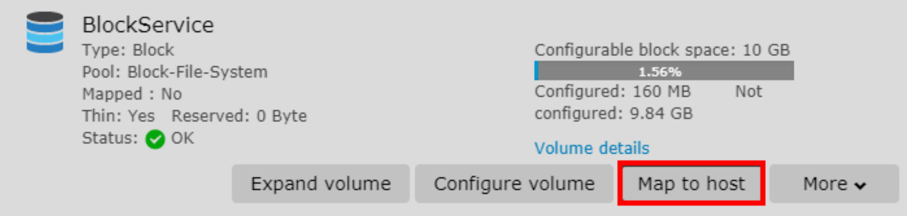
Mapping a Volume to a LUN

There must be at least one volume available to create LUN mapping.

Go to

Settings / Device management > Storage > Volumes

Select a “Type: Block” volume and click the **Map to host** button.

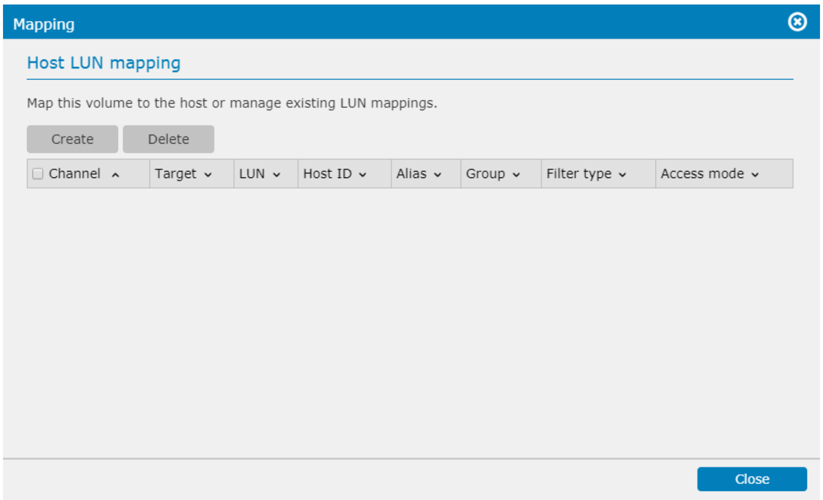


BlockService
Type: Block
Pool: Block-File-System
Mapped : No
Thin: Yes Reserved: 0 Byte
Status: OK

Configurable block space: 10 GB
1.56%
Configured: 160 MB Not configured: 9.84 GB

Steps

The Host LUN Mapping table will appear.



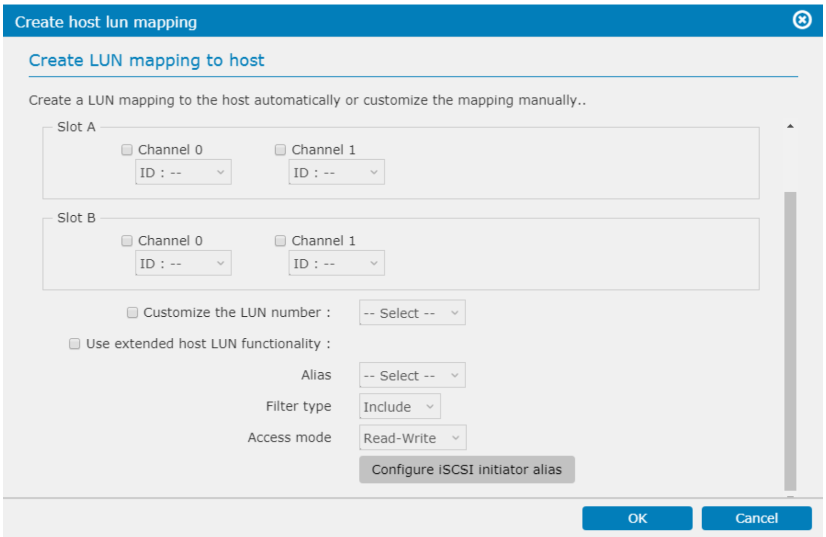
Mapping

Host LUN mapping

Map this volume to the host or manage existing LUN mappings.

☐ Channel	Target	LUN	Host ID	Alias	Group	Filter type	Access mode

Click **Create** and the Host Mapping Configuration Window will be shown.



Create host lun mapping

Create LUN mapping to host

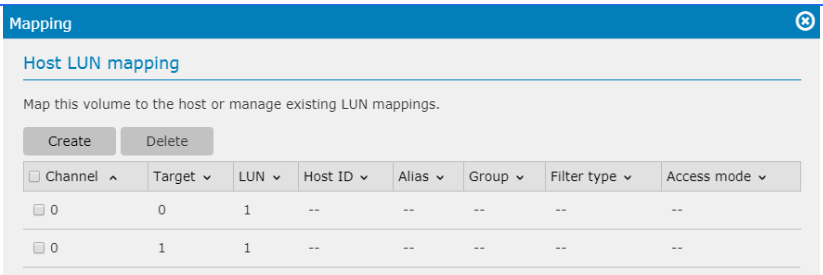
Create a LUN mapping to the host automatically or customize the mapping manually..

Slot A
☐ Channel 0 ID : --
☐ Channel 1 ID : --

Slot B
☐ Channel 0 ID : --
☐ Channel 1 ID : --

☐ Customize the LUN number : -- Select --
☐ Use extended host LUN functionality :
Alias: -- Select --
Filter type: Include
Access mode: Read-Write

Click **OK.** The list of Host LUN Mapping configurations will appear in the window.



Mapping

Host LUN mapping

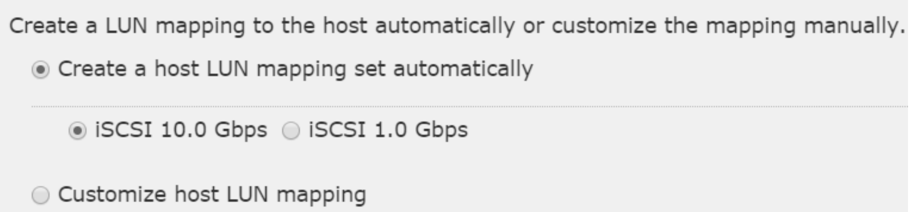
Map this volume to the host or manage existing LUN mappings.

Create Delete

□ Channel	Target	LUN	Host ID	Alias	Group	Filter type	Access mode
□ 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

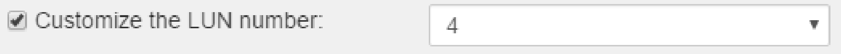
● iSCSI 10.0 Gbps ○ iSCSI 1.0 Gbps

○ Customize host LUN mapping

Manual Configuration

If you have manually configured the LUN mapping, select **Customize host LUN mapping** and select the channels or trunk groups for the mapping.

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.

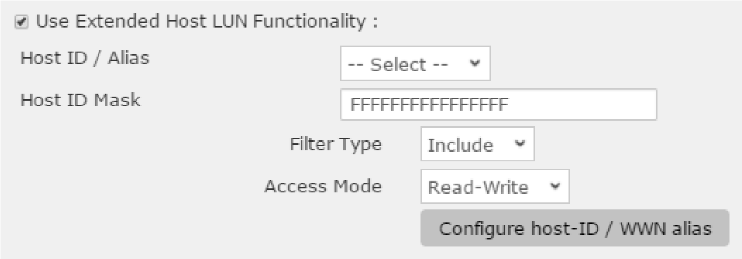
Go to

Settings / Device management > Storage > Volumes

Select a “Type: Block” volume and click the **Map to host** button.

Steps

Click **Use Extended LUN Functionality** and modify the parameters.



☑ Use Extended Host LUN Functionality :

Host ID / Alias: -- Select --

Host ID Mask: FFFFFFFFFFFFFFFF

Filter Type: Include

Access Mode: Read-Write

Parameters

Host ID/Alias

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 **Device Manager** page. Right click on the fiber channel adapter in the **Storage controllers** section and select **Properties** 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.

Host ID Mask

Works as a prefix mask in hexadecimal format.

Filter Type

Specifies whether to allow (include) WWNs or to forbid (exclude) them from accessing after filtering.

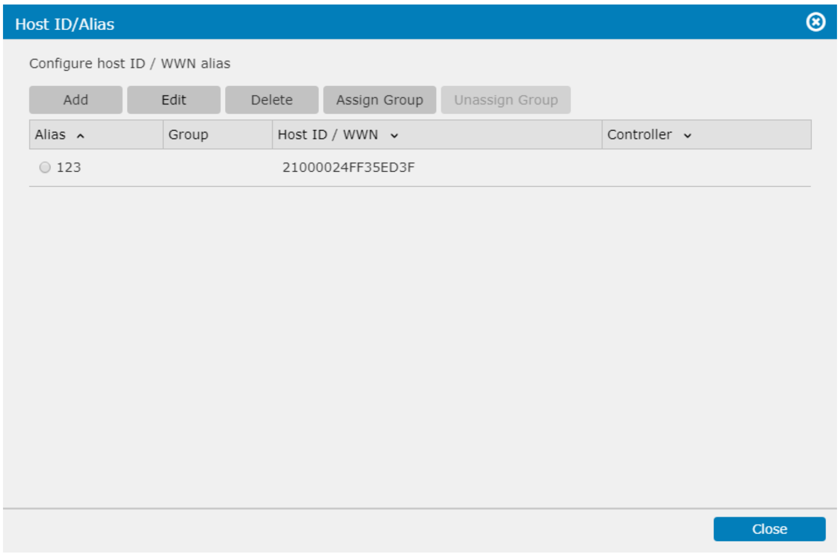
Access Mode

Specifies the access right of LUN mapping for the host: read-only or read-write.

Edit Host-ID/WWN

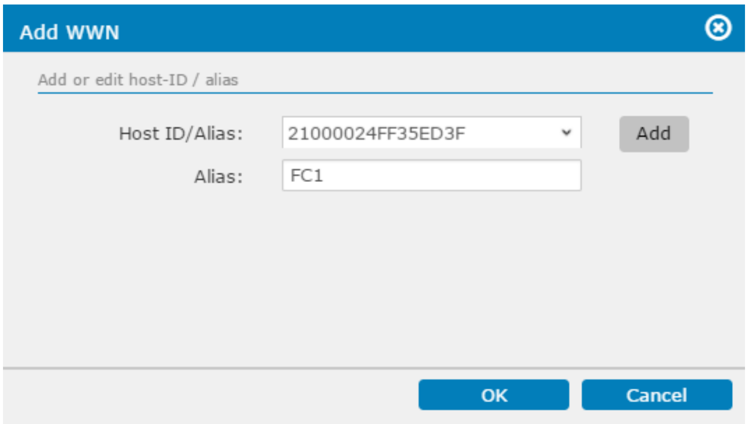
1. Click **Configure Host ID/WWN Alias**.

   Note: Edit Host-ID/WWN List enabled only when Extended Host LUN Functionality has been enabled.



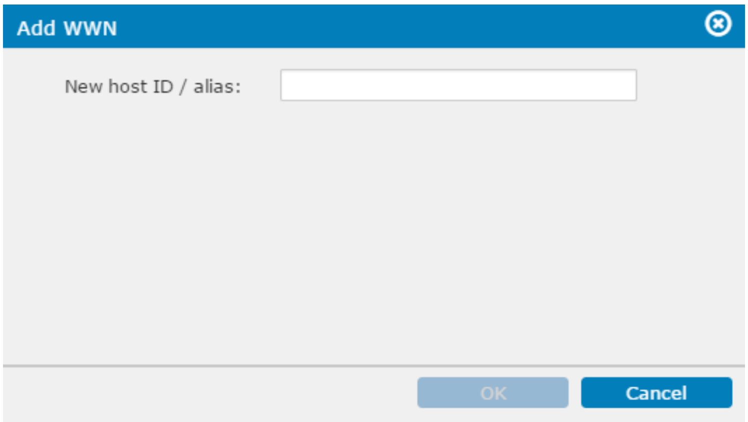
Alias	Group	Host ID / WWN	Controller
○ 123		21000024FF35ED3F	

2. 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.



Host ID/Alias: 21000024FF35ED3F

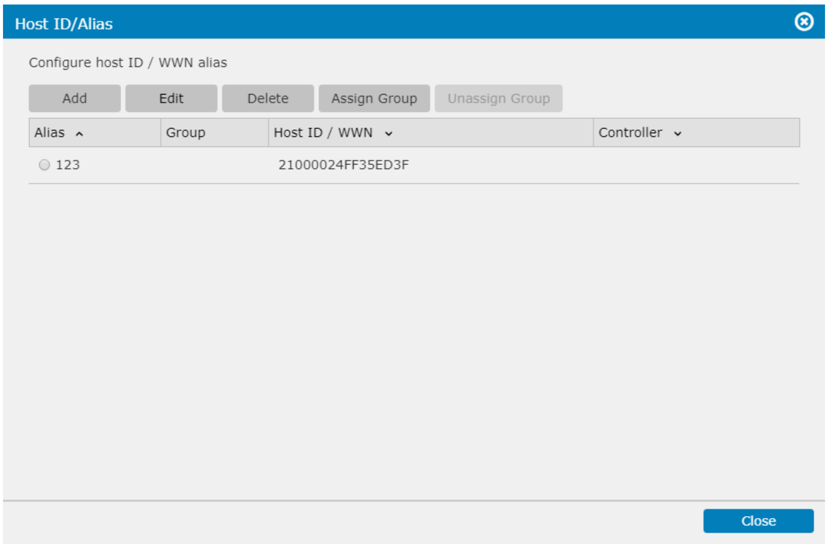
Alias: FC1



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).

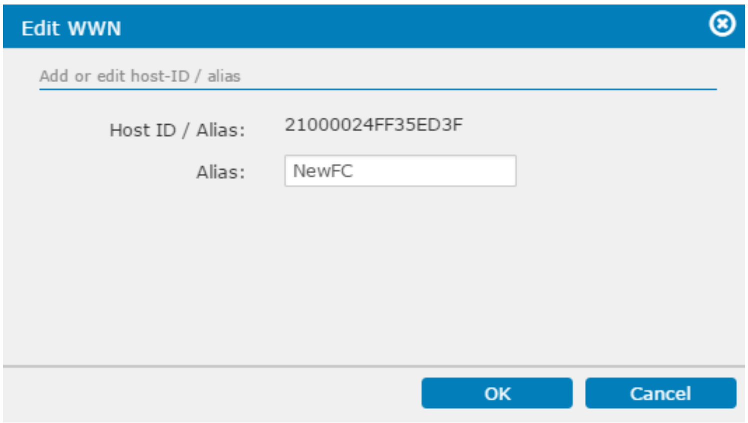
4. To delete a WWN Name from the List, Highlight a WWN in the list and click

Delete.



Alias	Group	Host ID / WWN	Controller
○ 123		21000024FF35ED3F	

5. To edit the alias name of the WWN, click **Edit** and enter the new name.



Host ID / Alias: 21000024FF35ED3F

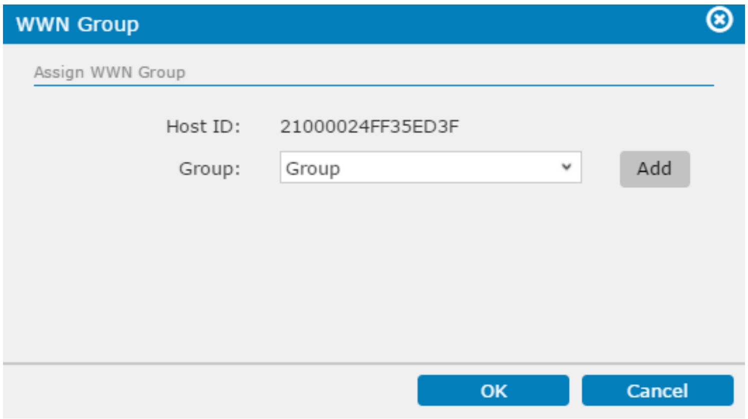
Alias: NewFC

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.

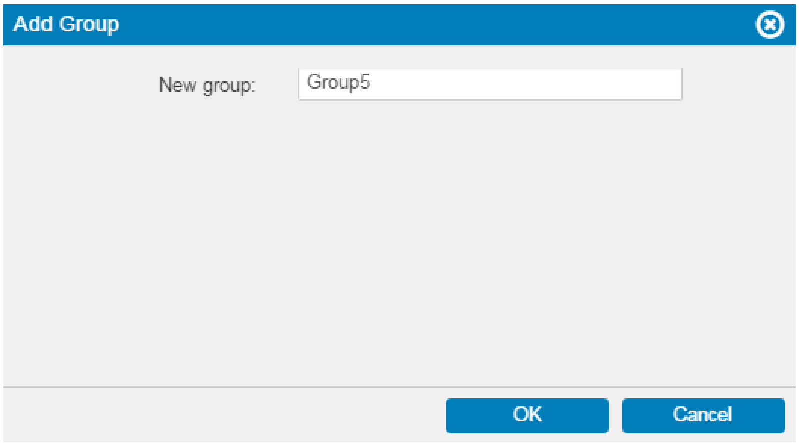
2. Click **Assign Group** and select the group from the drop down menu.



Host ID: 21000024FF35ED3F

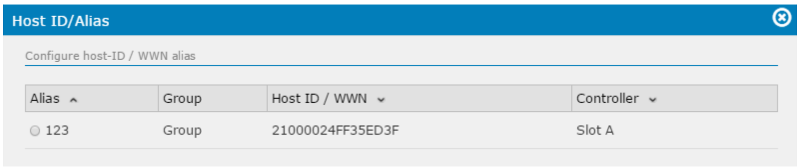
Group: Group

3. To add a new group, click **Add** and enter the group name.



New group: Group5

4. The group name will appear in the list.



Configure host-ID / WWN alias

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: 0xFFFFFFFFFFFFFFFC (Binary: 11111111 11111111 11111111 11111111 11111111 11111111 11111111 111111**00**)

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: 0x00000000000000A1 (Binary: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 10100001)

5. HBA-4: 0x00000000000000A2 (Binary: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 10100010)

The mask should be modified to reflect the changes such as:

6. For HBA-3: 0xFFFFFFFFFFFFFF5C (Binary: 11111111 11111111 11111111 11111111 11111111 11111111 11111111 **01011100**) (included)

7. For HBA-4: 0xFFFFFFFFFFFFFFFF (Binary: 11111111 11111111 11111111

11111111 11111111 11111111 11111111 **11111111**) (included)

Extended LUN Mapping (iSCSI Channel)

Extended LUN Mapping is available only for manual configuration.

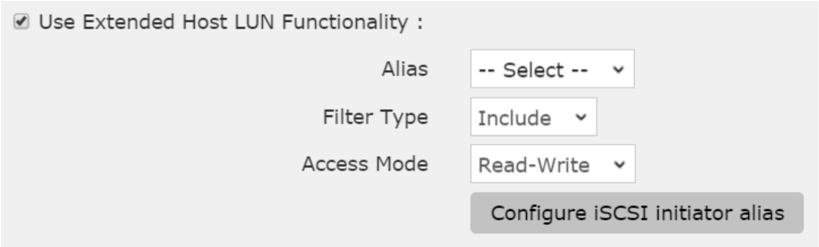
Go to

Settings / Device management > Storage > Volumes

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

Parameters

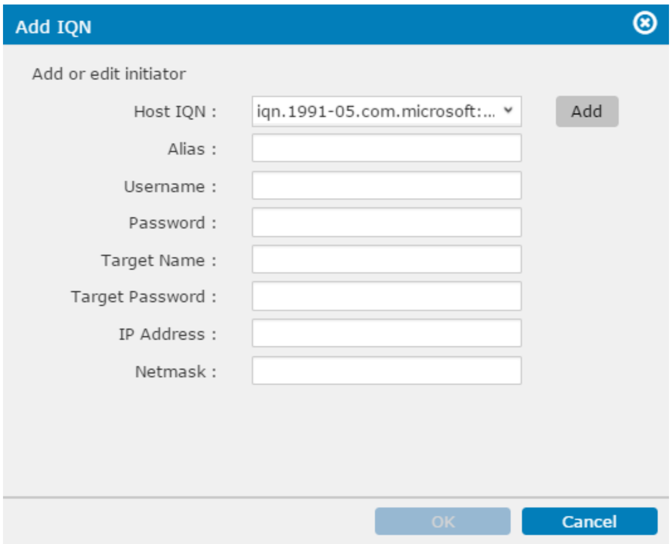
Alias: Specifies a pre-configured iSCSI initiator instance. To create a new initiator alias, click the Configure iSCSI Initiator Alias button.

Filter Type: Specifies whether to allow (include) initiators or to forbid (exclude) them from accessing after filtering.

Access Mode: 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.



Add IQN

Add or edit initiator

Host IQN : iqn.1991-05.com.microsoft:...

Alias :

Username :

Password :

Target Name :

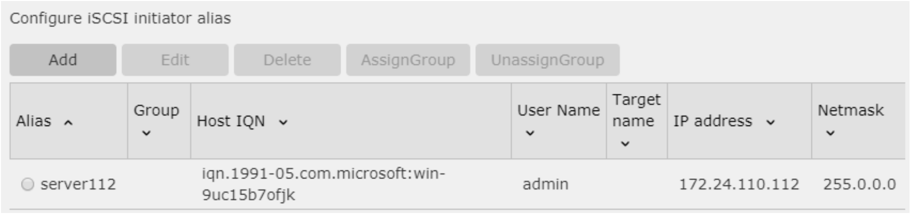
Target Password :

IP Address :

Netmask :

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).
Parameters	**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 easy to remember for the iSCSI initiator.
	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.
	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.
	IP Address/Netmask	Multiple initiator ports on an application server can sometimes share the same IQN.
Assign Group	Click the checkbox on one of the iSCSI initiator aliases and click the **Assign Group** button to set IQN groups for the aliases. An iSCSI initiator can be included in multiple groups.	



Configure iSCSI initiator alias

Alias	Group	Host IQN	User Name	Target name	IP address	Netmask
○ 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.

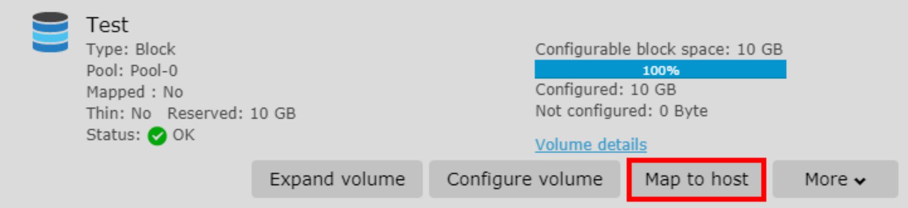
Deleting a LUN Mapping

There must be at least one volume of a pool available.

Go to

Settings / Device management > Storage > Volumes

Select a “Type: Block” volume and click the **Map to host** button.

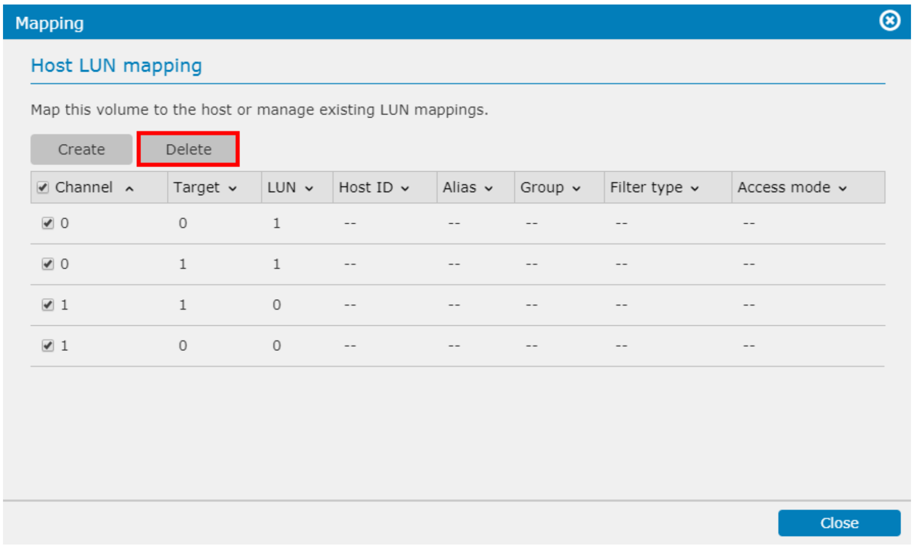


Test
Type: Block
Pool: Pool-0
Mapped : No
Thin: No Reserved: 10 GB
Status: ✓ OK

Configurable block space: 10 GB
100%
Configured: 10 GB
Not configured: 0 Byte

Steps

The host LUN mapping table will pop up. Select the host LUN you want to unmap and click **Delete**.



Map this volume to the host or manage existing LUN mappings.

☑ Channel	Target	LUN	Host ID	Alias	Group	Filter type	Access mode
☑ 0	0	1	--	--	--	--	--
☑ 0	1	1	--	--	--	--	--
☑ 1	1	0	--	--	--	--	--
☑ 1	0	0	--	--	--	--	--

About In-Band, Out-of-Band Flush

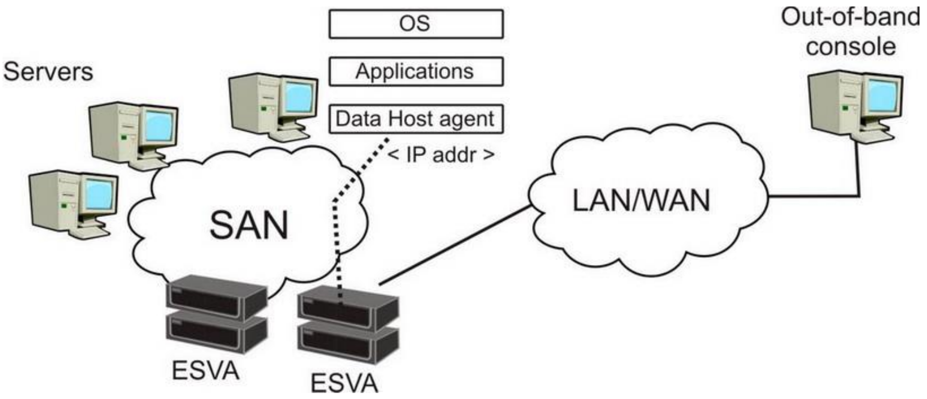
In-Band VS. Out-of-Band

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:

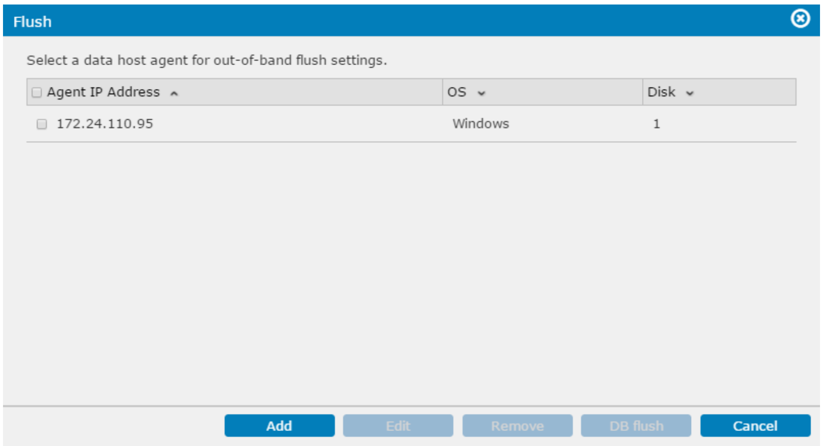
- Multiple host computers with database applications are connected to the subsystem. In-band flush might be in conflict when more than one host computers tries to back up user data at the same time. In this case, out-of-band flush allows multiple servers to perform data flushing in series without conflict.
- 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 / Device management > Storage > Volumes** Select a "Type: Block" volume and click the **More** button and select **Flush**.

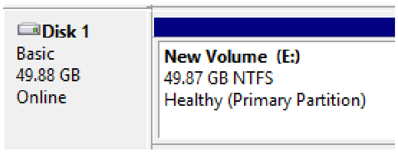
The Flush Settings window will appear.



Select a data host agent for out-of-band flush settings.

☐ Agent IP Address	OS	Disk
☐ 172.24.110.95	Windows	1

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)

Adding/Managing Volumes in the Cluster

You can create or manage the volumes on each appliance in the cluster.

Go to	**Cluster settings > Storage > Volumes**
Add a volume	Refer to Adding a Volume.
Manage a volume	1. Click on a desired volume. 2. To manage the volume, refer to the following sections for instructions: Setting a volume threshold Deleting a volume Expanding a volume Defragmenting a volume Mapping a volume to LUN Configuring out-of-band flush

Activating Deduplication on File-level Volumes (Btrfs File System)

For file-level volumes with Btrfs file system, data deduplication can be activated by schedule and free up your storage capacity.

Note: This functionality is only available when you have created a Btrfs volume and enabled deduplication.

Go to

Settings / Device management / Cluster settings > Storage > Volumes

Steps

1. Click **Deduplication (Btrfs Volumes)** tab.
2. Turn on deduplication function.
3. Specify a start date and time.
4. Specify the activation frequency.
5. Specify the maximum execution time for the schedule. Choose **Not limited** or **Customize**. If the schedule is customized, specify the time period.
6. Click **Save** to save the settings.
7. The deduplication status will indicate when will be the next time to run the schedule and the progress of the deduplication.

Pools

Go to	**Settings / Device management > Storage > Pools**	
View	The configuration window will appear.	
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

Click **Pool Details** to see more information.

Adding a Pool

Note:

- A logical drive must be at least 10 GB in size to form a pool.
- To manage storage tiering settings, see Storage Tiering.

Go to **Settings / Device management > Storage > Pools**

Steps

1. Click **Add Pool**.
2. Specify your pool name (this field is required). Enter a unique name for the volume. It accepts underscore (_) characters.
3. Select the write back in cache memory from the scroll down list. There are two options:

   Write-back (default): 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: Data write is done synchronously both to the cache and to the backing storage.

   Note:

   - The Write-Back and Write-Through setting overrides the write cache policy for the system.
   - When a critical event occurs, the writing policy may automatically switch to the more conservative Write-Through.

4. If needed, you can set writing policy and controller ownership policy by clicking Advanced settings.
5. Add Logical Drive:

   Click **Add logical drive**, you will be directed to the below page to configure logical drive parameters:

   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 how much of the logical drive to reserve for SSD over-provisioning.

7. Specify logical drive name: the name is preset (do not repeat Logical Drive name under the same pool).

8. Select a RAID protection 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).
   - **RAID 6**: at least 4 drives (improved performance with excellent data protection).

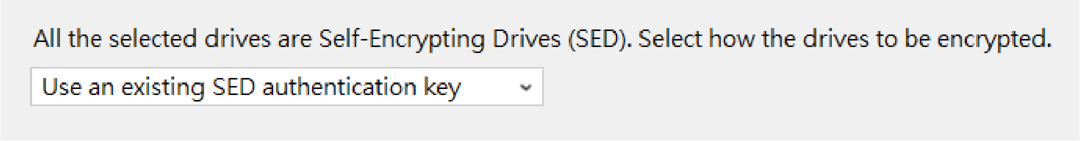
9. Select a stripe size for the logical drive, the default may be 128K.

   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

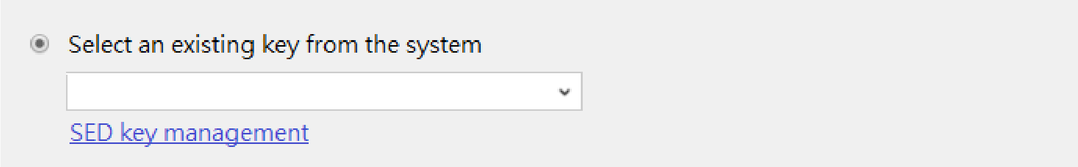


All the selected drives are Self-Encrypting Drives (SED). Select how the drives to be encrypted.

Use an existing SED authentication key

Select an existing key from the system from the scroll down list.

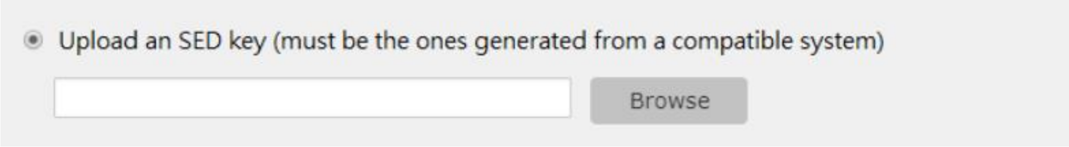
Press the SED key management link to direct you to SED key management page where you can choose two methods to upload your key file. Please refer to Advanced settings and find SED key management category.



● 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)

Once you have completed Logical Drive setting, your newly created Logical Drive will appear under Add Logical Drive button.

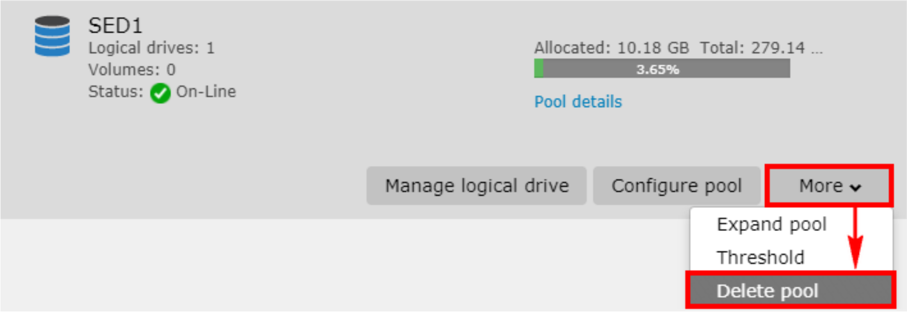
10. Click **OK**.

Deleting a Pool

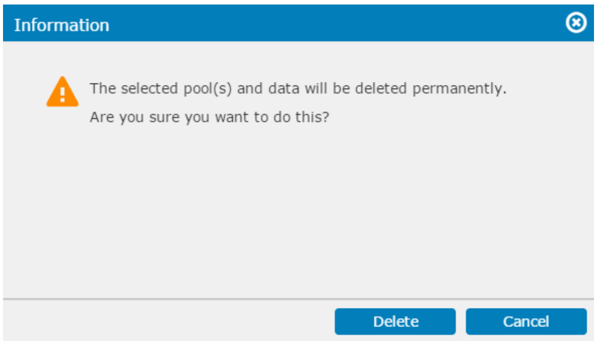
Go to	**Settings / Device management > Storage > Pools**

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.



Information

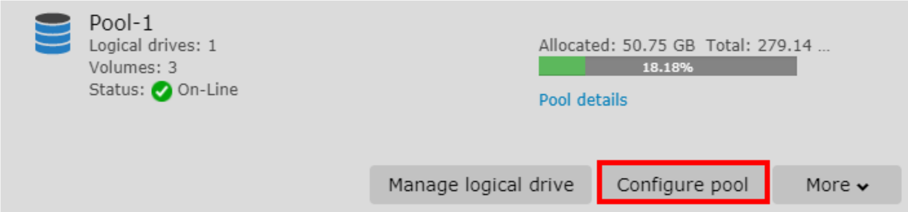
The selected pool(s) and data will be deleted permanently.
Are you sure you want to do this?

Configuring a Pool

Go to

Settings / Device management > Storage > Pools

Select a pool and click **Configure Pool**.

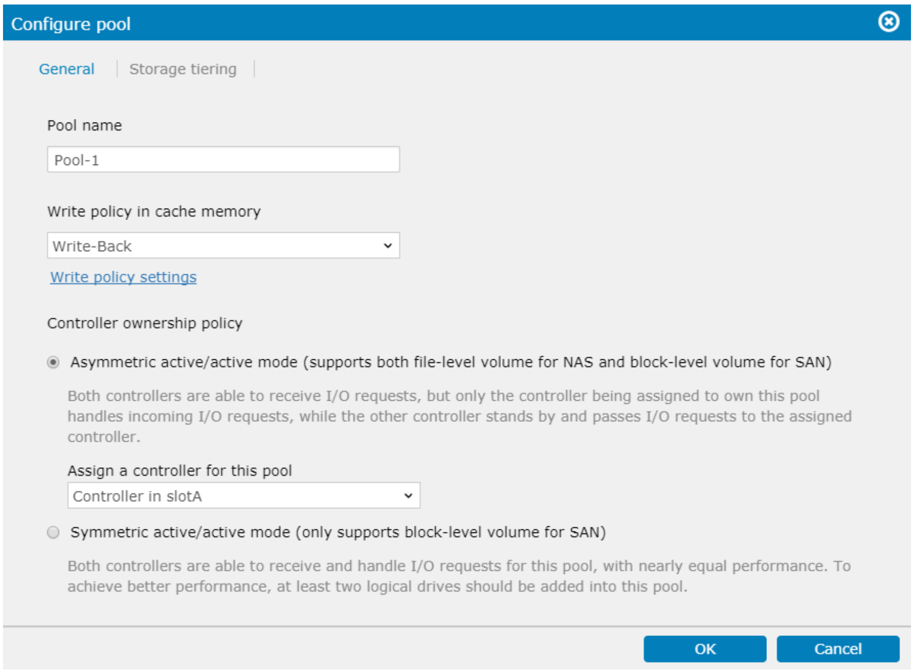


Pool-1
Logical drives: 1
Volumes: 3
Status: ✓ On-Line

Allocated: 50.75 GB Total: 279.14 ...
18.18%
Pool details

Steps

Change the parameters and click **OK** to confirm changes.



Configure pool

Pool name: Pool-1

Write policy in cache memory: Write-Back

Write policy settings

Controller ownership policy

● 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 slotA

○ 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.

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.

Assignment	Specifies which controller (Slot A or Slot B) this pool will be assigned to.
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.

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 EonStor GS/GSe 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.

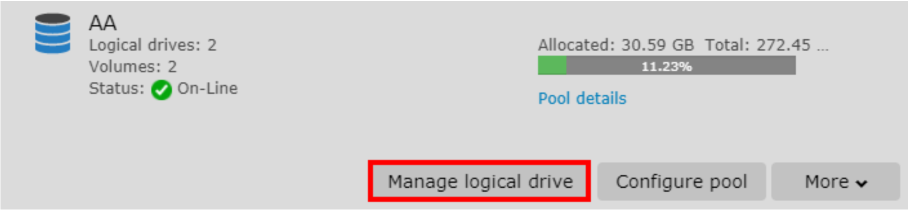
We recommended creating new logical drives in order to expand capacity of a pool. Adding new disks or replacing original disks with new ones requires reading data from old disks and writing data to the new ones, which consumes a lot more time than simply adding a logical drive to the pool.

The following steps show how to add new Logical Drives into a Pool.

Go to

Settings / Device management > Storage > Pools

Select a pool and click the **Manage Logical Drive** button.

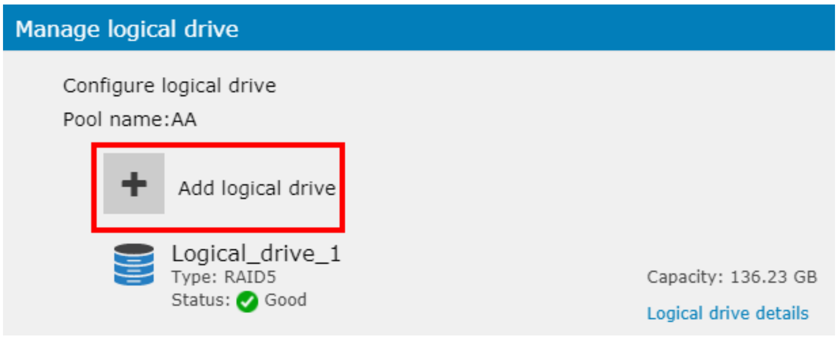


AA
Logical drives: 2
Volumes: 2
Status: ✓ On-Line

Allocated: 30.59 GB Total: 272.45 ...
11.23%

Steps

Click **Add logical drive button**.



Manage logical drive

Configure logical drive
Pool name:AA

Logical_drive_1
Type: RAID5
Status: ✓ Good
Capacity: 136.23 GB

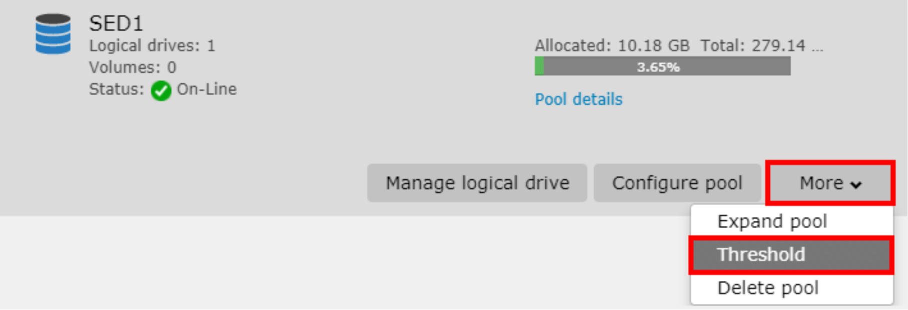
After a new Logical Drive has been added, select the Pool and click **Expand Pool** under **More**. In the window that appears, click **Expand** to expand the pool capacity with the new logical drive.

Pool Capacity Threshold

Go to

Settings / Device management > Storage > Pools

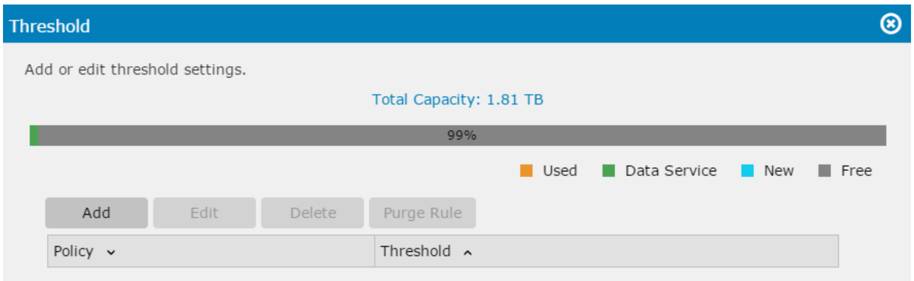
Select a pool and click the **More** button and select **Threshold**.



SED1
Logical drives: 1
Volumes: 0
Status: ✓ On-Line

Allocated: 10.18 GB Total: 279.14 ...
3.65%

Steps



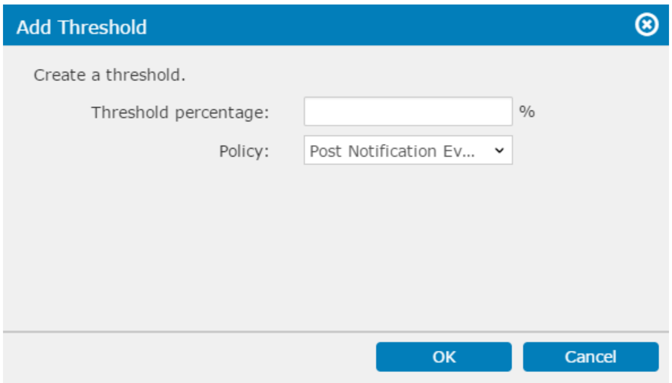
Threshold

Add or edit threshold settings.

Total Capacity: 1.81 TB

99%

Click **Add** and enter the threshold value (% of the pool). Choose the notification type. You may also modify or delete existing thresholds.



Add Threshold

Create a threshold.

Threshold percentage: %

Policy: Post Notification Ev...

Parameters	**Post Notification Event**	Creates a notification event when the amount of pool content reaches the threshold.
	Post Warning Event	Creates a warning event when the amount of pool content reaches the threshold.
	Post Critical Event	Creates a critical event when the amount of pool content reaches the threshold.
	Post Critical Event + Run Purge	Creates a critical event and purges all snapshot images when the amount of pool content reaches the threshold.

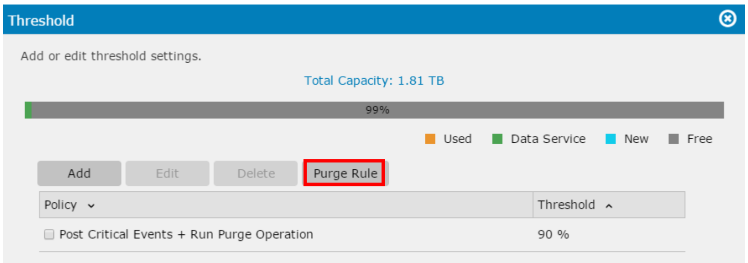
	Post Critical Event + Disassociate Snapshot Images	Creates a critical event and makes all snapshot images invalid when the amount of pool content reaches the threshold.

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.



Threshold

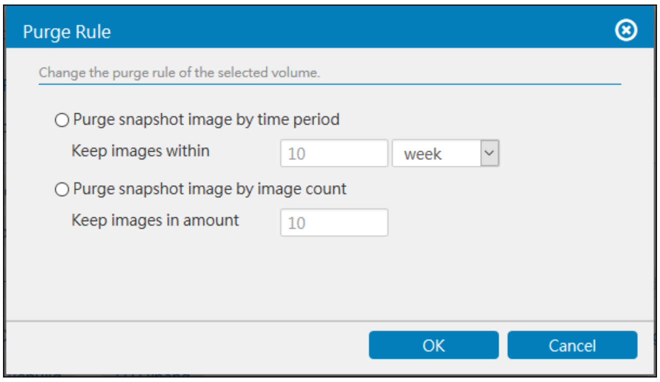
Add or edit threshold settings.

Total Capacity: 1.81 TB

99%

Policy	Threshold
□ Post Critical Events + Run Purge Operation	90 %

Highlight the purge setting and click **Edit**. The purge rule screen will appear.



Purge Rule

Change the purge rule of the selected volume.

○ Purge snapshot image by time period

Keep images within 10 week

○ Purge snapshot image by image count

Keep images in amount 10

Purge Parameters	**Purge Threshold**	Specifies the threshold policy: duration (by time) or the number of snapshot images (by SI count).
	Value	Specifies the values.

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.

Synchronize cache policy	Synchronize cache memory between both controllers on write-through.
Adaptive write policy	Apply adaptive write policy on writeback
Force write-through cache policy during CBM Failure	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.
Force write-through cache policy during power supply	This will force the system to use write-through cache policy during power supply failure.
Force write-through cache policy during fan failure	This will force the system to use write-through cache policy during cooling fan failure
Force write-through cache policy during critical components	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:
Critical component option	You can **Force the system to use write-through cache policy during abnormal status of critical components**. You can further configure this option by selecting one or more options: ● **CPU temperature too high or too low** ● **Controller temperature too high or too low** ● **Power supply voltage too high or too low**
Verify write on normal access	Performs Verify-after-Write during normal I/Os. Users may disable or enable this option. (This option might take up system resource)

	Verify write during logical drive initialization	Performs Verify-after-Write when initializing a logical drive. Users may disable or enable this option. (This option might take up system resource).
	Verify write during logical drive rebuild	Performs Verify-after-Write during the rebuild process. Users may disable or enable this option. (This option might take up system resource).
	Rebuild priority	Set the rebuild priority to High, Normal, Low.
	AV optimization	To fine-tune array performance for AV applications, choose **Customize**, **Light streaming**, or **Heavy streaming**. ● When choosing Customize, configure the following settings: ■ **Read-ahead option for media editing**: Set the option to **Auto**, **8MB**, **16MB**, or **32MB**. ■ **Maximum drive response timeout**: Set the waiting period for read/write request to **Disabled**, **160 (ms)**, **320 (ms)**, or **960 (ms)**.
	Read-ahead option for NAS file transfer	Set the option to **256K**, **512K**, **1M**, or **2M**.
	Write policy for NAS file transfer	Choose a way to write in-coming files to your NAS storage. **Write-Through**: The system writes in-coming files to both the cache and hard drives at the same time. **Write-Back**: The system first writes in-coming files to the cache and then to hard drives at later time.
	U.2 SSD endurance optimization	For U.2 SSDs, choose to reserve certain capacity, so that the drive endurance can be improved. **0% (1 DWPD)**: The U.2 SSD storage capacity is all available for use. **17% (3 DWPD)**: 17% of the U.2 SSD capacity is reserved to achieve 3 DWPD endurance. **Customize**: You can reserve 1% to 50% of the SSD space for better performance and SSD endurance.
	Controller ownership policy	**Note:** ● Before changing the pool assignment, the system needs to be reset to activate the assignment change.

- This feature is only available with two controllers attached on the storage device.
- File-level volumes and Automated Storage Tiering functionality cannot be configured on a pool in symmetric active/active mode.

Specifies which controller (Slot A or Slot B) this pool will be assigned to. Select **Asymmetric Active/Active** (default) or **Symmetric Active/Active mode.**

- **Asymmetric Active/Active:** Assign **Controller in SlotA** or **Controller in SlotB** for this pool.
- **Symmetric Active/Active:** 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.

Adding/Managing Pools in the Cluster

You can create or manage the pools on each appliance in the cluster.

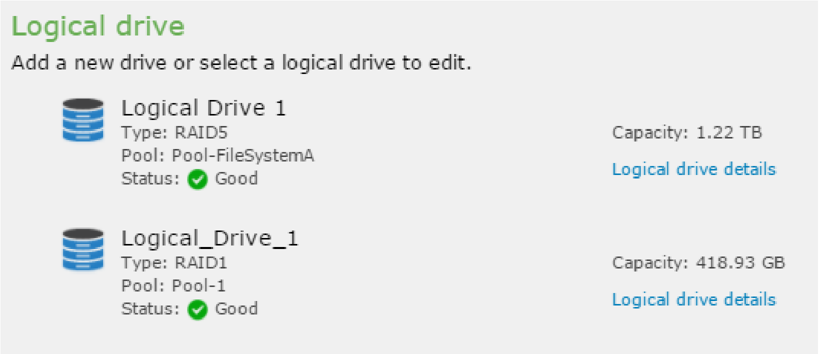
Go to	**Cluster settings > Storage > Pools**
Add a pool	Refer to Adding a Pool.
Manage a pool	1. Select the desired pool from the pool list. 2. Click **Configure pool**. To manage the pool, refer to the following sections for instructions: Deleting a Pool Configuring a Pool

Logical Drive

Go to

Settings / Device management > Storage > Pools

You can set the logical drive when creating or configuring the storage pool.



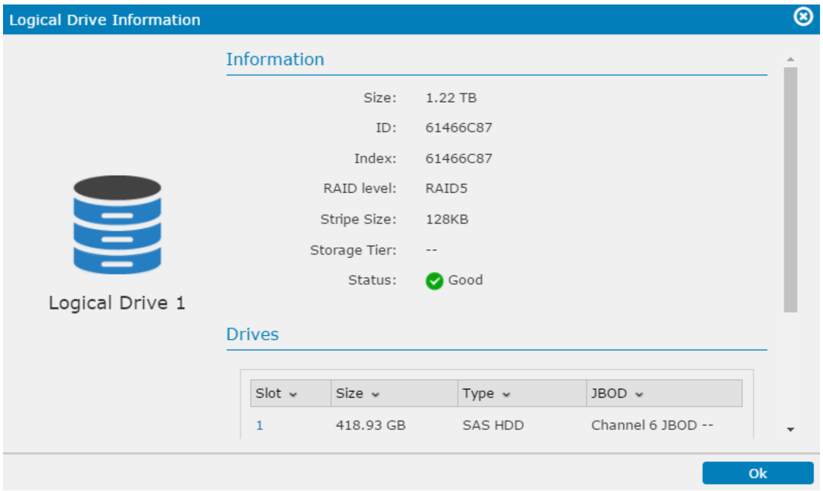
Logical drive

Add a new drive or select a logical drive to edit.

Logical Drive 1
Type: RAID5
Pool: Pool-FileSystemA
Status: ✓ Good
Capacity: 1.22 TB
Logical drive details

Logical_Drive_1
Type: RAID1
Pool: Pool-1
Status: ✓ Good
Capacity: 418.93 GB
Logical drive details

Click on **Logical drive details** to see the detailed information of the logical drive.



Logical Drive Information

Logical Drive 1

Information

Size: 1.22 TB
ID: 61466C87
Index: 61466C87
RAID level: RAID5
Stripe Size: 128KB
Storage Tier: --
Status: ✓ Good

Drives

Slot	Size	Type	JBOD
1	418.93 GB	SAS HDD	Channel 6 JBOD --

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.

	Index	Shows drive index.
	ID	Shows drive ID.
	RAID Level	Specifies the RAID level.
	Stripe Size	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. 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.
Logical Drive Status Message	**Online Initializing**	Drive is on-line and currently initializing.
	Online Expanding	Drive is on-line and currently expanding.
	Offline Initializing	Drive is being shutdown and currently initializing.
	Offline Expanding	Drive is being shutdown and currently expanding.
	Drive Missing	A member drive is missing (likely a result of loose drive insertion)
	Good	In good condition
	Checking/Updating parity	The system is checking/updating the Parity of the Logical Drive.
	Fatal Fail	The logical drive became inaccessible, likely a result of two or more member drives having failed.
	Incomplete	One or more member drives missing or failed
	Invalid	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.)
	Shutdown	Logical drive has been shut down. Users have to restart

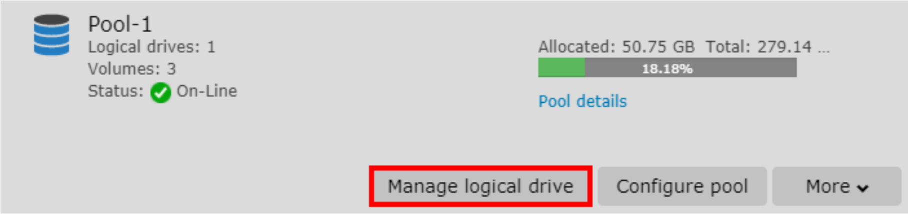
	the Logical Drive to bring it back online.
Rebuilding	Currently in rebuild process
Degraded	One or more member drives has failed, but the Logical Drive is still working because of RAID protection.
Adding	One or more non-member drives are being added into the Logical Drive.
Migrating	Data is migrating within tiers in the Logical Drive.
Add/Migrate Paused	An Adding/Migrating process is being paused.

Configuring Logical Drive Parameters

Go to

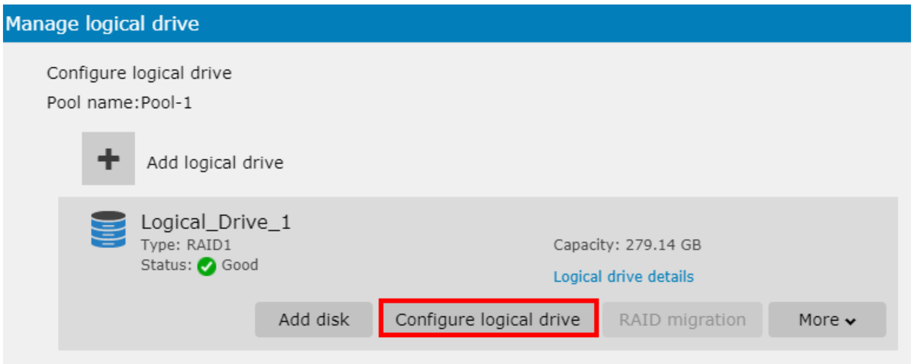
Settings / Device management > Storage > Pools

Select a pool and click the **Manage logical drive** button.



Pool-1
Logical drives: 1
Volumes: 3
Status: ✓ On-Line
Allocated: 50.75 GB Total: 279.14 ...
18.18%

In the Configure logical drive page, click **Configure logical drive** button.



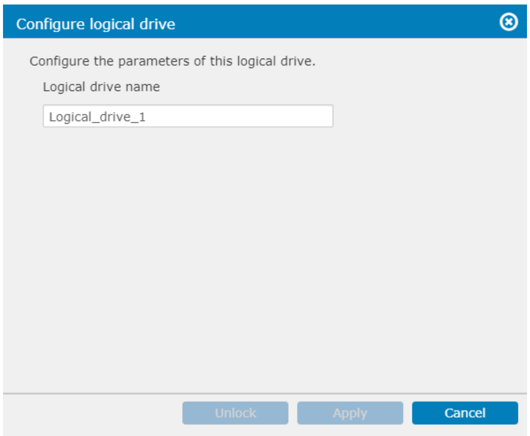
Manage logical drive

Configure logical drive
Pool name:Pool-1

Logical_Drive_1
Type: RAID1
Status: ✓ Good
Capacity: 279.14 GB

Steps

The following window will be shown. Click **Apply** to save your changes.



Configure logical drive

Configure the parameters of this logical drive.
Logical drive name
Logical_drive_1

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.

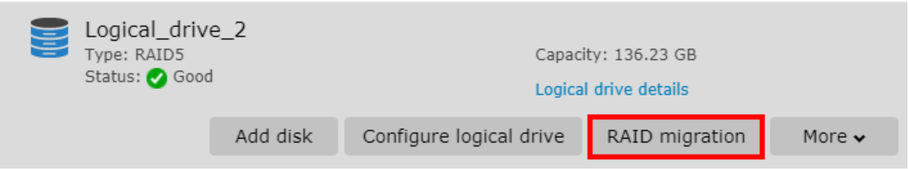
You cannot migrate a logical drive if it is already part of a pool.

RAID 5 VS RAID 6

	Member Drives	**Capacity**	**Redundancy**
RAID 5	N = 3 or more	N-1	Single disk failure
RAID 6	N = 4 or more	N-2	Dual disk failure

Steps

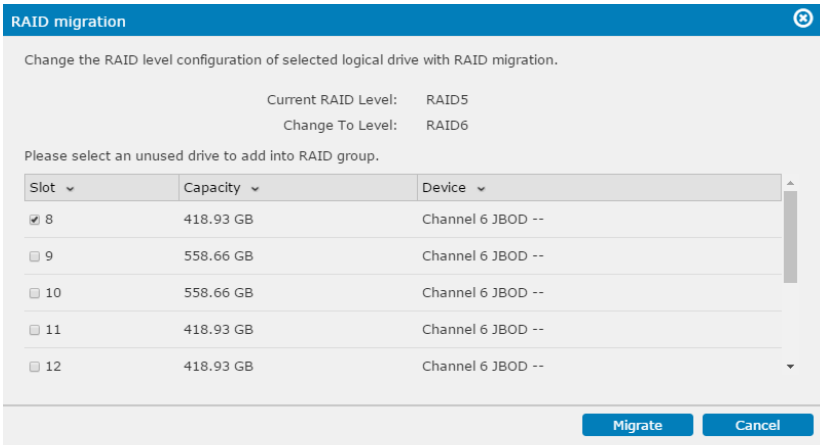
Select a logical drive and click the **RAID migration** button. Please note that this operation can only be implemented on RAID5 or RAID6 logical drives.



Logical_drive_2
Type: RAID5
Status: ✓ Good
Capacity: 136.23 GB

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

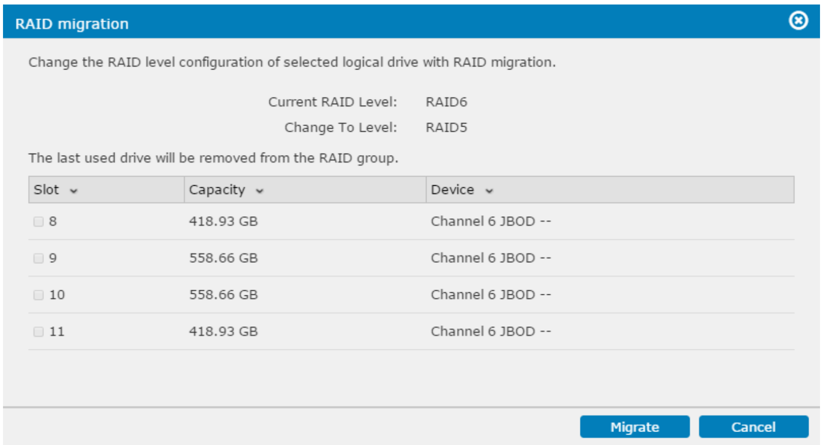
Change the RAID level configuration of selected logical drive with RAID migration.

Current RAID Level: RAID5
Change To Level: RAID6

Please select an unused drive to add into RAID group.

Slot	Capacity	Device
☑ 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 --
□ 12	418.93 GB	Channel 6 JBOD --

Example 2: Migrate from RAID 6 to RAID 5.



RAID migration

Change the RAID level configuration of selected logical drive with RAID migration.

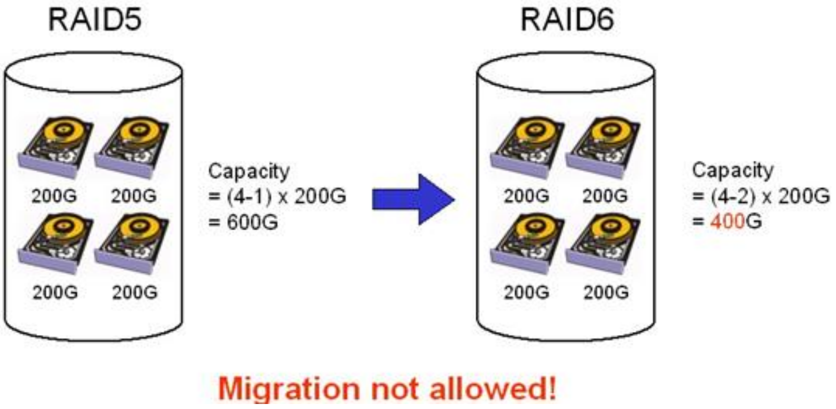
Current RAID Level: RAID6

Change To Level: RAID5

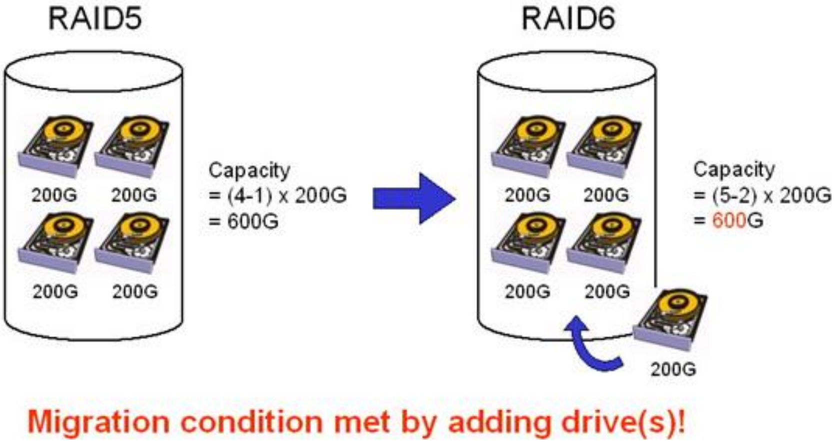
The last used drive will be removed from the RAID group.

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 --

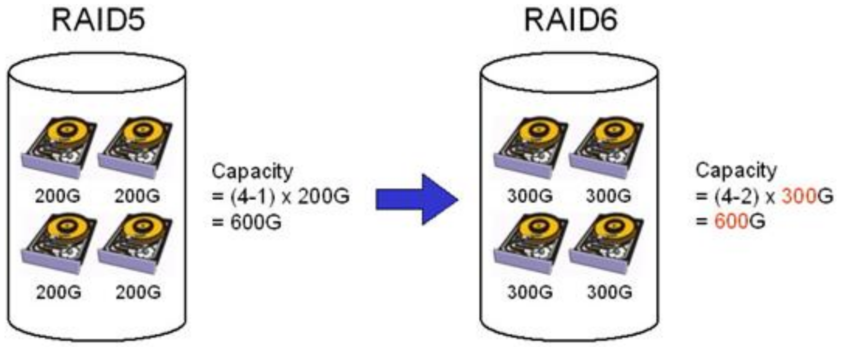
Migration Examples The usable capacity of the to-be RAID6 array is smaller than the usable capacity of the original RAID5 array.



The additional capacity for migrating to a RAID6 array is acquired by adding a new member drive.



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)!

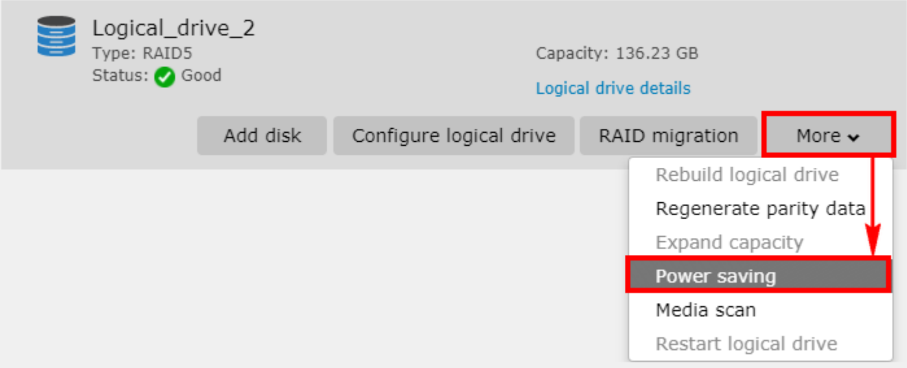
Configuring Power Saving Mode

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.

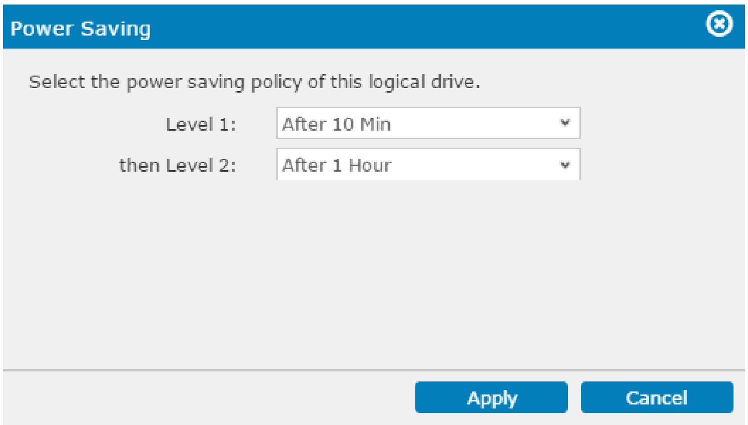
Go to **Settings / Device management > Storage > Logical Drive**

Steps Select a logical drive, click **More** and select the **Power Saving** option.



Logical_drive_2
Type: RAID5
Status: ✓ Good
Capacity: 136.23 GB

The power saving page will appear. Click **Apply** when ready.



Power Saving

Select the power saving policy of this logical drive.

Level 1: After 10 Min
then Level 2: After 1 Hour

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

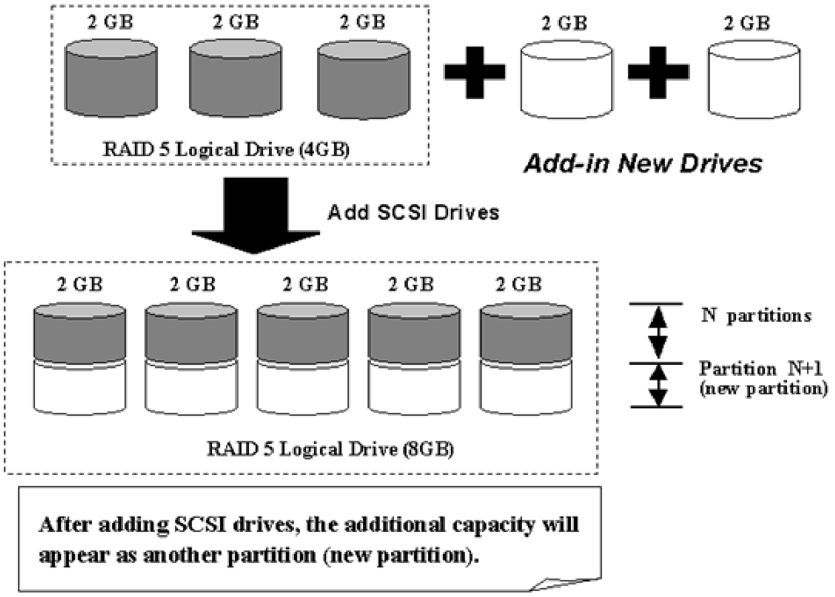
- When adding new drives to an existing logical drive, the new drives will be recognized as a new volume. Also, the new drive(s) must have the same or larger capacity than the existing member drives.
- RAID 0 or NRAID logical drives cannot be expanded because they lack parity information and therefore 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.

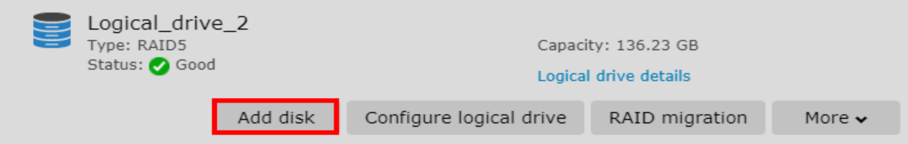


After adding SCSI drives, the additional capacity will appear as another partition (new partition).

Go to **Settings > Storage > Logical Drive**

Steps

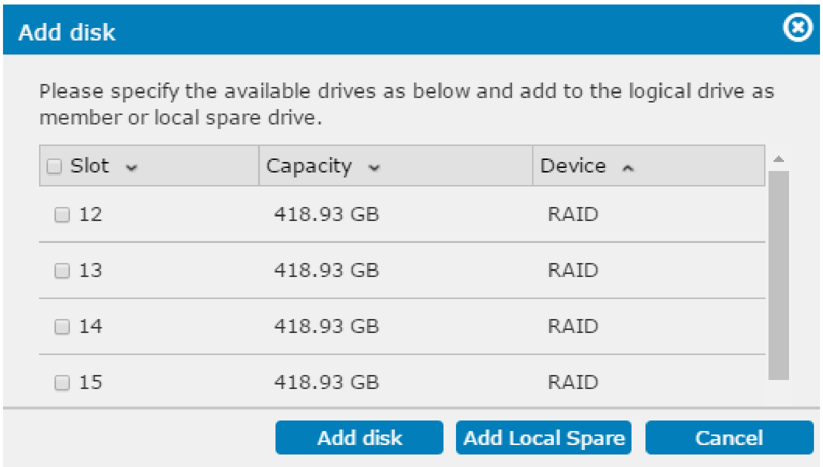
1. Select a logical drive and click **Add disk**.



Logical_drive_2
Type: RAID5
Status: ✓ Good

Capacity: 136.23 GB

2. In the pop up window, select one or more disks to be added as a member drive or a spare drive.

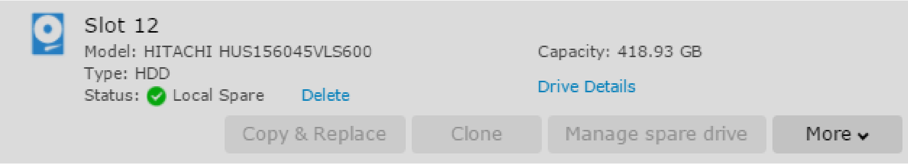


Add disk

Please specify the available drives as below and add to the logical drive as member or local spare drive.

□ Slot	Capacity	Device
□ 12	418.93 GB	RAID
□ 13	418.93 GB	RAID
□ 14	418.93 GB	RAID
□ 15	418.93 GB	RAID

3. If a local spare drive has been added, the newly added drive will be marked as Local Spare in the **Drive page**.



Slot 12
Model: HITACHI HUS156045VLS600
Type: HDD
Status: ✓ Local Spare

Capacity: 418.93 GB

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:

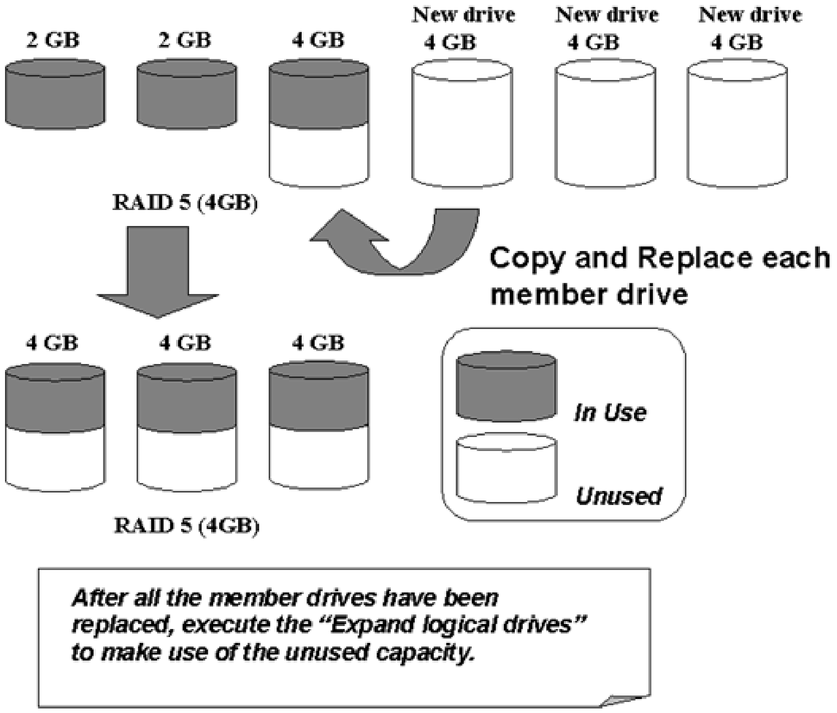
1. You may add more member drives.
2. You may copy and replace member disk drives with larger capacity drives,

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.



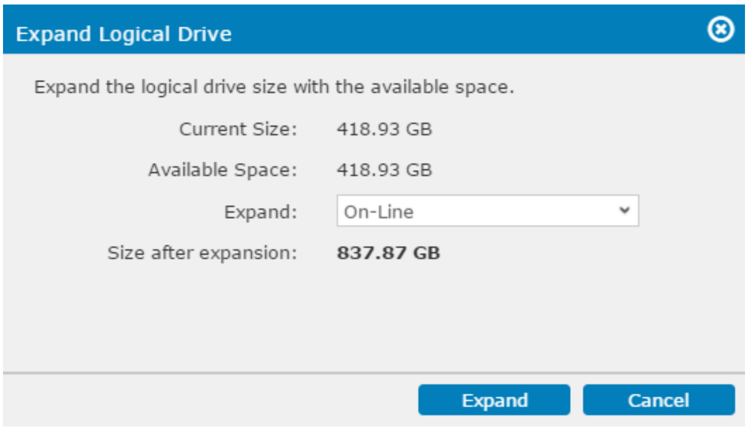
After all the member drives have been replaced, execute the "Expand logical drives" to make use of the unused capacity.

Go to

Settings > Storage > Logical Drive

Steps

The expanded logical drive page will appear. Select the initialization mode and click **Expand**.



Expand the logical drive size with the available space.

Current Size: 418.93 GB

Available Space: 418.93 GB

Expand: On-Line

Size after expansion: **837.87 GB**

Parameters

Expandable Size: Shows the available size to be expanded. The available size is automatically calculated by (Total capacity) – (Current logical drive capacity).

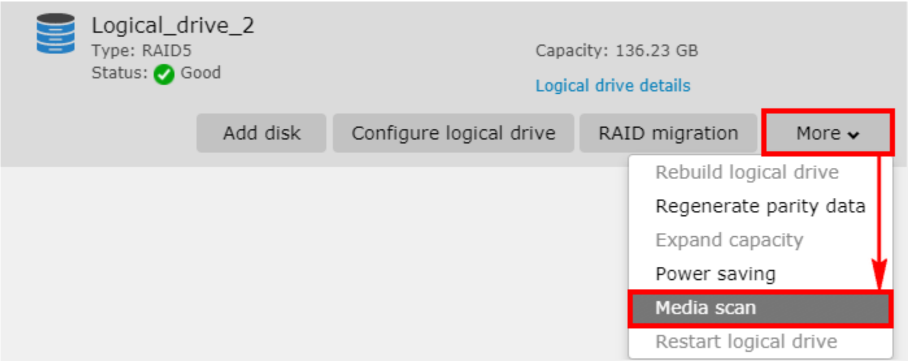
Execution (Initialize) Mode	Shows how the expansion will be executed: online (expansion continues in the background while users carry on with their tasks using the logical drive; this is a slower process) or offline (during expansion, users cannot use the logical drive; This is a faster process).

Scanning a Logical Drive Manually

You can only scan a logical drive after its initialization is completed.

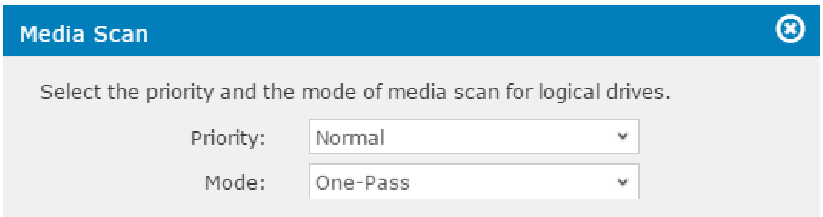
Steps

Select a logical drive, click the **More** button and then click the **Media Scan** option.



Logical_drive_2
Type: RAID5
Status: Good
Capacity: 136.23 GB

The scan configuration window will appear.



Media Scan

Select the priority and the mode of media scan for logical drives.

Priority: Normal
Mode: One-Pass

Parameters	**Priority**	The higher the priority, the faster the scanning but the system performance will decrease.
	Mode	Scans once (Execution Once) or continuously.

Rebuild a Logical Drive

The Rebuild menu appears only for RAID 1, 3, 5, of 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.

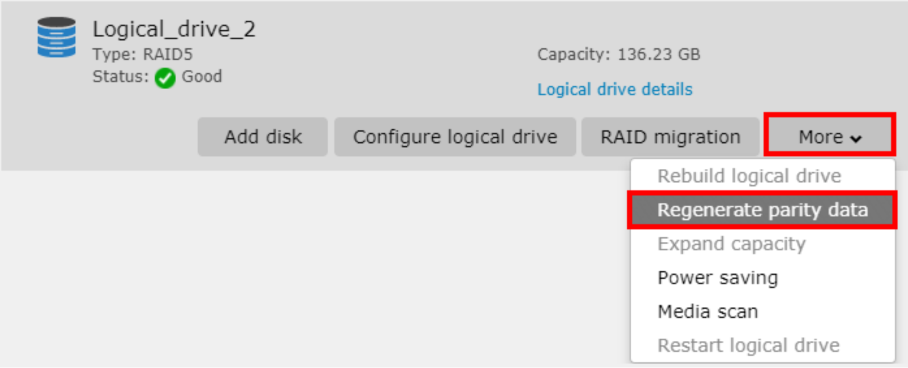
Steps	Select the logical drive that is in a degraded state and click the **Rebuild logical drive** button. If the logical drive does not go back to a healthy state after rebuilding, remove it and create the logical drive anew.

Regenerating Parity

This function does not apply to RAID0 or NRAID logical drives. You may regenerate parity to determine whether data parity inconsistency exists.

Steps

Select a logical drive. Click the **More** button and then click the **Regenerate parity data** 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

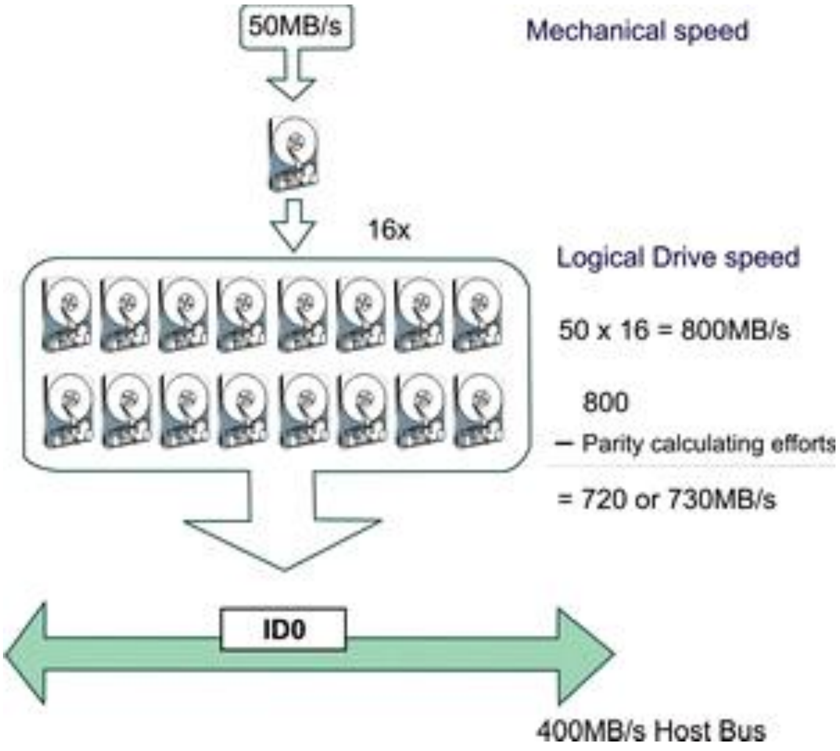
Select a logical drive that is currently in the Shutdown status. Click the **More** button and choose the **Restart logical drive** option. The logical drive will be restarted immediately.

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.

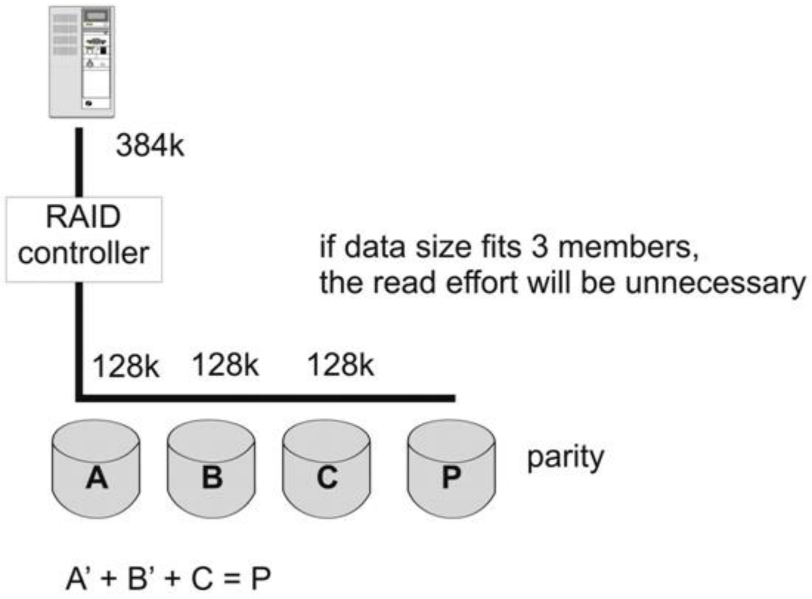
Optimizing Stripe Size

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.

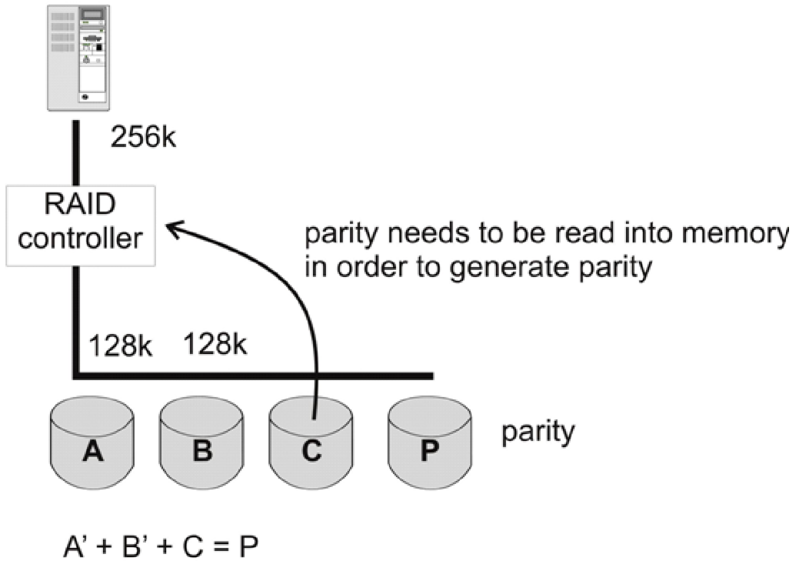
We will use RAID 3 in the example below.

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.


384k
RAID controller
if data size fits 3 members,
the read effort will be unnecessary
128k 128k 128k
A
B
C
P
parity
A' + B' + C = P

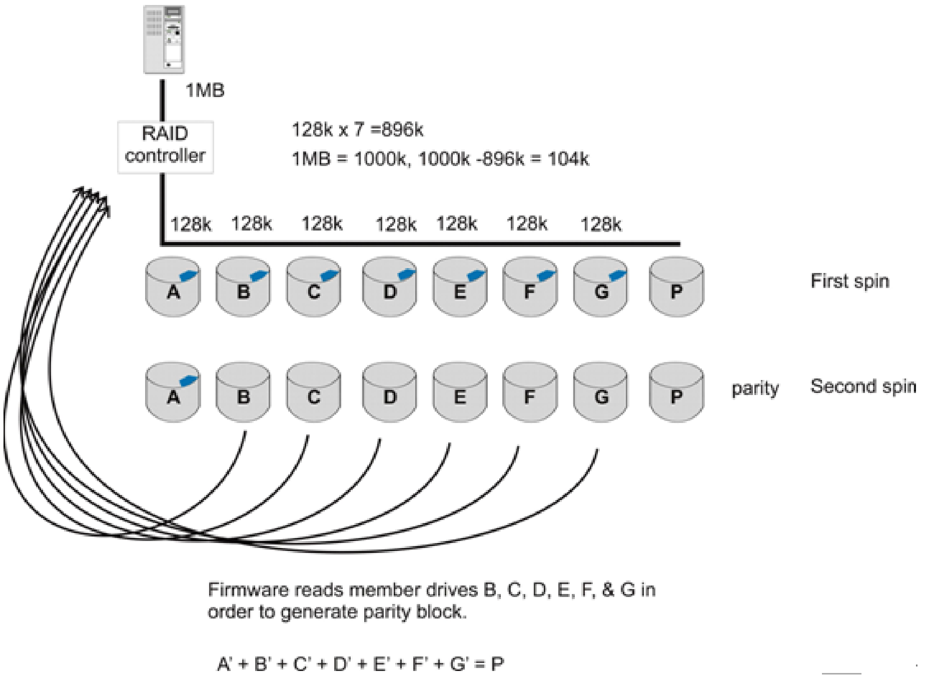
I/O Size > Stripe Depths

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.


256k
RAID controller
parity needs to be read into memory
in order to generate parity
128k 128k
A
B
C
P
parity
A' + B' + C = P

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 drags on performance (hard drive seek and rotation efforts) and will ensure optimal performance.


1MB
RAID controller
128k x 7 =896k
1MB = 1000k, 1000k -896k = 104k
128k
128k
128k
128k
128k
128k
128k
A
B
C
D
E
F
G
P
First spin
A
B
C
D
E
F
G
P
parity
Second spin
Firmware reads member drives B, C, D, E, F, & G in order to generate parity block.
A' + B' + C' + D' + E' + F' + G' = P

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) x 1TB = 7TB
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) x 100 x 85% = 595 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) x 180 x 85% = 1071 IOPS

Protecting a Logical Drive with Self-encrypting Drives (SED)

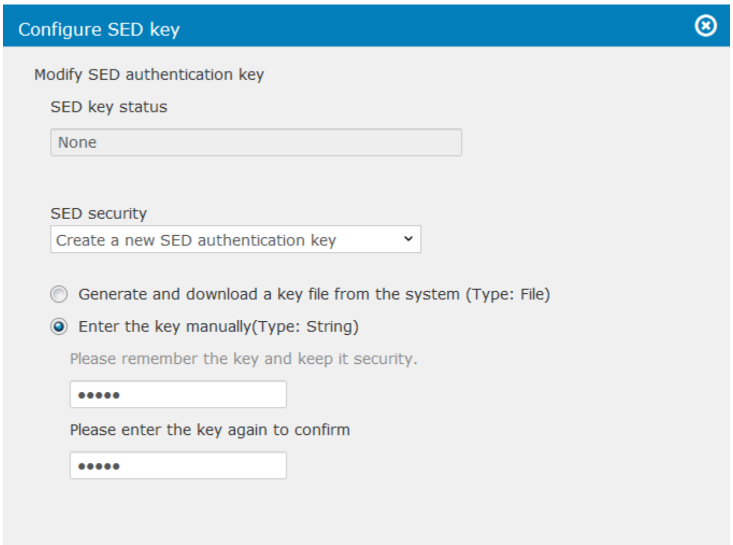
You can create and manage a local encryption key to protect a logical drive on the storage device when the logical drive is purely made up of self-encrypting drives (SED).

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 / Device management** > **Storage** > **Pool**
Steps	1. Click on the storage pool made up of SED drives. 2. Click **Manage logical drive**. 3. Click on the desired logical drive to encrypt. 4. Click **More** > **Modify SED authentication key**. 5. Go to the **SED security** drop-down menu and select how to encrypt the SED logical drive:

Disabled	The system does not encrypt the SED logical drive.
Use an existing SED authentication key	Encrypt the SED logical drive with an existing key: **Select an existing key from the system**: Select a global key or a local key stored in the system. **Upload an SED key**: Click **Browse** to upload a key file. Only the key file generated by an Infortrend/STORANDER system is compatible.
Create a new SED authentication key	Encrypt the SED logical drive with a new key: **Generate and download a key file from the system**: Click **Generate** to create a .key file that contains the SED authentication key. Then, upload the key file for confirmation by clicking **Browse**. **Enter the key manually**: Enter a custom key and confirm it. You must keep this key in a secure place. This key cannot be recovered once lost or forgotten.



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

•••••

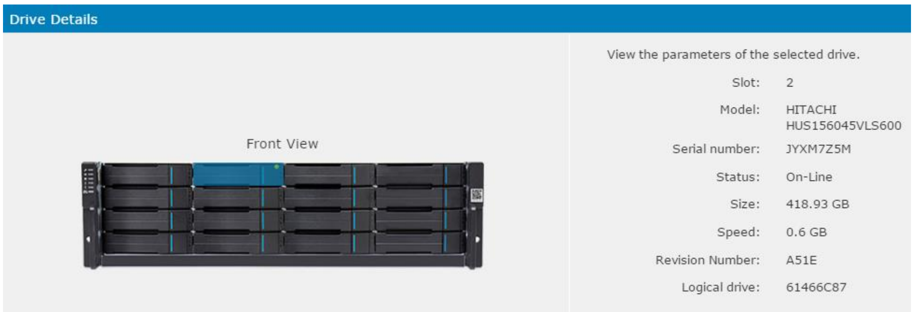
6. Click **Apply** to encrypt the SED logical drive.

Drives

Go to

Settings / Device management > Storage > Drives

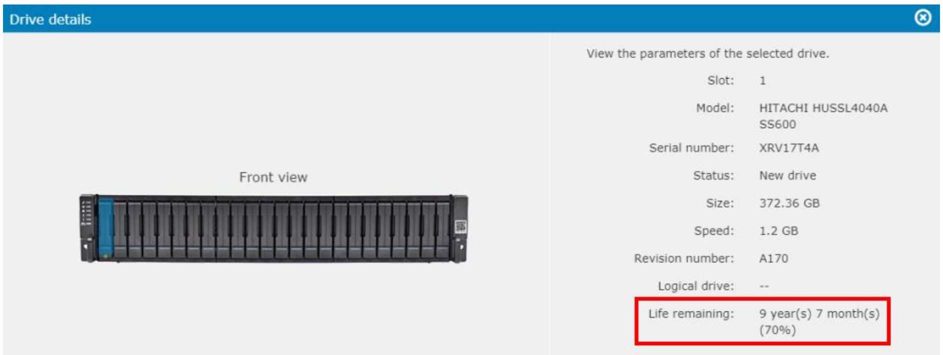
Click the drive slot to manage the disk drive, or click **Drive Details** to see the details of the hard drive.



View the parameters of the selected drive.

Slot: 2
Model: HITACHI HUS156045VLS600
Serial number: JYXM7Z5M
Status: On-Line
Size: 418.93 GB
Speed: 0.6 GB
Revision Number: A51E
Logical drive: 61466C87

SSD's life span is displayed under "Life remaining" in year/month/percentage format.

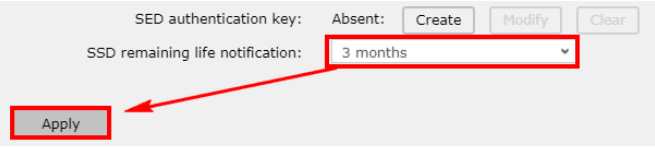


View the parameters of the selected drive.

Slot: 1
Model: HITACHI HUSSL4040A SS600
Serial number: XRV17T4A
Status: New drive
Size: 372.36 GB
Speed: 1.2 GB
Revision number: A170
Logical drive: --
Life remaining: 9 year(s) 7 month(s) (70%)

Drive Status	**Global Spare**	Global spare drive
	Local Spare	Local spare drive
	Enclosure Spare	Enclosure spare drive
	Initial	Currently initializing
	On-Line	In good condition
	Off-Line	The Logical Drive has been shutdown.
	Rebuilding	Currently in rebuilding process
	New Drive	An unformatted new drive which has not been included in a logical drive or configured as a spare drive
	Used	An used drive which has not been included in a logical

	drive or configured as a spare drive
Formatted	Formatted drive with a reserved section
Bad	Failed drive
Drive Absent	A drive does not exist in this slot
Adding	Being added to a logical drive
Ceding	Being dismissed from a logical drive (such as when migrating from RAID 6 to RAID 5)
Copying	Copying data from a member drive to be replaced
Cloned	Clone drive holding the replication of data from a source drive
Cloning	Cloning data
Missing	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.
SB-Missing	Spare drive missing
Exiled	Turned off by firmware for being unreliable
Media scan	The system is scanning the drive to check whether it’s still reliable.
Read-only	The drive is being tested for read only operations.
Read-Write	The drive is being tested for both read and write operations.
Life remaining	The life remaining of the SSD drive. The status shows the life span of the SDD drive For EonStor GS 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 **Apply** to complete the settings.



SED authentication key: Absent:

SSD remaining life notification: 3 months

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.

<u>Drive Types and Applicable Features</u>

	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.

Go to	**Settings / Device management > Storage > Drives**	
Advance options	**Model**	Enter the model name.
	Type	Choose which type of hard drives to search for: **Any**, **SSD**, **HDD**, or **NVMe SSD**.
	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.
	Health	Choose a health status as the search criterion.

Press **Search** to start searching for results, or press **Reset** button to set all parameters to their factory default.

Spare Drive Types

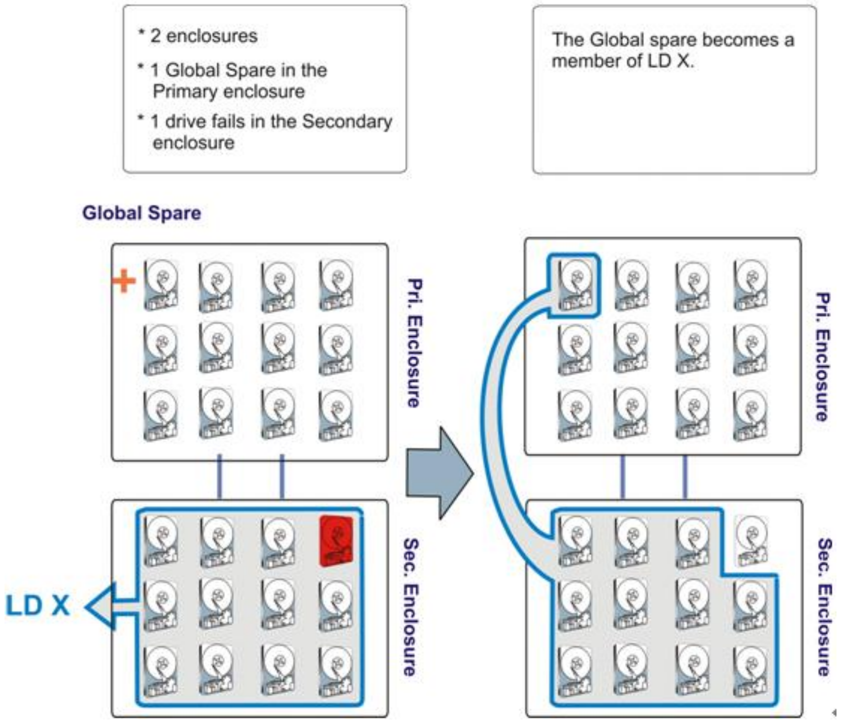
A spare drive replaces a failed disk drive. A spare drive is assigned to a logical drive. When a member drive of that logical drive fails, the spare drive takes place of the failed drive and becomes part of that logical drive. The logical drive starts rebuilding the data using parity information.

Types	**Local spare**	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.
	Global spare	A global spare drive is not dedicated to a specific logical drive. It can be used to replace any disk drive.
	Enclosure spare	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.

Why Enclosure Spare?

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.

The Enclosure Spare helps prevent the situation by rebuilding drives that only reside in the same enclosure.

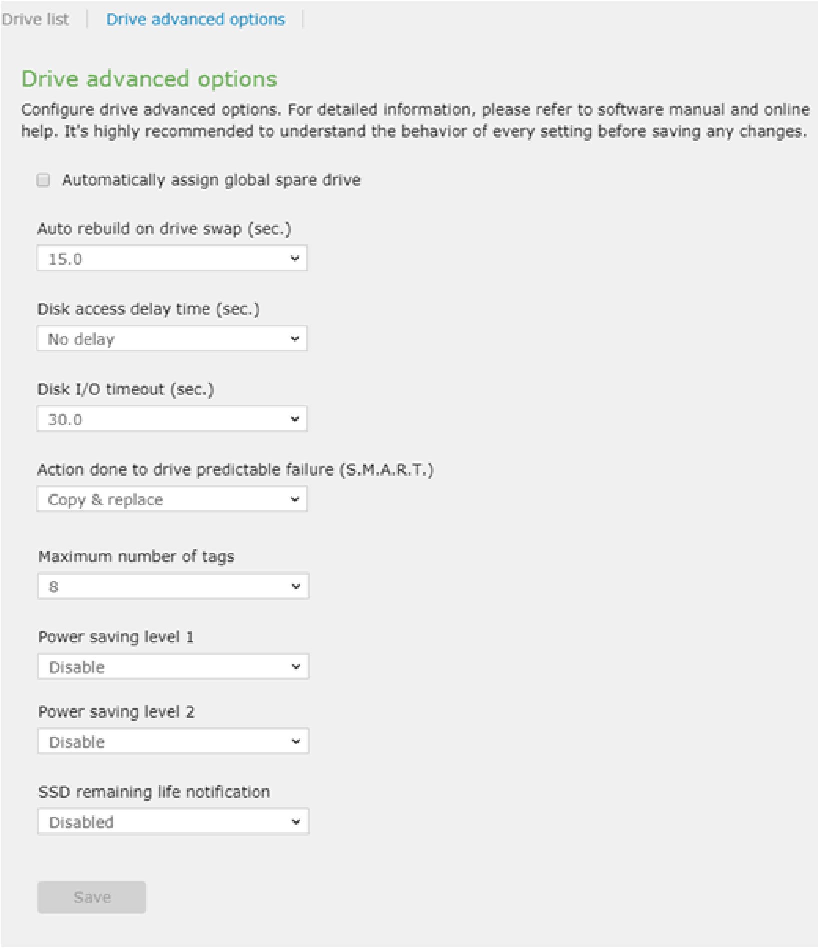


- 2 enclosures
- 1 Global Spare in the Primary enclosure
- 1 drive fails in the Secondary enclosure

The Global spare becomes a member of LD X.

Drive advanced options

To set advanced options for your drives, select **Drive advanced options** tab on the Drive page.



Drive advanced options

Configure drive 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.

□ Automatically assign global spare drive

Auto rebuild on drive swap (sec.): 15.0

Disk access delay time (sec.): No delay

Disk I/O timeout (sec.): 30.0

Action done to drive predictable failure (S.M.A.R.T.): Copy & replace

Maximum number of tags: 8

Power saving level 1: Disable

Power saving level 2: Disable

SSD remaining life notification: Disabled

When you complete the settings, click **Save** to save your configurations.

Parameters	**Automatically assign global spare drive**	Select this option to automatically assign a disk drive to be a global spare drive.
	Auto rebuild on drive swap	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)
	Disk access delay time	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.
	Drive I/O timeout (sec)	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 noth 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.

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.

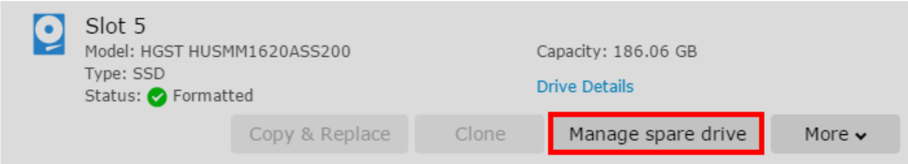
Mixing SATA and SAS Drives

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

Settings / Device management > Storage > Drives

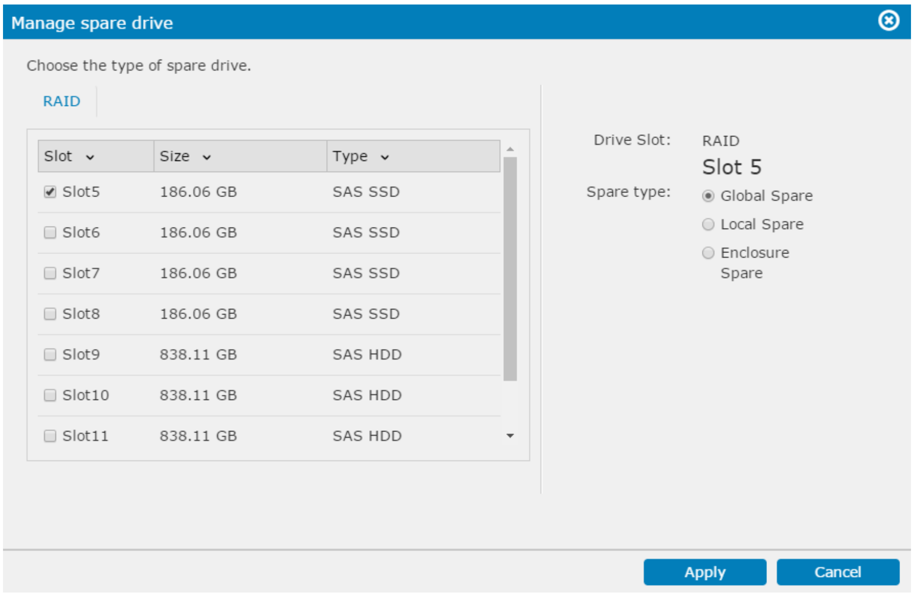
Click the **Manage Spare Drive** button.



Slot 5
Model: HGST HUSMM1620ASS200
Type: SSD
Status: ✓ Formatted
Capacity: 186.06 GB

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.



Manage spare drive

Choose the type of spare drive.

Slot	Size	Type
☑ Slot5	186.06 GB	SAS SSD
□ Slot6	186.06 GB	SAS SSD
□ Slot7	186.06 GB	SAS SSD
□ Slot8	186.06 GB	SAS SSD
□ Slot9	838.11 GB	SAS HDD
□ Slot10	838.11 GB	SAS HDD
□ Slot11	838.11 GB	SAS HDD

Drive Slot: RAID
Slot 5

Spare type: ● Global Spare
○ Local Spare
○ Enclosure Spare

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.

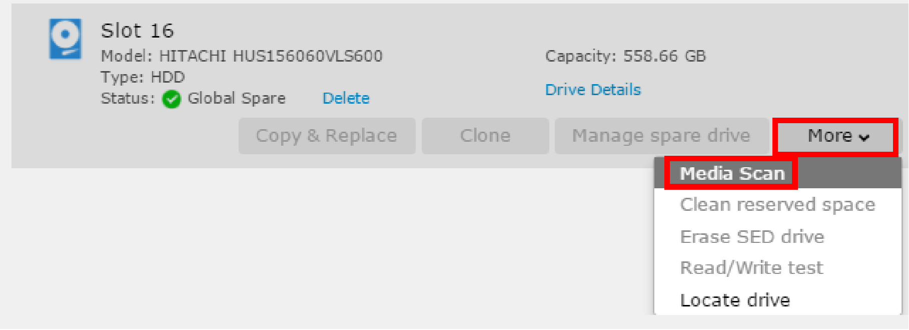
Scanning a Spare Drive

To scan a spare disk drive, it must be an enclosure spare drive or a global spare drive.

Go to

Settings / Device management >Storage > Drive

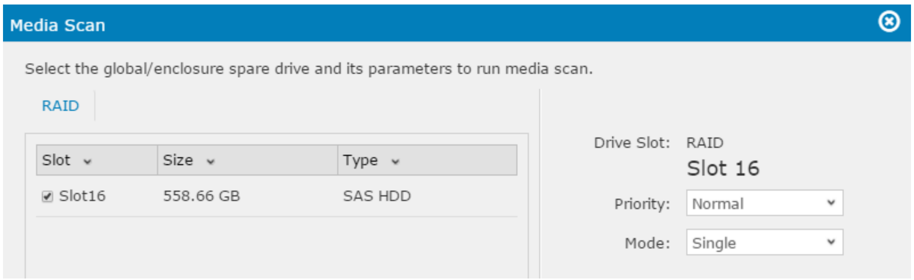
Select the drive and click **More** and select **Media Scan**.



Slot 16
Model: HITACHI HUS156060VLS600
Type: HDD
Status: Global Spare
Capacity: 558.66 GB

Steps

Click on the drive you wish to scan. Select **Priority** and **Mode** and click the **Scan** button to begin scanning.



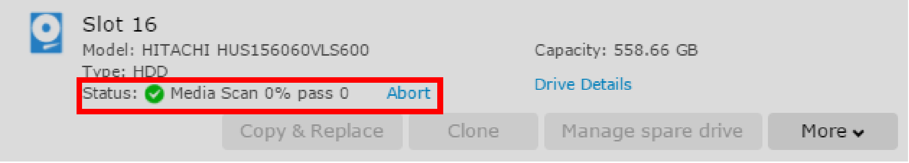
Media Scan

Select the global/enclosure spare drive and its parameters to run media scan.

Slot	Size	Type
☑ Slot16	558.66 GB	SAS HDD

Drive Slot: RAID
Slot 16
Priority: Normal
Mode: Single

The Scanning process can be seen in the drive status column. To stop the scan, click the **Abort** button to stop scanning.



Slot 16
Model: HITACHI HUS156060VLS600
Type: HDD
Status: Media Scan 0% pass 0
Capacity: 558.66 GB

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).

Sanitizing Drives

You can sanitize drives to erase their data permanently and completely.

Note: You cannot recover data sanitized from drives by any means.

Go to **Settings / Device management > Storage > Drives > Drives**

Steps

1. Go to the **Drives** list and select a desired drive.
2. Click **More** > **Sanitize drive**.
3. On the popup, choose one or more drives to sanitize.
4. Click **Sanitize** to erase data from the chosen drives.

   To terminate the sanitization process manually, click **Abort**. If you abort the process before it is complete, data erased before the process abort remain forever lost.

Running Read/Write Test

You can run a read/write test on hard drives to see if they contain bad disk blocks.

Note: You can only run a read/write test on new (unformatted) drives.

Go to **Settings / Device management > Storage > Drives > Drives**

Steps

1. Choose a desired drive in the **Drives** list.
2. Click **More** > **Read/Write test**.
3. Specify the test settings:

Test mode	Choose which test to run on the drives: **Read only** or **Read/Write**.
Error action	Choose what to do when an error occurs during the test: **No action**, **Abort on any error**, or **Abort on hard error only**.
Recovery process	Choose what to do to resume the test after an error occurs: **No recovery**, **Marking bad block**, **Auto reassignment**, **Attempting to reassign first**.
Drives	Choose one or more drives to run the test on.

4. Click **Test** to run the test.

   To abort the test, return to the **Drives** list and click on the cross icon on the drive entry.

Removing a Drive Reserved Space

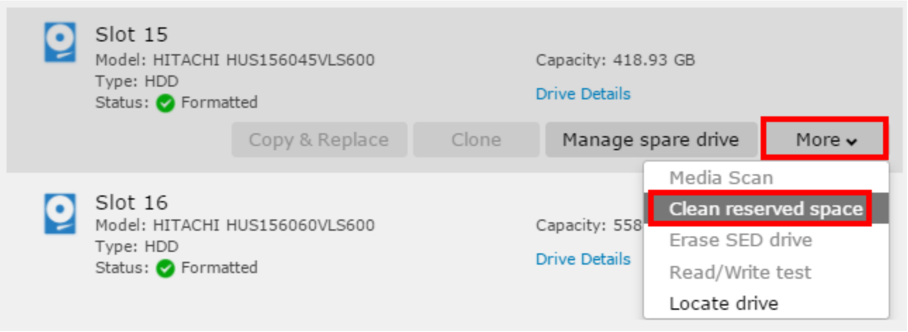
A formatted drive includes a reserved section (256MB block) to be used for event logs, configuration settings and storage virtualization so these contents will not be erased upon system reset. You may remove the reserved section (unformatting a drive) to bring the drive status to “new.” This operation 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 / Device management > Storage > Drives

Select the drive, click the **More** button and select the **Clean reserved space** option.

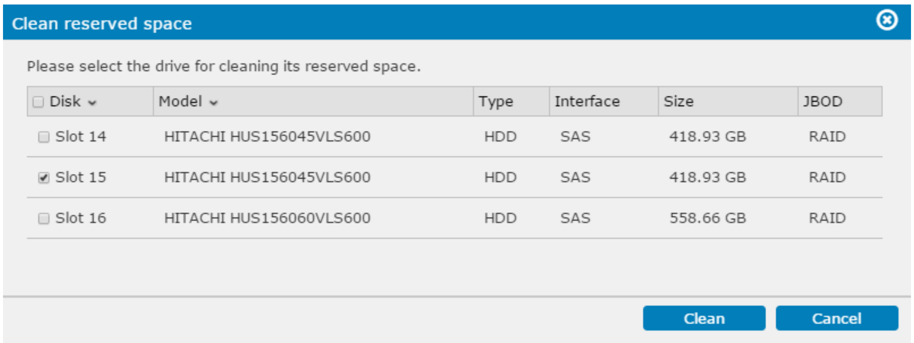


Slot 15
Model: HITACHI HUS156045VLS600
Type: HDD
Status: ✓ Formatted
Capacity: 418.93 GB
Drive Details

Slot 16
Model: HITACHI HUS156060VLS600
Type: HDD
Status: ✓ Formatted
Capacity: 558
Drive Details

Steps

Select the drives to be unformatted, and click **Clean**.



Clean reserved space

Please select the drive for cleaning its reserved space.

□ Disk ⌄	Model ⌄	Type	Interface	Size	JBOD
□ Slot 14	HITACHI HUS156045VLS600	HDD	SAS	418.93 GB	RAID
☑ Slot 15	HITACHI HUS156045VLS600	HDD	SAS	418.93 GB	RAID
□ Slot 16	HITACHI HUS156060VLS600	HDD	SAS	558.66 GB	RAID

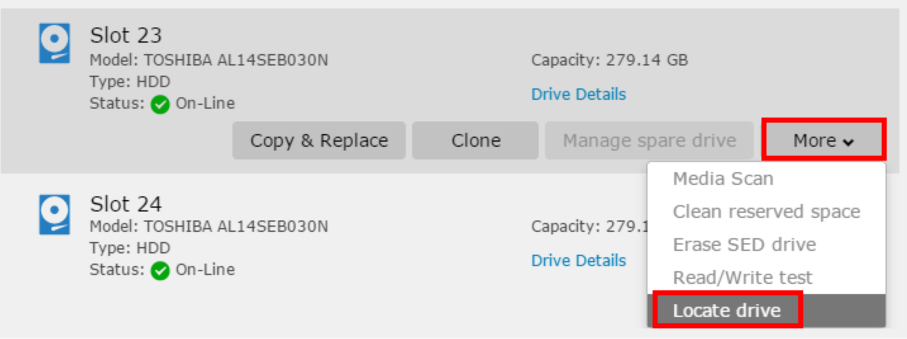
Identifying a Drive

You may flash the LED on the drive trays to identify the drive hardware-wise on a storage subsystem enclosure.

Go to

Settings / Device management > Storage > Drives

Select the drive, click the **More** button and select the **Locate drive** option.

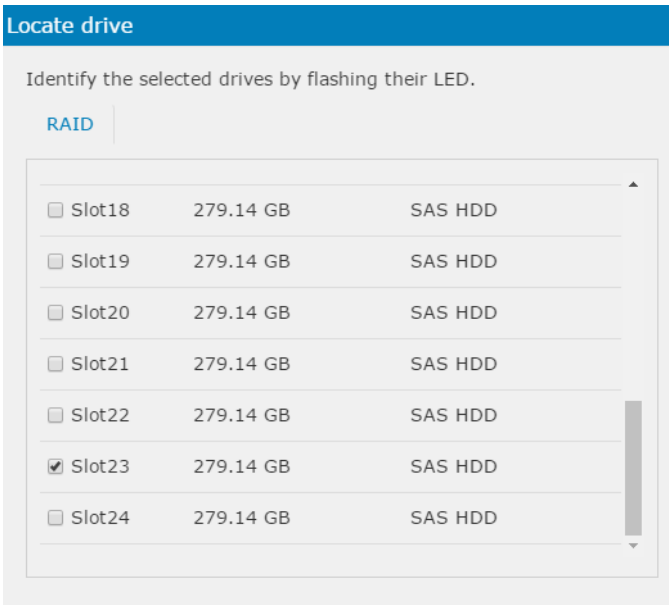


Slot 23
Model: TOSHIBA AL14SEB030N
Type: HDD
Status: ✓ On-Line
Capacity: 279.14 GB

Slot 24
Model: TOSHIBA AL14SEB030N
Type: HDD
Status: ✓ On-Line
Capacity: 279.1

Steps

1. Select the drive you would like to identify.



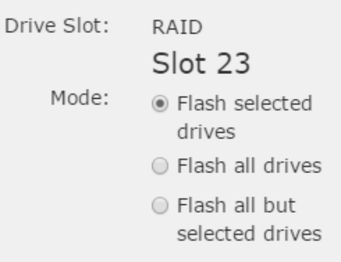
Locate drive

Identify the selected drives by flashing their LED.

RAID

□ Slot18	279.14 GB	SAS HDD
□ Slot19	279.14 GB	SAS HDD
□ Slot20	279.14 GB	SAS HDD
□ Slot21	279.14 GB	SAS HDD
□ Slot22	279.14 GB	SAS HDD
☑ Slot23	279.14 GB	SAS HDD
□ Slot24	279.14 GB	SAS HDD

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

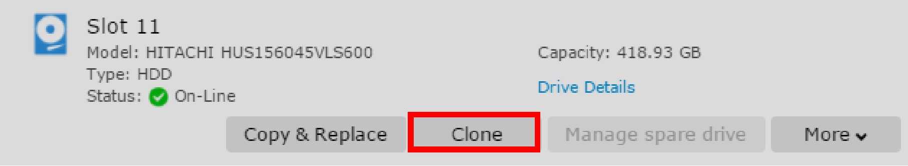
Prerequisites

- 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 / Device management > Storage > Drives

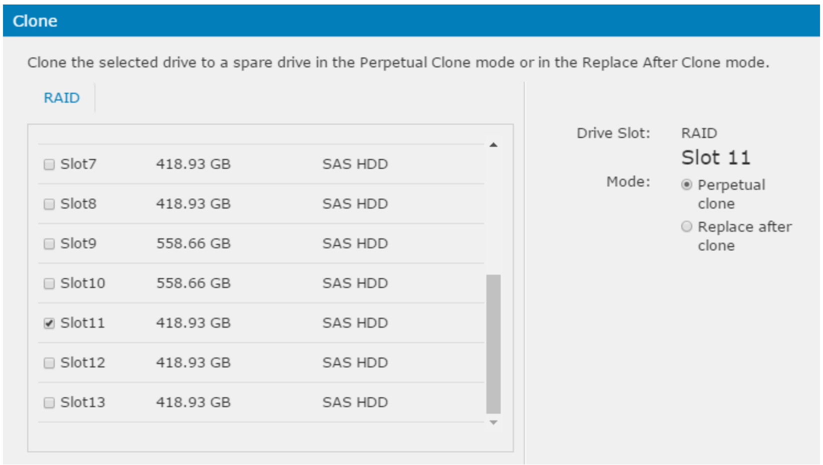
Select the drive and click the **Clone** button.



Slot 11
Model: HITACHI HUS156045VLS600
Type: HDD
Status: ✓ On-Line
Capacity: 418.93 GB

Steps

1. Select the drive to be cloned (Slot 11 in this example). The “source” drive must be a member of a logical drive.



Clone

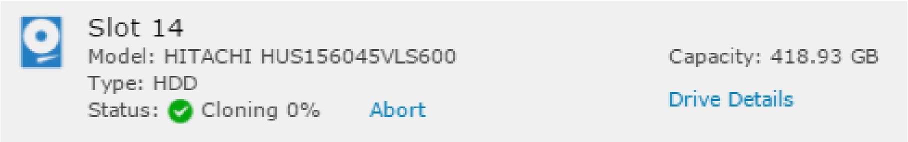
Clone the selected drive to a spare drive in the Perpetual Clone mode or in the Replace After Clone mode.

RAID

□ Slot7	418.93 GB	SAS HDD
□ Slot8	418.93 GB	SAS HDD
□ Slot9	558.66 GB	SAS HDD
□ Slot10	558.66 GB	SAS HDD
☑ Slot11	418.93 GB	SAS HDD
□ Slot12	418.93 GB	SAS HDD
□ Slot13	418.93 GB	SAS HDD

Drive Slot: RAID
Slot 11
Mode: ● Perpetual clone
○ Replace after clone

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.

	 Slot 14 Model: HITACHI HUS156045VLS600 Type: HDD Status: ✓ Cloning 0% Abort Capacity: 418.93 GB Drive Details	
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.”

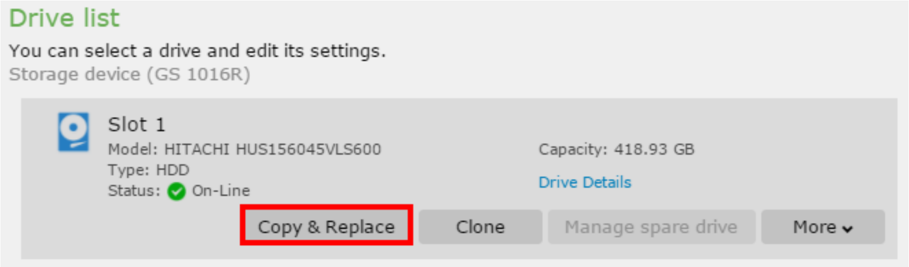
Copying & Replacing a Drive

- 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 / Device management > Storage > Drives

Select the drive and click the **Copy & Replace** button.



Drive list

You can select a drive and edit its settings.

Storage device (GS 1016R)

Slot 1

Model: HITACHI HUS156045VLS600

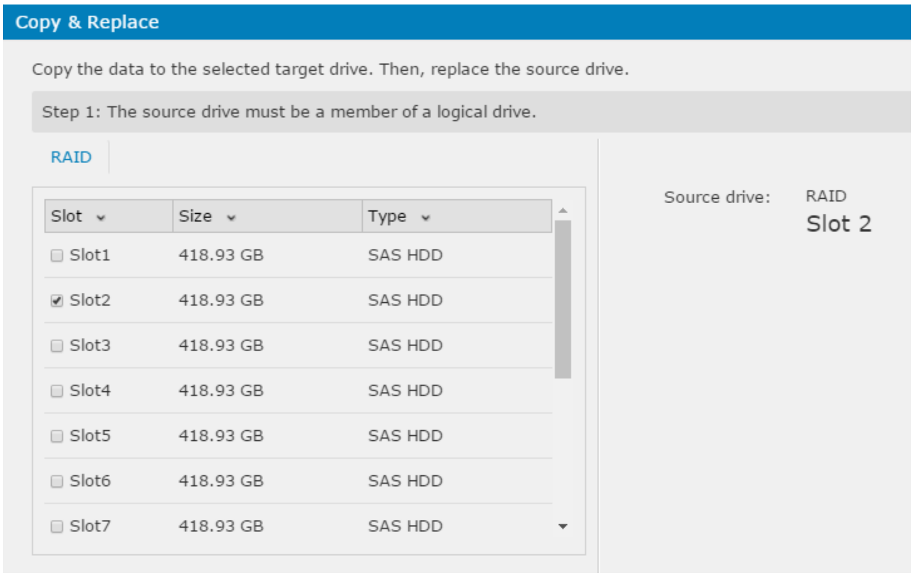
Type: HDD

Status: ✓ On-Line

Capacity: 418.93 GB

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.



Copy & Replace

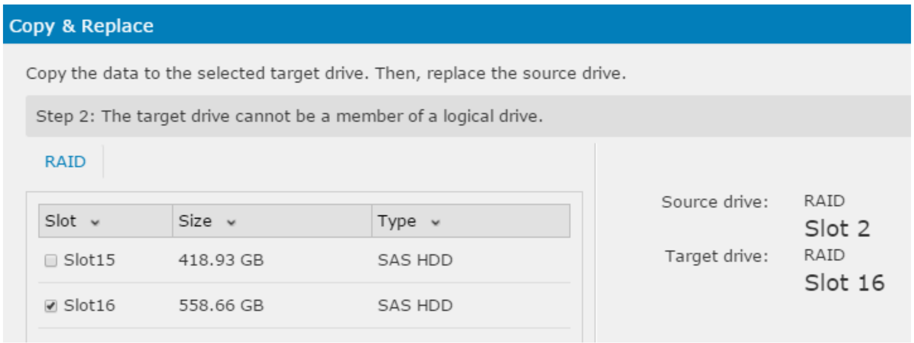
Copy the data to the selected target drive. Then, replace the source drive.

Step 1: The source drive must be a member of a logical drive.

Slot	Size	Type
□ Slot1	418.93 GB	SAS HDD
☑ Slot2	418.93 GB	SAS HDD
□ Slot3	418.93 GB	SAS HDD
□ Slot4	418.93 GB	SAS HDD
□ Slot5	418.93 GB	SAS HDD
□ Slot6	418.93 GB	SAS HDD
□ Slot7	418.93 GB	SAS HDD

Source drive: RAID Slot 2

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.



Copy & Replace

Copy the data to the selected target drive. Then, replace the source drive.

Step 2: The target drive cannot be a member of a logical drive.

RAID

Slot	Size	Type
□ Slot15	418.93 GB	SAS HDD
☑ Slot16	558.66 GB	SAS HDD

Source drive: RAID Slot 2

Target drive: RAID Slot 16

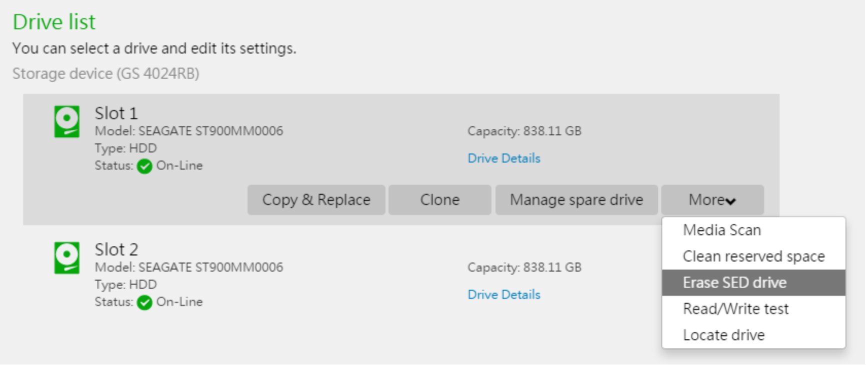
3. Click **OK**. The content of the source drive will be copied to the target drive, and the target drive will take the place of the source drive. The copying process cannot be seen in the spare target drive status column.

   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.



Drive list

You can select a drive and edit its settings.

Storage device (GS 4024RB)

Slot 1
Model: SEAGATE ST900MM0006
Type: HDD
Status: ✓ On-Line
Capacity: 838.11 GB
Drive Details

Slot 2
Model: SEAGATE ST900MM0006
Type: HDD
Status: ✓ On-Line
Capacity: 838.11 GB
Drive Details

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.

Creating a Disk Scan Schedule

Go to **Settings > Storage > Drives**

Steps

1. Click **Create media scan schedule**.
2. Select the drives that need to be scanned.

- **Destination Type:**
  - **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.
  - **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**.

3. The schedule parameters will appear.

- **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.

  Click **Next.**

4. The summary of the scheduled task will appear. Click **OK** to finish the settings.

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 system supports to create SSD cache automatically, and this feature is applied to H series models. For the other model types, you can create the cache and configure it when needed. To check your model type, refer to the model displayed in System Information.
- 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.
- "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.
- Maximum SSD cache capacity for general models is presented below:

DRAM Size	Max SSD cache pool capacity
8 GB	400 GB
16 GB	600 GB
32 GB	1000 GB
64 GB	1600 GB
128GB or more	3200 GB

- Maximum SSD cache capacity for GS3000/4000 Gen2 models is presented below:

DRAM Size	Max SSD cache pool capacity

8 GB	500 GB
16 GB	1000 GB
32 GB	2000 GB
64 GB or more	4000 GB

Creating File Cache Space

You can accelerate file read and write speeds by creating an SSD cache space to cache file data.

Note: For models with dedicated U.2 NVMe SSDs, the system creates SSD cache automatically. For more details about automatically-created cache, refer to View the Information about Automatically-Created Cache.

Go to	**Settings / Device management > Storage > SSD cache > File cache**

Steps

1. Enable a controller to create file cache space on it.
2. Choose one or more SSDs to create file cache space.
3. Specify the file cache space settings:

Type	Choose the type of data to cache into the file cache space: **Read**: The system caches read data. **Write**: The system caches write data. A write cache supports to configure its flush policy.
Select RAID level	Choose **RAID 1** or **RAID 5** for the file cache space.

4. Specify how much of the SSD cache space to reserve for SSD over-provisioning.
5. Choose what type of data to cache into the file cache space:

Metadata only	The system only caches file metadata to the cache space. This option helps minimize cache space usage as file metadata is small in size, and is suitable for search and file browsing.
Files and metadata	The system caches both files and their metadata to the cache space. Specify **Maximum block size** and **Minimum block size** to set a range of file block size. Only file blocks that fall in this range are cached. This option is suitable for general write operations (e.g., modifying file content) on small files.

6. For a write cache, you can edit its flush policy to choose when to flush the data:

Automatic	The system flushes data automatically. This option allows the system to flush the data in the background and adjust the amount of flushed data depending on the system workloads. This may take a longer time to flush data completely but can minimize the impact on access performance.
By schedule	The system flushes data according to the schedule you set. Choose the activate frequency as **Daily**, **Weekly**, or **Monthly**. When you choose daily, choose the start time and end time to specify the period of time. When you choose weekly or monthly, choose one or more days and specify the period of time to flush the data. This option allows the system to flush the data at high priority during the specified period of time. It is recommended that you set the schedule for non-peak hours to minimize the impact on access performance.

7. Click **OK** to save the settings. To create file cache space on the other controller, repeat the above steps.

8. You can manage the SSD space for file caching as follows:

   To free up SSD space: Turn off the function. The system saves cached data on the SSDs to the HDDs in the system.

   You can learn about dirty cache usage by clicking **Details** next to the cache size. To change the flush policy, click **Edit**.

Creating Block Cache Space

You can accelerate read access to block data by creating a dedicated SSD cache space.

Note: For models with dedicated U.2 NVMe SSDs, the system creates SSD cache automatically. For more details about automatically-created cache, refer to View the Information about Automatically-Created Cache.

Go to	**Settings / Device management > Storage > SSD cache > Block cache**

Steps

1. Enable this function.
2. Choose one or more SSDs to create an SSD cache space for block data. Then, click **OK**.
3. You can change the size of the SSD cache space in following ways:

   To expand the cache space, click **Add disk** and choose desired one or more SSDs to join the cache space.

   To free up SSD space, click on an unwanted SSD and then click **Remove**. The system saves cached data on the removed SSD to the HDDs in the system.

Viewing the Information about Automatically-Created Cache

Important: This feature applies on specific SAS HDD models with pre-configured U.2 NVMe SSDs.

With these pre-configured SSDs, the system can automatically create SSD cache for accelerating read/write access to data. You can view the information about the cache size, type, status, etc.

Note:

- Make sure you have installed the valid license of file cache and/or block cache. For more details about installing a license, refer to License Management.
- For the other models, you can create SSD cache when needed. For more details about creating SSD cache yourself, refer to Create File Cache Space or Create Block Cache Space.

Go to	**Settings / Device management > Storage > SSD cache**
SSD Cache	View the cache status, cache size, hit rate, etc. You can click **Details** to learn more information. For dual-controller models, you can view the information about the cache space on each controller.
Drives	View information about the SSDs. You can click **Details** in the drive list to locate the SSD and more details.

Storage Maintenance

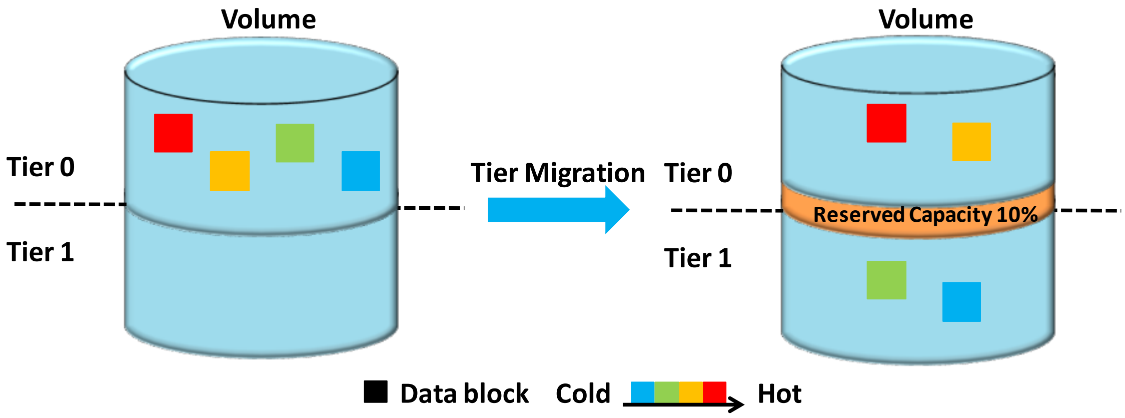
In this page, the system lists the invalid LUN and isolated logical drive when there are errors in the volumes (LUNs) or logical drives.

Go to	**Settings / Device management** > **Storage** > **Storage maintenance**
Invalid LUN	When users remove the drives which belongs to a mapped LUN from the storage system, EonStor GS/GSe will list the “invalid” LUN in the page to inform you that the LUN cannot retrieve its data from the current disks. 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.
Isolated Logical Drive	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.

Storage Tiering

Different types of data in a storage system experience different lifecycles. Data is usually accessed more frequently at creation and the access frequency decreases as it ages. Businesses are growingly looking to manage their data more efficiently by utilizing different types of storage media for different types of data. To cope with the issue, use Automated Storage Tiering that automatically leverages the high throughput and low latency feature of SSDs to deliver faster performance for frequently accessed data, while making better use of lower speed drives as data archiving media, thereby boosting system performance and reducing the cost of ownership.

The system scans the hotness of each data block. After scanning the hotness, the system starts to perform data migration during a specified schedule. To ensure there is sufficient space for new incoming hot data from the host, the system reserves 10% free space in higher tier storage and flushes relatively cold data to lower tier storage when tier migration is executed.



The storage system may have four tier levels to choose from: tier 0-4. The smaller the value is, the higher the performance that the tier delivers. Here are the recommended tier levels for RAID and drive types.

- Tier 0: SSD
- Tier 1: SAS
- Tier 2: Near-line SAS
- Tier 3: SATA

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.

For more details about storage tiering, see the application note *Automated Storage Tiering*.

The storage tiering setup includes:

1. Setting up Tiers in a Pool

2. Creating a Volume in a Tiered Pool

3. Creating a Tiered Data Migration Schedule

For the details about the setup procedures, see these sections above.

Note:

- Before using this feature, make sure you have installed a valid license.
- For a thin-provisioned volume, coming I/Os always go to the SSD tier first. Data will be migrated to the HDD tier later depending on its hotness. While for a full-provisioned volume, coming I/Os do not always go to the SSD tier first and may go to SSD/HDD tier according to the capacity ratio. That is, before migration to the SSD tier, there may not be improved access performance for hot data.

Setting up Tiers in a Pool

You can create tiered storage in a pool by setting up tiers.

Go to	**Settings / Device management > Storage > Storage Tiering**
Prerequisites	Add a pool, and the pool must contain at least two logical drives. For more details about adding a pool, see Adding a Pool.
Steps	1. Select a pool. 2. Click **Edit**. 3. Click the dropdown menu, and select the number. The smaller the number is, the higher the performance that the tier delivers. That is, 0 indicates that the tier delivers the highest performance. 4. Click **OK**. After setting up the tiers, create a volume in this tiered pool. For more details, see Creating a Volume in a Tiered Pool.

Creating a Tiered Data Migration Schedule

To migrate data between the tiers, create a schedule for each pool.

Go to	**Settings / Device management > Storage > Storage Tiering**

Steps

1. Click **Create tier migration schedule**.
2. Select a pool.
3. Specify an identifying name for this task.
4. Specify the following schedule information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an activate frequency less than one day: Choose **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**. ● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**. To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the current time that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a termination date and time** and specify the time.

5. Select the priority for this schedule.
6. Click **OK** to create the schedule.

VMware Volume

On the storage device, you can create storage containers to host virtual volumes and manage/check storage access settings registered on your vSphere server.

Note: Make sure you have connected the storage device with desired vCenters, ESXi hosts, and VASA Provider.

Create a Storage Container

A storage container is a virtual datastore created on your storage device, and it hosts virtual storage (i.e. virtual pools and volumes) to be used by virtual machines in the vCenter.

Note: Before creating a storage container, make sure you have created available capability profiles at **Settings** > **Storage** > **VMware volume** > **Capability profile**.

Go to **Settings / Device management** > **Storage** > **VMware volume** > **Storage container**

Steps

1. Click **Add a storage container**.
2. On the pop-up, go to **General** and provide needed information:

Name	Specify a name for the storage container. You can provide up to 42 UTF-8 characters.
Volume type	Select the type of volumes on your storage for creating virtual volumes.

3. Click **Add a capability profile**. Choose a created capability profile and set a storage capacity limit.

   As a storage container can host several virtual pools, you can add multiple capability profiles to it.
4. Click **OK** to apply the capability profile to the storage container.
5. Then, go to **ESXi host** and select desired ESXi hosts that can access the storage container:

Host domain	It shows the ESXi host's hostname followed by the domain name.
IP	It shows the ESXi host's IP address.
Version	It shows the ESXi version.
Protocol	It shows the protocol endpoints for communication between the storage container and the ESXi host.

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

Create a Capability Profile

A capability profile defines the attributes of a single virtual pool inside a storage container. As a storage container typically hosts several virtual pools, you can associate a storage container with multiple capability profiles.

Go to	**Settings / Device management** > **Storage** > **VMware volume** > **Capability profile**

Steps

1. Click **Add a capability profile**.
2. On the pop-up, create a capability profile by providing and checking information:

Name	Specify the name for the capability profile.
Associated pool	Select a pool on your storage device to be associated with the capability profile.
Service level	Check the service level calculated based on the pool's configurations.
Storage tiering	Check whether storage tiering is enabled for the pool.
Drive type & RAID level	Check the pool's drive type and RAID level.
SSD cache	Check whether SSD cache is enabled for the pool.
Tag	Check the tag attached to the capability profile. To add a tag, click **Add a tag** and provide identifying information.

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

View a Protocol Endpoint

A protocol endpoint is a communication protocol that an ESXi host uses to access a storage container.

Go to

Settings / Device management > **Storage** > **VMware volume** > **Protocol endpoint**

Steps

1. Check the protocol endpoint information pulled from your vSphere server.
2. To know more information, select a protocol endpoint and click **View details**:

Connection status	Check whether the storage container is connected with the ESXi host.
Type	Check the communication protocol between the ESXi host and the storage container.
Controller	Check which controller contains the storage container.
WWN/IQN	Check the WWN or IQN if the protocol endpoint is Fibre Channel or iSCSI/NFS.
VMware UUID	Check the VMware UUID assigned to a virtual machine running on the ESXi host.
ESXi IP	Check the IP address of the ESXi host.
Virtual volume	Check the total number of virtual volumes accessed by the ESXi host through the protocol.

View a Virtual Volume

A virtual volume is created on your storage device to store data of a virtual machine.

Go to	**Settings / Device management** > **Storage** > **VMware volume** > **Virtual volume**
Steps	1. Check the virtual volumes created on the storage device by the vSphere server. 2. Check information of each virtual volume:

Name	Check the virtual volume's name.
Type	Check the virtual volume's type.
Virtual machine	Check the name of the virtual machine accessing the virtual volume.
Storage container	Check the storage container hosting the virtual volume.
Size	Check the virtual volume's size.

Folder explorer

This functionality is available only when you have enabled scale-out cluster on EonStor GS appliances. You can view the whole cluster file system here. The system monitors whether the folder resides on a volume that meets the specified attributes.

If the volume is running out of space or it does not meet the folder’s attributes due to later changes, the system alerts you to migrate it to a suitable volume to ensure unaffected data access.

Edting a Folder

In the tree view, you can click the folder icon to view the details of the folder. Click **More** to view more details.

Note: To avoid inconsistent attribute settings between related folders, you cannot set attributes for a folder when its child or parent folder already has environment attributes set.

Go to	**Cluster settings > Storage > Folder explorer**

Steps

1. Click on the triangle next to the root shared folder to display folders inside. You can click on the two-arrow icon to expand the folder view.
2. Click on a desired folder and click **Edit**.
3. Go to the **Edit folder** section:

Auto-migration	Enable this option so that the system will suggest a migration task for this folder if the current volume does not match the folder's attributes or when the appliance exceeds its pre-set storage threshold. When enabling this function, it is also recommended that you enable **Auto-Balancing** and set the threshold for the volume. You will be able to learn and manage suggested migration tasks at **Migration**.
Folder attributes	You can simply set the folder attributes as: **default**, **performance**, or **capacity**. Or customize attributes. The levels of the following attributes will be displayed when they are available: **Performance**: Choose the level of performance that the folder’s volume should offer: **High**, **Medium**, or **Low**. **Protection**: Choose the level of data protection that the folder’s volume should offer: **RAID1**, **RAID5**, or **RAID6**. **Drive type**: Choose the type of hard drives that the folder’s volume should use: **HDD** or **SSD**. **Deduplication**: Enable this option to deduplicate data and reduce volume usage. **Compression**: Enable this option to compress

	data.

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

   If the folder attributes don’t match to the current volume’s attributes, click **Next** and migrate the folder to another volume which attributes are corresponded.

   Select a volume from the list. Only those volumes that meet the folder’s attributes will be listed for you to choose.

5. Set a time to run the migration task:

Start now	Select this option to run the migration task immediately.
By schedule	Select this option to set a schedule for the migration task. Then, set a start time.

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

Migrating a Folder to the Cluster File System or to another Volume

You can migrate a folder on one of the appliances into the cluster file system, or to any other volume that meets its attributes.

Go to **Cluster settings > Storage > Folder explorer**

Steps

1. Click on the triangle next to the root shared folder to display folders inside. You can click on the two-arrow icon to expand the folder view.
2. Click on the desired shared folder and click **Migrate**.
3. Choose to **Migrate to cluster folder** or **Migrate to another volume**. Only those volumes that meet the folder’s attributes will be listed for you to choose.
4. Set a time to run the migration task:

Start now	Select this option to run the migration task immediately.
By schedule	Select this option to set a schedule for the migration task. Then, set a start time.

5. Click **OK** to save the settings.
6. If needed, click **Refresh** to reload the changes.

Migrating a Cluster Folder to another Volume

Go to **Cluster settings > Storage > Folder explorer**

Steps

1. Click on the triangle next to the root shared folder to display folders inside. You can click on the two-arrow icon to expand the folder view.
2. Click on the desired shared folder and click **Migrate**.
3. Choose a destination volume in the **Select volume** section.
4. Set a time to run the migration task:

Start now

Select this option to run the migration task immediately.

If you wish to make the migration task run within a specific period of time, select **Set end time** and specify an end time for the task. The task will be aborted when it reaches the end time.

By schedule

Select this option to set a schedule for the migration task. Then, set a start time.

If you wish to make the migration task run within a specific period of time, select **Set end time** and specify an end time for the task. The task will be aborted when it reaches the end time.

5. Click **OK** to save the settings. The migration task is then added to **Migration** task list.
6. If needed, click **Refresh** to reload the changes.

Importing an Existing Shared Folder to the Cluster

Note: Before importing a shared folder into the cluster, clear the file service protocol settings of the folder.

Go to **Cluster settings > Storage > Folder explorer**

Steps

1. Click on the triangle next to the root shared folder to display folders inside. You can click on the two-arrow icon to expand the folder view.
2. Select a desired folder as the destination, and click **Import**.
3. Select a desired folder to import.
4. Click **OK** to save the settings.
5. If needed, click **Refresh** to reload the changes.

Cluster Folders

After creating cluster folders and setting their environment attributes, you can manage cluster folders' attributes, quota, and access permission.

Editing a Cluster Folder

Go to	**Cluster settings > Storage > Cluster folder**

Editing a cluster folder

1. Select the desired cluster folder.
2. Click Edit. Go to the **Edit folder** section:

Cluster folder name	If needed, modify the cluster folder name. However, renaming the root shared folder is not supported.
Folder attributes	You can set the folder attributes as: **default**, **performance**, or **capacity**. Or customize attributes. The levels of the following attributes will be displayed when they are available: **Performance**: Choose the level of performance that the folder's volume should offer: **High**, **Medium**, or **Low**. **Protection**: Choose the level of data protection that the folder's volume should offer: **RAID1**, **RAID5**, or **RAID6**. **Drive type**: Choose the type of hard drives that the folder's volume should use: **HDD** or **SSD**. **Deduplication**: Enable this option to deduplicate data and reduce volume usage. **Compression**: Enable this option to compress data.
Quota	This option is displayed if the folder is a shared folder. You can set the capacity limit for the folder. By default, the quota size is **Not limited** (i.e. until the whole volume space is used up.) 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.
Permission	This option is displayed if the folder is a shared

	folder. You can set access permission for the shared folder. Choose an access permission by user and by group: **Read/Write**, **Read only**, or **No access**.

7. **NFS permissions** option is displayed if the folder is a shared folder. You can set NFS permission by clicking **Add**:

IP/Hostname	Specify the client computer's IP address or hostname.
Access rights	Set the client computer's access permission: **Read only** or **Read/Write**.
Squash	Set access permission for remote users via the client computer. **All Squash**: All remote users are treated as anonymous users and have limited permission. **Root Squash**: A remote user with the root credentials is treated as an anonymous user and has limited permission. **No Root Squash**: A remote user with the root credentials is treated as a root user and has full permission.
Anonymous GID	Click **Configure** to set a group identifier to anonymous groups. Choose **Local groups** or **Domain groups** from the top-left menu, and choose a permission type from below. The permission type is applied to the chosen anonymous groups.
Anonymous UID	Click **Configure** to set a user identifier to anonymous users. Choose **Local users** or **Domain users** from the top-left menu, and choose a permission type from below. The permission type is applied to the chosen anonymous users.

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

Deleting a Cluster Folder

Go to	**Cluster settings > Storage > Cluster folders**
Steps	1. Select a cluster folder in the list. 2. Click **Delete**. 3. Confirm the action to delete the cluster folder and the data inside permanently.

Migration

You can migrate a folder into the cluster file system. You can also migrate a cluster folder or a cluster volume to a suitable location in the cluster to balance the storage and meet performance requirements.

Managing Folder Migration Tasks

Go to **Cluster settings > Storage > Migration**

Steps

1. Click **Folder migration** on the top.
2. If needed, click the filter to view tasks according to their status. You can click the two-arrow icon to expand the list view.

Suggested	Those tasks that have been suggested via auto-migration function.
Migrating	Those tasks that have been executing.
Waiting	Those tasks that have been set by schedules but have not been started.
Scheduled	Those tasks that have been set by schedules and will be started when it is the start time.

3. Select a desired task and click on a corresponding button: **Edit**, **Delete**, or **Abort** the task:

Edit	Re-schedule when to migrate this folder, or change the destination.
Delete	Delete the task if you want to cancel it.
Abort	Abort the task if the task has not been completed.

Migrating a Volume in the Cluster

You can migrate a block-level volume from one appliance to another.

Note:

- To migrate a volume, there must be at least two appliances in the cluster. To add an appliance, refer to Adding an Appliance.
- Only the following volumes can be migrated:
  - The volume does not reside in a pool which storage tiering is enabled.
  - The volume is not a source volume nor a target volume in any replication pair.
  - The volume is not a cloud-connected volume.
  - The volume has no scheduled tasks nor snapshot images related to it.
  - The volume has no on-going operations, including expanding capacity or renaming.

Go to	**Cluster settings > Storage > Migration**
Steps	1. Click on **Volume migration** on the top. 2. Click **Add a migration task**. 3. Choose a cluster volume to migrate. Then, click **Next**. 4. Choose a destination pool to receive the cluster volume. 5. Click **OK** to run the migration task immediately. 6. Go to the host server and have it rescan and relink the migrated volume on the cluster. The migrated volume only functions properly when relinked because it can have uninterrupted I/O communication with the host server. 7. When the task is near completion, click **Relink** to link the migrated volume to a host server to start normal I/O communication.

Auto-balancing

Auto-balancing makes the stored data evenly distributed in the cluster.

Auto-balancing Data Across the Cluster

Go to **Cluster settings > Storage > Auto-balancing**

Steps

1. Turn on the auto-balancing function.
2. Go to the **Settings** section to define the auto-balancing behavior:

   Threshold

   Set a storage threshold to all appliances in the cluster.

   When an appliance reaches the threshold, the cluster runs auto-balancing to move its extra data to other cluster volumes.

   Period

   Set an interval to run auto-balancing regularly: **Every day**, **Every week**, or **Every month**.

3. Click **Save** to save the settings.
4. To run an immediate auto-balancing check, go to the **Immediate scan** section and click **Scan**.

   The cluster checks if all the cluster folders reside on a suitable cluster volume and if the amount of stored data is well balanced across all the appliances.

Data Protection

Data protection provides several approaches to protect your data on this storage system, including taking snapshots, creating replication pairs between folder/volumes, back up data and store the copies of data in file servers or cloud storage.

Protection

To provide another layer of protection to your data on this storage system, you can make a copy of data and store it locally and remotely. You can take a snapshot, create a replication pair to sync data within two folders/volumes, and store backup data in a file server or cloud storage.

Creating a Snapshot-taking Task

You can take a snapshot for a local volume/folder on a regular basis.

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.
- For block-level and file-level volumes with XFS file system type, you can take up to 64 snapshots per volume and 128 per system. To take a snapshot for a file-level volume with Btrfs file system type, you can purchase a “File snapshot” license.

Go to **Settings > Data protection > Protection**

Steps

1. For the approach that you want to use to protect your data, choose **Snapshot**.
2. For **Task name** and **Tag**, the system has specified identifying names. If needed, change the task name and tag, and specify a task description in the **Description** field.
3. Choose one or more volumes/folders to take snapshots for. Click **Browse**.

   When taking snapshot for volumes, you can back up the snapshots to cloud once they are created. Go to **Cloud-integrated options,** and select **Backup the selected cloud-integrated volume snapshot to the cloud storage device**.

   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.

   When finishing selection and setting, click **OK**.
4. Go to the **Schedule & retention policy** section. Specify the following information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an activate frequency less than one day: Choose **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**.

	● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**. To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the **current time** that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a termination date and time** and specify the time.
Prune rule	Choose a policy to manage snapshots when the maximum number of snapshots is reached: ● **Rotate snapshots when the maximum number of snapshots is reached**: 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. ● **Delete a snapshot when its retention period is reached**: Select this option to remove snapshots that have reached its retention period after creation. Then, specify a retention period for snapshots.

5. Click **Create** to create the task.

Creating a Folder Replication Task

By pairing two volumes to create a replication pair, you can sync data between these two volumes on a regular basis.

Go to **Settings > Data protection > Protection**

Steps

1. For the approach that you want to use to protect your data, choose **Replication**.
2. For **Task name**, the system has specified an identifying name. If needed, change the task name.
3. Choose an existing replication pair of volumes, or create a new pair. Click **Browse**.
4. Go to the Select a replication pair page, and do one of the following:
    - Choose an existing pair with the type as **Folder**. Click **OK**. Continue to Step 5.
    - Create a new pair. To create one, click **Add**. For the adding procedure, see Step 2 in Adding a Folder Replication Pair.
5. On the Select a replication pair page. Select the pair, and click **OK**.
6. Go to the Schedule section. Specify the following information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an activate frequency less than one day: Choose **5 minutes**, **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**. ● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**. To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the current time that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a**

termination date and time and specify the time.

7. Click **Create** to create the task.

Creating a Volume Replication Task

By pairing two volumes to create a replication pair, you can sync data between these two volumes on a regular basis.

Note:

- You can create a volume replication pair while creating a task, or create a pair via settings in Replication pairs.
- If you want to create replication pairs between two devices, you will need an advanced license for remote replication actions. Before you start the remote replication process, we recommend you test the bandwidth between the two devices to verify whether the devices are connected.

Go to **Settings > Data protection > Protection**

Steps

1. For the approach that you want to use to protect your data, choose **Replication**.
2. For **Task name**, the system has specified an identifying name. If needed, change the task name.
3. Choose an existing replication pair of volumes, or create a new pair. Click **Browse**.
4. Go to the Select a replication pair page, and do one of the following:
   - Choose an existing pair with the type as **Volume**. Click **OK**. Continue to Step 5.
   - Create a new pair. To create one, click **Add**. For the adding procedure, see Step 2 in Adding a Volume Replication Pair.
5. On the Select a replication pair page. Select the pair, and click **OK**.
6. Go to the Schedule section. Specify the following information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an activate frequency less than one day: Choose **5 minutes**, **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**. ● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**.

	To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the current time that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a termination date and time** and specify the time.

7. Click **Create** to create the task.

Backing up Data to a File Server

You can add a file server during the process of creating a task, or add it on Backup Targets page. For more details, see Adding a File Server as a Backup Target.

Go to	**Settings > Data protection > Protection**

Steps

1. For the approach that you want to use to protect your data, choose **Back up data to a file server**.
2. For **Task name**, the system has specified an identifying name. If needed, change the task name and/or specify **Description** for this task.
3. Go to the Data section. Click **Browse**. On the Select backup data page, select one or more folders. Click **OK**.
4. To select a file server, do one of the following:
   - Choose an added file server. Continue to Step 5.
   - If this is the first time that you try to back up data to a file server, add a file server for this storage system to connect it. Click **+** and go to the Add a file server page. Specify the following information, and click **OK**:

File server name	Specify an identifying name for the file server.
IP address	Specify the IP address or the domain name of the file server.
Protocol	Select **CIFS** or **NFS**. For CIFS, specify an account and the password.

5. To select a target folder to store the data, click **Browse**.
6. Go to the Schedule & retention policy section. Specify the following information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an activate frequency less than one day: Choose **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**. ● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**.

	To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the current time that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a termination date and time** and specify the time.
Retention policy	Choose to retain the data according to a specific time period or a specific number of copies, or never delete the data. ● **By period**: specify how long the data should be retained. ● **By number of copies**: specify the maximum number of copies of the data. ● **Never delete**

7. Click **Create** to create the task.

Backing up Data to Cloud Storage

By pairing two volumes to create a replication pair, you can sync data between these two volumes on a regular basis.

Go to	**Settings > Data protection > Protection**

Steps

1. For the approach that you want to use to protect your data, choose **Back up data to a cloud**.
2. For **Task name**, the system has specified an identifying name. If needed, change the task name and/or specify **Description** for this task.
3. Go to the Data section. Click **Browse**. On the Select backup data page, select one or more folders. Click **OK**.
4. To select a cloud location, do one of the following:
   - Choose an added cloud location. Continue to Step 5.
   - If this is the first time that you try to back up data to cloud storage, add cloud storage for this storage system to connect it. Click **+** and go to the Add a location page. Specify the following information, and click **OK**:

Location name	Specify an identifying name for the cloud location.
Account	● Select an account name. The account information is used to access the cloud location. ● If this is the first time that you add cloud storage, add an account, too. Click **+** and go to the Add an account page. ■ Specify an identifying name for this account. ■ Select the cloud provider: **Aliyun**, **Amazon S3**, **Microsoft Azure**, or **Wasabi cloud**. ■ According to the cloud provider that you select, specify the corresponding access key / endpoint and key / secret key / share key. ■ Click **OK** to complete the settings.
Connect	Click **Connect** for this storage system to connect to the cloud storage.
Bucket	After clicking **Connect**, all available buckets are displayed here. Select a bucket.

5. To select a target folder to store the data, click **Browse**.

6. Go to the Schedule & retention policy section. Specify the following information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an activate frequency less than one day: Choose **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**. ● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**. To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the current time that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a termination date and time** and specify the time.
Retention policy	Choose to retain the data according to a specific time period or a specific number of copies, or never delete the data. ● **By period**: specify how long the data should be retained. ● **By number of copies**: specify the maximum number of copies of the data. ● **Never delete**

7. Click **Create** to create the task.

Restore

You can restore the backup data that stores in a file server and cloud storage to this storage system.

Note: Before restoring data, back up data to a file server and/or cloud storage first. For more details, see Backing up Data to a File Server and Backing up Data to Cloud Storage.

Restoring Backup Data from a File Server

Go to **Settings > Data protection > Restore**

Steps

1. Select the backup target as **File server**.
2. Select the file server that stores the data you want to restore.
3. Select the backup task name and the activate time of the backup operation. For a scheduled task, the backup operation can be activated at more than one time.
4. For the destination, choose to restore your data to the **Original** location, or choose **Customize** to specify a location that is different from the original one.

   When restoring data to the original location, the data in it will be overwritten.

   When selecting **Customize**, click **Browse** to select the folder in which you want to restore the backup data. If needed, click **Refresh** to get the latest status about all the available folders. Click **OK** to save the setting.
5. Click **Restore** to create the task.

Restoring Backup Data from Cloud Storage

Go to **Settings > Data protection > Restore**

Steps

1. Select the backup target as **Cloud**.
2. Select the cloud location that stores the data you want to restore.
3. Select the backup task name and the activate time of the backup operation. For a scheduled task, the backup operation can be activated at more than one time.
4. For the destination, choose to restore your data to the **Original** location, or choose **Customize** to specify a location that is different from the original one.

   When restoring data to the original location, the data in it will be overwritten.

   When selecting **Customize**, click **Browse** to select the folder in which you want to restore the backup data. If needed, click **Refresh** to get the latest status about all the available folders. Click **OK** to save the setting.
5. Click **Restore** to create the task.

Monitoring

Gain an overview of the number of snapshots and the status of each backup/restore task.

Editing/Deleting a Snapshot

Go to **Settings > Data protection > Monitoring**

Edit a snapshot

You can change the name and description of a snapshot.

1. Go to the Snapshot section. Click the link of the snapshot name.
2. A list of the snapshots that share the name and has taken at different moments are displayed. Select the snapshot that you want to edit.
3. Click **Edit**.
4. Change the **Tag** and **Description** of the snapshot.
5. Click **OK** to save the settings.

Delete a snapshot

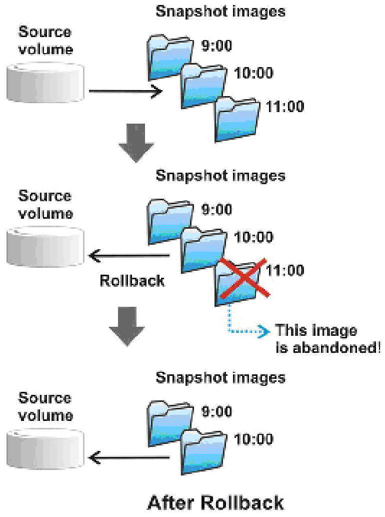
1. Go to the Snapshot section. Click the link of the snapshot name.
2. A list of the snapshots that share the name and has taken at different moments are displayed. Select the snapshot that you want to delete.
3. Click **Delete**.
4. To confirm your action, click **OK**. The snapshot will be deleted immediately.

Rolling Data Back to a Specific Moment

You can restore data to a specific moment by rolling back.

Note:

- If the volume of the snapshot has been mapped/mounted, you must unmap/unmount the volume before rolling back a snapshot.
- After rolling back, you can re-establish host LUN mappings for the volume.
- If a volume is rolled back based on a snapshot, the snapshots that have taken after the 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.



Go to **Settings > Data protection > Monitoring**

Steps

1. Go to the Snapshot section. Click the link of the snapshot name.
2. A list of the snapshots that share the name and has taken at different moments are displayed. Select the snapshot that contains the state you want to roll back to.
3. Click **More** and select **Roll back** option.
4. Depending on the size of the volume, the process of rolling back may take a few minutes.
5. When it is completed, click **OK**.

Mapping a Snapshot to a Host

Note:

- After mapping a snapshot in the EonOne, you need to assign a drive letter to it in the host computer environment.
- A snapshot taken in a file-level volume will not be able to be mapped to a host.

Go to **Settings > Data protection > Monitoring**

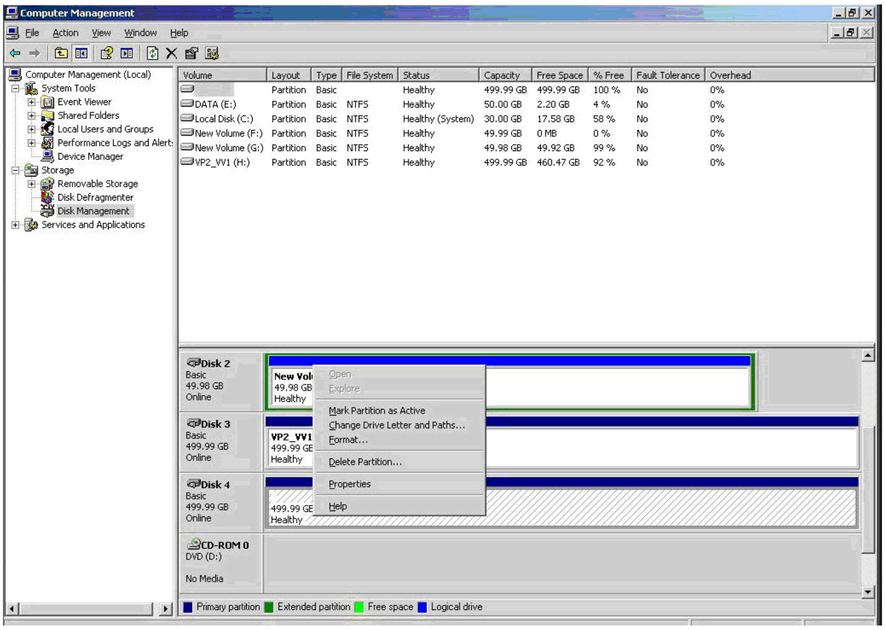
Map to a host

1. Go to the Snapshot section. Click the link of the snapshot name.
2. A list of the snapshots that share the name and has taken at different moments are displayed. Select the snapshot that you want to map.
3. Go to the Host LUN mapping page. For the setting procedure, see Mapping a Volume to a LUN.

Assign a drive letter to the snapshot

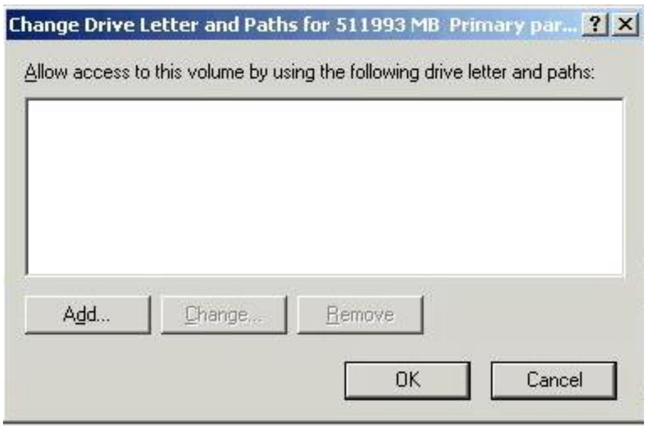
Before accessing data in the snapshot, you need to assign a drive letter to it. Here are the procedures for a Windows Server environment.

1. When an image is mapped, it will appear as a new drive to the computer.



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
	Partition	Basic		Healthy	499.99 GB	499.99 GB	100 %	No	0%
DATA (E:)	Partition	Basic	NTFS	Healthy	50.00 GB	2.20 GB	4 %	No	0%
Local Disk (C:)	Partition	Basic	NTFS	Healthy (System)	30.00 GB	17.58 GB	58 %	No	0%
New Volume (F:)	Partition	Basic	NTFS	Healthy	49.99 GB	0 MB	0 %	No	0%
New Volume (G:)	Partition	Basic	NTFS	Healthy	49.98 GB	49.92 GB	99 %	No	0%
VP2_VV1 (H:)	Partition	Basic	NTFS	Healthy	499.99 GB	460.47 GB	92 %	No	0%

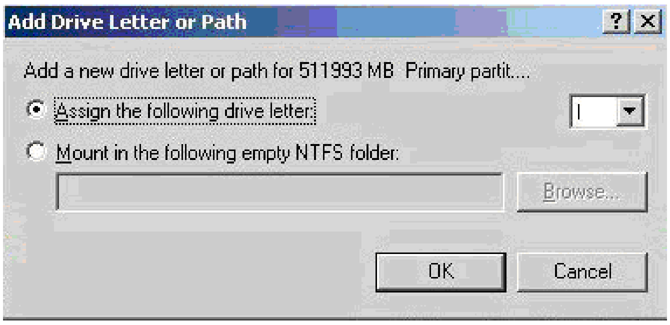
3. Right-click on the disk and select **Change Drive Letters and Path**.
4. Click **Add** in the prompt.



Change Drive Letter and Paths for 511993 MB Primary par...

Allow access to this volume by using the following drive letter and paths:

5. Select the drive letter and click **OK**.



Add Drive Letter or Path

Add a new drive letter or path for 511993 MB Primary partit....

● Assign the following drive letter: I

○ Mount in the following empty NTFS folder:

4. You should be able to access the data in the snapshot.

Creating a Volume Copy

The volume that created with a snapshot is referred to the target volume in the following procedure.

Note:

- To create a volume copy, you must have at least one snapshot ready.
- Snapshot volume copy allows you to do both read and write operations on the target volume.

Go to **Settings > Data protection > Monitoring**

Steps

1. Go to the Snapshot section. Click the link of the snapshot name.
2. A list of the snapshots that share the name and has taken at different moments are displayed. Select the snapshot that contains the state you want to roll back to.
3. Click **More** and select **Volume copy** option.
4. Go to the Volume copy page. Specify the target volume name.
5. Select a pool for the new volume to reside.
6. Choose the type of volume copy:
   - **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.
   - **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.
   - **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.

6. Click **OK**.

Viewing the Status of a Backup/Restore Task

Go to **Settings > Data protection > Monitoring**

Steps

1. Go to the Backup/Restore status section.
2. A list of the created tasks are displayed:
    - **Task type**: Indicate that the task is for backup or restore.
    - **Task name**: Click the link of a task name to view its details.
    - **Backup target**: Indicate where the backup data stores.
    - **Status**: Indicate the result of this task.

Scheduled Tasks

View all tasks that are created in Protection.

Editing/Deleting a Data Protection Task

Go to **Settings > Data protection > Scheduled tasks**

Edit a task

You can change the task name of a task, as well as its schedule and retention policy.

1. Find the task that you want to edit. Select the item block.
2. Click **Edit**.
3. Go to Edit schedule page. Change the task name, description, and/or the schedule and retention policy.
4. Click **OK** to save the settings.

Delete a task

1. Find the task that you want to edit. Select the item block.
2. Click **Delete**.
3. To confirm the action, click **Yes**.

Replication Pairs

A replication pair is created by pairing two volumes or folders. View and manage all replication pairs here. You can also create replication pairs by creating related tasks in Protection.

Adding a Folder Replication Pair

By pairing two volumes to create a replication pair, you can sync data between these two volumes on a regular basis.

Go to **Settings > Data protection > Replication pairs**

Steps

1. Go to the Folder replication pairs section. Click **Add**.
2. Go to the Create replication pair page. Specify the following information:

Replication pair name	Specify an identifying name for this pair.
Source folder	Choose an existing folder.
Channel for data transfer	Choose an available file channel of the controller. The available channels depend 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.
Rsync target type	Select **EonStor GS/GSe** or a third-party system **Rsync compatible server**.
Security level	If the Rsync target is EonStor GS/GSe, the security level will automatically set to **Encryption (security shell)**. If the Rsync target is a third-party system, you can choose to encrypt it or not when syncing data. To sync with encryption, select **Encryption (security shell)**. If not, select **None (rsync server)**.
Target IP address	Specify the IP address of the target device. The default port of EonStore Gs/GSe is **22**, while Rsync compatible server is **873**.
Target user name /	Specify the user information that can access the target

Target password	folder with complete permission (read and write).
Target folder path / Target shared name	Specify a valid directory of the target folder.
Compress file data	To duplicate the folder access control list (ACL) of the files, select **Duplicate the source folder ACL settings to target**. For detailed information of these features, please refer to the Application Note *EonStor GS Family Folder Replication*.
Delete other files on remote destination	
Handle sparse files efficiently	
Duplicate ACL settings of the source folder to target	

3. Click **OK**.

Managing a Folder Replication Pair

You can edit and delete a pair, start to sync the data between the two folders, and stop the syncing between them.

Go to **Settings > Data protection > Replication pairs**

Edit a pair

1. Go to the Folder replication pairs section. Select the pair that you want to edit.
2. Click **Edit**.
3. Go to the Edit page. Change the pair name and/or the target information.
4. Click **OK** to save the settings.

Start syncing

1. Go to the Folder replication pairs section. Select the pair that you want to start syncing.
2. Click **More** and select **Start folder replication** option.

Stop syncing

1. Go to the Folder replication pairs section. Select the pair that you want to stop syncing.
2. Click **More** and select **Stop folder replication** option.

Delete a pair

1. Go to the Folder replication pairs section. Select the pair that you want to delete.
2. Click **Delete**.
3. To confirm your action, click **OK**. The snapshot will be deleted immediately.

Adding a Volume Replication Pair

Pair two local volumes in this system to realize data synchronization between these two volumes.

Go to **Settings > Data protection > Replication pairs**

Steps

1. Go to the Volume replication pairs section. Click **Add**.
2. Go to the Create replication pair page. Specify the following information.

Replication pair type	Choose the replication pair type as **Volumes**.
Replication pair name	Specify an identifying name for this pair.
Source volume	Choose an existing volume. To create a volume, click **+**.
Target volume name / Target pool	Select the target pool and specify a name for the target volume.
Replication task type	● **Volume copy**: If you want to copy the data in the source volume to the target volume, select this option. Specify the task name and select its execution time. ● **Volume mirror**: If you want to mirror the source volume to the target volume, select this option. ■ **Mirroring type**: When selecting volume mirror, select **Synchronous mirror** or **Asynchronous mirror.** If you want to mirror changes in the source volume in real time, select **Synchronous mirror**. If you do not want to perform volume mirroring in real time, select **Asynchronous mirror**. You can further choose whether to create a snapshot in the target volume to avoid data loss. **Note:** Synchronous mirror is NOT recommended over WAN connections as high I/O latency may cause the process to fail.
Task priority	Select a priority level for this task.

3. Click **OK**.

Managing a Volume Replication Pair

You can edit and delete a pair, stop/resume the syncing between the two volumes, split the pair, mount/unmount the volume, map the target volume by auto mapping, and switch the source and the target.

Go to **Settings > Data protection > Replication pairs**

Edit a pair

1. Go to the Volume replication pairs section. Select the pair that you want to edit.
2. Click **Edit**.
3. Go to the Edit page. Change the settings.
4. Click **OK** to save the settings.

Pause/Resume data syncing

Note: This option is only available during volume copy tasks.

1. Go to the Volume replication pairs section. Select the pair.
2. Click **More** and select **Pause** or **Resume** option.

Mount/Unmount a source/target volume

Note:

- This option is only available for file-level volumes.
- The target volume cannot be mounted when the replication pair is in the "Mirror" status.

1. Go to the Volume replication pairs section. Select the pair.
2. Click **More** and select **Mount** or **Unmount** option.

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: 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).

1. Go to the Volume replication pairs section. Select the pair.
2. Click **More** and select **Target volume auto mapping** option.

Switch

Switch the roles (source and target) of a replication pair.

Note:

- 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.
- 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.

1. Go to the Volume replication pairs section. Select the pair.
2. Click **More** and select **Switch** option.

Delete a pair

1. Go to the Volume replication pairs section. Select the pair that you want to delete.
2. Click **Delete**.
3. To confirm your action, click **OK**.

Backup Targets

A file server or cloud storage can be a backup target, which stores the copy of your storage data. You can add and delete a backup target, or edit corresponding credential information for accessing a file server or cloud storage.

Adding a File Server as a Backup Target

You can also add a file server via creating a task. For more details, see Backing up Data to a File Server.

Go to	**Settings > Data protection > Backup Targets**
Steps	1. Select the backup target type as **File server**. 2. Go to the File servers section. Click **Add**. 3. Specify the following information: **File server name**: Specify an identifying name for the file server. **IP address**: Specify the IP address or the domain name of the file server. **Protocol**: Select **CIFS** or **NFS**. For CIFS, specify an account and the password. 4. Click **OK**. The newly-added file server is displayed in the list.

Adding Cloud Storage as a Backup Target

You can also add a file server via creating a task. For more details, see Backing up Data to Cloud Storage.

Note:

- After the feature is enabled, the folder cannot be changed.
- If EonCloud Gateway is enabled, the cloud backup feature shares the same folder. This folder stores the configurations of cloud storage. To learn more details about EonCloud Gateway, see EonCloud Gateway.

Go to **Settings > Data protection > Backup Targets**

Steps

1. Select the backup target type as **Cloud**.
2. Go to the Cloud storage accounts section. The account information is used to access the cloud location. Click **Add**.
3. Go to the Add an account page, and specify the following information:

Account name	Specify an identifying name for the account.
Cloud provider	Select **Aliyun**, **Amazon S3**, **Microsoft Azure**, or **Wasabi cloud**.
Access key / Endpoint	According to the cloud provider that you select, specify the corresponding access key / endpoint information.
Secret key / Share key / Key	According to the cloud provider that you select, specify the corresponding secret key / share key / key information.
Endpoint	When the cloud provider is set to **Aliyun**, select the endpoint information as **Auto**, **Manually**, or **Customize**. When you select the Manually option, select the **Region** of the cloud storage and specify the **Node name**. When you select the Customize option, specify the **Node name**.

4. Click **OK**. The newly-added account is displayed in the list.
5. Go to the Cloud locations section. Click **Add**.
6. Go to the Add a location page, and specify the following information:

Location name	Specify an identifying name for the cloud location.

Account	Select an account.
Connect	Click **Connect** for this storage system to connect to the cloud storage.
Bucket	After clicking **Connect**, all available buckets are displayed here. Select a bucket.

7. Click **OK**. The newly-added location is displayed in the list.

Viewing the Backup Targets of File Servers / Cloud Storage Locations

Go to **Settings > Data protection > Backup targets**

Steps

- To view all added file servers, select **File server**. The device names of the file servers, the IP address, and the connection protocols are displayed.
- To view all added cloud storage, select **Cloud**. The cloud storage accounts and the cloud locations are displayed.

Managing File Servers

You can edit and delete a file server.

Go to	**Settings > Data protection > Protection**
Edit a file server	1. Select the backup target type as **File server**. 2. Go to the File servers section. Select the file server that you want to edit. 3. Change the file server name, the IP address, and/or the credential information. 4. Click **OK** to save the settings.
Delete a file server	1. Select the backup target type as **File server**. 2. Go to the File servers section. Select the file server that you want to delete. 3. Click **Delete**.

Managing Cloud Storage Accounts / Cloud Locations

You can edit and delete an account.

Go to **Settings > Data protection > Protection**

Edit an account

1. Select the backup target type as **Cloud**.
2. Go to the Cloud storage accounts section. Select the account that you want to edit.
3. Change the account name and/or the credential information.
4. Click **OK** to save the settings.

Delete an account

Note: Deleting an account will also delete the related location and tasks.

1. Select the backup target type as **Cloud**.
2. Go to the Cloud storage accounts section. Select the account that you want to delete.
3. Click **Delete**.

Delete a cloud location

1. Select the backup target type as **Cloud**.
2. Go to the Cloud locations section. Select the location that you want to delete.
3. Click **Delete**.

Applications

By installing apps, you can add functionalities to your storage device and meet your various needs to data backup, file sharing, M&E, management, productivity, security and utilities.

- 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. To install the app, see Installing/Uninstalling Antivirus.
- **Backup server** is a backup solution that enables you to protect data on your PCs, file servers, and cloud. You can back up your data on a regular basis and restore it when needed, realizing centralized data management in a simple and convenient way. To install the app, see Installing/Uninstalling Backup Server.
- **Docker** is a lightweight virtualization application that allows you to run and test other applications in independent containers. To install the app, see Installing/Uninstalling Docker.
- **LDAP Server** provides directory services including centralized access control, authentication and account management. To install the app, see Installing/Uninstalling LDAP Server.
- **Mail Server** is a full-featured mail server suite allows your storage device becomes a mail server that supports SMTP, IMAP, and POP3 protocols. Not only being able to send and receive emails, you can manage accounts, back up emails and configure the server centrally. The app also has a web-based email client that provides full functionalities that you expect from an email client, including MIME support, address book, folder manipulation, message searching and spell checking. To install the app, see Installing/Uninstalling Mail Server.
- **Project Server** is dedicated to Blackmagic DaVinci Resolve to speed up multimedia collaboration. To install the app, see Installing/Uninstalling Project 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. To install the app, see Installing/Uninstalling Proxy Server.
- **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.

To install the app, see Installing/Uninstalling Syslog Server.

- **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. To install the app, see Installing/Uninstalling VPN Server.

- **Web Server** enables the storage device to be a website host, handling requests and serving web assets and content via HTTP. To install the app, see Installing/Uninstalling Web Server.

The Applications setting menu contains the following sub-settings.

1. Repository
2. Installed applications

Repository

View all apps and install/uninstall apps.

Installing/Uninstalling Antivirus

Go to	**Settings > Applications > Repository**
Installing the application	1. Click the application. 2. Go to application information. Click **Install**. 3. Specify a folder. In the case of dual controller models, specify folders for each controller. The antivirus service needs a working directory to save the log files and infected file(s) (quarantine zone). 4. Click **OK** to save the settings. The status of the app is displayed as “Installed”.
Uninstalling the application	1. Click the application. 2. Go to the application information. Click **Uninstall**.

Installing/Uninstalling Backup Server

You can back up your data in PCs, file servers, and cloud storage to this storage system.

Go to	**Settings > Applications > Repository**
Installing the application	1. Click the application. 2. Go to application information. Click **Install**. 3. Choose a volume for storing backup data. If needed, click the drop-down menu to choose another pool and another volume. If you want to create a volume, click **+**. For more details, see Adding a Volume. 4. Click **OK**.
Uninstalling the application	1. Click the application. 2. Go to the application information. Click **Uninstall**.

Installing/Uninstalling Docker

Go to	Settings > Applications > Repository
Installing the application	1. Click the application. 2. Go to the application information. Click **Install**. 3. 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. 4. Click **OK** to save the settings. The status of the application is displayed as “Installed”.
Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.

Installing/Uninstalling LDAP Server

Go to	**Settings > Applications > Repository**
Installing the application	1. Click the application. 2. Go to the application information. Click **Install**. 3. Specify the database domain name and the password. 4. Click **OK** to save the settings. The status of the application is displayed as “Installed”.
Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.

Installing/Uninstalling Mail Server

Go to	**Settings > Applications > Repository**
Installing the application	1. Click the application. 2. Go to application information. Click **Install**. 3. Specify the following information to complete the settings: **Domain name**: Specify the domain name. **HTTP port**: Specify the HTTP port. **HTTPs port**: Specify the HTTPs port. **User type**: Select the user type as **Local** or **AD/LDAP**. To acquire AD/LDAP users, enable AD/LDAP service first. For more details, see AD/LDAP Settings. 4. Click **OK** to keep the settings. The status of the app is displayed as “Installed”.
Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.

Installing/Uninstalling NextCloud

Go to	**Settings > Applications > Repository**
Installing the application	1. Click the application. 2. Go to application information. Click **Install**. 3. Specify the following settings: **Account**: Specify your account name. **Password**: Specify the password to the account. **HTTP port**: Specify the HTTP port. **HTTPs port**: Specify the HTTPs port. **SSL certificate**: If needed, upload the a crt file of an SSL certificate. **SSL key**: If needed, upload the a key file of an SSL key. 4. Click **OK** to keep the settings. The status of the app is displayed as “Installed”.
Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.

Installing/Uninstalling Project Server

Note:

- Docker is required for using the app. The enabling of Docker is included during the installation of the app.
- A WORM-enabled pool is not available for storing the project server’s data.

Go to	**Settings > Applications > Repository**
Installing the application	1. Click the application. 2. Go to application information. Click **Install**. 3. To store Docker data, select or create a file-level volume, and click **Next**. 4. To store the project server’s data, select a pool and a volume, and click **OK**. 5. The status of the application is displayed as “Installed”.
Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.

Installing/Uninstalling Proxy Server

The proxy server function is presented with the features:

- Cache the web contents which clients have accessed
- Access control functions
- User authentication

Note:

- Configure the DNS service before enabling Proxy Sever. To configure the service, see Configuring the DNS Service.
- 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.

<table>
<tr><th>Go to</th><th>Settings > Applications > Repository</th></tr>
<tr><td><b>Installing the application</b></td><td>
1. Click the application.
2. Go to app information. Click <b>Install</b>.
3. Choose a network channel to run the proxy server.
To know more about the selected channel’s current configuration, click <b>View detailed information</b>.
Specify the following information to complete the settings:
<table>
<tr><td><b>Available channel interface(s) to access Proxy Server</b></td><td>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.</td></tr>
<tr><td><b>Port</b></td><td>This is the port number to listen to client requests. The default value is 3128.</td></tr>
<tr><td><b>Location</b></td><td>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.</td></tr>
<tr><td><b>Cache Size (GB)</b></td><td>This specifies the cache size in GB. The default value is 10.</td></tr>
<tr><td><b>Min. file size for</b></td><td>This is the minimum size of a single cache file. The default value</td></tr>
</table>
</td></tr>
</table>

	disk cache (KB)	is 0.
	Max. file size for disk cache (KB)	This is the maximum size of a single cache file. The default value is 1024000.
	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.
	4. Click **OK** to keep the settings. The status of the application is displayed as “Installed”.	
Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.	

Installing/Uninstalling Syslog Server

Syslog Server provides 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 > Repository**

Installing the application

1. Click the application.
2. Go to application information. Click **Install**.
3. Choose a network channel to run the proxy server.

   To know more about the selected channel’s current configuration, click **View detailed information**.

   Specify the following information to complete the settings:

Available channel interface(s) to access Proxy 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	The system listens to and receives log data according to the specified protocol. You can select 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.

4. Click **OK** to keep the settings. The status of the application is displayed as “Installed”

Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.

Installing/Uninstalling VPN Server

VPN Server 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

Note: Please make sure UDP port 1701, 500, and 4500 are open on your router or firewall settings for VPN connection.

Go to	**Settings > Applications > Repository**
Installing the application	1. Click the application. 2. Go to application information. Click **Install**. 3. Choose a network channel to run the proxy server. To know more about the selected channel's current configuration, click **View detailed information**. Specify the following information to complete the settings:

Available channel interface(s) to access Proxy 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.
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.
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	You can specify the DNS server address in the VPN. The default is "Don't specify."
Don't specify	Clients use their own DNS configurations.

	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 to *MS-CHAPv2*. Choose to provide the service to local user accounts or domain user accounts. The default is to domain user accounts.
	4. Click **OK** to keep the settings. The status of the app is displayed as “Installed”	
Uninstalling the application	1. Click the application. 2. Go to application information. Click **Uninstall**.	

Installing/Uninstalling Web Server

Go to **Settings > Applications > Repository**

Installing the application

1. Click the application.
2. Go to application information. Click **Install**.
3. Specify the following information to complete the settings:

   Web server settings:

HTTP port	Specify the HTTP port.
HTTPS port	Specify the HTTPS port.
SSL certificate file (.crt)	Click **Browse** to upload a certificate file in crt format.
SSL key file (.key)	Click **Browse** to upload a certificate file in key format.
HTTP Strict Transport Security (HSTS)	If needed, click the toggle switch to enable it.
Website type	Choose the type of your website as **Static** or **Dynamic**.

4. If you select Dynamic for the website type, specify the Database settings:

HTTPS port **(for database administrators' access)**	Specify the HTTPS port.
Database name	Specify the database name.
Database password	Specify the database password.

5. Click **OK**.

Uninstalling the application

1. Click the application.
2. Go to application information. Click **Uninstall**.

Updating an Application

In the overview of all apps, when the status of an app is displayed as “Update available,” you can update it to the latest version.

Go to	**Settings > Applications > Repository**
Steps	1. Select the application. 2. Go to application information. Click **Update**.

Installed

You can manage all installed apps and start to use an app. To see detailed information about each app, find the app from the list, and click **Details**.

Editing an Application Settings

Go to	**Settings > Applications > Installed**
Steps	1. On the list of installed apps, find the app and click **Settings**. 2. Change the items that you want to edit. 3. Click **OK** to keep the settings.

Using Antivirus

Go to		**Settings > Applications > Installed**
Overview		1. On the list of installed apps, find the app and click **Open**. 2. View the number of quarantined files and the status.
Virus pattern update		1. On the list of installed apps, find the app and click **Open**. 2. Click **Virus pattern update**. You can view and change the version of virus definition and the update frequency.
	Updating the virus pattern	Click **Update now**. 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.
	Changing the frequency	1. Specify then number of the days to check the virus pattern. 2. Click **Apply** to save the settings.
	Locally installing virus pattern	If online update cannot work properly, you can update the ClamAV Virus Database (.CVD file) locally. Virus patterns can be downloaded from http://www.clamav.net. 1. Click **Browse**. 2. Select the .CVD file in the local host. 3. Click **Install** to upload the file to the storage device.
Scan jobs		1. On the list of installed apps, find the app and click **Open**. 2. Click **Scan jobs**. You can view the status of each scan job, add/edit/delete a job, starting a job immediately, and configure the global settings for all jobs.
	Adding a job	1. Click **Add job**. 2. Specify the job name. 3. For dual-controller models, select the controller. 4. Select the folders to be scanned, and click **Add**. The selected folders will be included in the list below. To remove a folder from the list, select it and click **Delete**. **Note:** For dual controller models, if you choose to scan all folders, the system will automatically divide the job into two

		jobs, respectively for controller A and B. 5. Select **Scan now**, **Scan daily**, or **Scan weekly**. For a daily/weekly schedule, specify the time / the time and day.
	Configuring global settings of scan jobs	1. Click **Settings**. 2. Specify the following information to complete the settings: **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. 3. Click **Apply** to save the settings.
Logs	1. On the list of installed apps, find the app and click **Open**. 2. Click **Logs**. All the scan results are listed in the list. Each scan result is saved in a log file. You can download/delete a log, and configure its settings.	
	Downloading logs	1. Select one or more scan results. 2. Click **Download logs**. If multiple selections are made, the log files will be saved as a zip file.
	Delete logs	1. Select one or more scan results. 2. Click **Delete**.
	Changing log settings	3. Specify the number of days to keep the logs. 4. Click **Apply**.
Quarantine	You can restore or delete the files in quarantine.	
	Restore files	1. Select one or more files. 2. Click **Restore**. The selected files will be restored to their original locations.
	Delete files	1. Select one or more files.

2. Click **Delete**. The selected files will be permanently deleted.

Using Backup Server: Backing up / Restoring Your Data in a File Server

Create a task to back up / restore your data in file servers. A task can automatically run on a regular basis.

In an event of disaster, you can restore data to the original locations or any location that you specify.

By monitoring the progress of these backup/restore tasks, Backup server realize centralized management of your backup data.

Note: For a file server, when backing up your data, the folder attributes, e.g. ACL settings, cannot be backed up. When restoring data, the ACL settings of the destination folder will apply to the restored folders/data.

Go to	**Settings > Applications > Installed**

Back up data in a file server

1. On the list of installed apps, find the app and click **Open**.

1. For the data source, select **File server**.

2. For **Task name**, the system has specified an identifying name. If needed, change the task name and/or specify **Description** for this task.

3. Go to the Data section. Select the file server that contains data you want to back up. To select a file server, do one of the following:

   - Choose an added file server. Continue to Step 5.

   - If this is the first time that you try to back up data in a file server, add a file server for this storage system to connect it. Click **+** and go to the Add a file server page. Specify the following information, and click **OK**:

File server name	Specify an identifying name for the file server.
IP address	Specify the IP address or the domain name of the file server.
Protocol	Select **CIFS** or **NFS**. For CIFS, specify an account and the password.

4. To select what data to back up, click **Browse**. On the Select backup data page, select one or more folders. Click **OK**.

5. To select a target folder to store the data, click **Browse**.

6. Go to the Schedule & retention policy section. Specify the following information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an

	activate frequency less than one day: Choose **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**. ● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**. To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the current time that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a termination date and time** and specify the time.
Retention policy	Choose to retain the data according to a specific time period or a specific number of copies, or never delete the data. ● **By period**: specify how long the data should be retained. ● **By number of copies**: specify the maximum number of copies of the data. ● **Never delete**

7. Click **Create** to create the task.

Restore your data to a file server

1. On the list of installed apps, find the app and click **Open**.
2. Click **Restore**. For the data source, select **File server**.
3. Select the file server.
4. Select the backup task name and the activate time of the backup operation. For a scheduled task, the backup operation can be activated at more than once.
5. For the destination, choose to restore your data to the **Original** location, or choose **Customize** to specify a location that is different from the original one.

   When restoring data to the original location, the data in it will be overwritten.

   When selecting **Customize**, click **Browse** to select the folder in which you want to restore the backup data. If needed, click **Refresh** to get the latest status about all the available folders. Click **OK** to save the setting.

6. Click **Restore** to create the task.

Using Backup Server: Backing up / Restoring Your Data in Cloud Storage

Create a task to back up / restore your data in cloud storage. A task can automatically run on a regular basis.

In an event of disaster, you can restore data to the original locations or any location that you specify.

By monitoring the progress of these backup/restore tasks, Backup server realize centralized management of your backup data.

Go to **Settings > Applications > Installed**

Back up data in cloud storage

1. On the list of installed apps, find the app and click **Open**.
2. For the data source, select **Cloud**.
3. For **Task name**, the system has specified an identifying name. If needed, change the task name and/or specify **Description** for this task.
8. Go to the Data section. Select the cloud location that contains data you want to back up. To select a cloud location, do one of the following:
   - Choose an added cloud location. Continue to Step 5.
   - If this is the first time that you try to back up data in cloud storage, add cloud storage for this storage system to connect it. Click **+** and go to the Add a location page. Specify the following information, and click **OK**:

Location name	Specify an identifying name for the cloud location.
Account	● Select an account name. The account information is used to access the cloud location. ● If this is the first time that you add cloud storage, add an account, too. Click **+** and go to the Add an account page. ■ Specify an identifying name for this account. ■ Select the cloud provider: **Aliyun**, **Amazon S3**, **Microsoft Azure**, or **Wasabi cloud**. ■ According to the cloud provider that you select, specify the corresponding access key / endpoint and key / secret key / share key. ■ Click **OK** to complete the settings.
Connect	Click **Connect** for this storage system to connect to the cloud storage.
Bucket	After clicking **Connect**, all available buckets are displayed

here. Select a bucket.

4. To select what data to back up, click **Browse**. On the Select backup data page, select one or more folders. Click **OK**.

5. To select a target folder to store the data, click **Browse**.

6. Go to the Schedule & retention policy section. Specify the following information:

Activate frequency	Choose **Once**, **Daily**, **Weekly**, **Bi-weekly**, **Monthly**, or **Customize**. ● The Customize option allows you to specify an activate frequency less than one day: Choose **10 minutes**, **20 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, or **12 hours**. ● To run this task weekly, select one or more days. ● To run this task bi-weekly, select a day. ● To run this task monthly, select one or more dates.
Start time	To start the task immediately, choose **Start now**. To start the task on a regular basis, choose **By schedule**, and specify the start date and execution time. You can check the current time that displayed below for you to consider the scheduling.
Termination policy	To run this task continuously, choose **Continuous, the schedule won't be terminated on its own**. To run this task until a specific moment, choose **Specify a termination date and time** and specify the time.
Retention policy	Choose to retain the data according to a specific time period or a specific number of copies, or never delete the data. ● **By period**: specify how long the data should be retained. ● **By number of copies**: specify the maximum number of copies of the data. ● **Never delete**

7. Click **Create** to create the task.

Restore your data to cloud	**Note:** The data can only restore to its original location. 1. On the list of installed apps, find the app and click **Open**.

2. Click **Restore**. For the data source, select **Cloud**.
3. Select the cloud location.
4. Select the backup task name and the activate time of the backup operation. For a scheduled task, the backup operation can be activated at more than one time.
5. Click **Restore** to create the task.

Using Backup Server: Restoring Your Data in a PC

To back up data in a PC, this feature must work with the software EonView. Go to Infortrend's website and download the software: Downloads

On EonOne, enable this feature on this storage system.

After downloading the software, install EonView on a PC, and then enable the backup feature in EonView. For more details, see *EonView User Manual*.

In an event of disaster, you can restore data to the original locations or any location that you specify.

By monitoring the progress of these backup/restore tasks, Backup server realize centralized management of your backup data.

Go to	**Settings > Applications > Installed**
Back up data in a PC	Create a backup task via EonView on a PC. For more details, see *EonView User Manual*.
Restore data to a PC	1. On the list of installed apps, find the app and click **Open**. 2. Click **Restore**. For the data source, select **PC**. 3. Select a PC client that is the source of your backup data. 4. Select the backup task name and the activate time of the backup operation. For a scheduled task, the backup operation can be activated at more than one time. 5. Select a PC client where the data will restore to, and specify the path. 6. If a file with the same name already exists in the specified path, select to **Overwrite** it, **Overwrite it when the restore file is newer**, **Overwrite it when the restore file is older**, or **Skip**. 7. Click **Restore** to create the task.

Using Backup Server: Managing File Servers

You can add, edit, and delete a file server.

<table>
<tr><td><b>Go to</b></td><td><b>Settings > Applications > Installed</b></td></tr>
<tr><td><b>Add a file server</b></td><td>
1. On the list of installed apps, find the app and click <b>Open</b>.
2. Click <b>Data sources</b>. Select the data source type as <b>File server</b>.
3. Go to the File servers section. Click <b>Add</b>.
4. Specify the following information:
<table>
<tr><td><b>File server name</b></td><td>Specify an identifying name for the file server.</td></tr>
<tr><td><b>IP address</b></td><td>Specify the IP address or the domain name of the file server.</td></tr>
<tr><td><b>Protocol</b></td><td>Select <b>CIFS</b> or <b>NFS</b>. For CIFS, specify an account and the password.</td></tr>
</table>
5. Click <b>OK</b>. The newly-added file server is displayed in the list.
</td></tr>
<tr><td><b>Edit a file server</b></td><td>
1. On the list of installed apps, find the app and click <b>Open</b>.
2. Click <b>Data sources</b>. Select the data source type as <b>File server</b>.
3. Go to the File servers section. Select the file server that you want to edit.
4. Change the file server name, the IP address, and/or the credential information.
5. Click OK to save the settings.
</td></tr>
<tr><td><b>Delete a file server</b></td><td>
1. On the list of installed apps, find the app and click <b>Open</b>.
2. Click <b>Data sources</b>. Select the data source type as <b>File server</b>.
3. Go to the File servers section. Select the file server that you want to delete.
4. Click Delete.
</td></tr>
</table>

Using Backup Server: Managing Cloud Accounts and Locations

You can add, edit, and delete cloud storage accounts and locations.

Go to	**Settings > Applications > Installed**
Add a file server	1. On the list of installed apps, find the app and click **Open**. 2. Click **Data sources**. Select the data source type as **Cloud**. 3. Go to the Cloud storage accounts section. The account information is used to access the cloud location. Click **Add**. 4. Go to the Add an account page, and specify the following information: **Account name**: Specify an identifying name for the account. **Cloud provider**: Select **Aliyun**, **Amazon S3**, **Microsoft Azure**, or **Wasabi cloud**. **Access key / Endpoint**: According to the cloud provider that you select, specify the corresponding access key / endpoint information. **Secret key / Share key / Key**: According to the cloud provider that you select, specify the corresponding secret key / share key / key information. **Endpoint**: When the cloud provider is set to **Aliyun**, select the endpoint information as **Auto**, **Manually**, or **Customize**. When you select the Manually option, select the **Region** of the cloud storage and specify the **Node name**. When you select the Customize option, specify the **Node name**. 5. Click **OK**. The newly-added account is displayed in the list.
Add a cloud location	1. On the list of installed apps, find the app and click **Open**. 2. Click **Data sources**. Select the data source type as **Cloud**. 3. Go to the Cloud locations section. Click **Add**. 4. Go to the Add a location page, and specify the following information: **Location name**: Specify an identifying name for the cloud location. **Account**: Select an account. **Connect**: Click **Connect** for this storage system to connect to the cloud storage.

	Bucket After clicking **Connect**, all available buckets are displayed here. Select a bucket. 5. Click **OK**. The newly-added location is displayed in the list.
Edit an account	1. On the list of installed apps, find the app and click **Open**. 2. Click **Data sources**. Select the data source type as **Cloud**. 3. Go to the Cloud storage accounts section. Select the account that you want to edit. 4. Change the account name and/or the credential information. 5. Click **OK** to save the settings.
Delete an account	**Note:** Deleting an account will also delete the related location and tasks. 1. On the list of installed apps, find the app and click **Open**. 2. Click **Data sources**. Select the data source type as **Cloud**. 3. Go to the Cloud storage accounts section. Select the account that you want to delete. 4. Click **Delete**.
Delete a cloud location	1. On the list of installed apps, find the app and click **Open**. 2. Click **Data sources**. Select the data source type as **Cloud**. 3. Go to the Cloud locations section. Select the account that you want to delete. **4.** Click **Delete**.

Using Backup Server: Managing Tasks and Monitoring Task Status

You can view all backup/restore tasks and the task status.

Note: You can edit and delete a task with its data source type as file servers or cloud storage. To manage the task with its type as PC, manage it via the PC client itself.

Go to **Settings > Applications > Installed**

Monitor task status

- **Task type**: Indicate that the task is for backup or restore.
- **Task name**: Click the link of a task name to view its details.
- **Data source**: Indicate where the data is backed up from.
- **Status**: Indicate the result of this task.
- **Start time**: Indicate when the task starts.

Edit a task

1. On the list of installed apps, find the app and click **Open**.
2. Click **Scheduled tasks**. Select the task with its data source as **File server** or **Cloud**.
3. Click **Edit**. Change the task name and/or the schedule.
4. Click **OK** to save the settings.

Delete a task

1. On the list of installed apps, find the app and click **Open**.
2. Click **Scheduled tasks**. Select the task with its data source as **File server** or **Cloud**.
3. Click **Delete**.

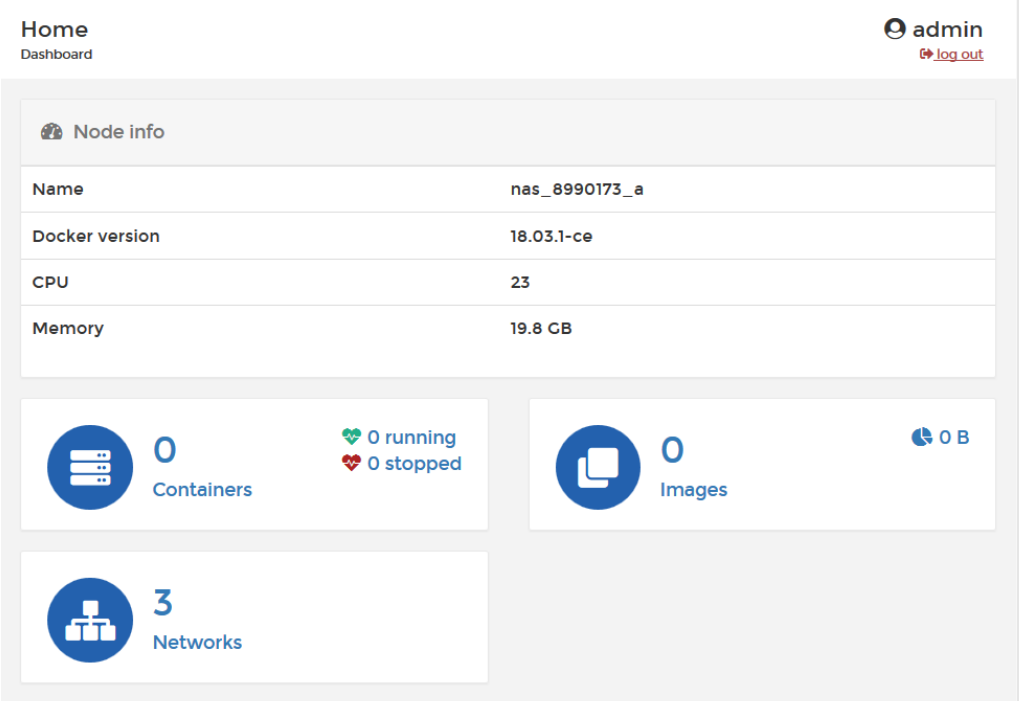
Using Docker

Go to **Settings > Applications > Installed**

Steps

1. On the list of installed apps, find the app and click **Open**.
2. Enter your EonOne credentials and click **Login** to enter the site.

Dashboard You can view information of the Docker node (i.e. your Docker-running device).



Home
Dashboard

admin
log out

Node info

Name	nas_8990173_a
Docker version	18.03.1-ce
CPU	23
Memory	19.8 GB

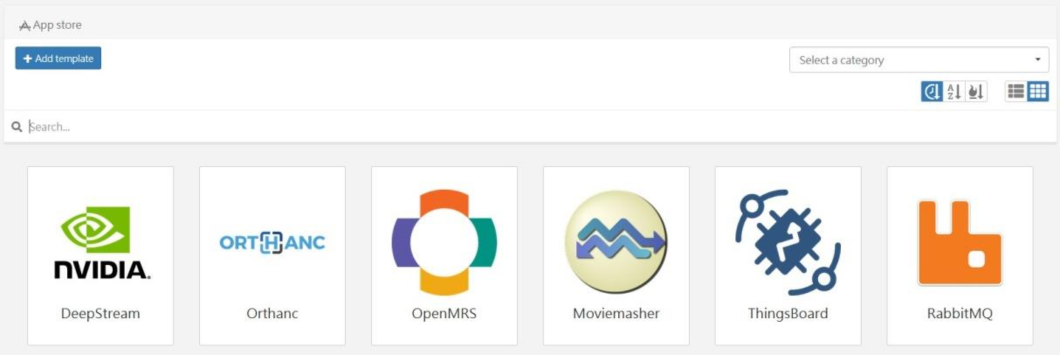
0 Containers
0 running
0 stopped

0 Images
0 B

3 Networks

Name	The hostname of your storage device
Docker version	The version of the Docker application
CPU	The number of CPU cores on your storage device
Memory	System RAM allocated for running Docker and its containers
Containers	The total number of containers
Networks	The number of created networks
Images	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.
Network	Select the network type.

	To prevent modification of this setting, turn on **Network lock** so that the template's users cannot change it.
Port mapping	Map a host port (TCP/UDP) to a container port (TCP/UDP) for communication.
Volume mapping	Bind a shared folder to the container. The folder works as a Docker volume and stores all data required and generated by the container. **Required**: This container setting must be specified by the user. **Default option of the configuration**: This container setting must be available in the template. **Label**: Assign a custom name to this container setting. You can find the custom name in the template configuration. **Description**: Provide a description of the container setting.
Restart policy	Specify when to restart the container: **Always**, **Unless stopped**, **On failure**, or **None**.
Privileged mode	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.
Interactive mode	Enable this option to run the container in the foreground so that the user can run commands in the container.
Memory reservation	Reserve a custom amount of system memory to run the container.
Memory limit	Set an upper limit on the container's memory usage.
CPU limit	Set an upper limit on the container's CPU usage.

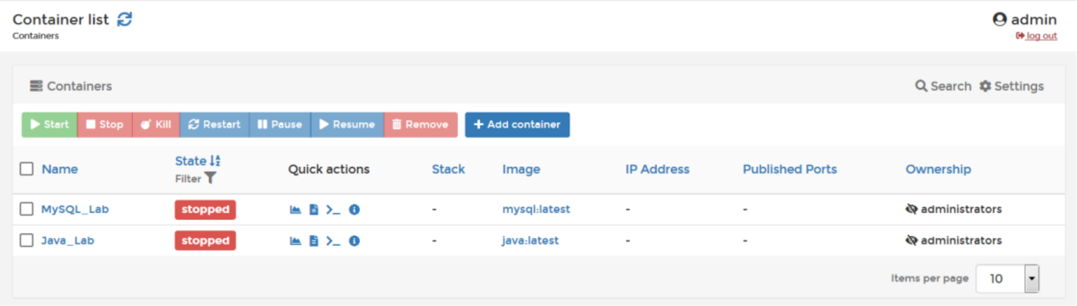
5. Specify the environment variables by providing their names and default values.

6. Click Create the template.

7. 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.

8. When Docker detects any update for your apps, click on Update to install the updates.

Containers	You can view and manage containers.



Container list
Containers

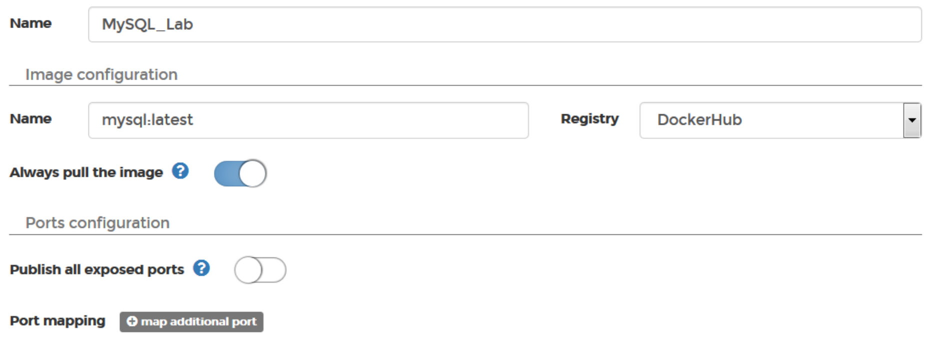
admin
log out

Containers

□ Name	State Filter	Quick actions	Stack	Image	IP Address	Published Ports	Ownership
□ MySQL_Lab	stopped		-	mysql:latest	-	-	administrators
□ Java_Lab	stopped		-	java:latest	-	-	administrators

Items per page 10

1. Create a container to execute a downloaded Docker image. Click Add container to start the setup.



Name: MySQL_Lab

Image configuration

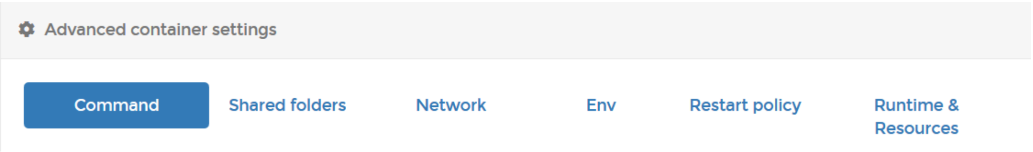
Name: mysql:latest
Registry: DockerHub
Always pull the image: on

Ports configuration

Publish all exposed ports: off
Port mapping

Name	Assign a name to the container.	
Image configuration	**Name**	Enter the downloaded image's name.
	Registry	Choose the registry where you downloaded the image. The default registry is DockerHub.
	Always pull the image	When enabled, this option pulls the specified image when you create a container for it.
Ports configuration	**Publish all exposed ports**	When enabled, this option maps a random host port to ports defined in the image's Dockerfile.
	Port mapping	Click **map additional port** if you want to map another host port to the ports defined in the Dockerfile.
Actions	Click **Deploy the container** to execute the image in the container.	

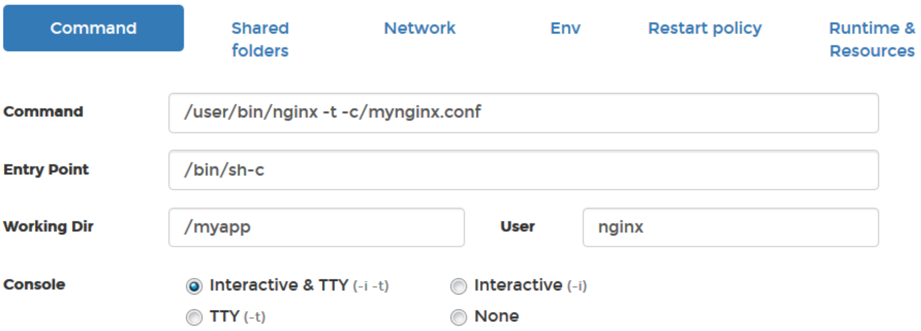
2. Go to the page bottom and configure the advanced settings on each tab.



Advanced container settings

3. 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: /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

Command	Specify the default command to execute when running an image.
Entry Point	Specify the command to run when the container starts up.
Working Dir	Specify a default directory for Docker to run its commands.
Console	Choose a desired set of console for accessing the container.

4. On the Volumes tab, you can choose a container to store generated data:

Volume	Select a volume within the Docker volume to store data.
Shared folder	Select a shared folder on the STORANDER storage to store data.
Bind	Select a file or a folder inside a shared folder to store data.
Writable/Read-only	Determine the access permission to the container.
add more volume	Add more containers.

5. On the Network tab, you can configure the network to be used by the container.

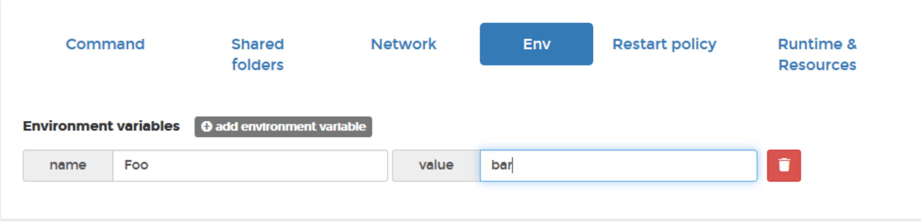
Network	Select a network driver to determine the network type.
Hostname	Specify a hostname to the container.
Domain Name	Specify a domain name for the Docker network.
Mac Address	Assign a MAC address to the container.
IPv4 Address	Assign an IPv4 address to the container.

IPv6 Address	Assign an IPv6 address to the container.
Hosts file entries	Click **add additional entry** 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.

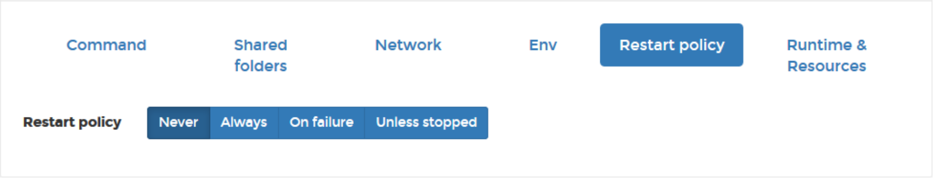


Environment variables

name Foo value bar

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.



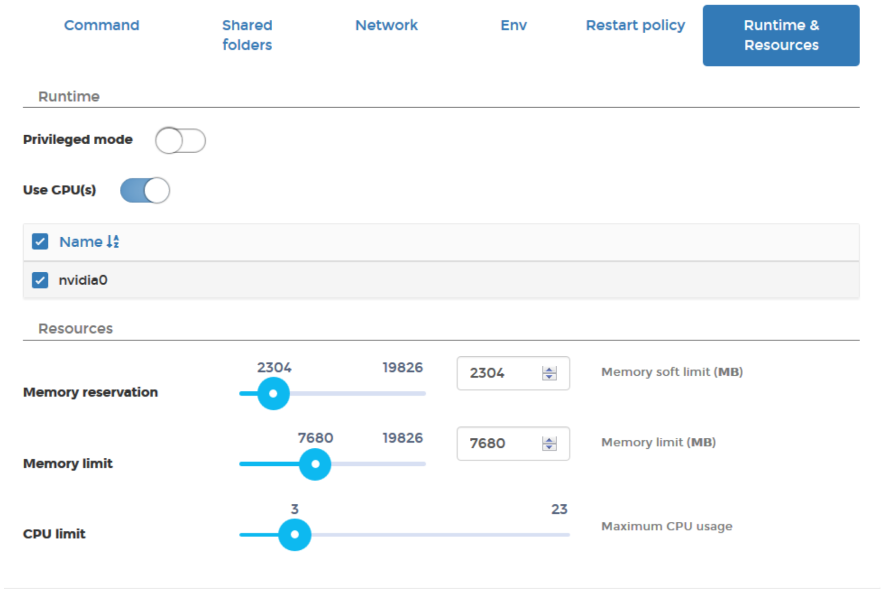
Restart policy [✓ Never] Always On failure Unless stopped

Never	Never automatically restart the container.
Always	Always restart the container when it is stopped.
On failure	Restart the container when it is stopped due to errors.
Unless stopped	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.



Runtime

Privileged mode ○

Use GPU(s) ●

☑ Name
☑ nvidia0

Resources

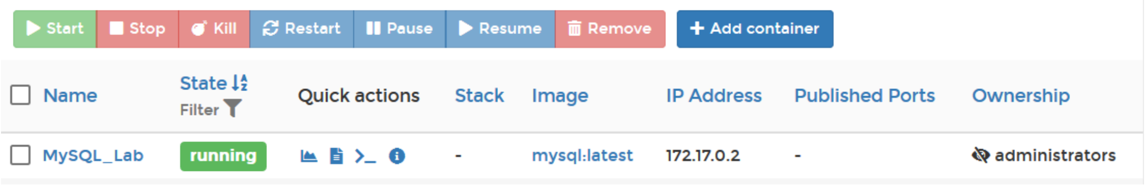
Memory reservation: 2304 (max 19826) — 2304 Memory soft limit (MB)

Memory limit: 7680 (max 19826) — 7680 Memory limit (MB)

CPU limit: 3 (max 23) — Maximum CPU usage

Privileged mode	When enabled, this option allows the container to access devices on your device.
Use GPU(s)	When enabled, this option allows you to use selected GPUs for running the container, alongside from the allocated CPU resources. This option is only available to GSi models.
Memory reservation	Specify the minimum amount of memory that can be used by the container.
Memory limit	Specify the maximum amount of memory that can be used by the container.
CPU limit	Specify how many CPU cores to use for running the container.

9. Go back to Containers to view and manage containers by selection.

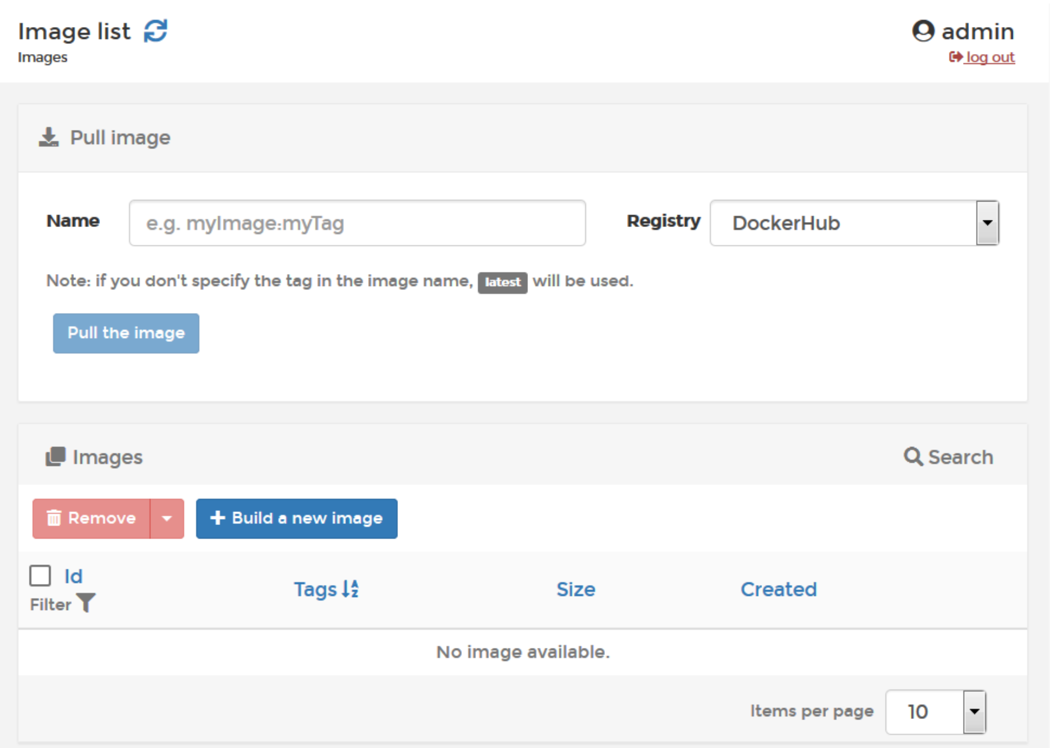


□ Name	State Filter	Quick actions	Stack	Image	IP Address	Published Ports	Ownership
□ MySQL_Lab	running		-	mysql:latest	172.17.0.2	-	administrators

Start	Start the container.
Stop	Stop the container.
Kill	Delete the container when it is running.
Restart	Restart the container when it is stopped.

Pause	Pause the container when it is running.
Resume	Resume the container when it is paused.
Remove	Remove the container when it is stopped.
Quick actions	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.



Note: if you don't specify the tag in the image name, latest will be used.

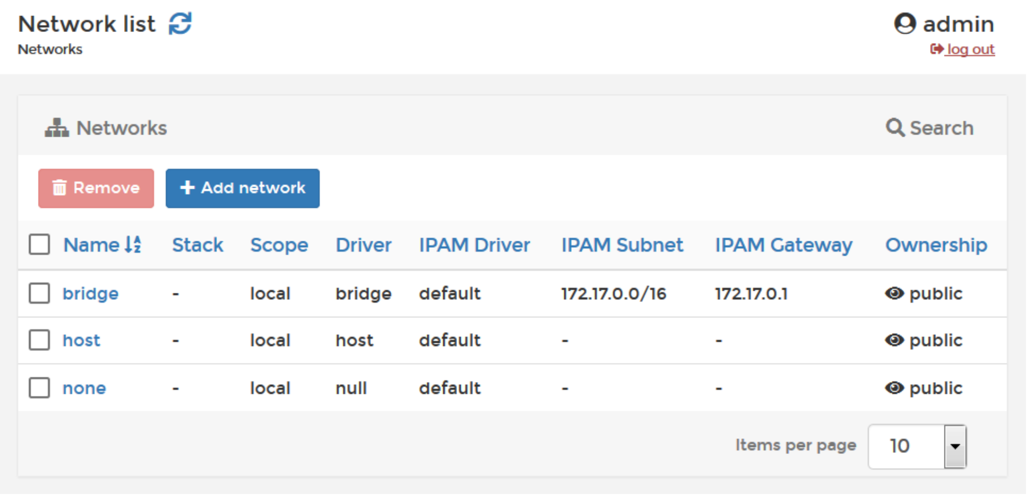
No image available.

Pull image	**Name**	Enter a keyword or full name to locate a Docker image.
	Registry	Select a registry where you can download the image.
	Pull the image	Download the image from the registry.
Images	**Remove**	Remove an unused Docker image. To remove an image being used by a container, click the arrow icon and **Force Remove**.
	Build a new	Build a new Docker image with the native web

	image	editor, the uploaded tarball file or Dockerfile, or a file URL.

Networks

You can add, remove, and monitor networks for a container.



Network list
Networks

admin
log out

Networks
Search

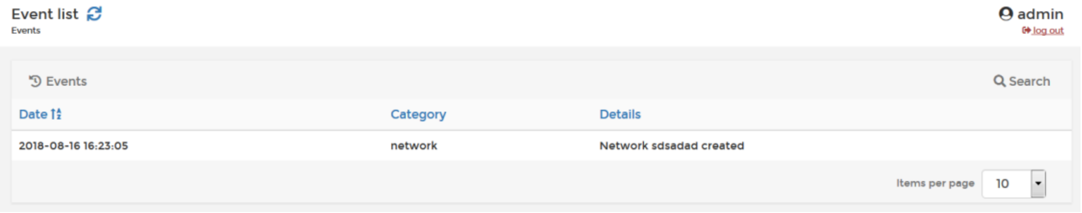
Remove
+ Add network

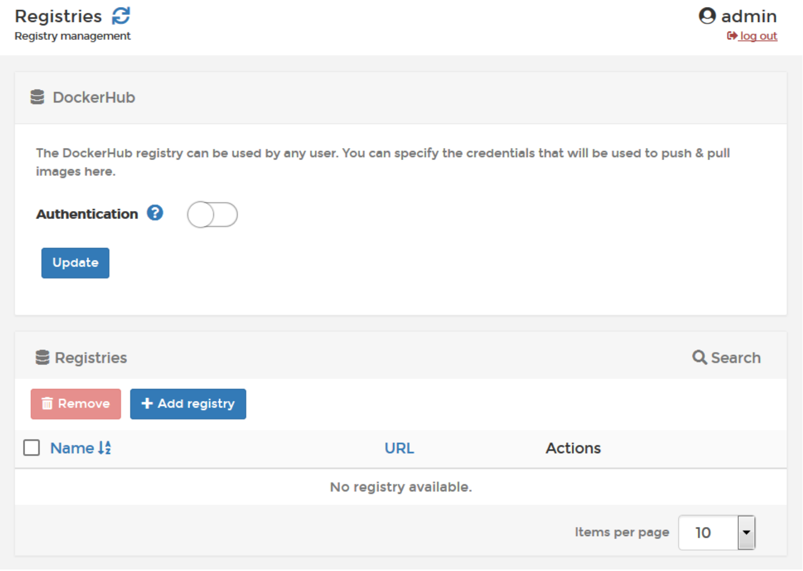
□	Name	Stack	Scope	Driver	IPAM Driver	IPAM Subnet	IPAM Gateway	Ownership
□	bridge	-	local	bridge	default	172.17.0.0/16	172.17.0.1	public
□	host	-	local	host	default	-	-	public
□	none	-	local	null	default	-	-	public

Items per page 10

1. Click Add network to set up a new network.

Name	Assign a name to the network.	
Network configuration	**Subnet**	Enter the subnet netmask.
	Gateway	Enter the gateway address.
Driver configuration	**Driver**	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.
	Driver options	Create a custom network driver by assigning a name and a value to it.
Advanced configuration	**Labels**	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.
	Restrict external access to the	When enabled, this option blocks any access from a different Docker network.

		network
	Actions	Click **Create the network** to complete the setup.
	2. After the setup, go back to Networks to manage and monitor existing networks.	
Volumes	You can create and manage volumes within the Docker volume.	
	Add volume	Click to add a new volume and specify the settings: **Name**: Specify a name for the volume **Driver**: Select a driver to run the volume. **Driver options**: 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 **add driver option**. Then, click **Create the volume** to create a volume.
	Remove	Select an unwanted volume and click **Remove** to delete it.
Events	You can check configuration changes and container behaviors on this management site.  Event list Events admin log out Events Search Date · Category · Details 2018-08-16 16:23:05 · network · Network sdsadad created Items per page 10	
Registries	You can manage the DockerHub credentials and add more Docker registries.	



Registries
Registry management

admin
log out

DockerHub

The DockerHub registry can be used by any user. You can specify the credentials that will be used to push & pull images here.

□ Name	URL	Actions
No registry available.		

Items per page 10

DockerHub	**Authentication**	When enabled, this option allows only users with the correct credentials to pull/push Docker images.
	Update	Sync with DockerHub.
Registries	**Add registry**	You can add more Docker registries for use: Provide user credentials and other required information. Then, click **Add registry** to connect.
	Remove	Remove a selected registry.

Using LDAP Server

Go to **Settings > Applications > Installed**

Manage users You can add, edit, and delete users.

Adding a user

1. Specify an identifying username and password. Repeat the password to confirm it.
2. If needed, specify an email address and the description about the account.
3. Select the option about whether the user must change its password: **User must change the password at the first time login**, or **User cannot change the password**.
4. Select **Account expiration** to configure when the account is expired: **Disable now**, or **Valid until: Date**.
5. Click **Next**.
6. To add the user to a user group, select the group and click **Add**.

Adding multiple users

1. Specify a username prefix, e.g. user.
2. Specify username start number and the number of users.
3. Specify the password and repeat it to confirm it.
4. Select the option about whether the user must change its password: **User must change the password at the first time login**, or **User cannot change the password**.
5. Select **Account expiration** to configure when the account is expired: **Disable now**, or **Valid until: Date**.
6. If needed, select the option to **Overwrite existing users**.
7. Click **Apply**.
8. To add these users into different user groups, go to **Manage groups** page and select to add users into the groups.

Importing a user list

Note: Before importing, make a list of all these users you want to add and save the list in a csv file.

1. Click **Browse** to select the csv file of your user list.
2. A content preview of the list will be displayed in the list below.
3. If needed, select the option to **Overwrite existing users**.

		4. Click **Apply**. 5. To add these users into different user groups, go to **Manage groups** page and select to add users into the groups.
	Editing a user	1. Select the user from the list, and click **Edit**. 2. Change the settings. 3. Click **Apply**.
	Deleting a user	Select a user, and click **Delete**.
Manage groups	You can add, edit, and delete user groups.	
	Adding a user group	1. Click **Add**. 2. Specify an identifying name and the description. 3. Click **Apply**.
	Editing a user group	1. Select a user group, and click **Edit**. 2. Change the settings. To add one or more users to the group, click the **Group Members** tab and select users. 3. Click **Apply**.
	Deleting a user group	Select a user group, and click **Delete**.
Backup/Restore LDAP database	You can back up or restore the LDAP database.	
	Backing up the database	1. Click the toggle switch to enable backup. 2. Specify the backup frequency: select **Daily**, **Weekly**, or **Monthly,** and specify **Start time**. 3. Select the **Destination folder**. 4. Click **Apply**. 5. If needed, click **Export Database Now** to download the database to the local host.
	Restoring the database	1. Click **Browse** to select the database in the local host. 2. Click **Restore** to upload the selected database to the system and activate restoration.

Using Project Server

<table>
<tr><th>Go to</th><th>Settings > Applications > Installed</th></tr>
<tr><td><b>View the status of Project Server</b></td><td>1. On the list of installed apps, find the app and click <b>Open</b>.
2. View the status and information about Project Server.</td></tr>
<tr><td><b>Manual backup</b></td><td>You can immediately back up the project server’s data.
1. On the list of installed apps, find the app and click <b>Open</b>. Go to the <b>Manual backup</b> page.
2. Click <b>Backup</b> to back up the project server’s data into a backup file.
3. After the backup is complete, a corresponding backup file appears in the <b>Backup history</b> page.</td></tr>
<tr><td><b>Scheduled backup</b></td><td>You can create a scheduled backup task for the project server.
1. On the list of installed apps, find the app and click <b>Open</b>. Go to the <b>Scheduled backup</b> page.
2. Specify the backup interval from the menu. The system regularly backs up the project server’s data following the specified interval.
3. After the backup is complete, a corresponding backup file appears in the <b>Backup history</b> page.</td></tr>
<tr><td><b>Backup history</b></td><td>You can export the project server’s data into a backup file. The backup file is useful for restoring the project server to a desired point in time. You can also delete data when needed.
To manage backup data, on the list of installed apps, find the app and click <b>Open</b>. Go to the <b>Backup history</b> page.
<table>
<tr><td><b>Exporting backup data</b></td><td>1. Select a desired backup file.
2. Click <b>Download</b> to download the backup file to the local computer.</td></tr>
<tr><td><b>Restoring backup data</b></td><td>1. Select a desired backup file.
2. Click <b>Restore</b> to restore data.</td></tr>
<tr><td><b>Deleting backup data</b></td><td>6. Select an unwanted backup file.
7. Click <b>Delete</b> to delete the backup file. Once deleted, the backup file cannot be recovered.</td></tr>
</table></td></tr>
</table>

Using Proxy Server

The proxy server function is presented with the features:

- Cache the web contents which clients have accessed
- Access control functions
- User authentication

<table>
<tr><td><b>Go to</b></td><td><b>Settings > Applications > Installed</b></td></tr>
<tr><td><b>Memory cache</b></td><td>1. On the list of installed apps, find the app and click <b>Open</b>.
2. Specify the following information to complete the settings:
<table>
<tr><td><b>Cache size (MB)</b></td><td>This specifies the memory size to be used as cache. The value should never exceed the available memory size. The default value is 16.</td></tr>
<tr><td><b>Maximum file size for memory cache (KB)</b></td><td>Files of sizes larger than this value will not be cached in memory.
The default value is 8.</td></tr>
</table>
3. Click <b>Save</b> to apply the settings.</td></tr>
<tr><td><b>Access control</b></td><td>You can add, edit, delete a rule or change a rule to higher priority or lower priority. On the list of installed apps, find the app and click <b>Open</b>. Go to the <b>Access control</b> page.
<table>
<tr><td><b>Adding a rule</b></td><td>1. Click <b>Add</b>.
2. Specify the following information to complete the settings:
<b>Action:</b> To allow or to deny the connections
<b>Type:</b> Specify the field to compare the connections with. The value can be one of <i>source IP</i>, <i>source host name</i>, <i>source MAC address</i>, <i>destination IP</i>, and <i>destination host name</i>.
<b>IP address:</b> The value of the specified field to be verified.
3. Click <b>OK</b> to save and apply the settings.</td></tr>
<tr><td><b>Edit a rule</b></td><td>1. Select the rule.
2. Click <b>Edit</b> and change the settings.
3. Click <b>OK</b> to save and apply the settings.</td></tr>
<tr><td><b>Delete a rule</b></td><td>3. Select the rule.
4. Click <b>Delete</b>.</td></tr>
</table></td></tr>
</table>

	Change priority of a rule 1. Select the rule. 2. Click **Up** or **Down** to change its priority. The higher a rule is in the list, the higher its priority.
Authentication	1. On the list of installed apps, find the app and click **Open**. 2. Enable user authentication by clicking the toggle switch.
Change the settings of the app	1. On the list of installed apps, find the app and click **Settings**. 2. Change the settings and click **OK** to save and apply.
Clear disk cache	1. On the list of installed apps, find the app and click **Clear disk cache**.

Using Syslog Server

Go to	**Settings > Applications > Installed**
View logs	1. On the list of installed apps, find the app and click **Open**. The fields of logs include *Severity, Facility, Hostname, Application, Time, and Message*. 2. If needed, click **Refresh** to update log data. **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.

Using VPN Server

Go to	**Settings > Applications > Installed**	
Connection list	You can view the connection status and disconnect a specific connection.	
	View connection status	On the list of installed apps, find the app and click **Open**. All connections are displayed in the list. If needed, click **Refresh** to see the latest status of connections.
	Have a connection terminated	1. Select the connection. 2. Click **Disconnect**.

Update & Security

The Update & Security setting menu contains the following sub-settings.

1. Security
2. Firmware Upgrade
3. Factory Reset

For cluster settings, the Update setting menu contains the following sub-settings.

1. Firmware Upgrade

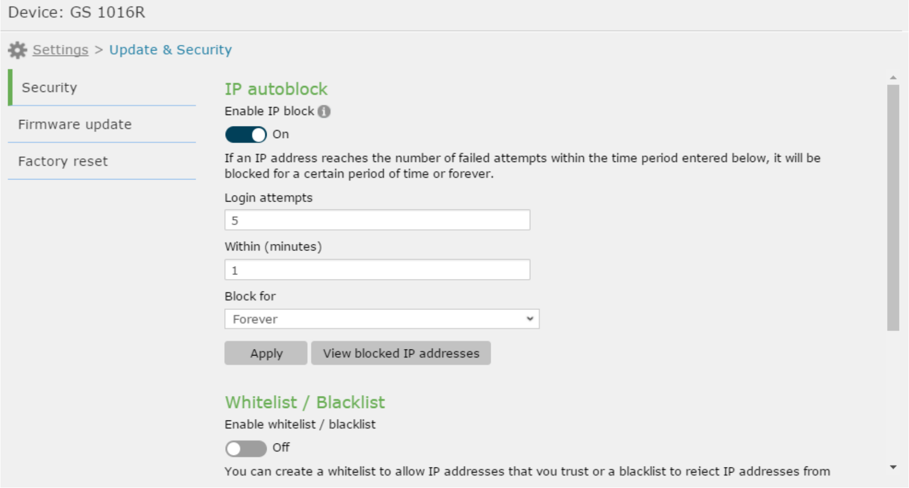
Security

IP autoblock: Access to EonStor GS/GSe 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.

Go to	**Settings / Device management > Update & Security > Security**
Enable IP autoblock	1. Switch **Enable IP block** to **ON**. **Note:** The supported services for IP autoblock include HTTP(s), FTP(s), AFP, Rsync, SSH/Telnet, VPN, and Amazon S3. **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: GS 1016R

Settings > Update & Security

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

Whitelist / Blacklist

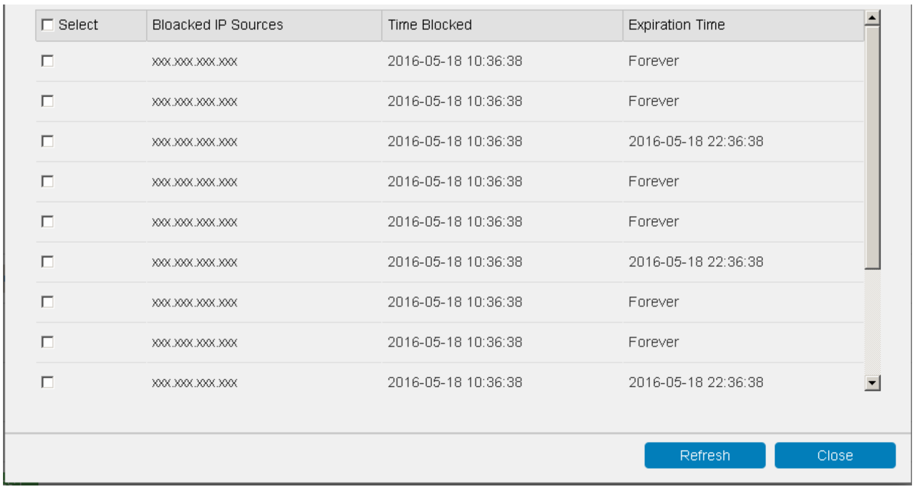
Enable whitelist / blacklist

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.



□ Select	Bloacked IP Sources	Time Blocked	Expiration Time
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	2016-05-18 22:36:38
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	2016-05-18 22:36:38
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	Forever
□	xxx.xxx.xxx.xxx	2016-05-18 10:36:38	2016-05-18 22:36:38

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 one or more IP addresses to the whitelist because the whitelist is empty.

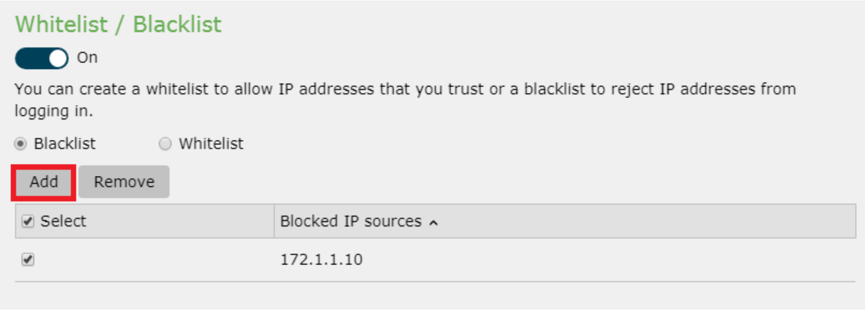
3. Change the activated list to the blacklist.

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.



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

☑ Select	Blocked IP sources ^
☑	172.1.1.10

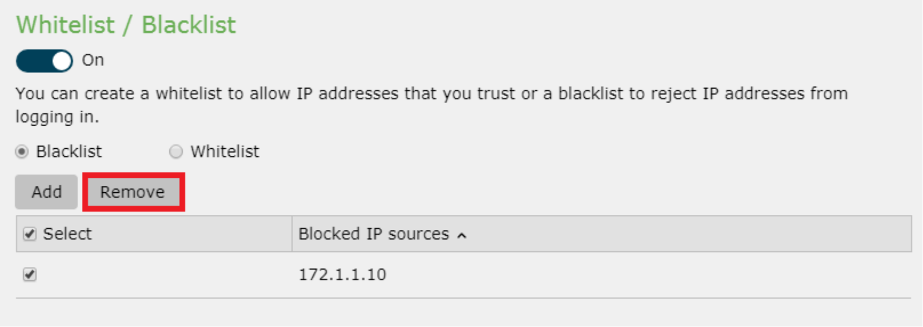
You can specify a single IP address or specify multiple IP addresses by their netmask or IP range.

Click **OK** to enable the settings.

When the scale-out cluster is enabled and a member appliance is added to the cluster, the management/data port IP address of the member appliance will be automatically added to the whitelist. Besides, these IP addresses cannot be deleted.

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

☑ Select	Blocked IP sources ^
☑	172.1.1.10

Firmware Update

Before starting the firmware update process, we recommend exporting the NVRAM file, which contains the configuration of the system. This file may be later imported back into the system in case of emergency. For the procedure of exporting the NVRAM file, see Exporting/Importing System Configuration.

Depending on the firmware version, some additional steps may be required. If you face any issues during the firmware update, please contact STORANDER technical support.

Note:

- Do not restart or turn off the computer, storage itself or any of its controllers. Doing so may result in an unrecoverable error that requires the service of the manufacturer.
- For dual-controller models, both controllers must share the same firmware version.

Go to **Settings / Device management > Update & Security > Firmware update**
Cluster settings > Update

Update Firmware

1. Check the current firmware version and the latest available firmware version and download it from Infortrend support site if necessary.
2. Upload the firmware file (.BIN) by clicking the **Browse** button.
3. Click **Update**.

Device to update

After HA service is enabled, you can choose to update the firmware on **this device** that you are accessing or **both devices in the HA storage**.

Firmware Package

The firmware package consists of the following files.

- **FAxyz_IFT_ESGS.BIN**: Firmware file is provided in the form of a binary file - FAxyz_IFT_ESGS.BIN, 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.

Rolling firmware update

For dual-controller models, after the firmware is updated on the primary controller, you will be prompted whether you want to restart the system or choose the Rolling Update function. Choose one of the following:

Rolling update The controllers apply the firmware update and restart one by one.

Note:

- Check the Release Note for the firmware to confirm if the Rolling Update feature is supported.
- During the controller synchronization window, the storage will be unavailable for I/O for approximately 30 seconds.

Restart	The controllers apply the firmware update and restart at the same time.

Factory Reset

Note: Restoring to default settings is the last resort to solving system errors as it will erases all system configurations. This task can only be done by a STORANDER engineer.

Pre-Restoration Works

Before you restore the default settings, save the current configurations:

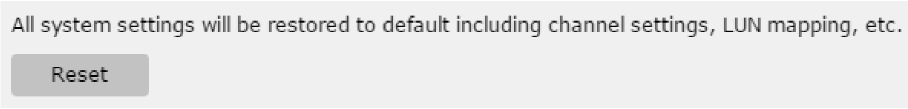
- Stop all host IOs.
- Export system configurations.
- Make a list of host ID/LUN mapping information.

Go to

Settings / Device management > Update & Security > Factory Reset

Factory Reset Menu

Click **Reset settings** to carry out Factory Reset. The EonStor GS/GSe will be reset to the original status.



All system settings will be restored to default including channel settings, LUN mapping, etc.

EonCloud Gateway

EonCloud Gateway is an enterprise-level hybrid cloud solution that integrates STORANDER 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 EonCloud 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, hicloud, and Hitachi Content Platform (HCP).
- 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 EonCloud Gateway license is installed on your STORANDER storage device by default.
- Before using EonCloud Gateway, ensure that you have correctly configured system time in **Settings** > **System** > **Time**.

The system setting menu contains the following sub-settings.

1. Quick Setup
2. Cloud Storage
3. Database

Quick Setup

EonCloud Gateway provides five quick setup methods to connect your local shared folders and local volumes to the cloud.

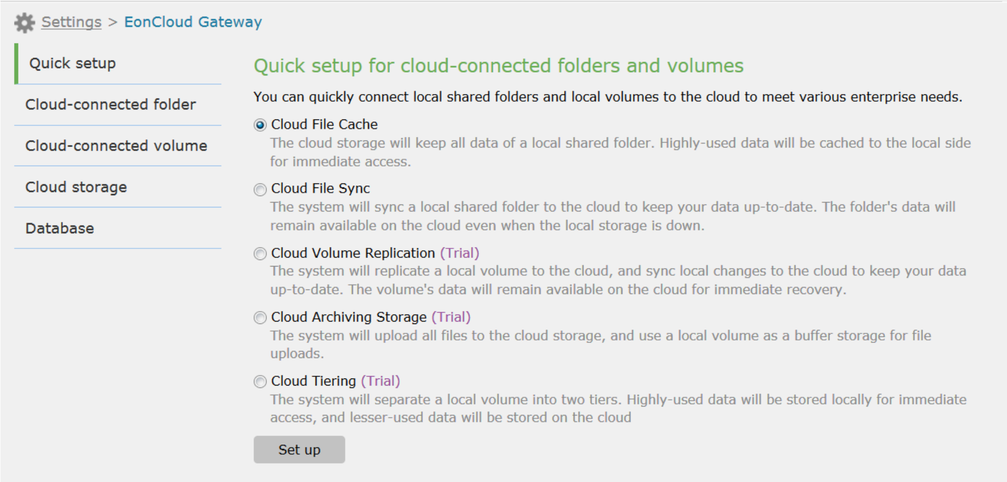
Five setup methods are available:

- **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 / Device management > EonCloud Gateway > Quick setup**



Quick setup for cloud-connected folders and volumes

You can quickly connect local shared folders and local volumes to the cloud to meet various enterprise needs.

● Cloud File Cache
The cloud storage will keep all data of a local shared folder. Highly-used data will be cached to the local side for immediate access.

○ Cloud File Sync
The system will sync a local shared folder to the cloud to keep your data up-to-date. The folder's data will remain available on the cloud even when the local storage is down.

○ Cloud Volume Replication (Trial)
The system will replicate a local volume to the cloud, and sync local changes to the cloud to keep your data up-to-date. The volume's data will remain available on the cloud for immediate recovery.

○ Cloud Archiving Storage (Trial)
The system will upload all files to the cloud storage, and use a local volume as a buffer storage for file uploads.

○ Cloud Tiering (Trial)
The system will separate a local volume into two tiers. Highly-used data will be stored locally for immediate access, and lesser-used data will be stored on the cloud

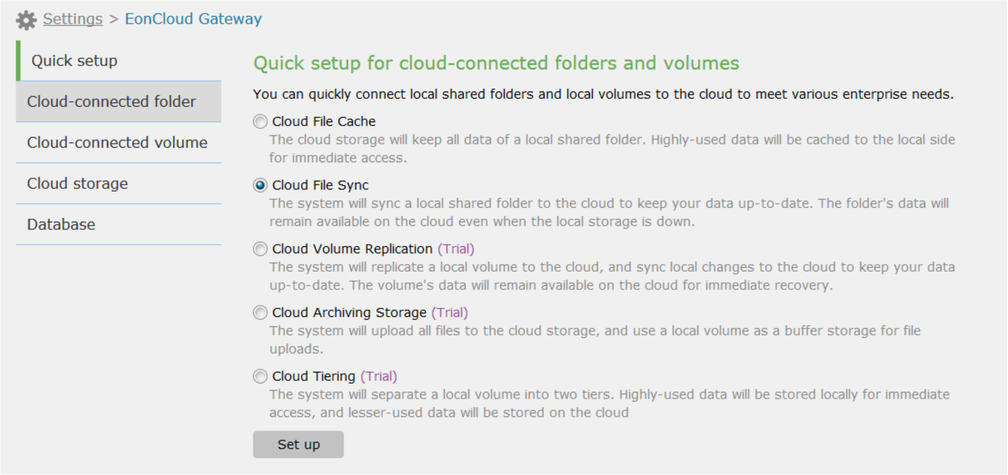
Steps

9. Select **Cloud File Cache** and click **Set up**.
10. Select a cloud storage to connect, or add one by clicking **+** (See Cloud Storage). Then, click **Next**.
11. Select a cloud storage folder to connect.
12. Select a local shared folder to connect, or add one by clicking **+**. Then, click **Next**.
13. Set **Local cache capacity** to reserve local space for caching highly-used data. Then, click **Next**.
14. Check the task settings. Then, confirm them by clicking **Create**.
15. The task is now listed at **EonCloud 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 / Device management > EonCloud Gateway > Quick setup**



Quick setup for cloud-connected folders and volumes

You can quickly connect local shared folders and local volumes to the cloud to meet various enterprise needs.

○ Cloud File Cache
The cloud storage will keep all data of a local shared folder. Highly-used data will be cached to the local side for immediate access.

● Cloud File Sync
The system will sync a local shared folder to the cloud to keep your data up-to-date. The folder's data will remain available on the cloud even when the local storage is down.

○ Cloud Volume Replication (Trial)
The system will replicate a local volume to the cloud, and sync local changes to the cloud to keep your data up-to-date. The volume's data will remain available on the cloud for immediate recovery.

○ Cloud Archiving Storage (Trial)
The system will upload all files to the cloud storage, and use a local volume as a buffer storage for file uploads.

○ Cloud Tiering (Trial)
The system will separate a local volume into two tiers. Highly-used data will be stored locally for immediate access, and lesser-used data will be stored on the cloud

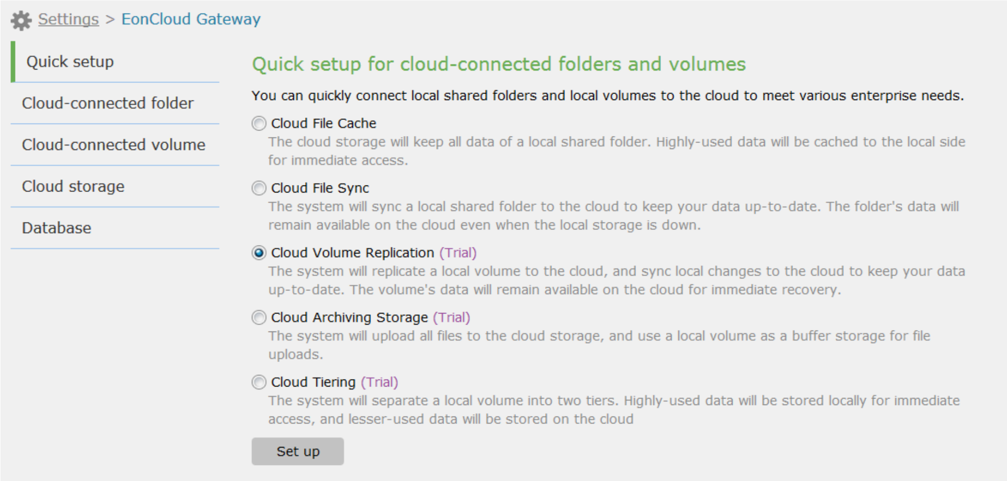
Steps

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 **EonCloud 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 / Device management > EonCloud Gateway > Quick setup**



Settings > EonCloud Gateway

Quick setup for cloud-connected folders and volumes

You can quickly connect local shared folders and local volumes to the cloud to meet various enterprise needs.

○ Cloud File Cache
The cloud storage will keep all data of a local shared folder. Highly-used data will be cached to the local side for immediate access.

○ Cloud File Sync
The system will sync a local shared folder to the cloud to keep your data up-to-date. The folder's data will remain available on the cloud even when the local storage is down.

● Cloud Volume Replication (Trial)
The system will replicate a local volume to the cloud, and sync local changes to the cloud to keep your data up-to-date. The volume's data will remain available on the cloud for immediate recovery.

○ Cloud Archiving Storage (Trial)
The system will upload all files to the cloud storage, and use a local volume as a buffer storage for file uploads.

○ Cloud Tiering (Trial)
The system will separate a local volume into two tiers. Highly-used data will be stored locally for immediate access, and lesser-used data will be stored on the cloud

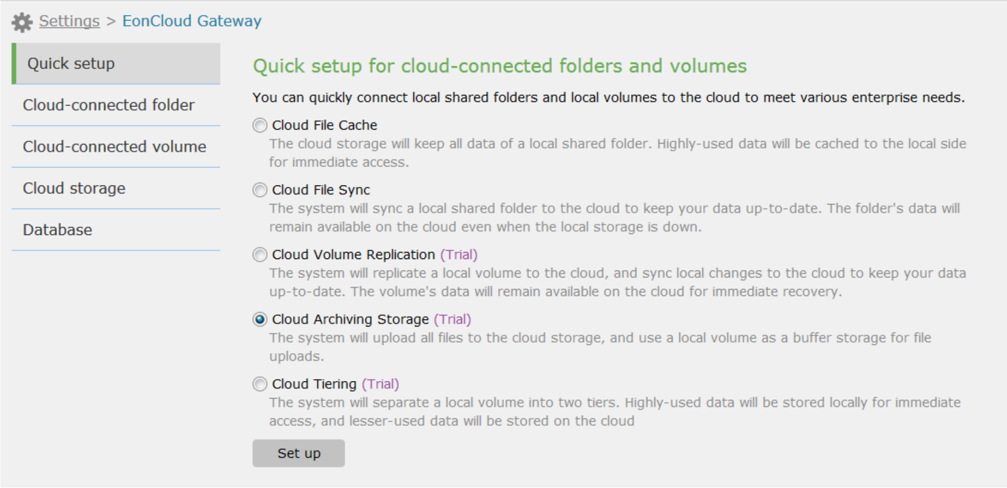
Steps

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 **EonCloud 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 / Device management > EonCloud Gateway > Quick setup**



Settings > EonCloud Gateway

Quick setup for cloud-connected folders and volumes

You can quickly connect local shared folders and local volumes to the cloud to meet various enterprise needs.

○ Cloud File Cache
The cloud storage will keep all data of a local shared folder. Highly-used data will be cached to the local side for immediate access.

○ Cloud File Sync
The system will sync a local shared folder to the cloud to keep your data up-to-date. The folder's data will remain available on the cloud even when the local storage is down.

○ Cloud Volume Replication (Trial)
The system will replicate a local volume to the cloud, and sync local changes to the cloud to keep your data up-to-date. The volume's data will remain available on the cloud for immediate recovery.

● Cloud Archiving Storage (Trial)
The system will upload all files to the cloud storage, and use a local volume as a buffer storage for file uploads.

○ Cloud Tiering (Trial)
The system will separate a local volume into two tiers. Highly-used data will be stored locally for immediate access, and lesser-used data will be stored on the cloud

Steps

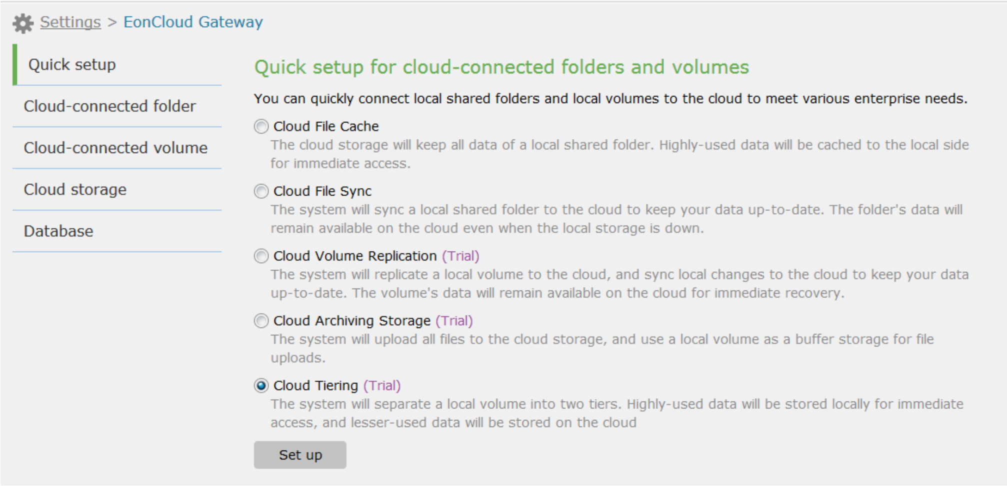
1. Select **Cloud Archiving Storage** and click **Set up**.
2. Select a cloud storage to connect, or add one by clicking **+** (See Cloud Storage). Then, click **Next**.
3. Select a local volume to connect to the cloud storage, or add one by clicking **+**.
4. Set **Local cache capacity** to reserve 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 **EonCloud 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 **Settings** > **Scheduling & Backup** > **Snapshot** > **Snapshot Schedule**.

Go to **Settings / Device management > EonCloud Gateway > Quick setup**



Quick setup for cloud-connected folders and volumes

You can quickly connect local shared folders and local volumes to the cloud to meet various enterprise needs.

○ Cloud File Cache
The cloud storage will keep all data of a local shared folder. Highly-used data will be cached to the local side for immediate access.

○ Cloud File Sync
The system will sync a local shared folder to the cloud to keep your data up-to-date. The folder's data will remain available on the cloud even when the local storage is down.

○ Cloud Volume Replication (Trial)
The system will replicate a local volume to the cloud, and sync local changes to the cloud to keep your data up-to-date. The volume's data will remain available on the cloud for immediate recovery.

○ Cloud Archiving Storage (Trial)
The system will upload all files to the cloud storage, and use a local volume as a buffer storage for file uploads.

● Cloud Tiering (Trial)
The system will separate a local volume into two tiers. Highly-used data will be stored locally for immediate access, and lesser-used data will be stored on the cloud

Set up

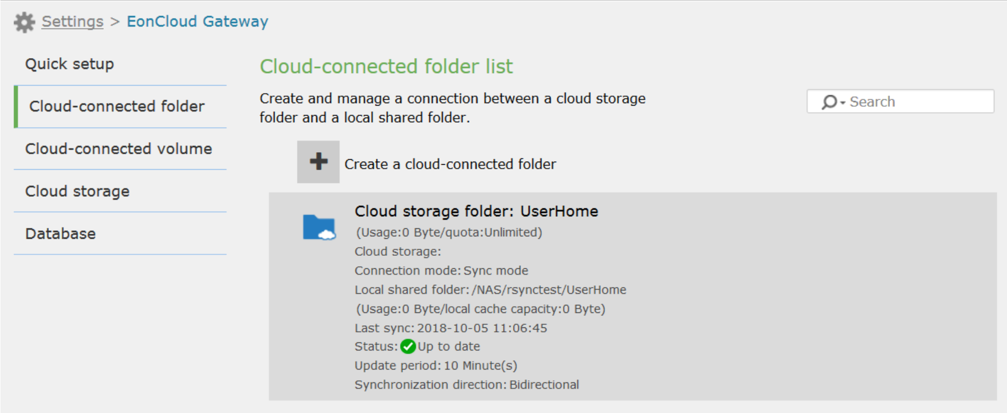
Steps

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 **EonCloud Gateway** > **Cloud-connected volume**. For further managements, click on the task entry and proceed.

Cloud-connected Folder

EonCloud Gateway provides detailed setup to create tasks that connect local shared folders with cloud storages.

Go to **Settings / Device management > EonCloud Gateway > Cloud-connected folder**



Cloud-connected folder list

Create and manage a connection between a cloud storage folder and a local shared folder.

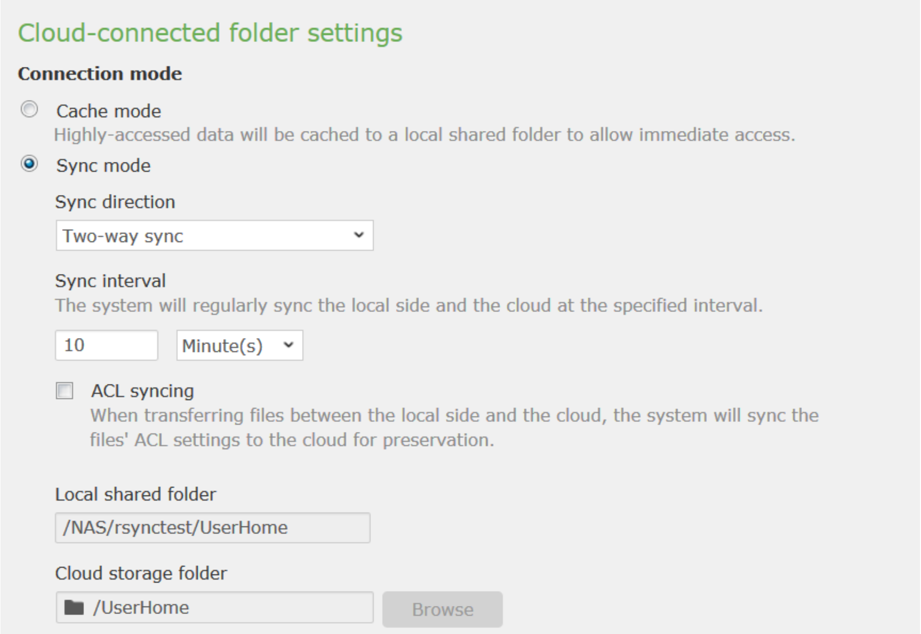
Cloud storage folder: UserHome
(Usage:0 Byte/quota:Unlimited)
Cloud storage:
Connection mode: Sync mode
Local shared folder: /NAS/rsynctest/UserHome
(Usage:0 Byte/local cache capacity:0 Byte)
Last sync: 2018-10-05 11:06:45
Status: ✓ Up to date
Update period: 10 Minute(s)
Synchronization direction: Bidirectional

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:

Cache mode 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.

Sync mode 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

4. To fine-tune the task, enable settings specific to the chosen connection mode:

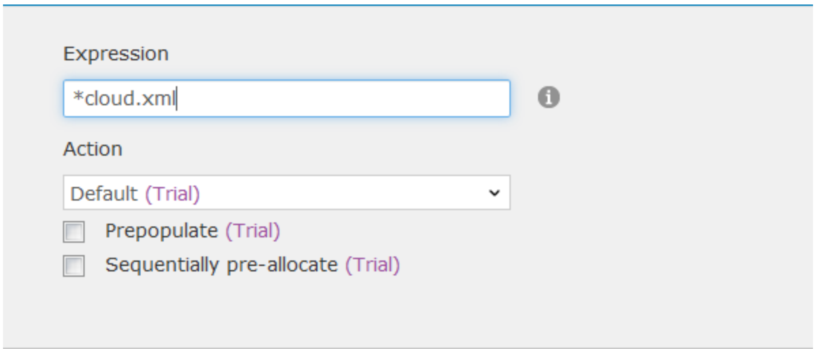
ACL syncing	The system will copy files' ACL settings to the cloud for preservation.
Instant cache update	When locally cached data are accessed, the system will immediately check the cloud and update the local cache.
Periodic cache update	The system will check the cloud to update the local cache at a specified interval.
Mark non-cached files by icon	When users browse files in the local shared folder via File Explorer or SMB, the system marks non-cached files with a different icon.
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 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	Set the maximum local capacity reserved for caching highly-used data.

Sync direction	Decide how to update changes between the local shared folder and the cloud: **Two-way sync**: The system will update all changes on the local shared folder or on the cloud to the other side. **Sync to the local side**: The system will update all changes on the cloud to the local shared folder. **Sync to the cloud**: The system will update all changes on the local shared folder to the cloud.
Sync interval	Decide how often the system syncs changes between the local shared folder and the cloud.

5. Select a local shared folder to connect, or add one by clicking **+**.
6. Select a cloud storage folder to connect.
7. 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:

Expression	Use a glob expression to specify files and folders that the cache policy will apply to. Use the wildcard “*” for multiple characters and “?” for a single character. You can enter up to 256 UTF-8 characters.
Action	Select a cache action to apply to files and folders specified in the glob expression: **Default**: 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. **High Priority**: The system will assign the highest retention priority to caches of specified files/folders, and will clear 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 up load 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)

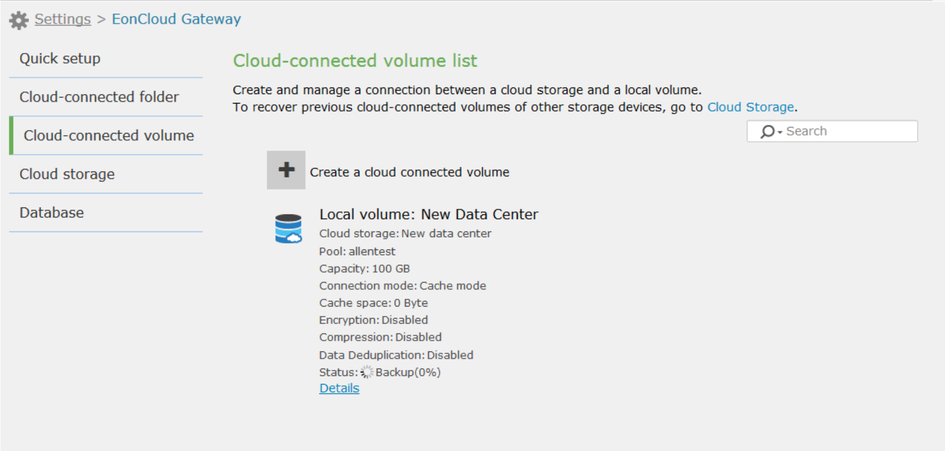
□ Sequentially pre-allocate (Trial)

8. You can reset policy priority by moving cache policies up or down. Cache polices at a higher position have higher priority than lower ones.
9. Click **OK** to finish the setup. The task is now listed at **EonCloud Gateway** > **Cloud-connected folder**.

Cloud-connected Volume

EonCloud Gateway provides detailed setup to create tasks that connect local volumes with cloud storages.

Go to **Settings / Device management > EonCloud Gateway > Cloud-connected volume**



Cloud-connected volume list

Create and manage a connection between a cloud storage and a local volume.
To recover previous cloud-connected volumes of other storage devices, go to Cloud Storage.

Local volume: New Data Center
Cloud storage: New data center
Pool: allentest
Capacity: 100 GB
Connection mode: Cache mode
Cache space: 0 Byte
Encryption: Disabled
Compression: Disabled
Data Deduplication: Disabled
Status: Backup(0%)

Steps

1. Click **Create a cloud connected volume** to set up a task.

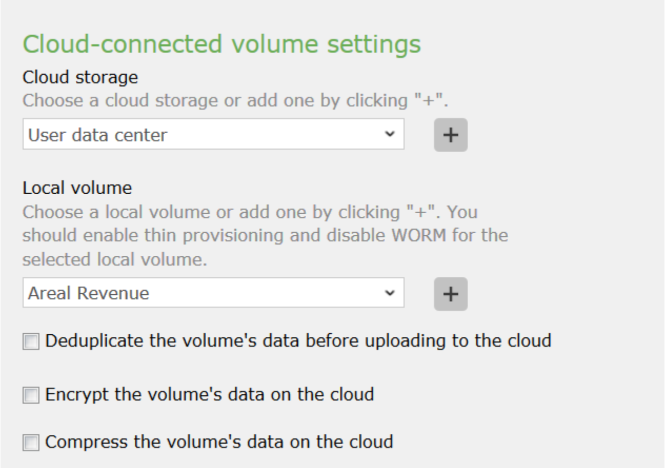
2. On the pop-up, select a cloud storage to connect, or add one by clicking **+** (See Cloud Storage).

3. Select a local volume to connect, or add one by clicking **+**.

   Note: When selecting a local volume, only thin-provisioning volumes are available for you to choose.

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 +

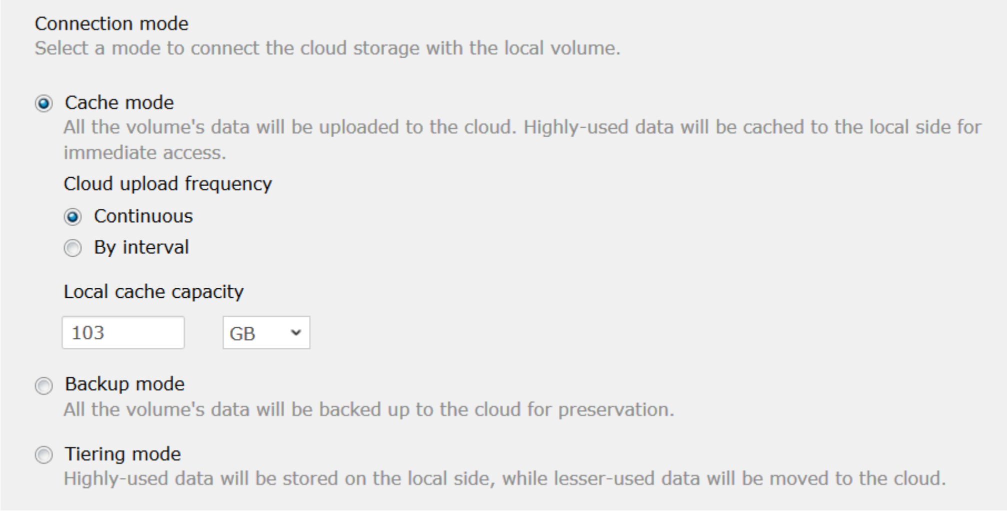
□ Deduplicate the volume's data before uploading to the cloud

□ Encrypt the volume's data on the cloud

□ Compress the volume's data on the cloud

5. Choose a connection mode:

Cache mode	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.
Backup mode	The system will back up the volume’s data to the cloud.
Tiering mode	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 **EonCloud Gateway** > **Cloud-connected volume**.

8. For a cloud-connected volume, you can do the following managements:

Pause	Stop data transfer between the local volume and the cloud. **Pause upload**: The local volume stops transferring data to the cloud. **Pause upload and download**: The local volume and the cloud stop mutual data transfer. To resume the data transfer, click **Resume** to recover the connection between the local volume and the cloud.
Edit	Edit the connection's configuration profile.
Delete	Delete the connection's configuration profile and end the data transfer between the local volume and the cloud. The data on the local volume and the cloud remain available.

Cloud Storage

Creating Cloud Storage

You can create a list of available cloud storages that are ready to connect to your local storage.

Go to	**Settings / Device management > EonCloud Gateway > Cloud storage**

Steps

1. Click **Create a cloud storage**.
2. On the pop-up, select a desired cloud service provider: **Aliyun**, **Amazon S3**, **KT ucloud**, **Microsoft Azure**, **OpenStack Swift, Tencent Cloud**, **Baidu Cloud**, **Backblaze**, **Google Cloud**, **Wasabi Cloud**, **Yandex Cloud**, **hicloud**, or **Hitachi Content Platform**.

   Note: For Google Cloud users, prerequisite settings on Google Cloud is required. For more details, see Setting up an OAuth Client ID for EonCloud Gateway.
3. Provide authentication credentials for login to the cloud service. Required information varies with cloud service providers.

Service IP/Port	Provide the OpenStack Swift server's IP and access port.
Access key **Authentication code**	Provide the first access key or authentication code acquired from the cloud service provider. For Google Cloud users, after logging in your account, the authentication code will be automatically displayed in the field.
Key **Secret key** **Client secret**	Provide the second access key acquired from the cloud service provider.
Project ID **Domain ID** **App ID** **Client ID**	Provide the ID acquired from the cloud service provider.
Endpoint	Select how to set up a communication channel with the cloud storage: **Auto**, **Manual**, and **Customize**.

	Then, fill in the fields with required information.
Region	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 **EonCloud Gateway** > **Cloud storage**.
11. For further managements, click on the cloud storage entry and proceed.

Access Control Management

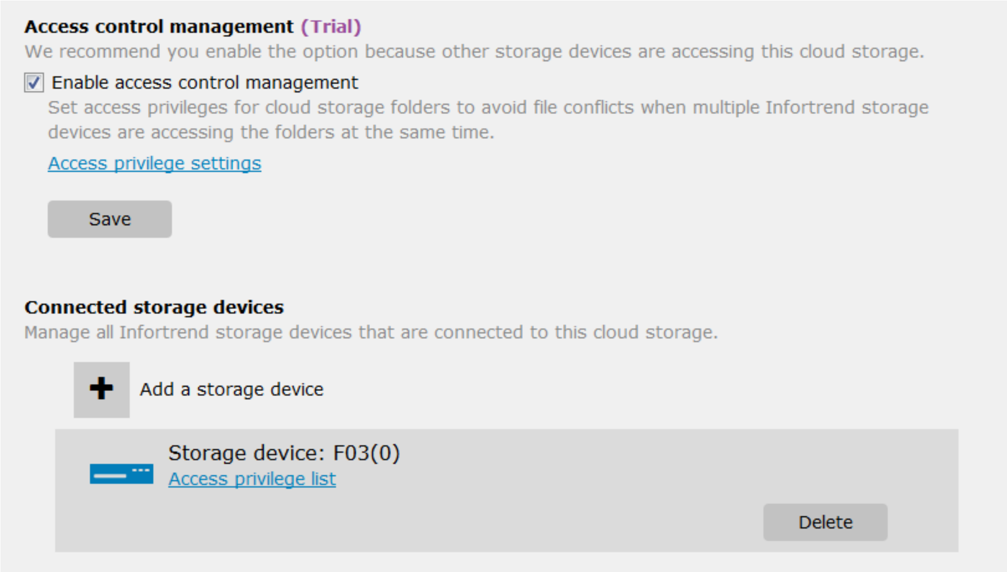
After you connect different storage devices to the same cloud storage bucket, you can enable access control management to avoid access conflicts.

Note: Access control management is only available to file-level cloud storages.

Go to **Settings / Device management > EonCloud Gateway > Cloud storage**

Steps

1. Click on a cloud storage that is connected with local shared folders on different storage devices.
2. Click **Edit**.
3. On the pop-up, select **Enable access control management** and click **Save**.



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

Connected storage devices

Manage all Infortrend storage devices that are connected to this cloud storage.

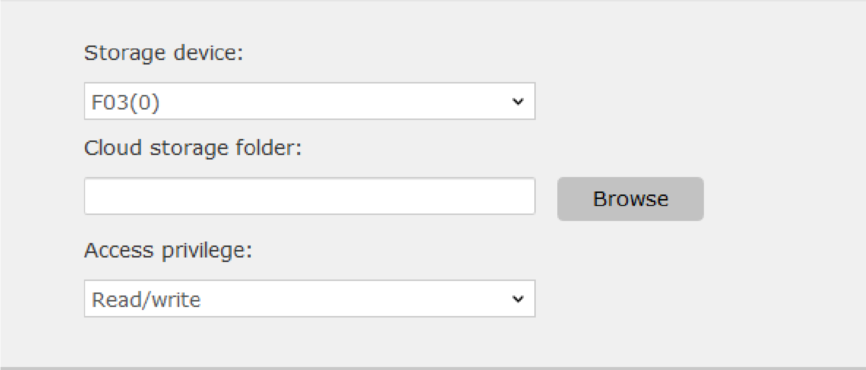
Storage device: F03(0)

Access privilege list

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:

Storage device	Select a connected storage device.
Cloud storage folder	Click **Browse** to select a cloud storage folder.
Access privilege	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.



Storage device:

F03(0)

Cloud storage folder:

Access privilege:

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**.

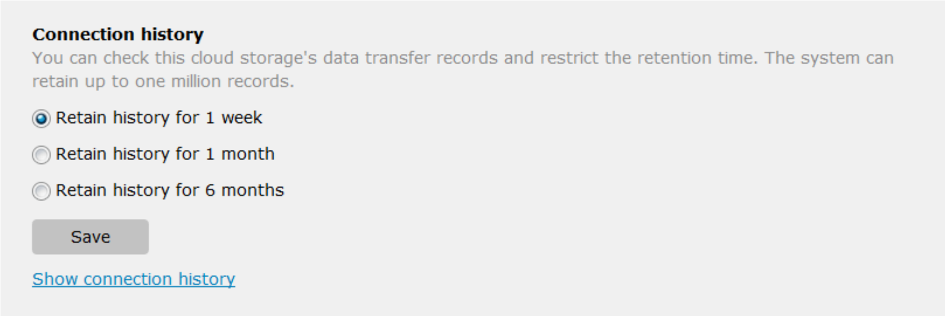
Connection History

The system logs data transfers between the local storage and the cloud storage for monitoring.

Go to **Settings / Device management > EonCloud Gateway > Cloud storage**

Steps

1. Click on a cloud storage entry and click **Edit**.
2. Go to the **Connection history** section.
3. Select how long the system should retain connection records: **Retain history for 1 week**, **Retain history for 1 month**, or **Retain history for 6 months**.



Connection history

You can check this cloud storage's data transfer records and restrict the retention time. The system can retain up to one million records.

● Retain history for 1 week

○ Retain history for 1 month

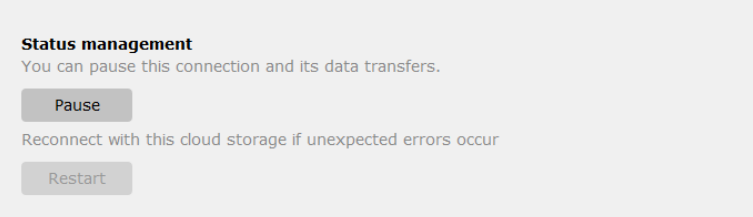
○ Retain history for 6 months

4. Click **Save** to finish the setup.
5. To view existing connection records, click **Show connection history**. To export the connection history, click **Export** on the connection history page.

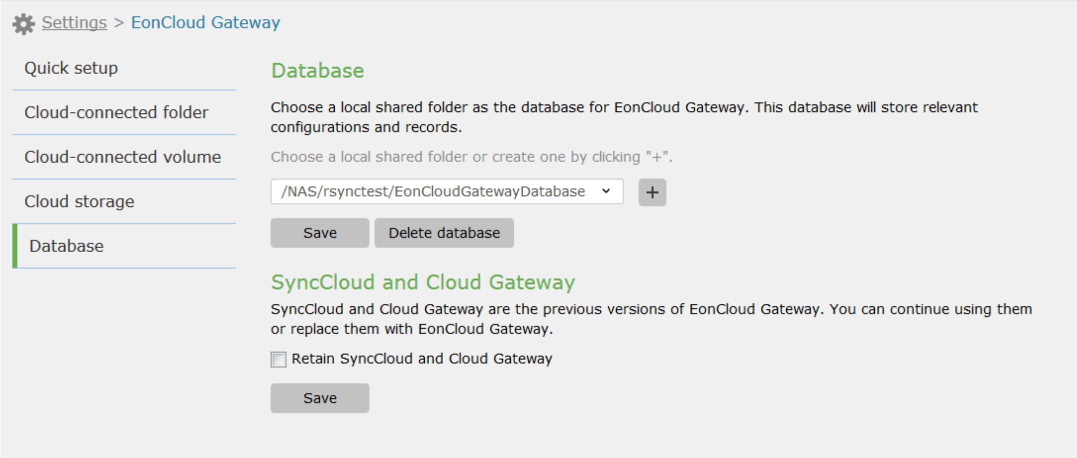
Status Management

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 / Device management > EonCloud Gateway > Cloud storage**
Steps	1. Click on a cloud storage entry and click **Edit**. 2. Go to the **Status management** section. 3. Click **Pause** to pause the connection; to reconnect the local storage with the cloud storage, click **Restart**.  **Status management** You can pause this connection and its data transfers. Reconnect with this cloud storage if unexpected errors occur

Database



Settings > EonCloud Gateway

Database

Choose a local shared folder as the database for EonCloud Gateway. This database will store relevant configurations and records.

Choose a local shared folder or create one by clicking "+".

/NAS/rsynctest/EonCloudGatewayDatabase

SyncCloud and Cloud Gateway

SyncCloud and Cloud Gateway are the previous versions of EonCloud Gateway. You can continue using them or replace them with EonCloud Gateway.

□ Retain SyncCloud and Cloud Gateway

Database

EonCloud 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.

Go to	**Settings / Device management > EonCloud Gateway > Database > Database**
Steps	1. Select an available local shared folder, or click **+** to create one. 2. Click **Save** to finish the setup. 3. To delete the database from the local shared folder, click **Delete database**. All data in the deleted database can never be recovered.

SyncCloud and Cloud Gateway

SyncCloud and Cloud Gateway are legacy versions of EonCloud Gateway. You can retain the two legacy versions or upgrade them to EonCloud Gateway.

Go to	**Settings / Device management > EonCloud Gateway > Database > SyncCloud and Cloud Gateway**
Steps	1. Select **Retain SyncCloud and Cloud Gateway**. 2. Click **Save** to finish the setup.

Cluster

You can improve storage capacity and performance by integrating several storage devices into one file cluster.

The cluster setting menu contains the following sub-settings.

1. General
2. File cluster
3. Maintenance

General

Enabling the Scale-out Cluster

Once your appliances are connected with each other, you can turn the appliances into a storage cluster to store block data or both file and block types of data.

Note: You can only enable the cluster via the master appliance.

Go to	**Settings / Device management > Cluster > General**
Steps	1. Turn on the scale-out function. 2. Specify an identifying name for the cluster. 3. Click **Save** to save the settings. The appliance role and the cluster name will be then displayed.

File cluster

Enabling the File Cluster

After the scale-out cluster is enabled, you can enable file cluster to manage file-level data service on all appliances in the cluster.

Note: To run a snapshot-taking task, make sure that every appliance in the cluster has installed a file scale-out license and a snapshot license.

Go to	**Settings > System > File cluster**

Steps

1. Turn on the file cluster function.
2. Specify the file cluster settings:

Root shared folder name	Specify an identifying name for the cluster's root shared folder. The root folder is responsible for storing mappings between cluster volumes and appliances.
Cluster root volume	Choose a volume as the cluster's root volume from the list. Only qualified file volumes appear in the list: ● A volume in a RAID1, RAID5, or RAID6 storage pool ● A volume that is not used to run Docker ● A volume that is not set as a WORM volume

3. CIFS/SMB is pre-selected.

   If needed, change the following file protocol settings:

File protocols	Choose how to encrypt the CIFS/SMB connection from the menu: **Allow only unencrypted connections**, **No restriction**, or **Allow only encrypted connections**. You can enable other functions to suit your needs: **Enable access-based enumeration**: This option hides folders or resources that the user is not allowed access to. **Enhance SMB compatibility with macOS and iOS clients**:

	This option increases compatibility of an SMB client running on the macOS system. **Transfer files in asynchronous mode**: This option allows the system to transfer files asynchronously to minimize file transfer wait time and avoid transfer bottlenecks.
NFS	Select to enable the NFS protocol.

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

5. After enabling, go to **Data ports** section to find the IP addresses that you can use to access the file cluster.

6. If needed, enable File explorer. See File explorer for more details.

   After File explorer is enabled, you can click **File explorer** to access local shared folders and attached USB storage devices with a web browser.

Maintenance

It is able to run a backup of the cluster's configurations, and the backup can be exported for future system recovery.

Backing up/Exporting the Cluster Configurations

Go to **Settings / Device management > Cluster > Maintenance**

Steps

1. Go to the **Last backup time** section. You can check when the last time the cluster ran a backup.
2. Go to the **Export cluster configurations** section. Click **Export** to export current cluster configurations for system recovery.

HA Service

You can enable both file-level HA service and block-level HA service, or enable only one of them depending on your need.

- Block-level HA service

Block-level HA service is an active-active solution to remote backup and disaster recovery, ensuring high availability of data access across different sites of data centers. With deployments of two storage devices and a witness server, data can be stored and managed in the HA storage. The arbitration mechanism enables the witness server to determine which device should take over the service in an event of a disaster, allowing continuous access to the storage for users. Hosts can access the storage via Fibre Channel or iSCSI.

- File-level HA service

File-level HA service, on the other hand, is an active-passive solution to service continuity. The active device provides access to data and handles all the requests. The passive device remains on standby and is unavailable until the active device fails. Hosts can access the storage via CIFS/SMB, NFS, FTP, etc.

Note: To use block-level HA service and file-level HA service at the same time, you must use the same two storage devices and pair them with each other. For example, if device A has been paired with device B and block-level HA service has been enabled on these two devices, when you are going to enable file-level HA service on device A, it can only be paired with device B other than any other devices.

The HA service menu contains the following sub-settings.

1. General
2. Block-level HA service
3. File-level HA service
4. Witness Server
5. Networks
6. Maintenance
7. Backup & Restore

General

View the status of block-level HA service and/or file-level HA service.

When HA service is enabled, in the HA storage information section, the information of both storage devices are displayed. If needed, click **Details** to view more information about each device.

Enabling Block-level HA Service and/or File-level HA Service

Enable HA service to manage your data and ensure high availability of your data access. After either one of these HA services is enabled, some settings will be synced between these two storage devices.

For block-level HA service, the following settings of the device to be paired with will be changed during the initialization: TLS certificate, time, notification, initiators, channels and trunk, and VMware configurations. After the service is successfully enabled, these settings above will sync between the two devices. If needed, you can change any one of these settings via one of the devices. The changes will be synced on both.

For file-level HA service, all file services on the device to be paired with will be cleared at first, and then synced with the device that initiates the pairing.

Note:

- When the first-time initialization is completed, you must restart the two devices for HA service to take effect.
- For specific SAS HDD models with pre-configured U.2 NVMe SSDs, when file-level HA service is successfully enabled, the system only supports read cache.

Go to	**Settings > HA service > General**
Steps	1. If HA service has never been enabled on your storage device, check the Before you start section to prepare the two storage devices. Click **Start HA service**. If either block-level HA service or file-level HA service has been enabled, turn on the currently desired service to enable it by clicking the toggle switch. 2. Specify the device management IP and the password of the device that is going to be paired with. Select **Enable block-level HA service** and/or **Enable file-level HA service**. Click **Next**. 3. Choose the network type and the channels/trunk groups of the internal network. Click **Next**. 4. Specify at least one IP address and the port of the witness server. It is optional to provide another IP address in case any connection problem occurred. Choose the

channels of the witness network. Click **Next**.

5. (Optional) For file-level HA service, the system will create one or more volumes on the paired device, which correspond to the file-level volumes on the active device, so that there will be file-level volume pairs on both device. Check the one or more volume pairs. Click **Next**.

   If you want a specific volume to be created in another pool on the passive device, select the volume and click **Select pool**. When completing selecting another pool, click **OK** to go back to the volume pairs page. Click **Next**.

6. View the summary of the settings. If any setting needs to be modified, click **Previous**. To continue, click **Next**.

7. Check these configurations. To continue, click **Next**. If not, click **Cancel**.

8. HA service starts to initialize. Click **Close** when the initialization is completed. You will be prompted to restart the system on the two devices for HA service to take effect. Click **Yes** to confirm the action and restart the system.

   For more information about restarting the system, refer to General.

Disabling Block-level HA Service

Note: After you disable the service and there is no HA service is enabled, you must restart the two devices for HA service to take effect.

Go to	**Settings > HA service > General**
Steps	1. Make sure all HA volumes have been disassociated or deleted. 2. Turn off block-level HA service by clicking the toggle switch.

Disabling File-level HA Service

After you disable file-level HA service, all the HA volumes will turn into normal volumes and the data will be kept on the device which is used to be active device.

Note: After you disable the service and there is no HA service is enabled, you must restart the two devices for HA service to take effect.

Go to	**Settings > HA service > General**
Steps	1. Turn off file-level HA service by clicking the toggle switch.

Block-level HA Service

Create an HA volume on both primary and secondary devices to manage block-level data.

Checking the Overview of Block-level HA Service

Go to	**Settings > HA service > Block-level HA service**
Steps	Go to Block-level HA service section. Check the following information about the service:

Status	View the status of HA service. If there is any error, check the error message here for troubleshooting.
Status of the individual device	View the status of individual storage device.
Number of HA volumes	View the number of HA volumes. You can create up to 16 HA volumes.

Adding an HA Volume

Go to	**Settings > HA service > Block-level HA service**

Steps

1. Click **Add an HA volume**.

2. Go to Add an HA volume section:

Volume name	Specify an identify name for the HA volume.
Primary device	Choose which device is the primary device.
A pool for primary/secondary device	Check each pool on the primary/secondary device which are suggested by the system. To choose other pools rather than those suggested, click **Browse**. Select a pool for primary/secondary device: select the desired controller, and select a pool which resides on the controller from the list. Click **OK** to save the settings.
Volume size	Specify the volume size.
Auto failback	If needed, check **Auto failback** to enable this function.

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

Editing an HA Volume

You can change the primary device of the HA volume, and enable/disable auto failback function.

Go to	**Settings > HA service > Block-level HA service**
Steps	1. Select the desired volume from the list. Click **Edit**. 2. Go to Edit an HA volume section:

Primary device	If needed, select the other device to be the primary device.
A pool for primary/secondary device	If the volume on the primary or secondary device is lost, click **Browse** to select a pool again.
Auto failback	If needed, check **Auto failback** to enable or disable this function.

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

Managing an HA Volume

You can expand an HA volume, or map an HA volume to a LUN.

Go to	**Settings > HA service > Block-level HA service**
Steps	Select the desired volume from the list.
Expanding an HA volume	Click **Expand**. Refer to Expanding a volume.
Mapping an HA volume to a LUN	Click **Map to host**. Refer to Mapping a volume to LUN.

Switching over Devices to Provide the Service

You can change which device to provide HA service by switching over. For example, if currently the service is provided by device A, after switching over, the service will be then provided by device B, and vice versa. During the process, the service will not be interrupted.

Please note that switching over will not change the primary device of the HA volume. If you need to change the primary device, see Editing an HA volume for more details.

Note: Auto failback function will be disabled after switching over.

Go to **Settings > HA service > Block-level HA service**

Steps

1. Select the desired volume from the list.
2. Click **More** and select **Switchover** option.
3. To confirm the action, click **Yes** and change the device to provide the service.

Disassociating an HA Volume

You can disassociate an HA volume, which means cancelling the pairing relationship between the HA volume on its primary device and its secondary device. After disassociation, the data is still accessible via one of the devices.

Go to **Settings > HA service > Block-level HA service**

Steps

1. Select the desired volume from the list.
2. Click **More** and select **Disassociate** option.
3. To confirm the action, click **Yes** to disassociate the HA volume.

Deleting an HA Volume

Go to	**Settings > HA service > Block-level HA service**
Steps	1. Select the desired volume from the list. 2. Click **More** and select **Delete** option. 3. To confirm the action, click **Yes** to delete the volume.

File-level HA Service

Create an HA volume pairs on both active device and passive device to manage file-level data.

Checking the Overview of File-level HA Service

Go to **Settings > HA service > File-level HA service**

Steps Go to File-level HA service section. Check the following information about the service:

Status	View the status of HA service. If there is any error, check the error message here for troubleshooting.
Number of HA volumes	View the number of HA volumes. You can create up to 16 HA volumes.
Active device	View the device name of the active device.
Passive device	View the device name of the passive device.

Adding an HA Volume

Note:

- For file-level HA service, adding an HA volume is only available on the active device.
- The source pool on the active device and the target pool on the passive device must be on the same controller. For example, if the source pool is on the controller A of the active device, you can only choose the pools on the controller A of the passive device.

Go to	**Settings > HA service > File-level HA service**
Steps	1. Click **Add an HA volume**. 2. Go to Add an HA volume section:

Pool	Select a pool on the active device for the volume to claim capacity.
Target pool on the passive device	Select a pool on the passive device.
Volume Name	Enter the name of the volume.
Enable case-insensitive file and folder names	Enable this option so that the system does not distinguish folders or files sharing the same name but in different cases. For example, folders named “xyz” and “XYZ” are treated as the same.
Volume Size	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. **Note:** The minimum size of a volume is 10GB.
Advanced ACL	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.
Enable WORM	Enable WORM (Write Once Read Many) functionalities. Refer to Creating a WORM Volume for more details.

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

Managing an HA Volume

You can manage an HA volume including configuring the HA volume, expanding the volume size, setting a threshold for the volume usage, etc.

Note: If an HA volume is unmounted, it cannot be expanded or set a threshold for its usage.

Go to	**Settings > HA service > File-level HA service**
Expand volume	**1.** Select the desired volume from the list. **2.** Click **Expand volume**. For more details, refer to Expanding a volume.
Configure volume	1. Select the desired volume from the list. 2. Click **Configure volume**. 3. To change advanced ACL settings, select the checkbox. 4. Click **OK** to save the settings.
Set a threshold	1. Select the desired volume from the list. 3. Click **Threshold**. For more details, refer to Setting a Volume Threshold.
Mount/Unmount a volume	**1.** Select the desired volume from the list. 2. To unmount the volume, click **More** and select **Unmount** option. To mount the volume, click **More** and select **Mount** option. 2. For more details, refer to Mounting/Unmounting a Volume.
Defragmentation	**1.** Select the desired volume from the list. 2. Click **More** and select **Defragmentation** option. For more details, refer to Defragmenting a Volume.

Switching over Devices to Provide the Service

You can change which device to provide HA service by switching over. For example, currently the service is provided by device A, which is the active device; after switching over, the service will be then provided by device B, and device B is now the active device.

Note: This functionality is only available on the active device.

Go to	**Settings > HA service > File-level HA service**
Steps	1. Go to the File-level HA service section. Click **Switchover**. 2. To confirm the action, click **Yes** and change the device to provide the service.

Repairing an HA Volume

When there has been a problem during creating an HA volume pair, the data will only be stored on the active device without syncing to the passive device. You can repair the volume pair to ensure the data can be synced.

Go to	**Settings > HA service > File-level HA service**
Steps	1. Select the desired volume from the list. 2. Click **Repair**.

Deleting an HA Volume

Go to	**Settings > HA service > File-level HA service**
Steps	1. Select the desired volume from the list. 2. When the HA volume status is OK and provides the service normally, click **More** and select **Delete** option. When the HA volume status is error and fails to provide the service, click **Delete**.

Witness Server

The witness server is located at a site that is different from where the other two storage devices are located. The arbitration mechanism enables the witness server to determine which device should take over the service in an event of a disaster.

Editing the IP Address of the Witness Server

If needed, update the settings of the witness server to remain the connection between the witness server and the HA storage.

Go to	**Settings > HA service > Witness server**
Steps	1. Click **Edit**. 2. Go to Edit witness server section. Change one or both of the IP addresses and the port of the witness server. 3. Click **OK** to save the settings.

Changing the Witness Server

Go to	**Settings > HA service > Witness server**
Steps	1. Click **Edit**. 2. Go to Edit witness server section. Change the IP address and the port to those of the new witness server. 3. The system will indicate that an unknown witness server has been detected. Click **Yes** to change the witness server.

Networks

You can change the channels/trunk groups being in use by the internal network and the witness network.

Changing the Channels/Trunk Groups of the Internal/Witness Network

Note: When the channels/trunk groups used in the internal network have been changed, you must restart the system for the changes to take effect.

Go to	**Settings > HA service > Networks**
Steps	1. Click **Edit** in the internal/witness network section. 2. Go to Edit internal/witness network section. Select another available channel/trunk group. If a channel/trunk group has been in use, you can check its information by hovering the info icon next to it. 3. Click **OK** to save the settings. When editing the internal network, restart the system for the changes to take effect. For more information about restarting the system, refer to General.

Maintenance

You can pause one of the two devices for maintenance and have it resume when finished, and still have continuous data access during the process.

Pausing a Device or Having a Device Resume in the HA Storage

Go to	**Settings > HA service > Maintenance**
Pause a device	1. Click **Pause (device name)** to pause the desired device. 2. To confirm the action, click **OK** to pause the device.
Have a device resume	1. Click **Resume (device name)** to have the device resumed. 2. To confirm the action, click **OK** to have the device resumed.

Backup & Restore

Back up the configurations of the HA storage manually or by schedule.

Backing up and Exporting the Configurations of the HA Volume

Go to	**Settings > HA service > Backup & restore**
Manually backup	1. Go to the **Last backup time** section. You can check when the last time the HA storage ran backup. 2. Click **Back up now** to manually back up the HA storage configurations.
Backup by schedule	1. Configure the backup schedule by choosing the frequency of **Every week** or **Every month**. 2. Click **Save** to save the settings.
Export the configurations	1. Go to the **Export HA storage configurations** section. 2. Click **Export** to export current configurations for future system recovery. A zip file will be then generated.

Appendix

Working with iSCSI Initiator

This option is available only for iSCSI host models.

Configuration Steps for iSCSI Initiator

1. Get the IQN name in the subsystem.
2. Configure IQN (iSCSI Qualified Name) in the OS.
3. Configure CHAP authentication in the OS.
4. Configure the iSCSI Initiator in the subsystem.

Acquiring the IQN Name

STORANDER's storage IQN is composed of the system serial number and 3 more digits in the following format:

iqn.2002-10.com.infortrend:raid.snXXXXXX.XXX

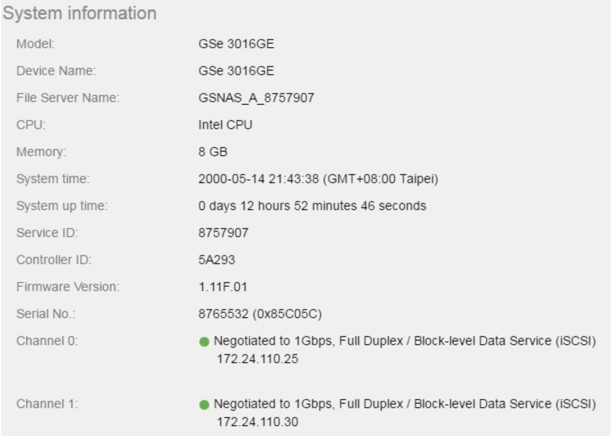
- A serial number of 6 digits follows "sn."
- The next 3 digits are: channel number, host ID and LD ownership.

The LD ownership digit is either "1" or "2" where "1" indicates Controller A and "2" indicates Controller B.

The IQN is in accordance with how you map your logical drive to the host ID/LUN. For example, if you map a logical drive to host channel 0 and AID1, the last 3 digits will be 011.

For firmware version prior to 3.64, only two digits follow the serial number: channel and host ID.

Go to Setting> System Settings > System Information



System information

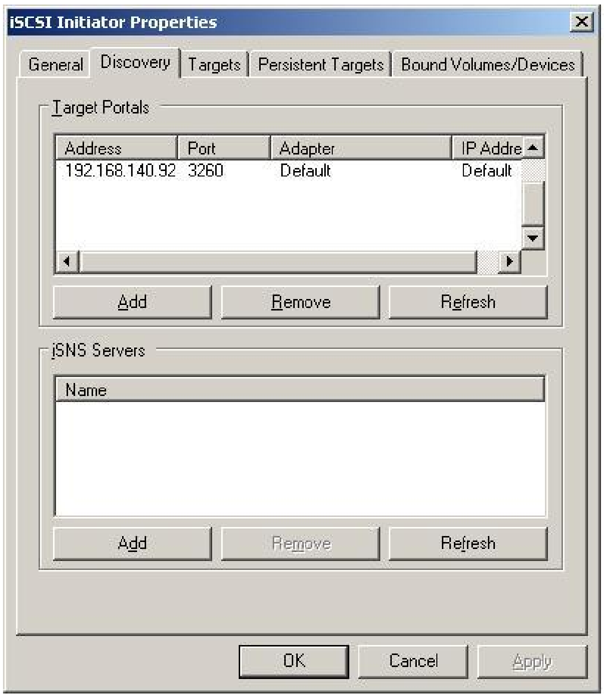
Model:	GSe 3016GE
Device Name:	GSe 3016GE
File Server Name:	GSNAS_A_8757907
CPU:	Intel CPU
Memory:	8 GB
System time:	2000-05-14 21:43:38 (GMT+08:00 Taipei)
System up time:	0 days 12 hours 52 minutes 46 seconds
Service ID:	8757907
Controller ID:	5A293
Firmware Version:	1.11F.01
Serial No.:	8765532 (0x85C05C)
Channel 0:	● Negotiated to 1Gbps, Full Duplex / Block-level Data Service (iSCSI) 172.24.110.25
Channel 1:	● Negotiated to 1Gbps, Full Duplex / Block-level Data Service (iSCSI) 172.24.110.30

Configuring iSCSI Initiator (Windows OS)

Here we introduce how to configure iSCSI initiator in Windows OS environment.

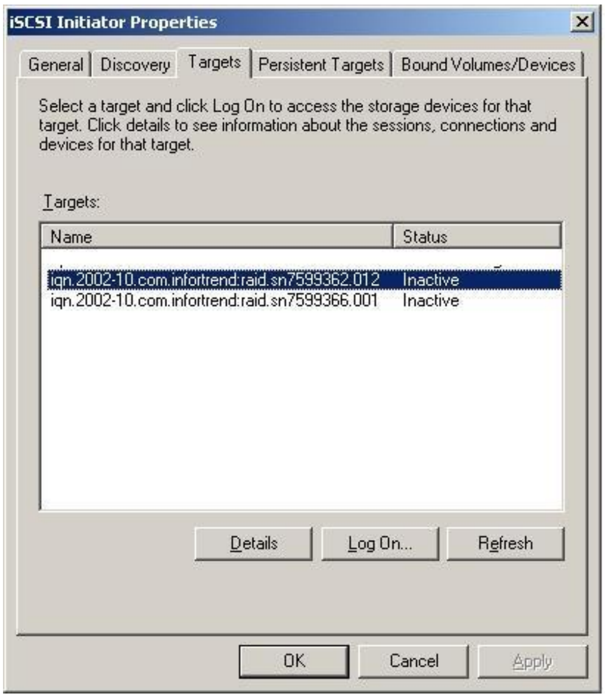
Step 1:
Setting the Target Address

5. Open the iSCSI initiator properties windows and manually key in the target port address, e.g., 192.168.140.90 and click **Add**.



Address	Port	Adapter	IP Addre
192.168.140.92	3260	Default	Default

6. In the **Targets** tab, select an IQN number from the list. Identify the iSCSI targets by the last 3 digits of their IQN names.
If the last digit is "1," the target is a logical drive managed by controller A.
If the last digit is "2," the target is a logical drive managed by controller B.



Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

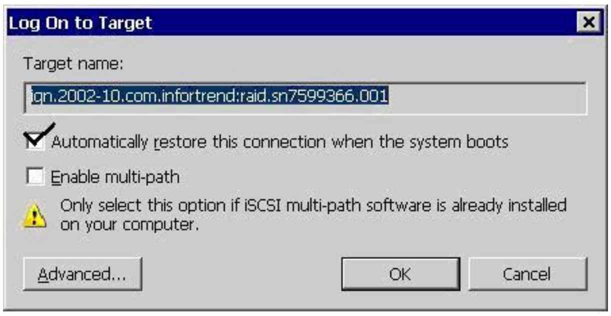
Targets:

Name	Status
iqn.2002-10.com.infortrend:raid.sn7599362.012	Inactive
iqn.2002-10.com.infortrend:raid.sn7599366.001	Inactive

2. Click **Log On**.

Step 2:
Setting Log On

7. In the Log On to Target window that appears, check the automatic restoration option.



Log On to Target

Target name:

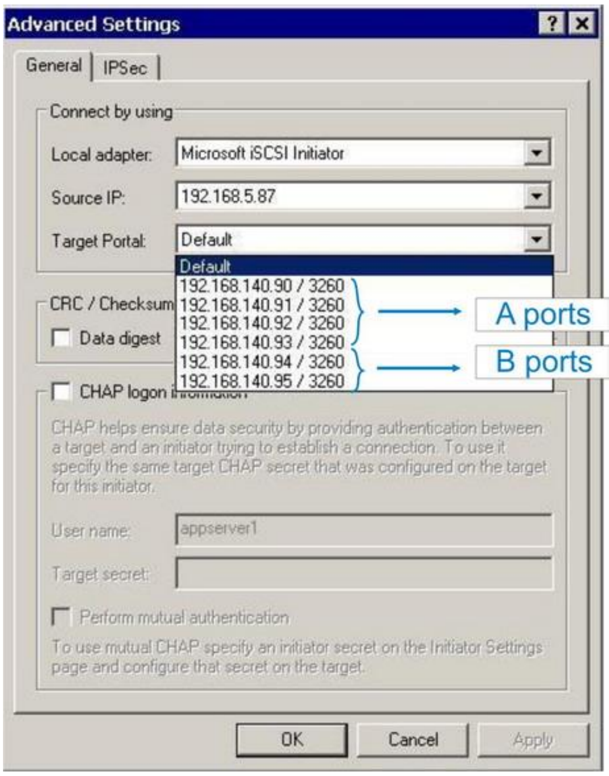
iqn.2002-10.com.infortrend:raid.sn7599366.001

☑ Automatically restore this connection when the system boots

□ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

2. Click the **Advanced** button. Select appropriate options for Local adapter, Source IP, and Target Portal from their respective pull-down lists.
When selecting a Target Portal from the pull-down list, make sure you correctly associate a Target with the target portals. For example, a Target (Logical Drive) managed by Controller A should be associated with target portals that are controller A ports.
Iqn.2002-10.com.infortrend:raid.snXXXXXX.XX1 <- with -> A port target portals
Iqn.2002-10.com.infortrend:raid.snXXXXXX.XX2 <- with -> B port target portals



Advanced Settings

General | IPSec

Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: 192.168.5.87

Target Portal: Default

Default
192.168.140.90 / 3260
192.168.140.91 / 3260
192.168.140.92 / 3260
192.168.140.93 / 3260
192.168.140.94 / 3260
192.168.140.95 / 3260

CRC / Checksum

□ Data digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.

User name: appserver1

Target secret:

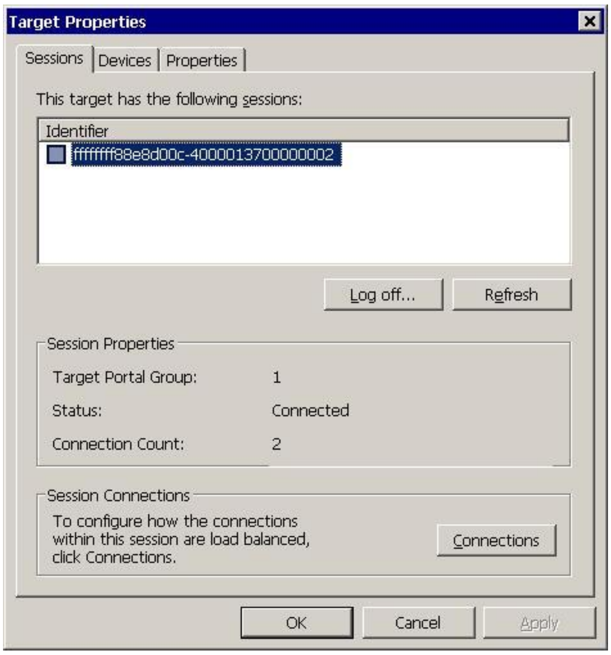
□ Perform mutual authentication

To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.

3. Click **OK** to close the window.

Step 3:
Adding More Targets

8. In the iSCSI Initiator Properties > Targets tab, click on the **Details** button. The Target Properties window will appear.



This target has the following sessions:

Identifier
ffffffff88e8d00c-4000013700000002

Session Properties

Target Portal Group: 1

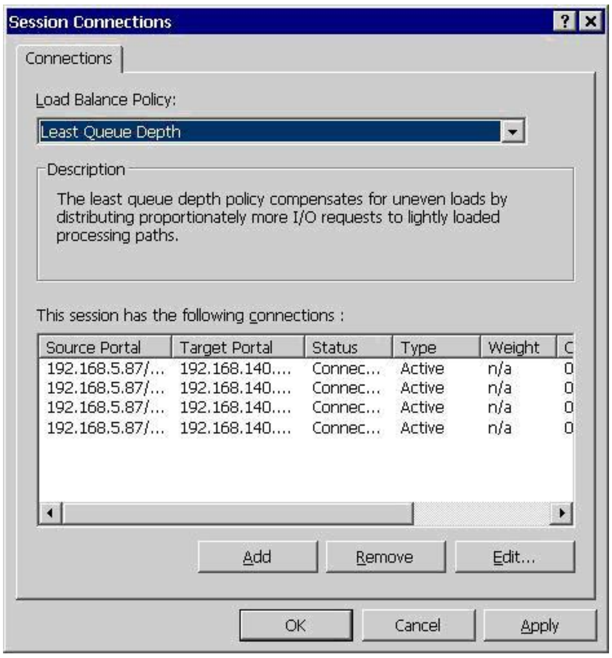
Status: Connected

Connection Count: 2

Session Connections

To configure how the connections within this session are load balanced, click Connections.

2. Click the **Connections** button. Select the **Least Queue Depth** load-balancing policy from the **Load Balance Policy** pull-down list.



Load Balance Policy: Least Queue Depth

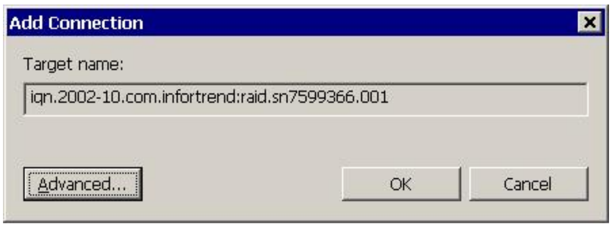
Description

The least queue depth policy compensates for uneven loads by distributing proportionately more I/O requests to lightly loaded processing paths.

This session has the following connections :

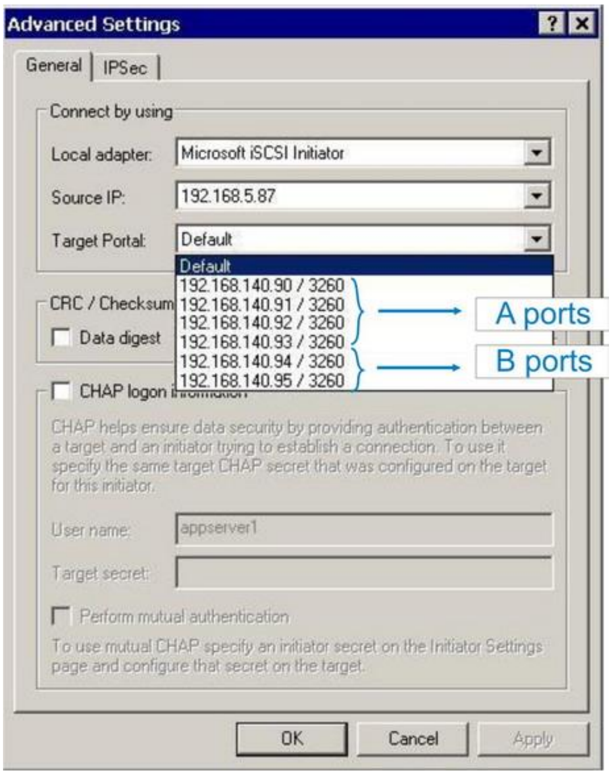
Source Portal	Target Portal	Status	Type	Weight	C
192.168.5.87/...	192.168.140....	Connec...	Active	n/a	0
192.168.5.87/...	192.168.140....	Connec...	Active	n/a	0
192.168.5.87/...	192.168.140....	Connec...	Active	n/a	0
192.168.5.87/...	192.168.140....	Connec...	Active	n/a	0

3. Click **Add** to include other target portals (A port portals at this stage) into the iSCSI session.



Target name: iqn.2002-10.com.infortrend:raid.sn7599366.001

4. Select a load-balancing policy and add a target port using the **Add** button. Click **OK** on the following screens to complete the configuration process.



Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: 192.168.5.87

Target Portal: Default

Default
192.168.140.90 / 3260
192.168.140.91 / 3260
192.168.140.92 / 3260
192.168.140.93 / 3260
192.168.140.94 / 3260
192.168.140.95 / 3260

CRC / Checksum

□ Data digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.

User name: appserver1

Target secret:

□ Perform mutual authentication

To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.

5. Repeat the above steps to add all portals.

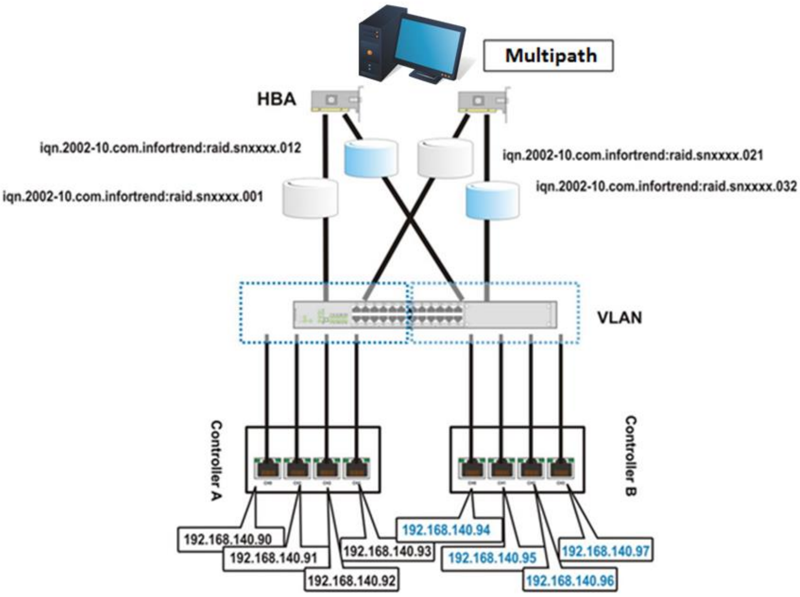
Completing the Procedure

9. You may repeat those steps to associate another logical drive target with target portals from controller B. When you finish the configuration process, the volumes will appear as multiple disk devices in the Windows Disk Drive management window.

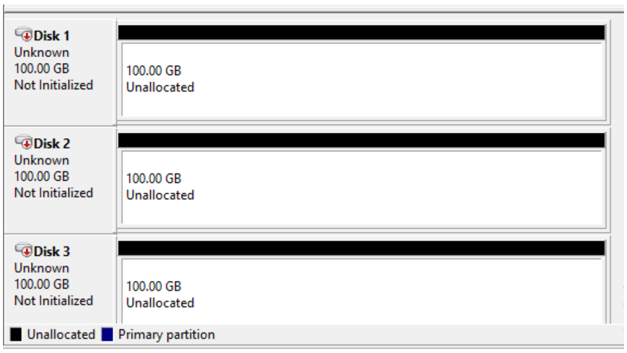
10. Enable the multipath feature on the windows server so that the host can recognize them as devices accessed through fault-tolerant links.
    Please refer to Working with Multipath for more information.

Working with Multipath

Multi-path I/O functionality can recognize and manage redundant data paths to an individual volume. It ensures greater reliability through the path failover mechanism in the event of cabling component failures.


Multipath
HBA
iqn.2002-10.com.infortrend:raid.snxxxx.012
iqn.2002-10.com.infortrend:raid.snxxxx.001
iqn.2002-10.com.infortrend:raid.snxxxx.021
iqn.2002-10.com.infortrend:raid.snxxxx.032
VLAN
Controller A
Controller B
192.168.140.90
192.168.140.91
192.168.140.92
192.168.140.93
192.168.140.94
192.168.140.95
192.168.140.96
192.168.140.97

Before and After enabling MPIO on Windows server



Disk 1
Unknown
100.00 GB
Not Initialized
100.00 GB
Unallocated

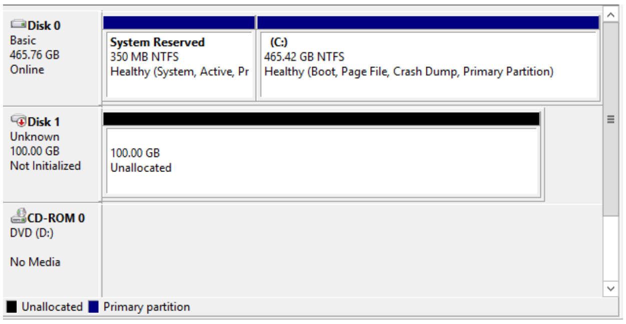
Disk 2
Unknown
100.00 GB
Not Initialized
100.00 GB
Unallocated

Disk 3
Unknown
100.00 GB
Not Initialized
100.00 GB
Unallocated

■ Unallocated ■ Primary partition

Before

↓



Disk 0
Basic
465.76 GB
Online
System Reserved
350 MB NTFS
Healthy (System, Active, Pr
(C:)
465.42 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Unknown
100.00 GB
Not Initialized
100.00 GB
Unallocated

CD-ROM 0
DVD (D:)

No Media

■ Unallocated ■ Primary partition

After

For Linux OS

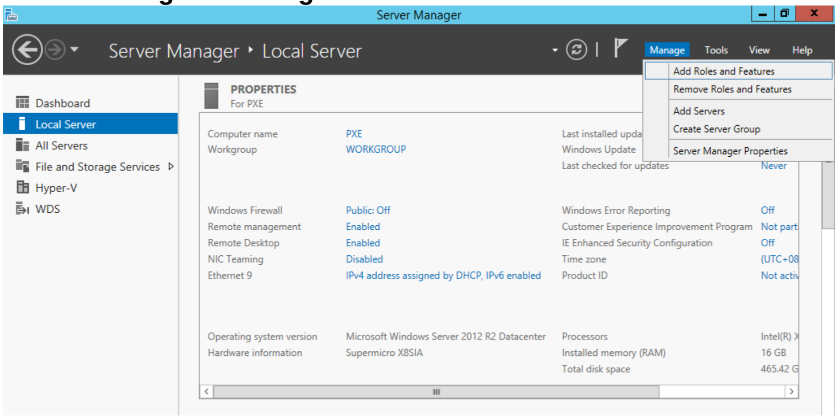
On Linux/Unix platforms, it is recommended using the native MPIO driver. For detailed configurations, refer to the application note.

Enabling Linux Device Mapper Multipath on EonStor®

Enabling the MPIO on Windows server 2012 R2

Steps

1. **Server Manager > Manage > Add Roles and Features**



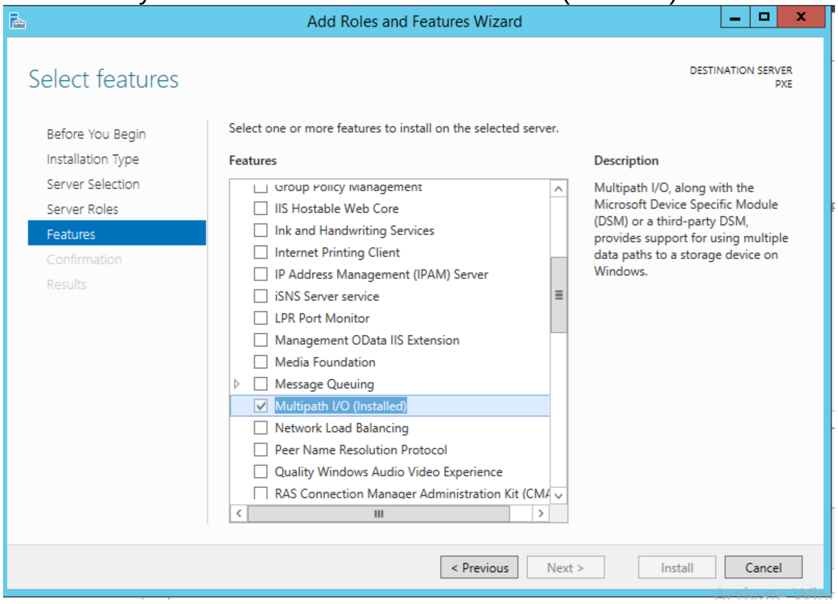
PROPERTIES
For PXE

Computer name PXE
Workgroup WORKGROUP
Last installed upda
Windows Update
Last checked for updates Never

Windows Firewall Public: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 9 IPv4 address assigned by DHCP, IPv6 enabled
Windows Error Reporting Off
Customer Experience Improvement Program Not parti
IE Enhanced Security Configuration Off
Time zone (UTC+08
Product ID Not activ

Operating system version Microsoft Windows Server 2012 R2 Datacenter
Hardware information Supermicro X8SIA
Processors Intel(R) X
Installed memory (RAM) 16 GB
Total disk space 465.42 G

2. Click **Next** until selecting the Features step and check the Multipath I/O. We have already installed the features so it shows “(Installed).”



Select features

DESTINATION SERVER
PXE

Select one or more features to install on the selected server.

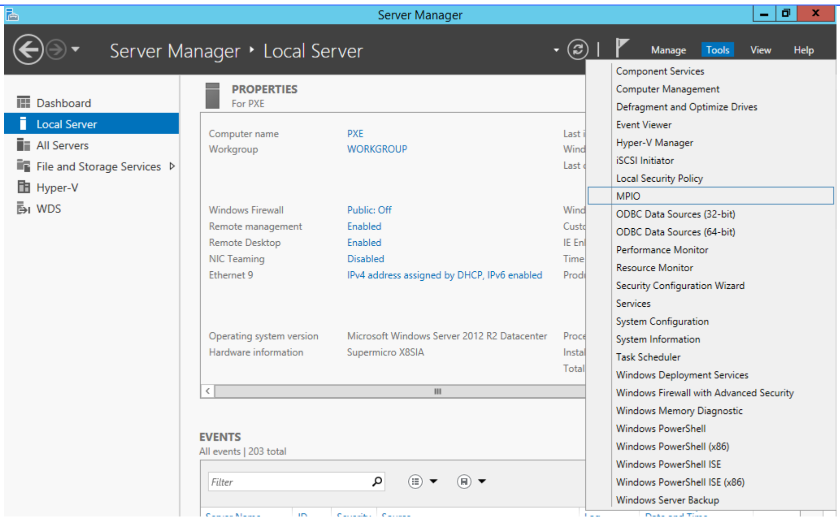
Features

□ Group Policy Management
□ IIS Hostable Web Core
□ Ink and Handwriting Services
□ Internet Printing Client
□ IP Address Management (IPAM) Server
□ iSNS Server service
□ LPR Port Monitor
□ Management OData IIS Extension
□ Media Foundation
□ Message Queuing
☑ Multipath I/O (Installed)
□ Network Load Balancing
□ Peer Name Resolution Protocol
□ Quality Windows Audio Video Experience
□ RAS Connection Manager Administration Kit (CMA

Description

Multipath I/O, along with the Microsoft Device Specific Module (DSM) or a third-party DSM, provides support for using multiple data paths to a storage device on Windows.

3. **Server Manager > Tools > MPIO**

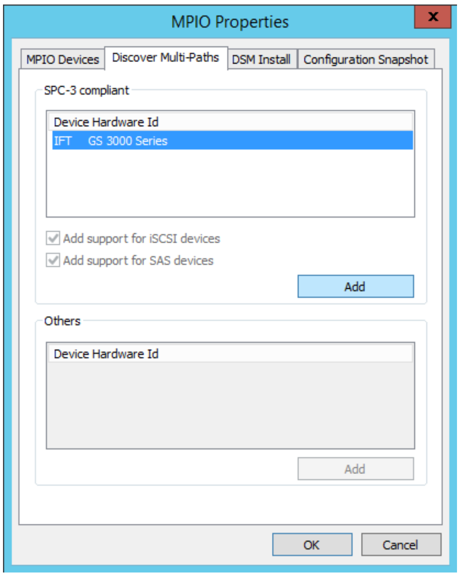


Computer name PXE
Workgroup WORKGROUP

Windows Firewall Public: Off
Remote management Enabled
Remote Desktop Enabled
NIC Teaming Disabled
Ethernet 9 IPv4 address assigned by DHCP, IPv6 enabled

Operating system version Microsoft Windows Server 2012 R2 Datacenter
Hardware information Supermicro X8SIA

4. You will find the storage device showing in the **Discover Multi-Paths** tab. Click **Add** and reboot the server to enable MPIO.



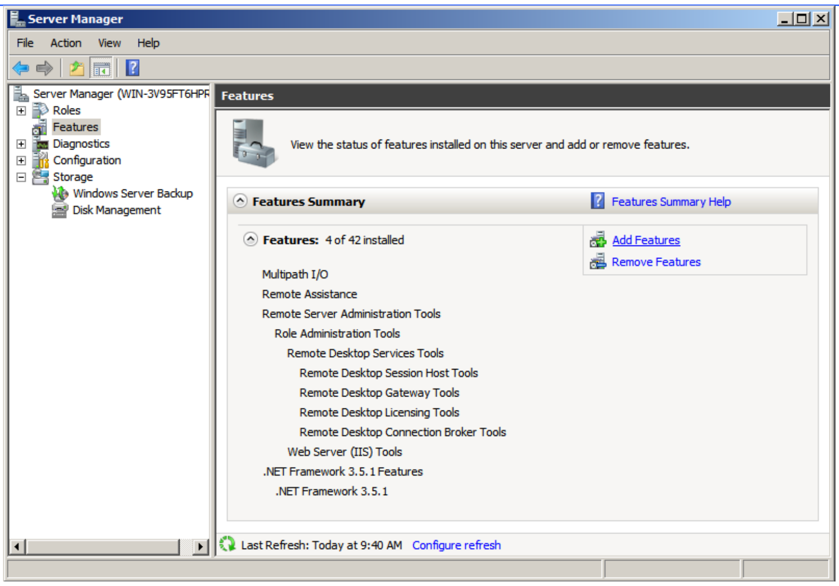
Device Hardware Id
IFT GS 3000 Series

☑ Add support for iSCSI devices
☑ Add support for SAS devices

Device Hardware Id

Enabling the MPIO on Windows server 2008 R2

Steps 1. **Server Manager > Features > Add Features**



Server Manager

Server Manager (WIN-3V95FT6HPR
Roles
Features
Diagnostics
Configuration
Storage
Windows Server Backup
Disk Management

Features

View the status of features installed on this server and add or remove features.

Features Summary

Features Summary Help

Features: 4 of 42 installed

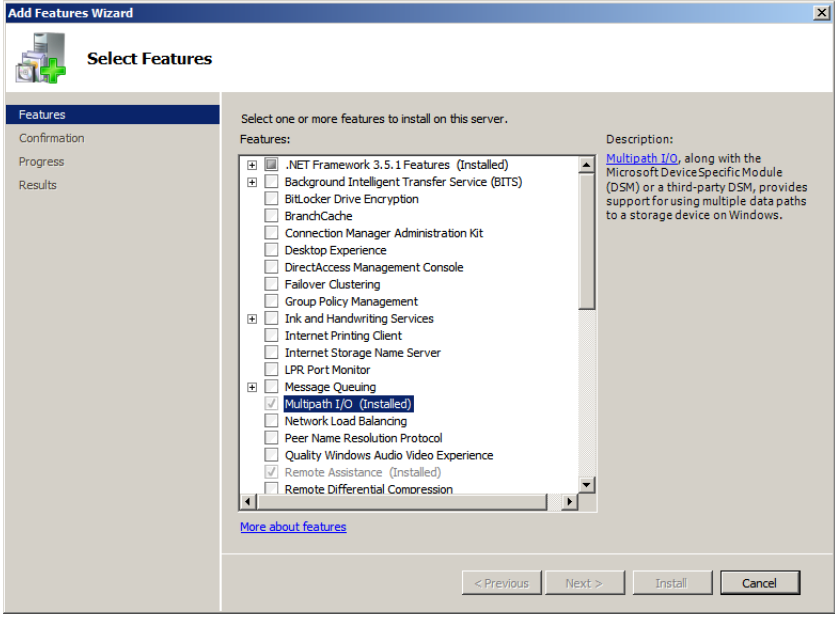
Add Features

Remove Features

Multipath I/O
Remote Assistance
Remote Server Administration Tools
Role Administration Tools
Remote Desktop Services Tools
Remote Desktop Session Host Tools
Remote Desktop Gateway Tools
Remote Desktop Licensing Tools
Remote Desktop Connection Broker Tools
Web Server (IIS) Tools
.NET Framework 3.5.1 Features
.NET Framework 3.5.1

Last Refresh: Today at 9:40 AM Configure refresh

2. Check the Multipath I/O. We have already installed the features so it shows “(Installed).”



Add Features Wizard

Select Features

Select one or more features to install on this server.

Features:

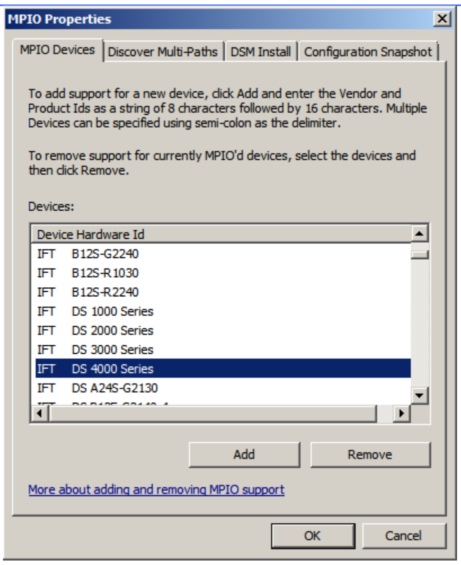
- ☑ .NET Framework 3.5.1 Features (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BranchCache
- □ Connection Manager Administration Kit
- □ Desktop Experience
- □ DirectAccess Management Console
- □ Failover Clustering
- □ Group Policy Management
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ Internet Storage Name Server
- □ LPR Port Monitor
- □ Message Queuing
- ☑ Multipath I/O (Installed)
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience
- ☑ Remote Assistance (Installed)
- □ Remote Differential Compression

Description:

Multipath I/O, along with the Microsoft Device Specific Module (DSM) or a third-party DSM, provides support for using multiple data paths to a storage device on Windows.

More about features

3. Click **Start** and type “MPIO” to launch the MPIO Properties panel. Click on the **Discover Multi-Paths** tab and check the box for **Add support for iSCSI devices**. Click **Add** and reboot the system.



To add support for a new device, click Add and enter the Vendor and Product Ids as a string of 8 characters followed by 16 characters. Multiple Devices can be specified using semi-colon as the delimiter.

To remove support for currently MPIO'd devices, select the devices and then click Remove.

Devices:

```
Device Hardware Id
IFT     B12S-G2240
IFT     B12S-R1030
IFT     B12S-R2240
IFT     DS 1000 Series
IFT     DS 2000 Series
IFT     DS 3000 Series
IFT     DS 4000 Series
IFT     DS A24S-G2130
```

Setting up an OAuth Client ID for EonCloud Gateway

Before adding Google Cloud storage on EonCloud Gateway, you need a client ID with its application type as **Web application**. You can create a new client ID or use an existing one, and complete the following settings.

Create a new client ID	1. Go to https://console.cloud.google.com/apis/credentials and log in. 2. Click **Create credentials** and select **OAuth client ID**. 3. Specify a name for the OAuth 2.0 client. 4. Go to the Authorized redirect URIs section. Specify the URI as follows: **https://oauth.srvprovider.com/cloud/redirect.html**. 5. Click **Create**.
Use an existing client ID	1. Go to https://console.cloud.google.com/apis/credentials and log in. 2. Select an OAuth 2.0 client ID with the type set to **Web application**. 3. Go to the Authorized redirect URIs section. Click **Add URI** and specify the URI as follows: **https://oauth.srvprovider.com/cloud/redirect.html**. 4. Click **Save**.

After completing the settings, you can add your Google Cloud on the EonCloud Gateway. To add it on EonCloud Gateway, see Creating Cloud Storage.

Firmware Specifications

Cache Memory

Auto cache flush on critical conditions **(caching mode dynamic switch)**	When critical conditions occur, e.g., component failure or BBU under charge, cached data will be flushed and the write policy will be changed to write-through mode. Configurable "Trigger Events" for Write-through/Write-Back Dynamic Switch. The configuration can also be set with the OEM "Iappend" utility.
Write-back cache	Supported.
Write-through cache	Supported.
Supported memory type	DDR memory for enhanced performance. Fast Page Memory with Parity for enhanced data security.
Read-ahead operation	Intelligent and dynamic read-ahead operation for processing sequential data requests.
Multi-threaded operation	Yes, internal parameters adjusted in accordance with the number of outstanding I/Os.
Scatter / Gather	Supported
I/O sorting	Supported. Optimized I/O sorting for enhanced performance.
Adaptive Write-back/Write-through switching	For a better performance when handling large sequential writes, firmware temporarily disables write-back cache and the synchronized cache operation between partner controllers if operating with dual-active controllers. Firmware automatically restores the write-back mode when encountering random and small writes later.
Periodic Cache Flush	Firmware can be configured to flush the cached contents in memory at every preset interval: If data integrity is of the concern, e.g., the lack of a battery backup protection. Cache flush on preset intervals to avoid the latency when cache memory is full due to write delays.
Stripe Size	128kb, except for RAID 3
Caching Optimization	Cache buffer sorting prior to cache flush operation. Gathering of writes during flush operation to minimize the number of I/Os required for parity update. Elevator sorting and gathering of drive I/Os. Multiple concurrent drive I/Os (tagged commands). Intelligent, predictive multi-threaded read-aheads. Multiple, concurrent host I/O threads (host command queuing).

Data Safety

Data Services	Snapshot, Volume Copy, Volume Mirror.
Regenerate parity of logical drives	Supported. Can be manually executed to ensure that bad sectors do not cause data loss in the event of drive failure.
Scheduled Media Scan	Media Scan can be scheduled starting at a specified start time and repeated at regularly timed intervals. The start time and time intervals can be selected from drop down menus. Start time is manually entered using its numeric representatives in the following order [MMDDhhmm[YYYY]], and it reads the date and time set for the controller's real-time clock. The selectable time intervals (the Execution Period) range from one (1) second to seven (7) weeks. Each such schedule can be defined to operate on individual hard drives, all members of a specified logical drive, or members of selected logical drives.
Bad block auto-reassignment	Supported. Automatic reassignment of bad block
Battery backup for cache memory	Supported. The battery backup unit supports cache memory when power failure occurs. The unwritten data in the cache memory can be committed to drive media when power is restored.
Verification on normal writes	Supported. Performs read-after-write during normal write processes to ensure data is properly written to drives.
Verification on rebuild writes	Supported. Performs read-after-write during rebuild write to ensure data is properly written to drives.
Verification on LD initialization writes	Supported. Performs read-after-write during logical drive initialization to ensure data is properly written to drives.
Drive S.M.A.R.T. support	Supported. Drive failure is predictable with reference to the different variables detected. Reaction schemes are selectable from Detect only, Perpetual Clone, Copy + Replace, and Fail Drive. These options help to improve MTBF.
Clone failing drive	Users may choose to clone data from a failing drive to a backup drive manually.
Automatic shutdown on over-temperature condition	Controller automatically enters an idle state (stops answering I/O requests) upon the detection of high-ambient temperature for an extended period of time.

Disk Drive

Bad Block Handling in degraded mode	A method for handling low quality drives. The operation is performed on the logical drive in degraded mode or those that are being rebuilt. If bad blocks should be encountered during Rebuild, Add Drive, Host Write, or Regenerate Parity operation, the controller will first attempt to reconstruct affected data and those irrecoverable bad blocks are stated as bad and the controller return to host. Users have the option to abandon data on the unrecoverable sectors to continue rebuild in a degraded mode. Low quality drive handling comes with transparent resetting of hung hard drives.
Transparent reset of hung HDDs	Supported
Drive identification (flash drive function)	Supported. Force a drive to light on its activity indicator for users to visually recognize its position in a configuration consisting of numerous disk drives.
Drive information listing	Supported. Drive vendor name, model number, firmware revision, capacity (blocks), serial number, narrow/wide and current sync. speed
Drive read/write test	Supported
Configuration on disks (Drive Roaming)	Will be supported in next release. The logical drive information is recorded on drive media. The logical drives can still be accessed if using different STORANDER controllers/subsystems, e.g., drives removed and installed in a different subsystem. *Note: Remote replication and disk roaming cannot be executed between EonStor DS and EonStor GS.
Drive motor spin-up	Supported. The controller will send spin-up (start unit) command to each drive at the 4 sec. intervals.
Drive I/O timeout	User adjustable
I/O channel diagnostics	Supported; please contact your dealer for more details.
Power Saving	Idle and Spin-down modes
Maximum Drive Response Time (Guaranteed Latency I/O)	User adjustable from 160 to 960ms. If a disk drive fails to return data on read requests before the timeout value is exceeded, the array immediately generates data from the parity data and the other members of a logical drive.
Drive-side tagged command queuing	Supported. User adjustable up to 128 for each drive.

Environment

SAF-TE/S.E.S. support	Supported. The SAF-TE/S.E.S. modules can be connected to the drive channels. The RAID controller will detect errors from SAF-TE/S.E.S. devices or notify drive failures via SAF-TE/S.E.S. Both SAF-TE/S.E.S. via drive and device-self-interfaced methods are supported. Redundant SAF-TE/S.E.S. devices are supported Multiple S.E.S. devices are supported
Dynamic on-lining of enclosure services	Once an expansion unit with supported monitoring interface is combined with a storage system, its status will be automatically polled.
SAF-TE/S.E.S. polling period	User configurable (50ms, 100ms, 200ms, 500ms, 1~60sec)
ISEMS (Infortrend Simple Enclosure Management Service)	Supported via an I2C serial bus.
Multiple SAF-TE/S.E.S. modules on the same channel	Supported.
Multiple SAF-TE /S.E.S. modules on different channels	Supported.
Mapping SAF-TE/S.E.S. device to host channel for use with host-based SAF-TE/S.E.S. monitoring	Supported.
Event Triggered Operation	When any of the following happens, the firmware disables write-back caching to minimize the chance of losing data: Battery, controller, cooling fan, or PSU failure The upper temperature thresholds are exceeded Low battery charge UPS AC loss or low battery charge The triggering factors are user-configurable
Multi-speed cooling fan control	Yes, firmware triggers high rotation speed in the event of elevated temperature or component failure, e.g., a fan failure.
Dual-LED drive status indicators	Supported. Both single-LED and dual-LED drive status indicators are supported.
SAF-TE/ S.E.S. temperature value display	Supported. Display the temperature value provided by enclosure SAF-TE/S.E.S. module (if available).
On-board controller voltage monitors	Supported. Monitors the 3.3V, 5V, and 12V voltage status. Event triggered thresholds user configurable.
On-board controller temperature sensors	Supported. Monitors the CPU and board temperature status. Event trigger threshold user configurable.
Enclosure redundant power supply status monitoring	Supported. SAF-TE/S.E.S./ISEMS
Enclosure fan status monitoring	Supported. SAF-TE/S.E.S/ISEMS
Enclosure UPS status monitoring	Supported. SAF-TE/S.E.S/ISEMS
Enclosure temperature monitoring	Supported. SAF-TE/S.E.S/ISEMS

High Availability

Custom inquiry serial number	Custom Inquiry Serial Number (for support of multi-pathing software like Veritas, QLogic, etc.).
Continuous rebuild	Rebuild automatically continues if power outage or operator errors occur during a rebuild.
Asymmetric Logical Unit Access (or later known as Target Port Group Service)	Support for multipath drivers to select an optimal I/O path and for more flexible utilization of internal I/O paths in the event of path failure or controller failover/failback.
High Availability hardware modules	Continuous controller failover/failback. IP address of the 10/100BaseT Ethernet port is handed over to a surviving controller in the event of a single controller failure. Multiple drive channel across the backplane to disk drives.

I/O

Concurrent I/O	Supported
Tag Command Queuing (TCQ)	Supported
Native Command Queuing (NCQ)	Supported

Logical Drive

Maximum number of logical drives	30
Maximum logical drive capacity	512TB
RAID level dependency to each logical drive	Independent. Logical drives configured in different RAID levels can co-exist in a pool and within a storage subsystem
Maximum number of logical drive members	128
Configurable stripe size	16KB, 32KB, 64KB, 128KB, 256KB, 512KB, or 1024KB per logical drive
Configurable Write Policy (write policy per array)	Write-Back or Write-Through per logical drive. This policy can be modified later.
Logical drive identification	Unique, controller randomly generated logical drive ID; Logical Drive and Pool name user-configurable for ease of identification in a multi-array configuration
Maximum number of volumes for each pool	1024
Immediate logical drive availability	Supported; Logical arrays are immediately ready for Host I/Os. Initialization task is completed in the background except when the logical array is stated as “INCOMPLETE” or “BAD;” e.g., has a failed member right after the creation.
Auto-rebuild onto failed drive replacement	Supported. With no spare drive, the subsystem will auto-scan the failed drive and starts rebuild automatically once the failed drive has been replaced.
Auto recovery from logical drive failure (configuration on drives)	Supported. If a user accidentally removed the wrong drive to cause the 2nd drive failure of a one-drive-failed RAID5 / RAID3 logical drive, fatal error may occur. However, you may force the system to reaccept the logical drive by switching off the subsystem, installing the drive back to its original drive slot, and then power on the subsystem. You may have the chance to restore the logical drive into the one-drive-failed status.
Concurrent rebuild / expansion	Multiple logical drives can proceed with a Rebuild/Regenerating Parity, and/or Expansion/Initialization/Add Drive operation at the same time. *Note: Regenerate Parity and Rebuild cannot take place on a logical drive at the same time. Create, Expand, and Add Drive operations cannot take place on a logical drive at the same time.

Users/User Groups/Folders

Maximum number of users	20000
Maximum number of user groups	512
Maximum number of folder sharing (NFS/CIFS/AFP/FTP)	EonStor GSe 1024 EonStor GS 2048 AFP: 255
Maximum number of Rsync jobs	1024
Maximum number of Rsync concurrent processes	64
Maximum number of connections	2,048 (NFS/CIFS/AFP) 1,024 (FTP)

Pool / Host LUN

Maximum size of pool	2PB
Maximum number of pools	30
Maximum number of LUNs Mappable	4000

Media Scan

Maximum number of Media Scan task schedules	32
Media Scan	Supported. Verify written data on drives to avoid bad blocks from causing data inconsistency. If bad blocks are found, data can be reconstructed by comparing and recalculating parity from adjacent drives (RAID1/3/5/6). The “Reconstruction Writes” are followed by “Write Verification” operation.

RAID Expansion

On-line RAID expansion	Supported. Capacity brought by array expansion is immediately ready for Host I/Os when its status changes from “EXPAND” to “INITIALIZING.” Initialization task is then completed in the background except when the logical array is stated as “INCOMPLETE” or “BAD;” e.g., has a failed member right after creation.
Mode-1 RAID expansion -add drive	Supported. Multiple drives can be added concurrently. Though not recommended, Add Drive can even be performed in the degraded mode.
Mode-2 RAID expansion – copy and replace drives	Supported. Replace members with drives of larger capacity.
Expand capacity with no extra drive bays required	Supported in Mode 2 RAID expansion, which provides “Copy and Replace Drive” function to replace drives with drives of greater capacity. Protect your investment for there is NO need for hardware upgrade, e.g., adding a new enclosure for the extra drives.
Operating system support for RAID expansion	No. No operating system driver required. No software needs to be installed for this purpose.

Redundant Controller

Active-active redundant controller	Supported
Synchronized cache	Supported. Through one or multiple, dedicated synchronizing channels on a common backplane or external cabling. Synchronized cache over SCSI channels, Fibre loops, or SATA channels is supported. Synchronized cache can be disabled via a UI option when using write-through mode in a redundant controller configuration to prevent performance trade-offs.
Write-back cache enabled in redundant controller mode	Yes, with synchronized cache connection and mirrored cache between controllers.
Automatic failover	Yes (user's interaction necessary; e.g., to restart the software management console)
Automatic failback	Yes (user's interaction necessary)
Controller hot-swap	No need to shut down the failed controller before replacing the failed controller. Support online hot-swap of the failed controller. There is no need to reset or shutdown the failed controller. One controller can be pulled out during active I/Os to simulate the destructive controller failure.
Parity synchronization in redundant controller write-back mode to avoid write-hole	Supported.
No single-point-of-failure	Supported.
Automatic engagement of replacement controller	Disabled
Dynamic cache memory allocation	Yes. Cache memory is dynamically allocated, not fixed.
Environment management	Supported. SAF-TE, S.E.S., ISEMS (I2C interface), or S.E.S. over SAS links; and on-board controller voltage/temp monitor are all supported in both single and redundant controller mode. In the event of controller failure, services can be taken over by the surviving controller.
Cache Backup Module (CBM)	Supported. Battery backup modules support the transaction of cached data to flash memory on the occurrence of power outage. With EEPROM battery modules, firmware will be aware of the life expectancy of battery cells.
Load sharing	Supported. Workload can be flexibly divided between different controllers by assigning logical configurations of drives (Pools) to different controllers.
User configurable channel mode	Supported. Channel modes configurable (SCSI or Fibre) as HOST or DRIVE on specific models.
Require a special firmware for redundant controller?	No.

S.M.A.R.T.

Copy & replace drive	Supported. User can choose to clone a member drive showing symptoms of defects before it fails.
Drive S.M.A.R.T. support	Supported, with intelligent error handling implementations.
User selectable modes on the occurrence of S.M.A.R.T.-detected errors	Detect only Perpetual Clone: using a hot-spare to clone the drive reporting SMART errors; the hot-spare remains a clone drive Clone + Replace: using a hot-spare to replace the drive reporting SMART errors; the drive reporting errors is pulled offline Fail Drive: disband faulty drive from a logical drive.

Spare Drive

Dedicated spare drive	Supported, hereby defined as the spare drive specifically assigned to a logical drive. Also known as Local Spare
Global spare drive	Supported, the spare drive that serves all logical drives (as long as it is equal in size or larger than logical drive members)
Global spare auto-assign	Supported, applies to all unused drive(s); safeguards the array if a spare has been used in the previous array rebuild and users forget to configure a new drive as a spare.
Enclosure spare drive	A Spare that participates only in the rebuild of a failed drive within the same enclosure.
Co-existing Dedicated (Local), Enclosure-specific, and Global spare drives	Supported
Auto-rebuild onto spare drive	Supported
Auto-scan of replacement drive upon manually initiated rebuild	Supported
One-step rebuild onto a replacement drive	Supported

System Security

Password protection	Supported. All configuration changes require the correct password (if set) to ensure system security. Password protection is also bundled with all user interfaces.
User-configurable password validation timeout	Supported. After certain time in absence of user interaction, the password will be requested again. This helps to avoid unauthorized operation when user is away.
SSL-enabled EonOne Agents	Agents communicate to the controller through limited set of authorization options.

User Interface

EonOne	Out-of-band configuration and monitoring via Ethernet.
Graphical user interface (Java-based GUI manager)	Provides user-friendly graphical interface. Communicates with controller via Out-of-band Ethernet, In-band SCSI, In-band Fibre or SNMP traps.
External interface API for customized host-based management	Supported.
Buzzer alarm	Warns users when any failures or critical events occur.

Default TCP and UDP Port Settings

Use these ports if you or the system administrators need to manually configure secure access to your NAS system (to bypass firewall settings, for example)

AFP	TCP	548
CIFS	TCP	138, 445
	UDP	137, 138
Finder agent	TCP	8097
	UDP	8097, 58740, 58741
FTP	TCP	20, 21
FTP-SSL	TCP	20, 21, 989, 990
HTTP	TCP	80
HTTP	TCP	8816 (Management port)
HTTPS	TCP	8080, 8989 (File Explorer)
HTTPS	TCP	8817 (Management port via SSL)
iSCSI	TCP	860, 3260
NFS	TCP	111, 2049, 4045
Rp_daemon	TCP	5100
Rsync daemon	TCP	873
Rsync ssh	TCP	22
Rsync rsh	TCP	514
SFTP	TCP	22
SNMP trap	UDP	162 (default)
SNMP query	UDP	161 (default)

Others

RAID Level	RAID levels	0, 1(0+1), 3, 5, 6, 10, 30, 50, 60, and NRAID. Levels 10, 30, 50, and 60 are the multi-level RAID defined as the pool implementations; pools consist of logical drives of different RAID levels that are striped together. Including logical drives of different RAID levels in a pool is, however, not recommended.
Firmware	Background firmware download	Firmware can be downloaded during active I/Os, and takes effect after a system reboot.
Parity	RAID parity update tracking and recovery	Yes, to avoid write holes.
Host	Host-side Ordered Tag support	Supports write commands with embedded Ordered Tags.
Import/export configuration	Save/ restore NVRAM to / from disks	Supported. Save all the settings stored in the controller NVRAM to the logical drive members. Now this feature comes with an option whether to restore the previously saved password in case an administrator changed the password some time before or simply forgets the previous password.
	Save / restore NVRAM to / from a file	Supported. Save all the settings stored in the controller NVRAM to a file (via GUI manager) on user’s computer. Now this feature comes with an option whether to restore the previously saved password in case an administrator changed the password some time before.
Host Parameters	Host-side 64-bit LBA support	Supports array configuration (logical drive, pool, or a volume of them) of a capacity up to 64TB.
	Host-side maximum queued I/O count	User adjustable up to 1024
Shutdown	Controller shutdown	Flushes cached contents upon the detection of critical conditions, e.g., a high temperature condition persists for a long time.

Default System Settings

Event Trigger	Controller failure	Disabled
	BBU low or failed	Enabled
	UPS AC power loss	Disabled
	Power supply failure	Disabled
	Fan failure	Disabled
	Temperature exceeds threshold	Disabled
Peripheral Device Parameters	Peripheral device type	Enclosure Service Device (0xD)
	Peripheral device qualifier	Connected
	Device support removable media	Disabled
	LUN applicability	First Undefined LUN (automatically selected by firmware)
	Cylinder/Head/Sector- variables	N/A
Drive-side Parameters	Disk Access Delay Time	Per product interface
	Drive I/O Timeout	7 seconds
	Max. Tag Count	8: Fibre drives 4: SAS drives
	Periodic SAF-TE and SES Check Time	30 seconds
	Auto Rebuild on Drive Swap check time	15 seconds
	Drive Predictable Failure Mode (S.M.A.R.T.)	Disabled
	Drive Delayed Write for single-controller models without BBU	Enabled
	Drive Power Saving	Enabled
Voltage & Temperature Parameters*	+3.3V thresholds	3.6V – 2.9V
	+5V thresholds	5.5V – 4.5V
	+12V thresholds	13.2V - 10.8V
	CPU temperature	90 - 5°C
	Board temperature (controller board)	80 - 5°C
	*Note: The thresholds for other sensors within the chassis are not user-configurable.	
Disk Array Parameters	Rebuild Priority	Normal
	Write Verification on LD Initialization	Disabled
	Write Verification on LD Rebuild	Disabled
	Write Verification on Normal Drive Writes	Disabled
	Max. Drive Response Timeout	Disabled

RAID Levels

What is RAID?

The term RAID(Redundant Array of Independent Disks) summarizes technologies that can distribute data to multiple drives, to achieve a high data transfer rate and fail-safe system. “Redundant” means that the failure of a single drive will not cause the failure or disruption of the entire system and will not result in data loss.

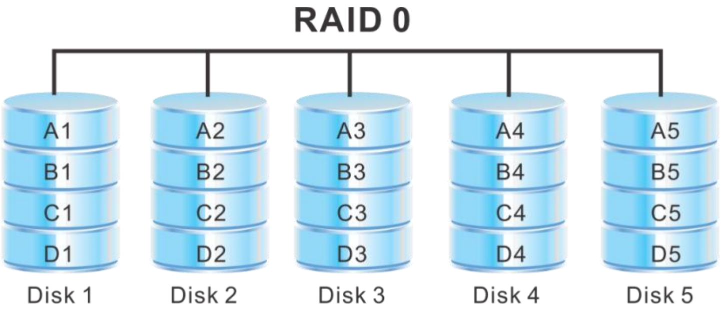
RAID is built on technologies such as mirroring (mirroring two or more drives), duplexing (mirroring with 2 controllers) and striping (combination of multiple drives to a logical drive and block-wise data distribution to these drives).

There are different ways to distribute data to multiple disks to achieve the highest possible data throughput and reliability. These are referred to as RAID level.

The following sections further describe the configurations of and applications for each RAID level, as well as how to calculate the capacity utilization.

RAID 0

RAID 0 is the fastest RAID mode. In a RAID 0 array, the available capacities of each disk are added together so that one pool mounts on the computer. If one physical disk in the array fails, the data of all disks becomes inaccessible because parts of the data have been written to all disks.

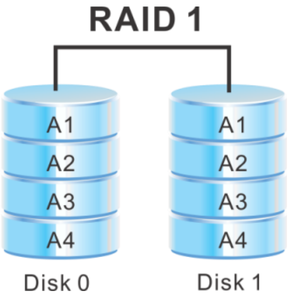


Applications

RAID 0 is ideal for users who need maximum speed and capacity. Video editors working with very large files may use RAID 0 when editing multiple streams of video for optimal playback performance. A RAID 0 array is more suited for actively working with files (e.g. editing video) and should not be used as a single storage backup solution or on mission critical systems.

RAID 1

In a RAID 1 array, the data is written again to a second physical disk. This is the so-called mirror disk. If one of the two disks fails, the data is still fully available on the other disk. Use of the disk can continue normally. The disadvantage of RAID 1 is the TCO, because double the capacity than net required has to be calculated and invested.

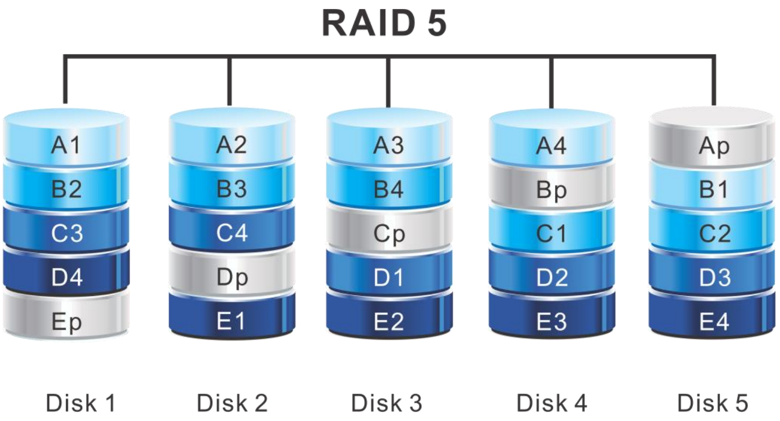


Applications

RAID 1 is ideal for applications requiring high fault tolerance at a low cost, without heavy emphasis on large amounts of storage capacity or top performance. It is especially useful in situations where the perception is that having a duplicated set of data is more secure than using parity. For this reason, RAID 1 is frequently used in data bases for accounting and other financial data. It is also commonly used for enterprise servers, and for individual users requiring fault tolerance with minimum hassle and cost.

RAID 5

In RAID 5, data is striped across all disks (minimum of three) and a parity block for each data block (#p in the diagram) is written on the same stripe. If one physical disk fails, the data from the failed disk can be rebuilt onto a replacement disk. No data is lost in the case of a single disk failure, but if a second disk fails before data can be rebuilt to a replacement drive, all data in the array will be lost.

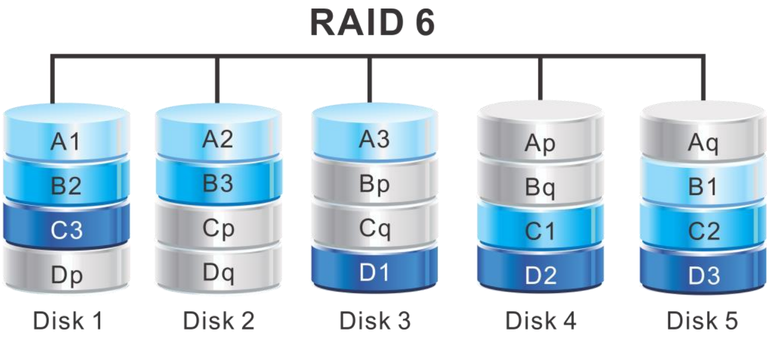


Applications

RAID 5 combines data safety with efficient use of disk space. Disk failure does not result in a service interruption because data is read from parity blocks. RAID 5 is useful for archiving and for people who need performance and constant access to their data, like video editors.

RAID 6

In RAID 6, data is striped across all disks (minimum of four) and a two parity blocks for each data block (p and q in the diagram at right) is written on the same stripe. If one physical disk fails, the data from the failed disk can be rebuilt onto a replacement disk. This Raid mode can support up to two disk failures with no data loss. RAID 6 provides for faster rebuilding of data from a failed disk.



Applications

RAID 6 provides data reliability with the addition of efficient rebuilding in case of a failed drive. RAID 6 is therefore useful for people who need serious security with less of an emphasis on performance.

ASCII Code Table

This table shows the supported Characters for controller name, password, WWPN port nick names, etc.) Note that ox5c back slash is not supported.

Symbol	DEC	OCT	HEX	BIN
(Space)	32	40	20	100000
!	33	41	21	100001
"	34	42	22	100010
#	35	43	23	100011
$	36	44	24	100100
%	37	45	25	100101
&	38	46	26	100110
'	39	47	27	100111
(	40	50	28	101000
)	41	51	29	101001
*****	42	52	2A	101010
+	43	53	2B	101011
,	44	54	2C	101100
-	45	55	2D	101101
.	46	56	2E	101110
/	47	57	2F	101111
0	48	60	30	110000
1	49	61	31	110001
2	50	62	32	110010
3	51	63	33	110011
4	52	64	34	110100
5	53	65	35	110101
6	54	66	36	110110
7	55	67	37	110111
8	56	70	38	111000
9	57	71	39	111001
:	58	72	3A	111010
;	59	73	3B	111011
<	60	74	3C	111100
=	61	75	3D	111101
>	62	76	3E	111110
?	63	77	3F	111111
@	64	100	40	1000000
A	65	101	41	1000001
B	66	102	42	1000010
C	67	103	43	1000011
D	68	104	44	1000100
E	69	105	45	1000101

F	70	106	46	1000110
G	71	107	47	1000111
H	72	110	48	1001000
I	73	111	49	1001001
J	74	112	4A	1001010
K	75	113	4B	1001011
L	76	114	4C	1001100
M	77	115	4D	1001101
N	78	116	4E	1001110
O	79	117	4F	1001111
P	80	120	50	1010000
Q	81	121	51	1010001
R	82	122	52	1010010
S	83	123	53	1010011
T	84	124	54	1010100
U	85	125	55	1010101
V	86	126	56	1010110
W	87	127	57	1010111
X	88	130	58	1011000
Y	89	131	59	1011001
Z	90	132	5A	1011010
[	91	133	5B	1011011
****	92	134	5C	1011100
]	93	135	5D	1011101
^	94	136	5E	1011110
_	95	137	5F	1011111
`	96	140	60	1100000
a	97	141	61	1100001
b	98	142	62	1100010
c	99	143	63	1100011
d	100	144	64	1100100
e	101	145	65	1100101
f	102	146	66	1100110
g	103	147	67	1100111
h	104	150	68	1101000
i	105	151	69	1101001
j	106	152	6A	1101010
k	107	153	6B	1101011
l	108	154	6C	1101100
m	109	155	6D	1101101
n	110	156	6E	1101110
o	111	157	6F	1101111
p	112	160	70	1110000
q	113	161	71	1110001
r	114	162	72	1110010
s	115	163	73	1110011
t	116	164	74	1110100

u	117	165	75	1110101
v	118	166	76	1110110
w	119	167	77	1110111
x	120	170	78	1111000
y	121	171	79	1111001
z	122	172	7A	1111010
{	123	173	7B	1111011
|	124	174	7C	1111100
}	125	175	7D	1111101