Thecus®

User's Manual

N2520/N2560/N4520/N4560 Series

❖ Copyright and Trademark Notice

Thecus and other names of Thecus products are registered trademarks of Thecus Technology Corp. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. Apple, iTunes and Apple OS X are registered trademarks of Apple Computers, Inc. All other trademarks and brand names are the property of their respective owners. Specifications are subject to change without notice.

Copyright © 2014 Thecus Technology Corporation. All rights reserved.

❖ About This Manual

All information in this manual has been carefully verified to ensure its correctness. In case of an error, please provide us with your feedback. Thecus Technology Corporation reserves the right to modify the contents of this manual without notice.

Product name: Thecus N2520/N2560/N4520/N4560 Series

Manual Version: 6.5

Release Date: June 2014

❖ Limited Warranty

Thecus Technology Corporation guarantees all components of Thecus NAS products are thoroughly tested before they leave the factory and should function normally under general usage. In case of any system malfunctions, Thecus Technology Corporation and its local representatives and dealers are responsible for repair without cost to the customer if the product fails within the warranty period and under normal usage. Thecus Technology Corporation is not responsible for any damage or loss of data deemed to be caused by its products. It is highly recommended that users conduct necessary back-up practices.

Check the functions that are available on your particular Thecus NAS model at:

http://www.thecus.com.

❖ Safety Warnings

For your safety, please read and follow the following safety warnings:

- Read this manual thoroughly before attempting to set up your Thecus IP storage.
- Your Thecus IP storage is a complicated electronic device. DO NOT attempt to repair it under any circ umstances. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
- DO NOT allow anything to rest on the power cord and DO NOT place the power cord in an area where it can be stepped on. Carefully place connecting cables to avoid stepping or tripping on them.
- Your Thecus IP storage can operate normally under temperatures between 5°C and 40°C, with relative humidity of 20% – 85%. Using Thecus IP storage under extreme environmental conditions could damage the unit.
- Ensure that the Thecus IP storage is provided with the correct supply voltage (AC 100V ~ 240V, 50/60 Hz, 3A). Plugging the Thecus IP storage to an incorrect power source could damage the unit.
- Do NOT expose Thecus IP storage to dampness, dust, or corrosive liquids.
- Do NOT place Thecus IP storage on any uneven surfaces.
- DO NOT place Thecus IP storage in direct sunlight or expose it to other heat sources.
- DO NOT use chemicals or aerosols to clean Thecus IP storage. Unplug the power cord and all connected cables before cleaning.
- DO NOT place any objects on the Thecus IP storage or obstruct its ventilation slots to avoid overheating the unit.
- Keep packaging out of the reach of children.
- If disposing of the device, please follow your local regulations for the safe disposal of electronic products to protect the environment.

CAUTION
RISK OF EXPLOSION IF BATTERY IS REPLACED
BY AN INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING
TO THE INSTRUCTIONS

❖ Table of Contents

§Chapter 1: Introduction

1.1 Overview

Thank you for choosing the Thecus IP Storage Server. The Thecus IP storage is an easy-to-use storage server that allows a dedicated approach to storing and distributing data on a network. Data reliability is ensured with RAID features that provide data security and recovery—over multiple Terabyte of storage are available using RAID 5 and RAID 6. Gigabit Ethernet ports enhance network efficiency, allowing Thecus IP storage to take over file management functions, increase application and data sharing and provide faster data response. The Thecus IP storage offers data mobility with a disk roaming feature that lets you swap working hard drives for use in other Thecus IP storage, securing the continuity of data in the event of hardware failure. The Thecus IP storage allows data consolidation and sharing between Windows (SMB/CIFS), UNIX/Linux, and Apple OS X environments. The Thecus IP storage's user-friendly GUI supports multiple Languages.

1.2 Package Contents

- **N2520/N2560**

The Thecus IP storage should contain the following common items:

- System Unit x1
- QIG (Quick Installation Guide) x1
- CD-Title (Universal CD) x1
- Ethernet Cable x1
- Accessory bag x1
- HDD Compatibility list Card x1
- Multiple Language Warranty Card x1
- Power adapter x1
- Power cord x1

- **N4520/N4560**

The Thecus IP storage should contain the following common items:

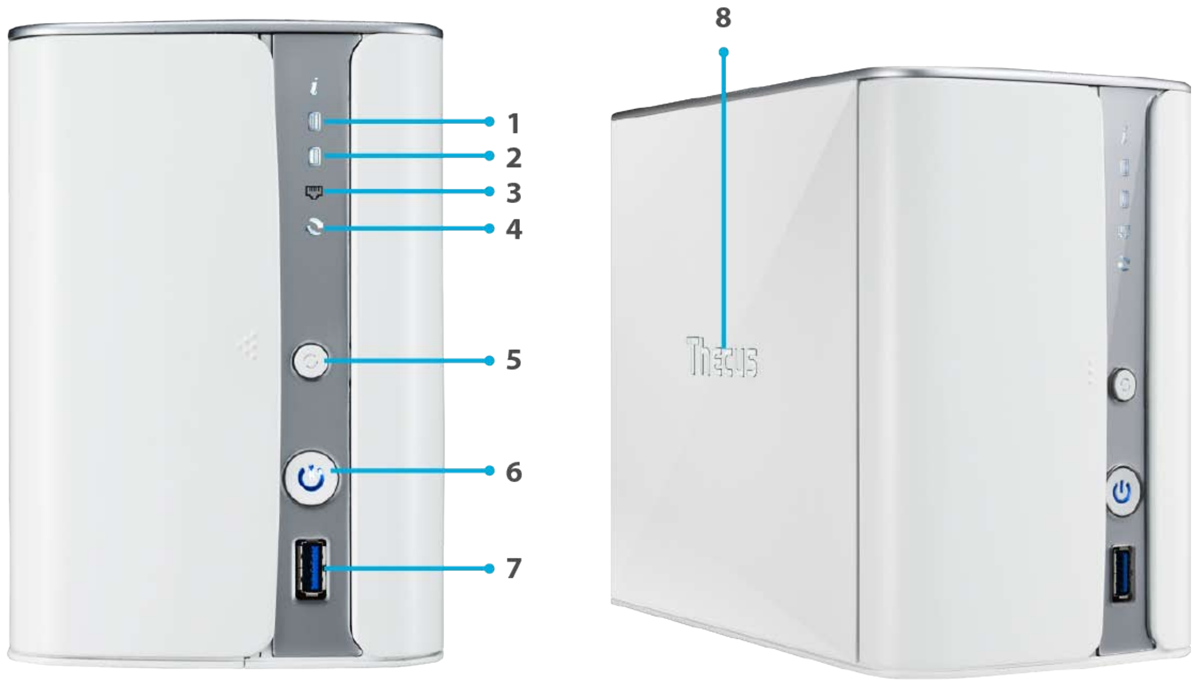
- System Unit x1
- QIG (Quick Installation Guide) x1
- CD-Title (Universal CD) x1
- Ethernet Cable x1
- Accessory bag x1
- HDD Compatibility list Card x1
- Multiple Languages Warranty Card x1
- Power cord x1

Please check to see if your package is complete. If you find that some items are missing, contact your dealer.

1.3 Front Panel

- **N2520/N2560:**

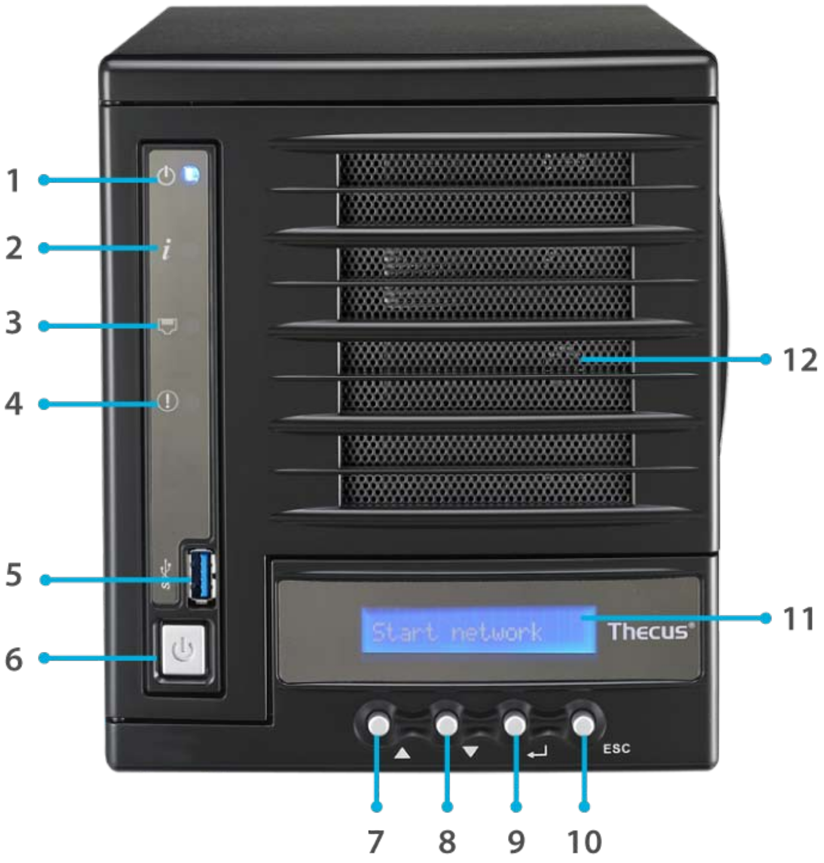
The Thecus N2520/N2560's front panel shows the device's indicators and hard disk install slots:



Front Panel	
Item	**Description**
1. HDD1 LED	Blinking white: HDD activity Red: HDD failure
2. HDD2 LED	Blinking white: HDD activity Red: HDD failure
3. LAN LED	Solid white: LAN Cable link Blinking : Network activity
4. USB LED	Solid white: Installed Blinking white: USB copy activity Solid Red: USB copy failure
5. USB Copy Button	Copies USB storage contents to N2520/N2560.
6. Power Button/LED	Power the N2520/N2560 on/off. Solid blue: System ready Blinking blue: Power on process
7. USB Port	USB 3.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
8. Thecus Logo LED	Solid white: System ready Blinking white: System booting

- **N4520/N4560:**

The Thecus N4520/N4560 front panel shows the device's indicators, system information and hard disk trays:

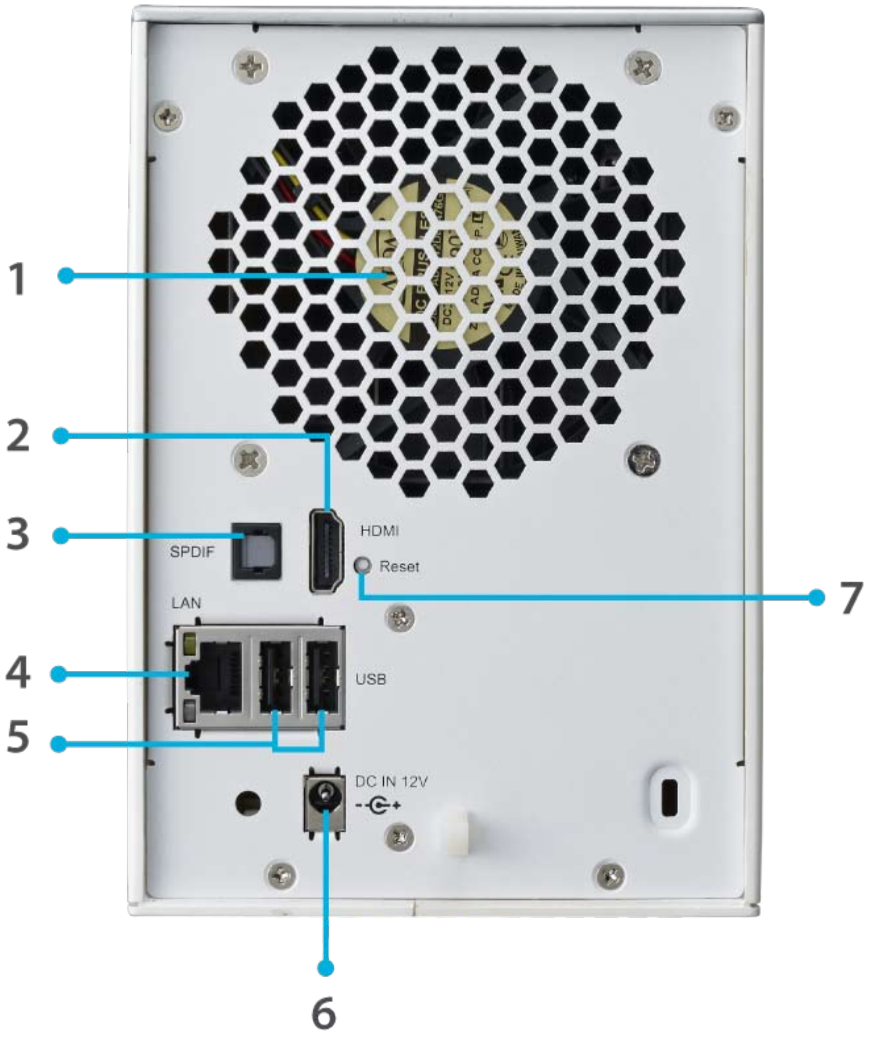


Front Panel	
Item	**Description**
1. Power LED	Solid blue: Power on
2. System status	Blinking orange: Diagnostic mode kick-in Solid orange: Diagnostic completed
3. LAN LED	Green : Network activity
4. System Failure	Red on while diagnostic test failed.
5. USB Port	USB 3.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
6. Power Button	Powers the N4520/N4560 on/off.
7. Up Button	Select the previous configuration settings option.
8. Down Button	USB copy confirmation display.
9. Enter	Enter the selected menu option, sub-menu, or parameter setting.
10. Escape	Escape and return to the previous menu.
11. LCD Display	Displays current system status and warning messages.
12. HDD Tray	Four HDD trays support 4x 3.5" or 4 x 2.5" HDDs

1.4 Rear Panel

- **N2520/N2560:**

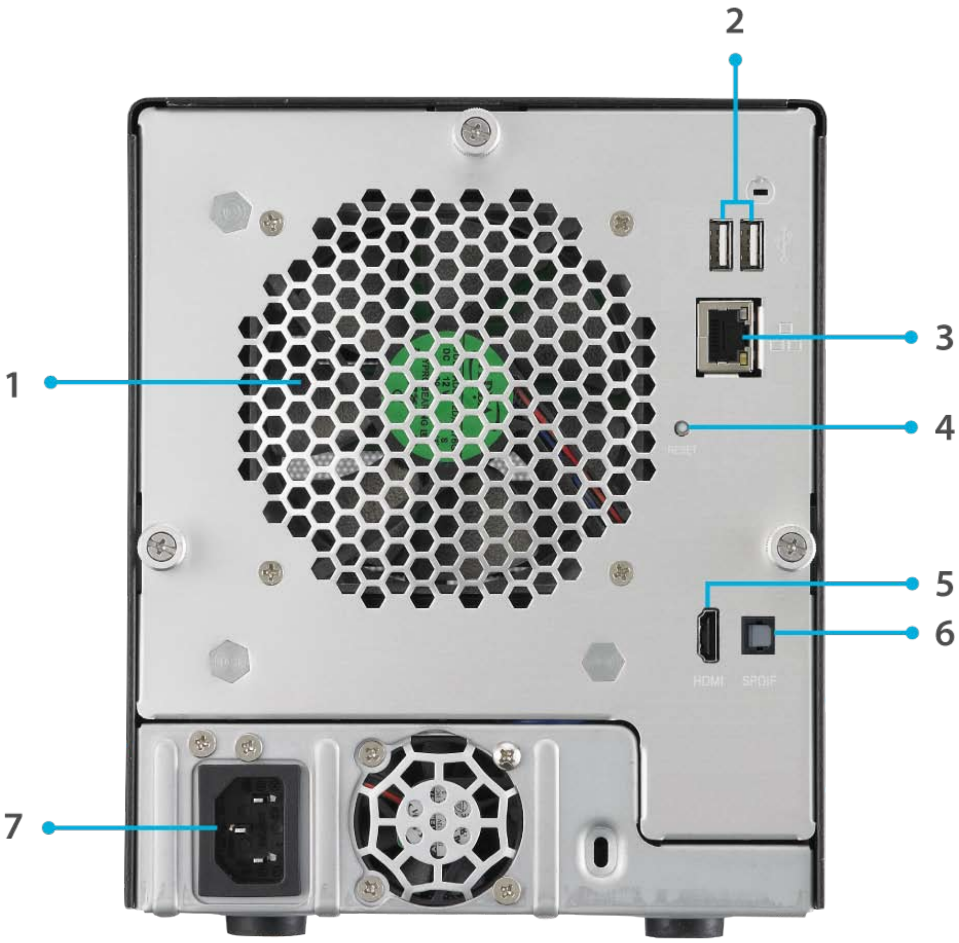
The N2520/N2560 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1. System Fan	System fan that exhausts heat from the unit.
2. HDMI	For Video/Audio out
3. SPDIF	For Audio out
4. LAN Port	LAN port for connecting to an Ethernet network through a switch or a router.
5. USB Port	USB 2.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
6. Power Connector	Connect the included power cords to this connector.
7. Reset Button	Resets the N2520/N2560. Pressing and holding the Reset button on the back for 5 seconds will reset your network setting and password, and turn off Jumbo Frame Support.

- ### N4520/N4560:

The N4520/N4560 rear panel features ports and connectors.



Back Panel	
Item	**Description**
1. System Fan	System fan that exhausts heat from the unit.
2. USB Ports	USB 2.0 port for compatible USB devices, such as digital cameras, USB disks, and USB printers.
3. LAN Port	LAN port for connecting to an Ethernet network through a switch or router
4. Reset Button	Resets the N4520/N4560. Pressing and holding the Reset button on the back for 5 seconds will reset your network setting and password, and turn off Jumbo Frame Support.
5. HDMI	For Video/Audio out
6. SPDIF	For Audio out
7. Power Connector	Connect the included power cords to this connector.

§Chapter 2: Hardware Installation

2.1 Overview

Your Thecus IP storage is designed for easy installation. To help you get started, the following chapter will help you quickly get your Thecus IP storage up and running. Please read it carefully to prevent damaging your unit during installation.

2.2 Before You Begin

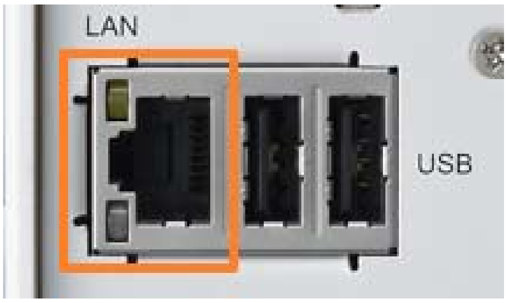
Before you begin, be sure to take the following precautions:

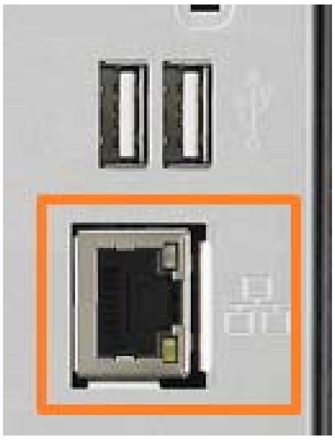
1. Read and understand the Safety Warnings outlined in the beginning of the manual.
2. If possible, wear an anti-static wrist strap during installation to prevent static discharge from damaging the sensitive electronic components on the Thecus IP storage.
3. Be careful not to use magnetized screwdrivers around the Thecus IP storage's electronic components.

2.3 Cable Connections

To connect the Thecus IP storage product to your network, follow the steps below:

1. Connect an Ethernet cable from your network to the LAN port on the back panel of the Thecus IP storage.

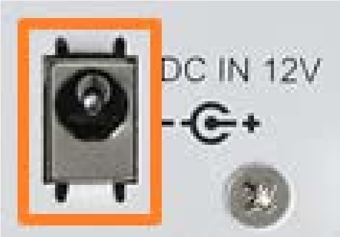




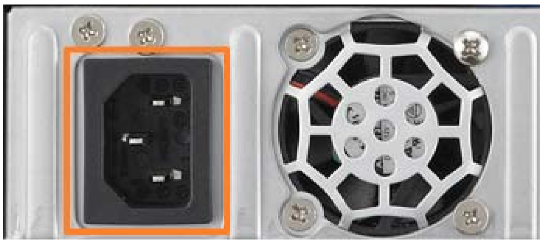
▲ N2520/N2560 LAN port

▲ N4520/N4560 LAN port

2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket.

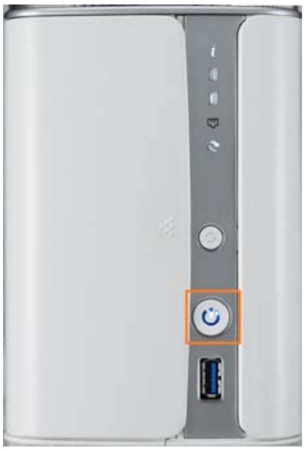


▲ N2520/N2560 power socket

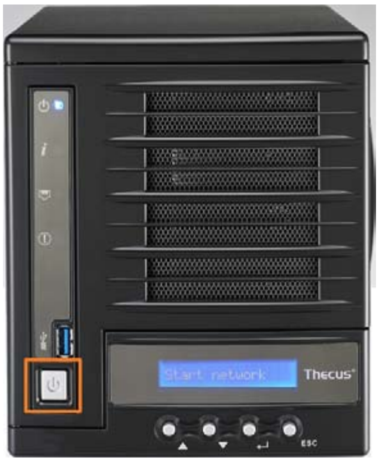


▲ N4520/N4560 power socket

3. Press the power button on the Front Panel to boot up the Thecus IP storage.



▲ N2520/N2560 power button



▲ N4520/N4560 power button

§Chapter 3: System Administration

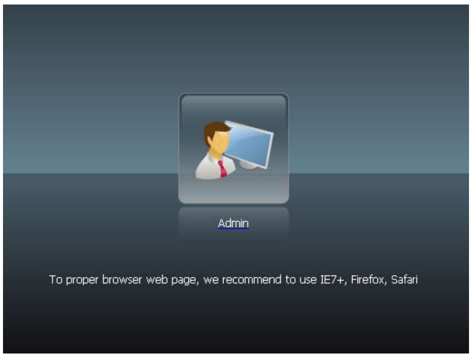
3.1 Overview

The Thecus IP storage provides an easily accessible Web Administration Interface. With it, you can configure and monitor the Thecus IP storage anywhere on the network.

3.2 Web Administration Interface

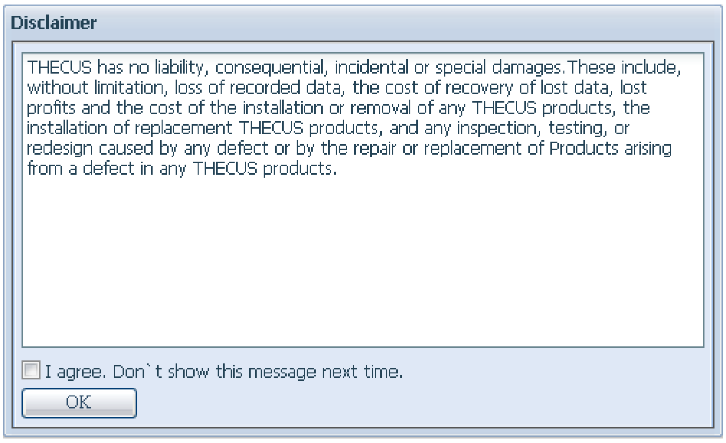
Make sure your network is connected to the Internet. To access Thecus IP storage Web Administration Interface:

1. Type the Thecus IP storage IP address into your browser. (Default IP address can be found through IntelligentNAS utility or LCD panel (N4520/N4560 only))


Admin
To proper browser web page, we recommend to use IE7+, Firefox, Safari

2. Login to the system using the administrator user name and password. The factory defaults are:
   User Name: admin
   Password: admin

   Once you are logged in as an administrator, the disclaimer page will appear as below. Please click the check box if you do not want to have this page displayed during the next login.



Disclaimer

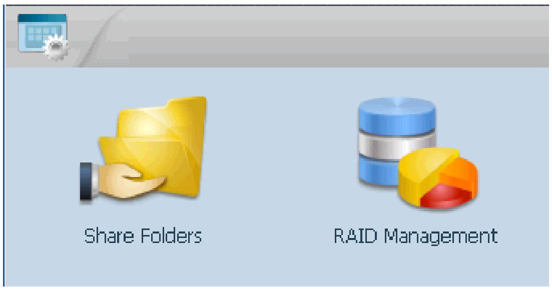
THECUS has no liability, consequential, incidental or special damages.These include, without limitation, loss of recorded data, the cost of recovery of lost data, lost profits and the cost of the installation or removal of any THECUS products, the installation of replacement THECUS products, and any inspection, testing, or redesign caused by any defect or by the repair or replacement of Products arising from a defect in any THECUS products.

☐ I agree. Don`t show this message next time.

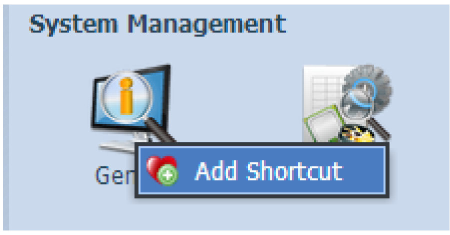
Following the disclaimer page, you will see the Web Administration Interface. From here, you can configure and monitor virtually every aspect of the Thecus IP storage from anywhere on the network.

3.2.1 Add Shortcut

The user interface with "Add Shortcut" shortcut allows the user to designate often used items and have them display on the main screen area. The figure below displays system add shortcut functions.

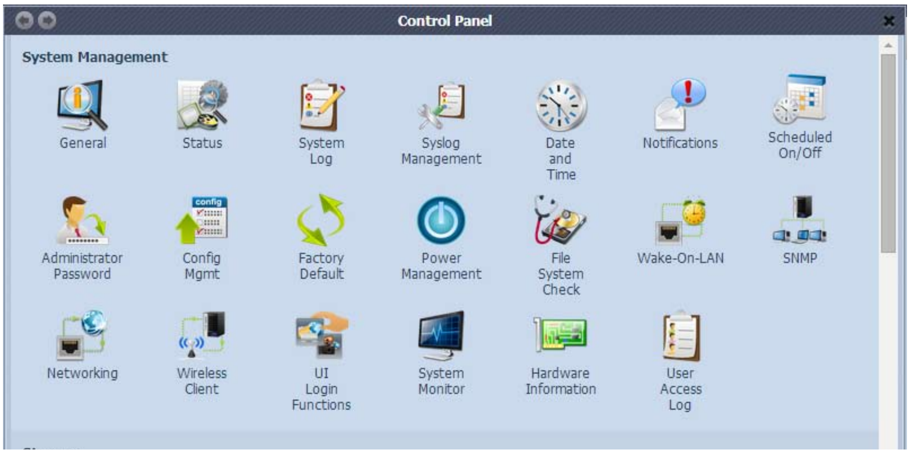


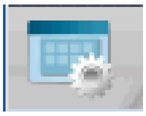
Administrators can add or remove add shortcut functions to My Favorites by right clicking the mouse on the item..



3.2.2 Control Panel

The Control Panel is where you will find all of the information screens and system settings of Thecus IP storage.



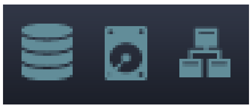


Control Panel	
Item	**Description**
System Management	Current system status of the Thecus IP storage.
Storage	Information and settings for storage devices installed into the Thecus IP storage.
File Sharing / Privilege	Allows configuration of users and groups.
Network Service	To setup varies protocols which has supported by system
Application Server	Application based program for system build-in, additional installed from official or 3rd party.
Backup	Category of Backup Features setup of the Thecus IP storage.
External Devices	Setting for devices where has installed through external interface such as USB

In the following sections, you will find detailed explanations of each function, and how to configure your Thecus IP storage.

3.2.3 Message Bar

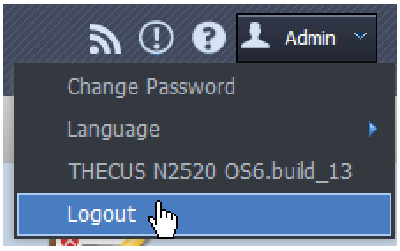
You can get quick information about your system status by moving your mouse over these icons.



Message Bar		
Item	**Status**	**Description**
🛢	RAID Management	Display the status of created RAID volume. Click to go to RAID Management page as short cut.
💽	Disks Information	Display the status of disks installed in the system. Click to go to Disk information page as short cut.
🖧	Network	Green: Connection to the network is normal. Red: abnormal connection to the network

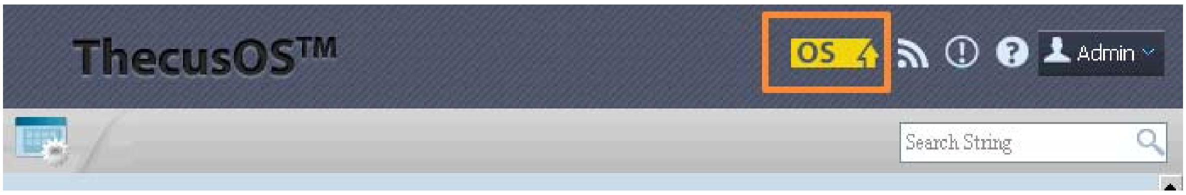
3.2.4 Logout

Click to logout Web Administration Interface.



3.2.5 Online Update Notification

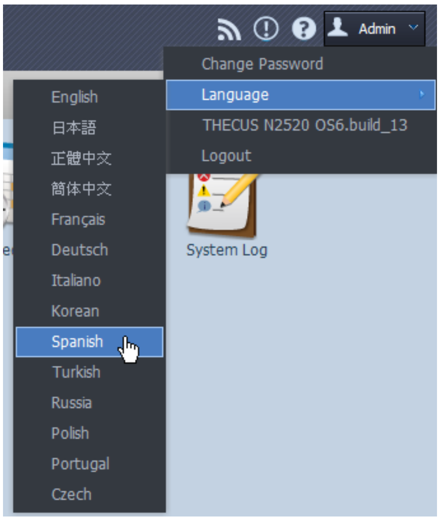
When there is a new update for system files or applications, the system will notify you through the admin UI and also send an email. Click on the flashing icon then the system will link you directly to the associated page.



3.2.6 Language Selection

The Thecus IP storage supports multiple Languages, including:

- English
- Japanese
- Traditional Chinese
- Simplified Chinese
- French
- German
- Italian
- Korean
- Spanish
- Russian
- Polish
- Portuguese



On the menu bar, click Language and the selection list appears. This user interface will switch to the selected language for Thecus IP storage.

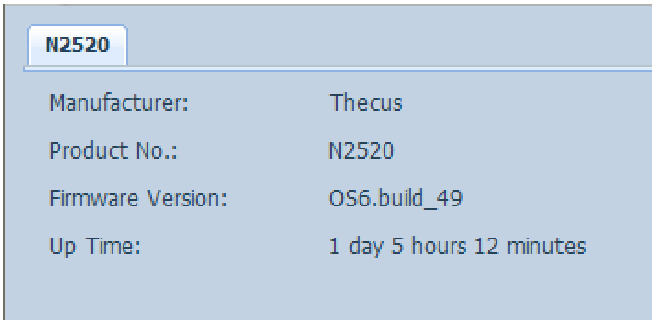
3.3 System Management

Information provides viewing on current Product info, System Status, Service Status and Logs.

The menu bar allows you to see various aspects of the Thecus IP storage. From here, you can discover the status of the Thecus IP storage, and also other details.

3.3.1 General

Once you login, you will first see the basic system Information screen providing Manufacturer, Product No., Firmware Version, and System Up Time information.



N2520

Manufacturer: Thecus

Product No.: N2520

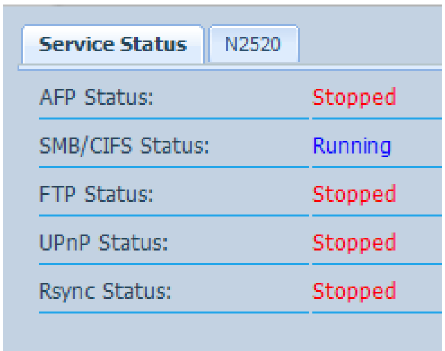
Firmware Version: OS6.build_49

Up Time: 1 day 5 hours 12 minutes

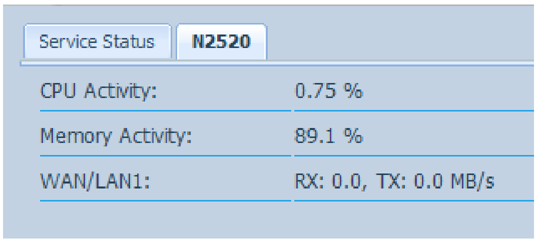
General	
Item	**Description**
Manufacturer	Displays the name of the system manufacturer.
Product No.	Shows the model number of the system.
Firmware version	Shows the current firmware version.
Up time	Displays the total run time of the system.

3.3.2 System/Service Status

From the System Management category,, choose the Status item, System Service Status and HW Status screens appear. These screens provide basic system and service status information.



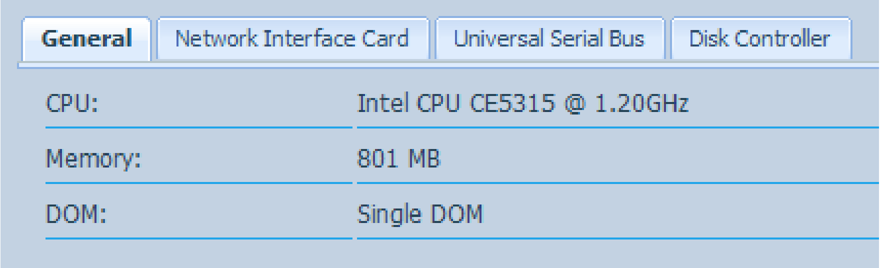
AFP Status:	Stopped
SMB/CIFS Status:	Running
FTP Status:	Stopped
UPnP Status:	Stopped
Rsync Status:	Stopped



CPU Activity:	0.75 %
Memory Activity:	89.1 %
WAN/LAN1:	RX: 0.0, TX: 0.0 MB/s

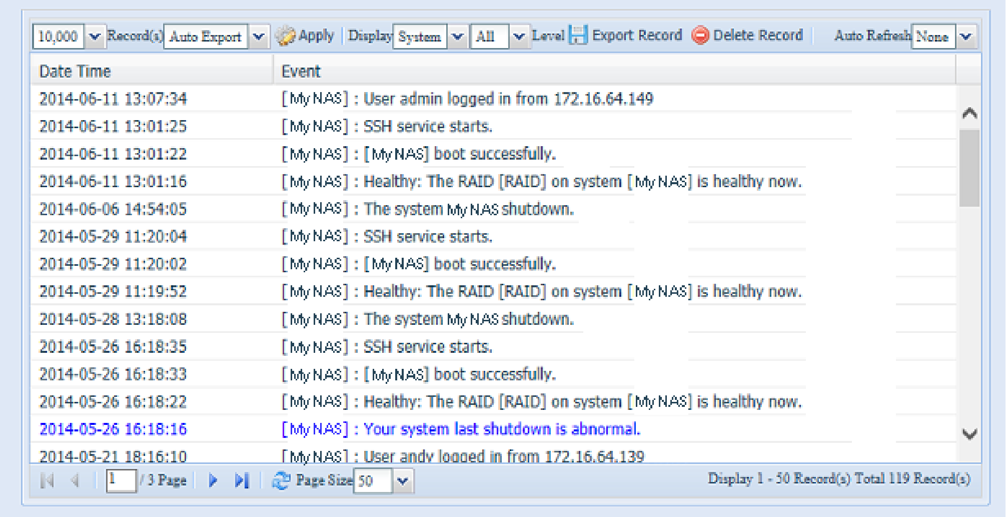
3.3.3 Hardware Information

From the System Management category,, choose the Hardware Information item and the system will display the related HW details for the associated model. Below is an example of the information for a Thecus N2520.



CPU:	Intel CPU CE5315 @ 1.20GHz
Memory:	801 MB
DOM:	Single DOM

3.3.4 Logs



Date Time	Event
2014-06-11 13:07:34	[My NAS] : User admin logged in from 172.16.64.149
2014-06-11 13:01:25	[My NAS] : SSH service starts.
2014-06-11 13:01:22	[My NAS] : [My NAS] boot successfully.
2014-06-11 13:01:16	[My NAS] : Healthy: The RAID [RAID] on system [My NAS] is healthy now.
2014-06-06 14:54:05	[My NAS] : The system My NAS shutdown.
2014-05-29 11:20:04	[My NAS] : SSH service starts.
2014-05-29 11:20:02	[My NAS] : [My NAS] boot successfully.
2014-05-29 11:19:52	[My NAS] : Healthy: The RAID [RAID] on system [My NAS] is healthy now.
2014-05-28 13:18:08	[My NAS] : The system My NAS shutdown.
2014-05-26 16:18:35	[My NAS] : SSH service starts.
2014-05-26 16:18:33	[My NAS] : [My NAS] boot successfully.
2014-05-26 16:18:22	[My NAS] : Healthy: The RAID [RAID] on system [My NAS] is healthy now.
2014-05-26 16:18:16	[My NAS] : Your system last shutdown is abnormal.
2014-05-21 18:16:10	[My NAS] : User andy logged in from 172.16.64.139

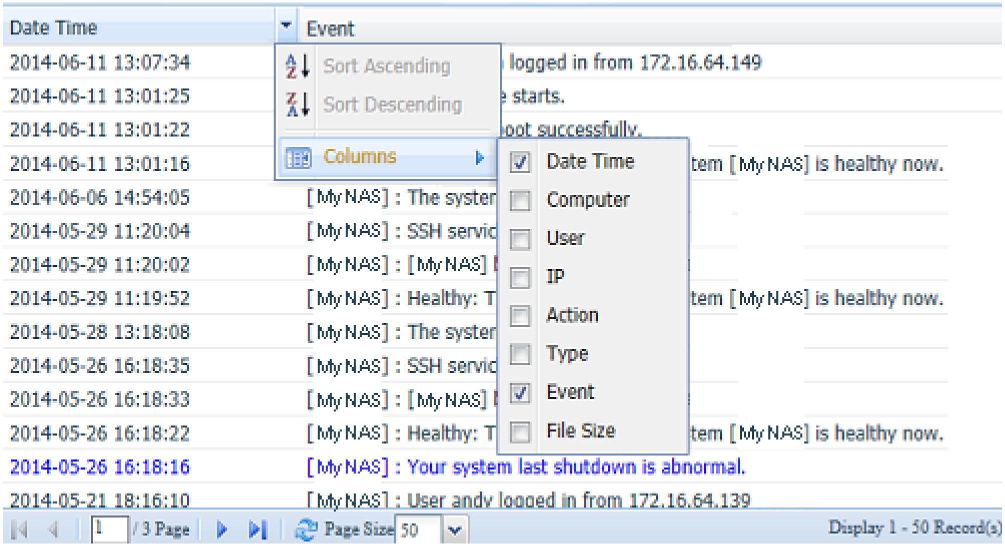
From the System Management category, choose the System Logs item and the System Logs screen will appear. This screen shows a history of system usage and important events such as disk status, network information, and system booting.

See the following table for a detailed description of each item:

System Logs	
Item	**Description**
Number of records to export	This can be selected from a dropdown list to export the log(s) as a single file.

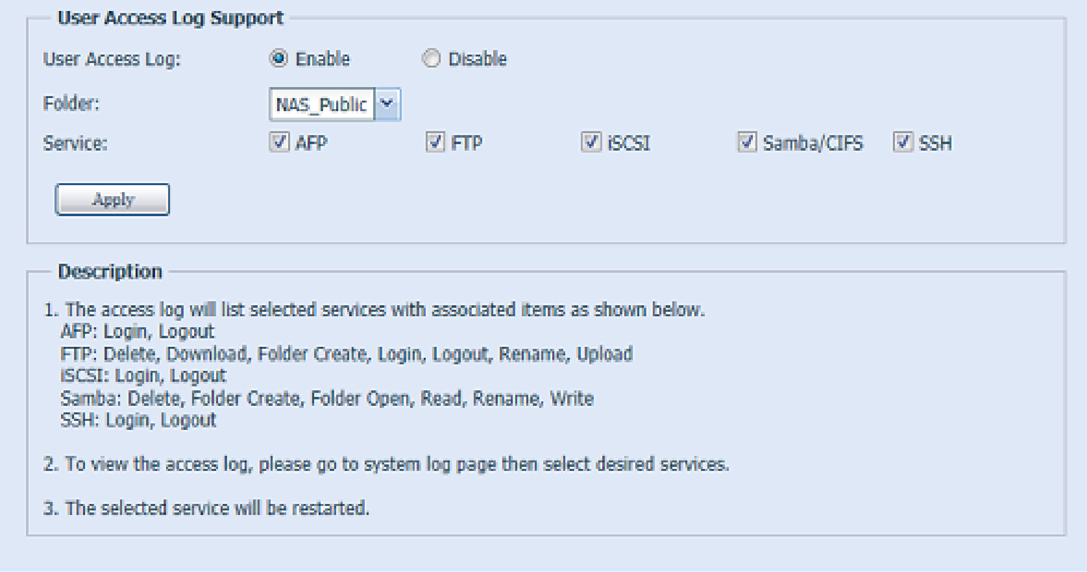
Export log option	This can be set to Auto Export or Auto Delete.
Log Type	The default logs displayed are for system events. From the dropdown list, administrators can choose from various forms of user access, such as AFP, Samba, etc. Note: Users need to enable the "User Access Log" service to view these details.
Log Level	ALL: Provides all log information including system, warning, and error messages. INFO: Shows information about system messages. WARN: Shows only warning messages. ERROR: Shows only error messages.
Export Records	Export all logs to an external file.
Delete Records	Clear all log files.
The number of lines per page	Specify the desired number of lines to display per page.
Sort Ascending	Shows logs by date in ascending order.
Sort Descending	Shows logs by date in descending order.
|<< < > >>|	Use the forward (> >>|) and backward (|<< <) buttons to browse through the log pages.
🔄	Reload logs.

Columns can also be added to display additional information about each event.



```
Date Time             Event
2014-06-11 13:07:34   logged in from 172.16.64.149
2014-06-11 13:01:25   starts.
2014-06-11 13:01:22   oot successfully.
2014-06-11 13:01:16   tem [MyNAS] is healthy now.
2014-06-06 14:54:05   [MyNAS] : The syster
2014-05-29 11:20:04   [MyNAS] : SSH servic
2014-05-29 11:20:02   [MyNAS] : [MyNAS]
2014-05-29 11:19:52   [MyNAS] : Healthy: T   tem [MyNAS] is healthy now.
2014-05-28 13:18:08   [MyNAS] : The syster
2014-05-26 16:18:35   [MyNAS] : SSH servic
2014-05-26 16:18:33   [MyNAS] : [MyNAS]
2014-05-26 16:18:22   [MyNAS] : Healthy: T   tem [MyNAS] is healthy now.
2014-05-26 16:18:16   [MyNAS] : Your system last shutdown is abnormal.
2014-05-21 18:16:10   [MyNAS] : User andy logged in from 172.16.64.139
```

3.3.5 User Access Log



User Access Log Support

User Access Log: ● Enable ○ Disable

Folder: NAS_Public

Service: ☑ AFP ☑ FTP ☑ iSCSI ☑ Samba/CIFS ☑ SSH

Description

1. The access log will list selected services with associated items as shown below.
   AFP: Login, Logout
   FTP: Delete, Download, Folder Create, Login, Logout, Rename, Upload
   iSCSI: Login, Logout
   Samba: Delete, Folder Create, Folder Open, Read, Rename, Write
   SSH: Login, Logout

2. To view the access log, please go to system log page then select desired services.

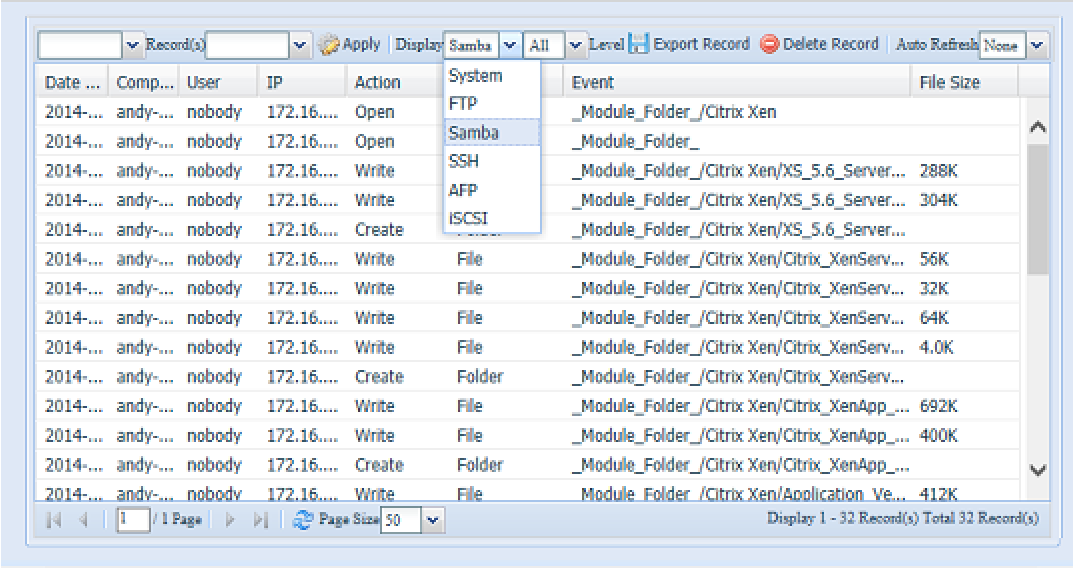
3. The selected service will be restarted.

The User Access Log Support section allows administrators to select the desired protocols to record user activity for.

User Access Log	
Item	**Description**
User access log	Enable or disable the User Access Log service.
Folder	Select from the dropdown list where to store the user access log.
Service	Select from the check box which access details to record.
Apply	Click Apply to save changes.
Description	The user access list will record different activities depending on which protocol is selected.1. AFP: User login and logout. 2. FTP: User file deletion, uploads/downloads, folder creation, object renaming, and login and logout. 3. iSCSI (if applicable): User login and logout. 4. Samba: User file deletion, folder creation, folder opening, and object reading, renaming, and writing. 5. SSH (if applicable): User login and logout.

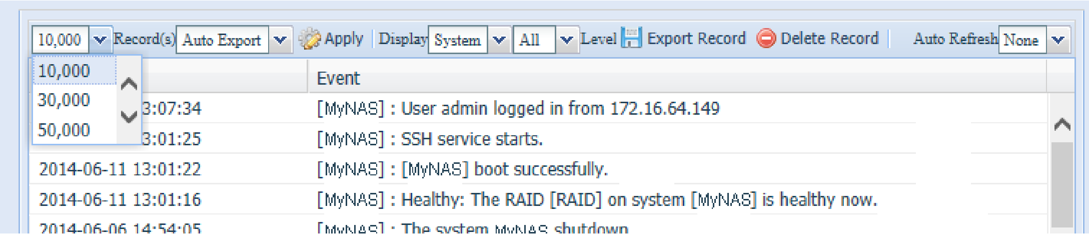
After the User Access Log Support has been set up and the "Apply" button selected, all selected services will restart.

To view user access details related to the selected service(s), please go to System Log and choose a service from the "Display" dropdown list.

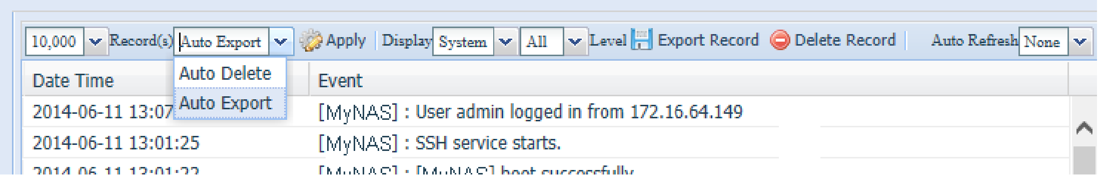


Date ...	Comp...	User	IP	Action		Event	File Size
2014-...	andy-...	nobody	172.16....	Open		_Module_Folder_/Citrix Xen	
2014-...	andy-...	nobody	172.16....	Open		_Module_Folder_	
2014-...	andy-...	nobody	172.16....	Write		_Module_Folder_/Citrix Xen/XS_5.6_Server...	288K
2014-...	andy-...	nobody	172.16....	Write		_Module_Folder_/Citrix Xen/XS_5.6_Server...	304K
2014-...	andy-...	nobody	172.16....	Create		_Module_Folder_/Citrix Xen/XS_5.6_Server...	
2014-...	andy-...	nobody	172.16....	Write	File	_Module_Folder_/Citrix Xen/Citrix_XenServ...	56K
2014-...	andy-...	nobody	172.16....	Write	File	_Module_Folder_/Citrix Xen/Citrix_XenServ...	32K
2014-...	andy-...	nobody	172.16....	Write	File	_Module_Folder_/Citrix Xen/Citrix_XenServ...	64K
2014-...	andy-...	nobody	172.16....	Write	File	_Module_Folder_/Citrix Xen/Citrix_XenServ...	4.0K
2014-...	andy-...	nobody	172.16....	Create	Folder	_Module_Folder_/Citrix Xen/Citrix_XenServ...	
2014-...	andy-...	nobody	172.16....	Write	File	_Module_Folder_/Citrix Xen/Citrix_XenApp_...	692K
2014-...	andy-...	nobody	172.16....	Write	File	_Module_Folder_/Citrix Xen/Citrix_XenApp_...	400K
2014-...	andy-...	nobody	172.16....	Create	Folder	_Module_Folder_/Citrix Xen/Citrix_XenApp_...	
2014-...	andy-...	nobody	172.16....	Write	File	_Module_Folder_/Citrix Xen/Application_Ve...	412K

To export details from the User Access Log as a single file from target folder, administrators must first select the desired number of records from the dropdown list and also select the "Auto export" option. Please choose the number of logs export and click "Apply" to activate these settings.

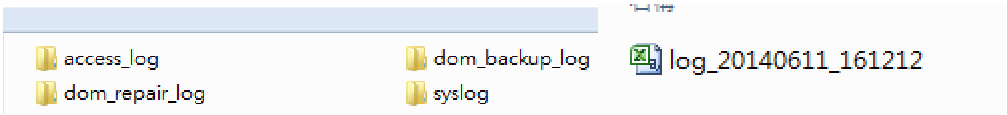


	Event
3:07:34	[MyNAS] : User admin logged in from 172.16.64.149
3:01:25	[MyNAS] : SSH service starts.
2014-06-11 13:01:22	[MyNAS] : [MyNAS] boot successfully.
2014-06-11 13:01:16	[MyNAS] : Healthy: The RAID [RAID] on system [MyNAS] is healthy now.
2014-06-06 14:54:05	[MyNAS] : The system MyNAS shutdown



Date Time	Event
2014-06-11 13:07	[MyNAS] : User admin logged in from 172.16.64.149
2014-06-11 13:01:25	[MyNAS] : SSH service starts.
2014-06-11 13:01:22	[MyNAS] : [MyNAS] boot successfully.

Once (for example) 10,000 records have been reached, the log file will appear in /NAS_public/access_log/



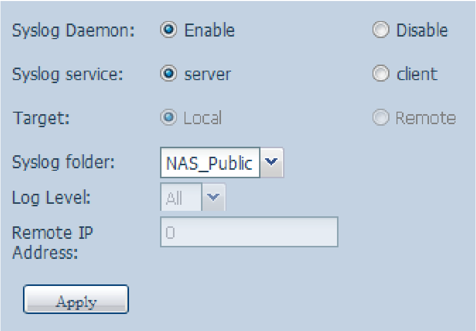
3.3.6 Syslog Management

Generates system log to be stored locally or remotely, it also can be chose to act as syslog server for all other devices.

These messages are stored on your NAS in: Nsync > log> messages.

Information can be obtained in two ways: locally and remotely.

- **Configuration with syslog server:**
- **Configuration with syslog client and target to store locally:**



Syslog Daemon: ● Enable ○ Disable

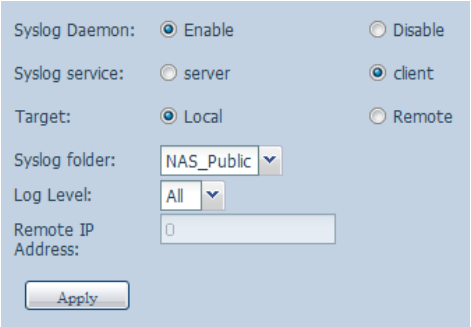
Syslog service: ● server ○ client

Target: ● Local ○ Remote

Syslog folder: NAS_Public

Log Level: All

Remote IP Address: 0



Syslog Daemon: ● Enable ○ Disable

Syslog service: ○ server ● client

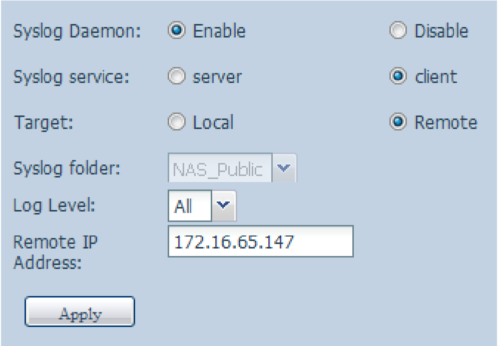
Target: ● Local ○ Remote

Syslog folder: NAS_Public

Log Level: All

Remote IP Address: 0

- **Configuration with syslog client and target to store remotely:**



Syslog Daemon: ● Enable ○ Disable

Syslog service: ○ server ● client

Target: ○ Local ● Remote

Syslog folder: NAS_Public

Log Level: All

Remote IP Address: 172.16.65.147

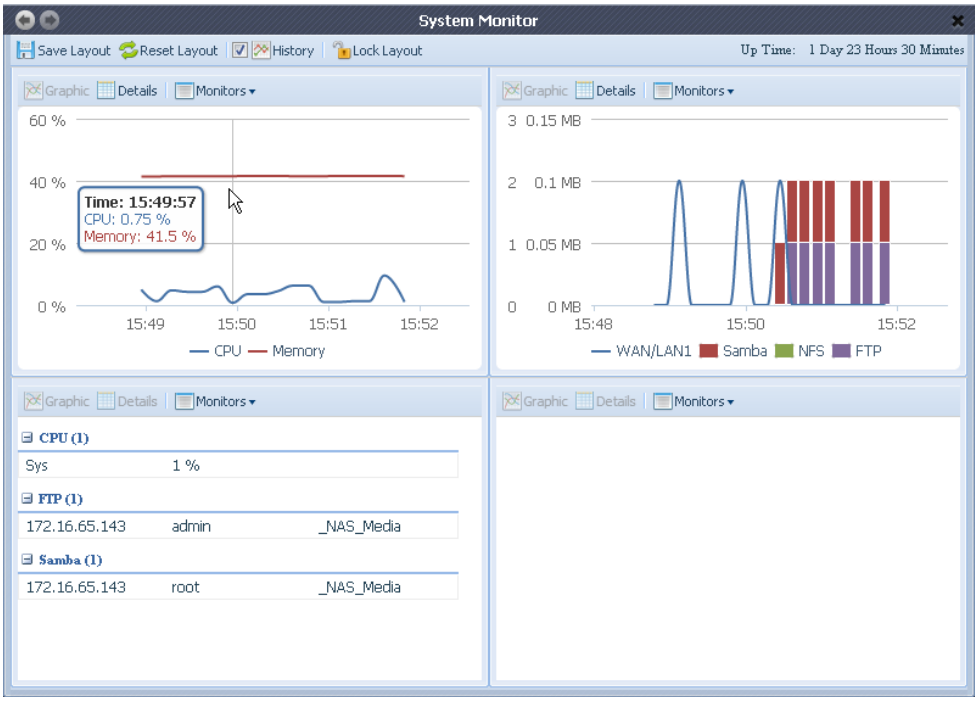
See the following table for a detailed description of each item:

Syslog Management	
Item	**Description**
Syslog Daemon	Enable/Disable syslog daemon.
Syslog service	If Server has been selected then associated syslog folder will be used to store all system logs from other NAS devices which has assigned this system for syslog server as well as syslog of this server unit. It can be seen from associated syslog folder with files "error", "Information" and "warning". If client has been selected then "Local" or "Remotely" can be choose.
Target	Choose Local, all system logs will be stored in an associated syslog folder filled in from next filed. And the syslog folder will have file "Associated log info" to store all system logs. If Remotely has been selected, a syslog server is needed and an IP address is required=.
Syslog folder	Select from a drop down share list, all of the system logs will be stored on it. This syslog folder is applied to "syslog server" or "syslog client" with "local" selected.
Log Level	The user can choose from 3 different levels. "All", "Warning/Error" or "Error".
Remote IP Address	Input the syslog server IP address if choose to store syslog info remotely.

3.3.7 System Monitor

The system monitor is capable to monitor system status including CPU/memory utilization, network throughput and on-line user list in various protocols.

To monitor system status, simply click on “System Monitor” from the tree menu and the screen will appear as below.



Up Time: 1 Day 23 Hours 30 Minutes

⊟ CPU (1)

Sys	1 %	

⊟ FTP (1)

172.16.65.143	admin	_NAS_Media

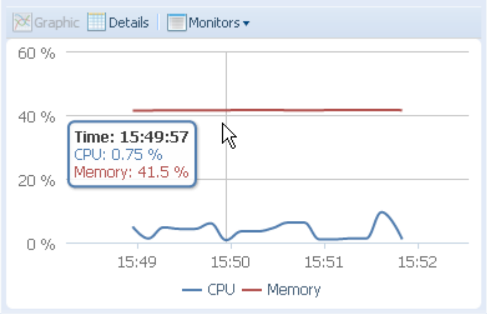
⊟ Samba (1)

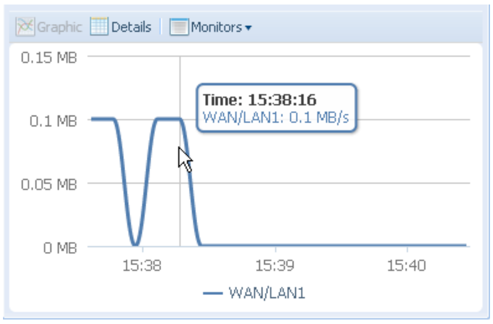
172.16.65.143	root	_NAS_Media

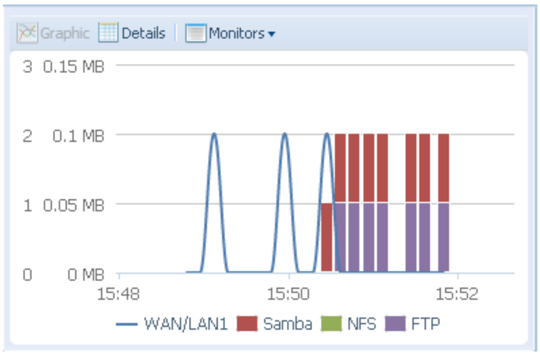
It is divided into 4 sections. Each section can be modified to monitor specific items by using the drop down list from the “Monitors” tab, simply click on the items you would like to monitor. From each section, you can also choose to display the information graphically by selecting “Graphic” or by plain text mode by selecting “Details”.

Only 2 sections can be set in graphic mode at the same time.

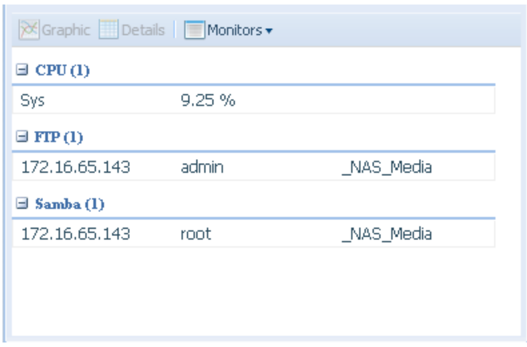
If graphic mode is chosen, 3 minutes of information is displayed on the x-axis. A resume of the information is displayed by dragging the mouse over the graphic at a specific time. See example below:







For the on-line users list, system monitor will display the on-line users and the share folder they have visited.



⊟ CPU (1)

Sys	9.25 %	

⊟ FTP (1)

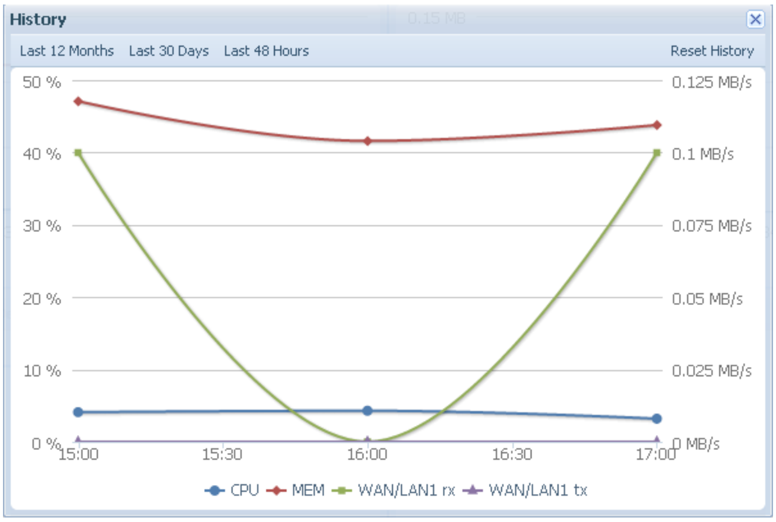
172.16.65.143	admin	_NAS_Media

⊟ Samba (1)

172.16.65.143	root	_NAS_Media

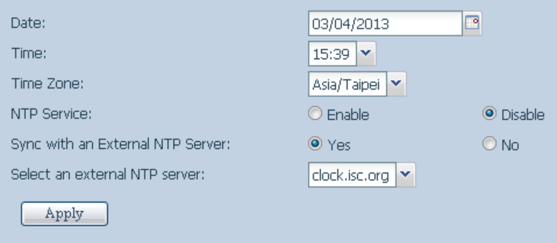
System Monitor	
Item	**Description**
Save Layout	Saving selected monitoring items. Layout will remain the same for future visits.
Reset Layout	Set back to default monitoring settings and layout.
History	Click on this check box and system monitor will write the monitoring history to a designate path in the RAID volume.
Lock Layout	All of the monitoring items are fixed and cannot be changed. Click again to unlock it.

If the History has been enabled, click on ☑ History and system monitor will display the history with different period for selection.



3.3.8 Date and Time: Setting system time

From the System Management category, choose the Date and Time item and the Date and Time screen appears. Set the desired Date, Time, and Time Zone. You can also elect to synchronize the system time on Thecus IP storage with an NTP (Network Time Protocol) Server.

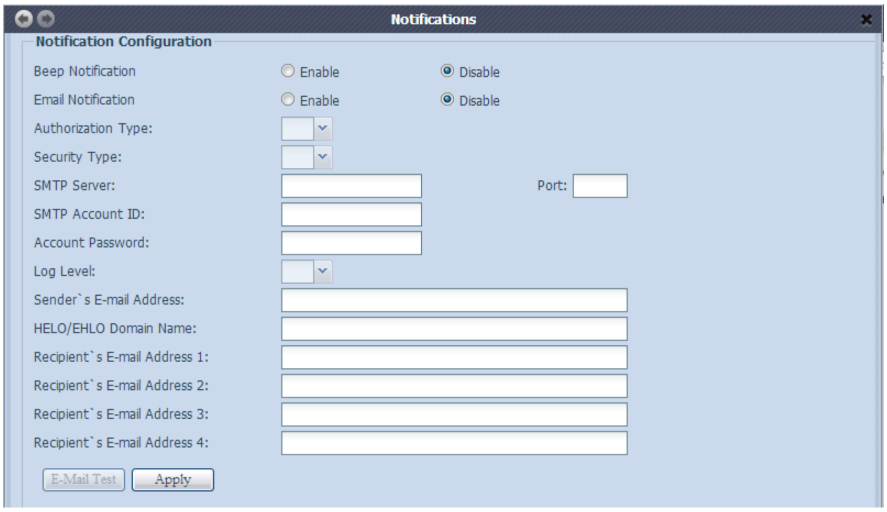


Date: 03/04/2013
Time: 15:39
Time Zone: Asia/Taipei
NTP Service: ○ Enable ● Disable
Sync with an External NTP Server: ● Yes ○ No
Select an external NTP server: clock.isc.org

See the following table for a detailed description of each item:

Date and Time	
Item	**Description**
Date	Sets the system date.
Time	Sets the system time.
Time Zone	Sets the system time zone.
NTP Service	Select ***Enable*** to synchronize with the NTP server. Select Disable to close the NTP server synchronization.
Sync with external NTP Server	Select YES to allow Thecus IP storage to synchronize with an NTP server of your choice. Press Apply to change.

3.3.9 Notifications configuration



Notifications

Notification Configuration

Beep Notification ○ Enable ● Disable
Email Notification ○ Enable ● Disable
Authorization Type:
Security Type:
SMTP Server: Port:
SMTP Account ID:
Account Password:
Log Level:
Sender`s E-mail Address:
HELO/EHLO Domain Name:
Recipient`s E-mail Address 1:
Recipient`s E-mail Address 2:
Recipient`s E-mail Address 3:
Recipient`s E-mail Address 4:

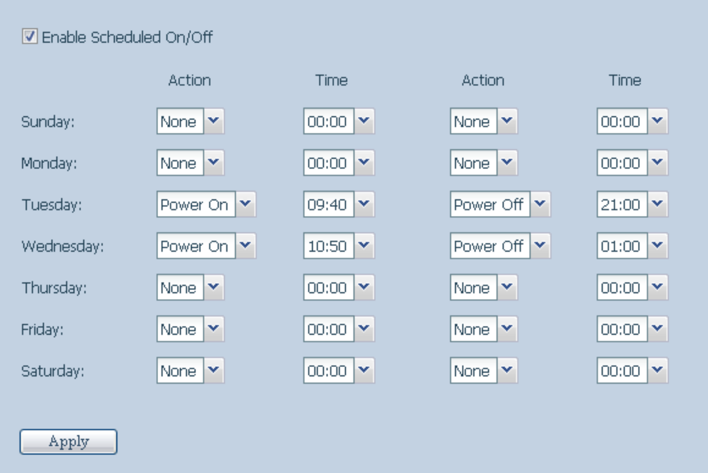
From the System Management category, choose the Notifications item, and the Notifications Configuration screen appears. This screen lets you have Thecus IP storage notify you in case of any system malfunction. Press Apply to confirm all settings. See following table for a detailed description of each item.

Notifications Configuration	
Item	**Description**
Beep Notification	Enable or disable the system buzzer that beeps when a problem occurs.
Email Notification	Enable or disable email notifications of system problems.
Authentication Type	Select the SMTP Server account authentication type.
Secuity Type	Select desired security type from dropdown list.
SMTP Server	Specifies the hostname/IP address of the SMTP server.
Port	Specifies the port to send outgoing notification emails.
SMTP Account ID	Set the SMTP Server Email account ID.
Account Password	Enter a new password.
Log Level	Select the log level to send the e-mail out.
Sender's E-mail Address	Set senders email address to send email notifications.
HELO/EHLO Domain Name	Filled in valid HELO/EHLO Domain Name.
Receiver's E-mail Address (1,2,3,4)	Add one or more recipient's email addresses to receive email notifications.

3.3.10 Scheduled On/Off

Using the Thecus IP storage System Management, you can save energy and money by scheduling the Thecus IP storage to turn itself on and off during certain times of the day.

From the System Management category, choose the Scheduled On/Off item and the Scheduled On/Off screen appears.



☑ Enable Scheduled On/Off

	Action	Time	Action	Time
Sunday:	None	00:00	None	00:00
Monday:	None	00:00	None	00:00
Tuesday:	Power On	09:40	Power Off	21:00
Wednesday:	Power On	10:50	Power Off	01:00
Thursday:	None	00:00	None	00:00
Friday:	None	00:00	None	00:00
Saturday:	None	00:00	None	00:00

To designate a schedule for the Thecus IP storage to turn on and off, first enable the feature by checking the Enable Scheduled On/Off checkbox.

Then, simply choose an on and off time for each day of the week.

Finally, click Apply to save your changes.

Example - Monday: On: 8:00; Off: 16:00

System will turn on at 8:00 AM on Monday, and off at 16:00 on Monday. System will turn on for the rest of the week.

If you choose an on time, but do not assign an off time, the system will turn on and remain on until a scheduled off time is reached, or if the unit is shutdown manually.

Example - Monday: On: 8:00

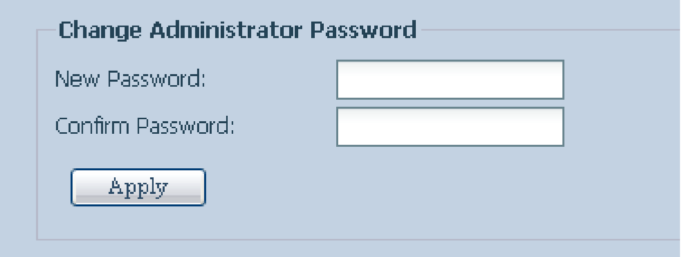
System will turn on at 8:00 AM on Monday, and will not shut down unless powered down manually. You may also choose two on times or two off times on a particular day, and the system will act accordingly.

Example - Monday: Off: 8:00; Off: 16:00

System will turn off at 8:00 AM on Monday. System will turn off at 16:00 PM on Monday, if it was on. If the system was already off at 16:00 PM on Monday, system will stay off.

3.3.11 Administrator Password

From the System Management category, choose the Administrator Password item and the Change Administrator Password screen appears. Enter a new password in the New Password box and confirm your new password in the Confirm Password box. Press Apply to confirm password changes.

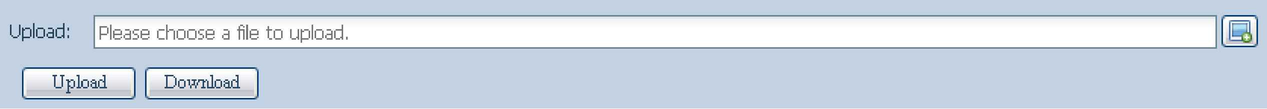


See the following table for a detailed description of each item.

Change Administrator	
Item	**Description**
New Password	Type in a new administrator password.
Confirm Password	Type the new password again to confirm.
Apply	Press this to save your changes.

3.3.12 Config Mgmt

From the System Management category, choose the Config Mgmt item and the System Configuration Download/Upload screen appears. From here, you can download or upload stored system configurations.



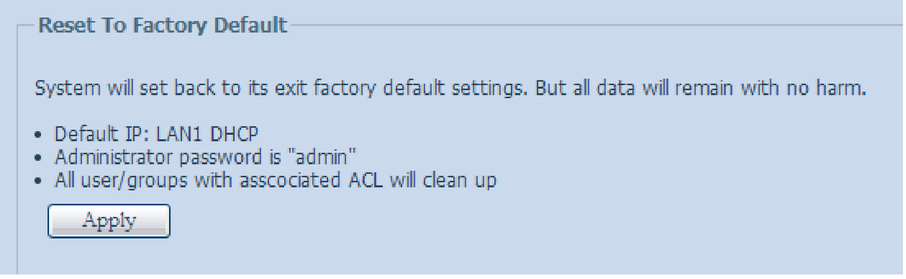
See the following table for a detailed description of each item.

System Configuration Download/Upload	
Item	**Description**
Download	Save and export the current system configuration.
Upload	Import a saved configuration file to overwrite the current system configuration.

Backing up your system configuration is a great way to ensure that you can revert to a working configuration when you are experimenting with new system settings.
The system configuration you have backed up can only be restored in the same firmware version. The backup details exclude user/group accounts.

3.3.13 Factory Default

From the System Management category, choose the Factory Default item and the Reset to Factory Default screen appears. Press Apply to reset Thecus IP storage to factory default settings.



Reset To Factory Default

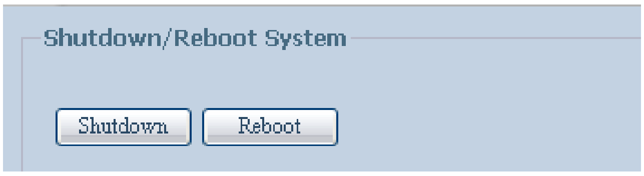
System will set back to its exit factory default settings. But all data will remain with no harm.

- Default IP: LAN1 DHCP
- Administrator password is "admin"
- All user/groups with asscociated ACL will clean up

Resetting to factory defaults will not erase the data stored in the hard disks, but WILL revert all the settings to the factory default values

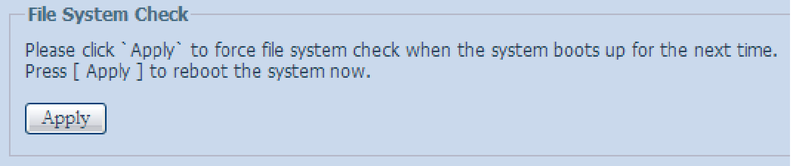
3.3.14 Power Management

From the System Management category, choose Power Management item, and the Shutdown/Reboot System screen appears. Press Reboot to restart the system or Shutdown to turn the system off.



3.3.15 File System Check

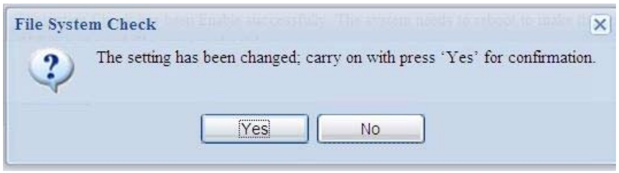
The File System Check allows you to perform a check on the integrity of your disks' file system. Under the System Management category, click File system Check and the File System Check prompt appears.



Please click `Apply` to force file system check when the system boots up for the next time.
Press [Apply] to reboot the system now.

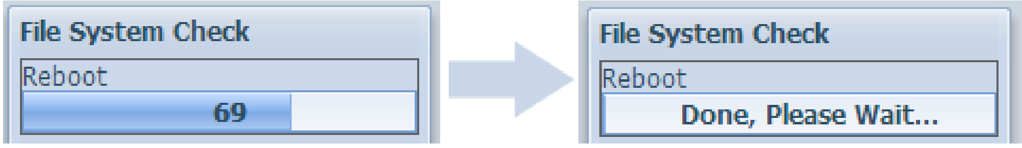
To perform a file system check, click Apply.

Once clicked, the following prompt will appear:

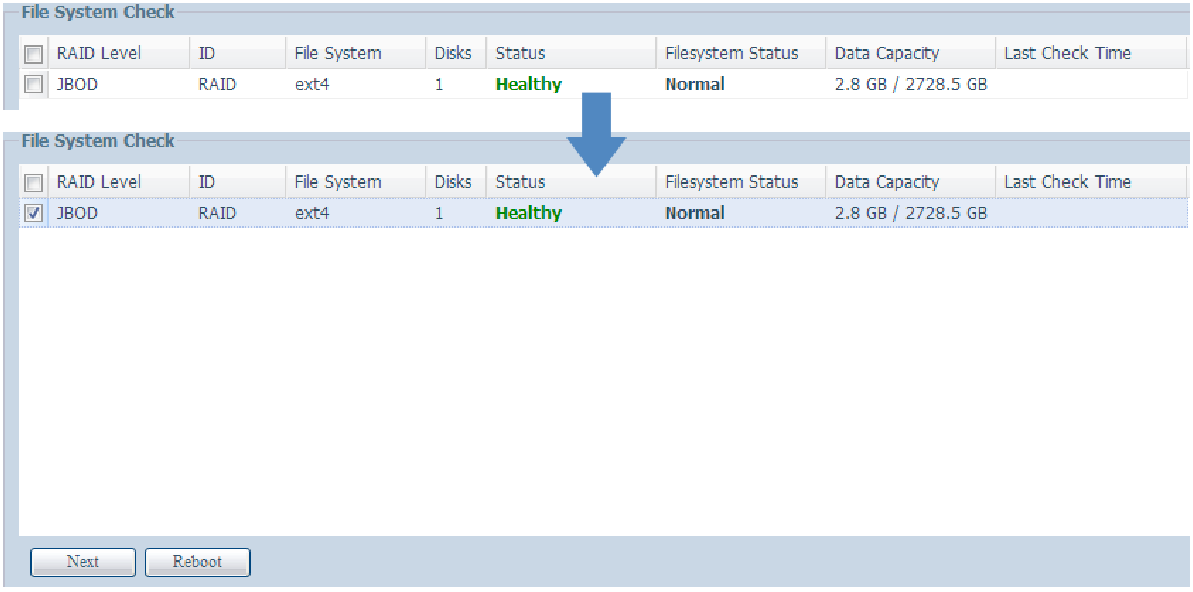


The setting has been changed; carry on with press 'Yes' for confirmation.

Click Yes to reboot the system.



Once the system has rebooted, you will be returned to the File System Check prompt. There you will see the available RAID volumes to run the file system check. Check the desired RAID volumes and click Next to proceed with the file system check. Click Reboot to reboot without running the check.



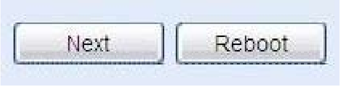
File System Check

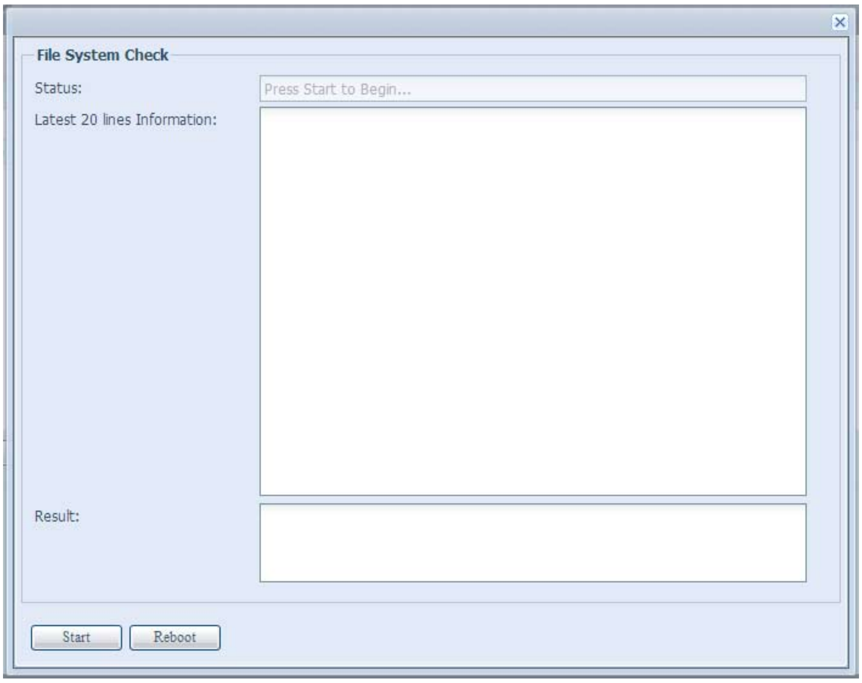
□	RAID Level	ID	File System	Disks	Status	Filesystem Status	Data Capacity	Last Check Time
□	JBOD	RAID	ext4	1	**Healthy**	**Normal**	2.8 GB / 2728.5 GB	

File System Check

□	RAID Level	ID	File System	Disks	Status	Filesystem Status	Data Capacity	Last Check Time
☑	JBOD	RAID	ext4	1	**Healthy**	**Normal**	2.8 GB / 2728.5 GB	

Once you click Next, you will see the following screen:





File System Check

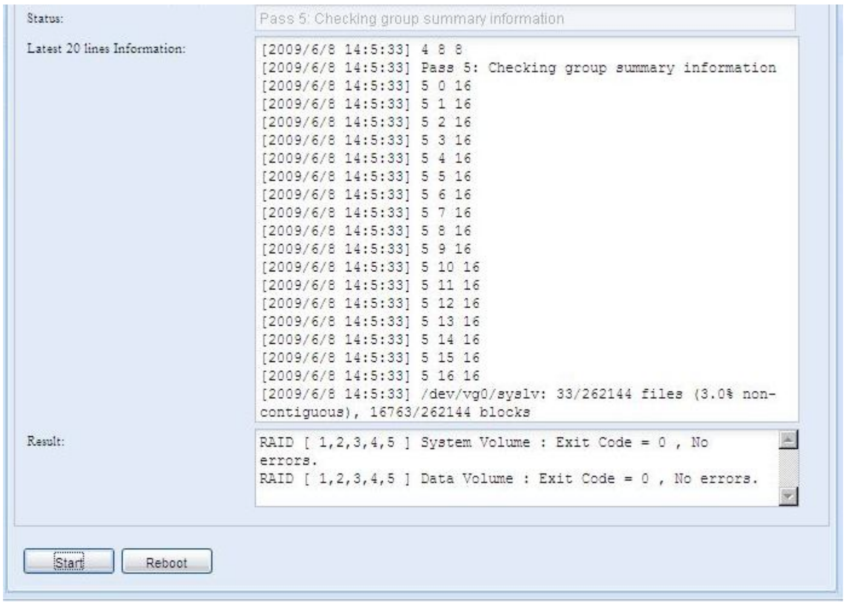
Status: Press Start to Begin...

Latest 20 lines Information:

Result:

Click Start to begin the file system check. Click Reboot to reboot the system.

When the file system check is running, the system will show 20 lines of information until it is complete. Once complete, the results will be shown at the bottom.



Status: Pass 5: Checking group summary information

Latest 20 lines Information:

```
[2009/6/8 14:5:33] 4 8 8
[2009/6/8 14:5:33] Pass 5: Checking group summary information
[2009/6/8 14:5:33] 5 0 16
[2009/6/8 14:5:33] 5 1 16
[2009/6/8 14:5:33] 5 2 16
[2009/6/8 14:5:33] 5 3 16
[2009/6/8 14:5:33] 5 4 16
[2009/6/8 14:5:33] 5 5 16
[2009/6/8 14:5:33] 5 6 16
[2009/6/8 14:5:33] 5 7 16
[2009/6/8 14:5:33] 5 8 16
[2009/6/8 14:5:33] 5 9 16
[2009/6/8 14:5:33] 5 10 16
[2009/6/8 14:5:33] 5 11 16
[2009/6/8 14:5:33] 5 12 16
[2009/6/8 14:5:33] 5 13 16
[2009/6/8 14:5:33] 5 14 16
[2009/6/8 14:5:33] 5 15 16
[2009/6/8 14:5:33] 5 16 16
[2009/6/8 14:5:33] /dev/vg0/syslv: 33/262144 files (3.0% non-
contiguous), 16763/262144 blocks
```

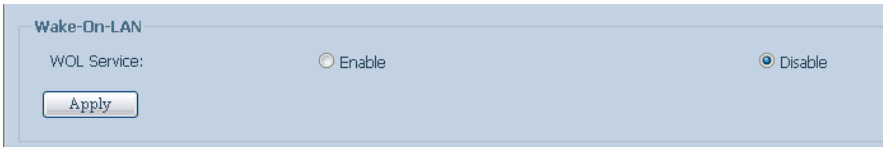
Result:

```
RAID [ 1,2,3,4,5 ] System Volume : Exit Code = 0 , No
errors.
RAID [ 1,2,3,4,5 ] Data Volume : Exit Code = 0 , No errors.
```

The system must be rebooted before Thecus IP storage can function normally after file system check completes.

3.3.16 Wake-Up On LAN (WOL)

The Thecus IP storage has the ability to be awoken from sleep mode via LAN port.



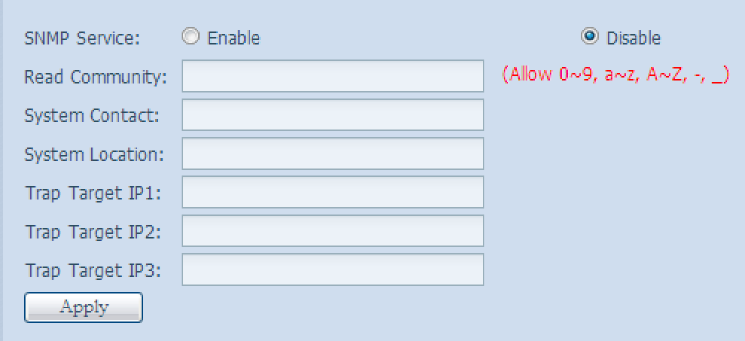
Wake-On-LAN

WOL Service: ○ Enable ● Disable

From the System Management category, choose the WOL item, and the Wake-up On LAN screen appears. From here, you can Enable or Disable.

3.3.17 SNMP Support (N4520/N4560 Only)

From the System Management category, choose the SNMP item and the SNMP Support screen appears. You could enable the SNMP function and filled in the related information in each fields. With the SNMP management software, you can get other system's basic information.



SNMP Service: ○ Enable ● Disable

Read Community: (Allow 0~9, a~z, A~Z, -, _)

System Contact:

System Location:

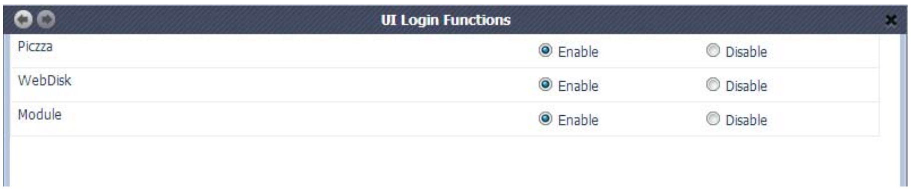
Trap Target IP1:

Trap Target IP2:

Trap Target IP3:

3.3.18 UI Login Function

Adjusts UI Login Configuration settings, you can enable/disable the Web Disk, Photo Server and modules functions, according to your needs.

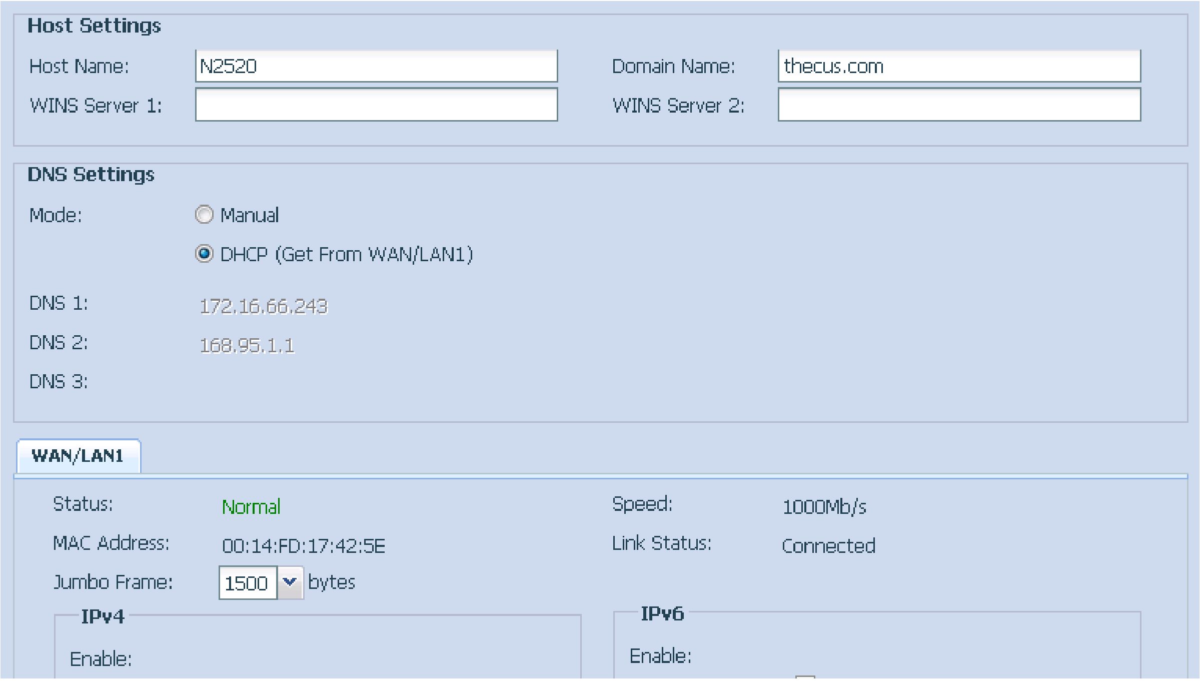


UI Login Functions

Piczza	● Enable	○ Disable
WebDisk	● Enable	○ Disable
Module	● Enable	○ Disable

3.3.19 Networking

From the System Management category, choose Networking, and the Networking Configuration screen appears. This screen displays the network parameters of the global setting and available network connection. You may change any of these items and press Apply to confirm your settings. See a description of each item in the following table:



Host Settings

Host Name: N2520 Domain Name: thecus.com

WINS Server 1: WINS Server 2:

DNS Settings

Mode: ○ Manual

● DHCP (Get From WAN/LAN1)

DNS 1: 172.16.66.243

DNS 2: 168.95.1.1

DNS 3:

WAN/LAN1

Status: Normal Speed: 1000Mb/s

MAC Address: 00:14:FD:17:42:5E Link Status: Connected

Jumbo Frame: 1500 bytes

IPv4

Enable:

IPv6

Enable:

Network Configuration (Global parameter)	
Item	**Description**
Host name	Host name that identifies the Thecus IP storage on the network.
Domain name	Specifies the domain name of Thecus IP storage.
WINS Server	To set a server name for NetBIOS computer.
DNS Mode	Select the DNS server is coming from DHCP server or manual input. A total of 3 DNS servers can be input. If the DNS setting is chosen from DHCP server, then it will refer to WAN/LAN1 port.
DNS Server 1,2,3	Domain Name Service (DNS) server IP address.
Network Configuration (NIC port)	
Link speed	Display associated NIC port link speed.
Link status	Display associated NIC port link status.
MAC address	MAC address of the network interface.
Jumbo Frame Support	Enable or disable Jumbo Frame Support of associate interface on your Thecus IP storage.
IPv4/IPv6	Click to enable IPv4/IPv6 for TCP/IP. The default is IPv4 enabled.
Mode	It can choose a static IP or Dynamic IP.
IP	IP address of associate NIC interface.

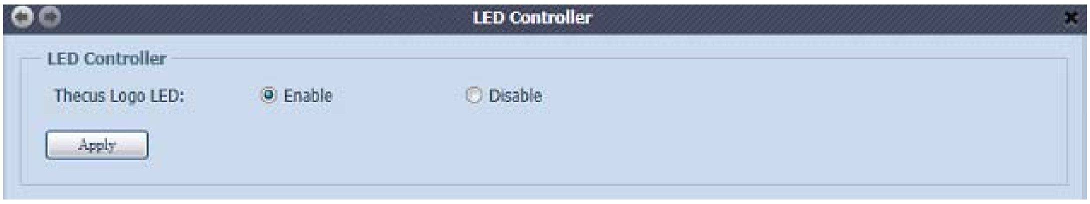
Netmask/Prefix Length	Input netmask for IPv4 and Prefix length for IPv6.
Gateway	Gateway for associate NIC.
Default gateway	It can be chosen from a drop down list of default gateway that's been used for the Thecus IP storage.

- Only use Jumbo Frame settings when operating in a Gigabit environment where all other clients have Jumbo Frame Setting enabled.
- Proper DNS setting is vital to networks services, such as SMTP and NTP.

Most faster Ethernet (10/100) Switches/Routers do not support Jumbo Frame and will not be able to connect to your Thecus NAS after Jumbo Frame is turned on.

3.3.20 Thecus LED Controller

There is an LED with the Thecus logo on the left hand side of the system. The LED light can be turned on or off by enabling or disabling it.



LED Controller

LED Controller

Thecus Logo LED: ● Enable ○ Disable

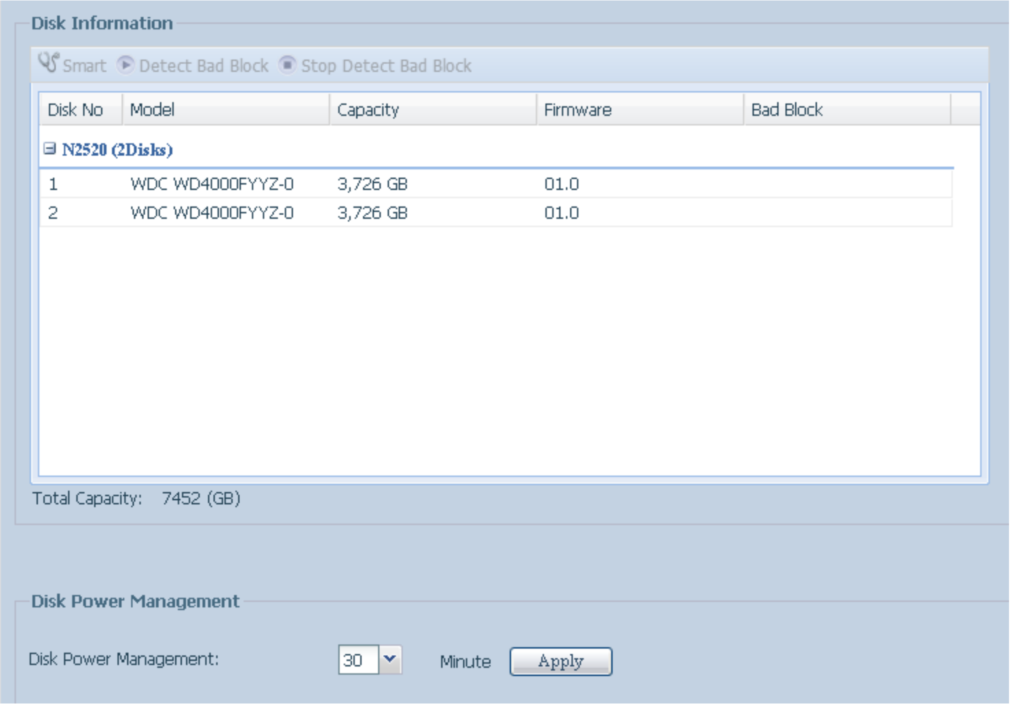
3.4 Storage Management

The Storage category displays the status of storage devices installed in the Thecus IP storage. It includes storage configuration options such as RAID and disk settings, iSCSI (N4520/N4560) and ISO Mount (N4520/N4560).

3.4.1 Disks Information

From the Storage menu, choose the Disk Information item and the Disk Information screen appears. From here, you can see various installed hard disks. The disk slot position will appear if the mouse is moved over the installed disk.

The screen shot below is just an example from a Thecus IP Storage. The disk slots number can range from 1,2 to 4 slots depending on the model of Thecus IP storage. Also it will list the disk info of JBOD devices if applicable.

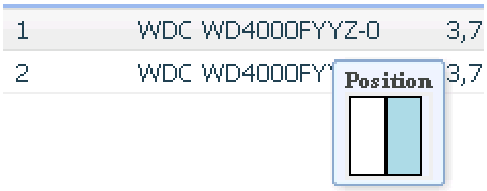

Disk Information

Disk No	Model	Capacity	Firmware	Bad Block
N2520 (2Disks)				
1	WDC WD4000FYYZ-0	3,726 GB	01.0	
2	WDC WD4000FYYZ-0	3,726 GB	01.0	

Total Capacity: 7452 (GB)

Disk Power Management

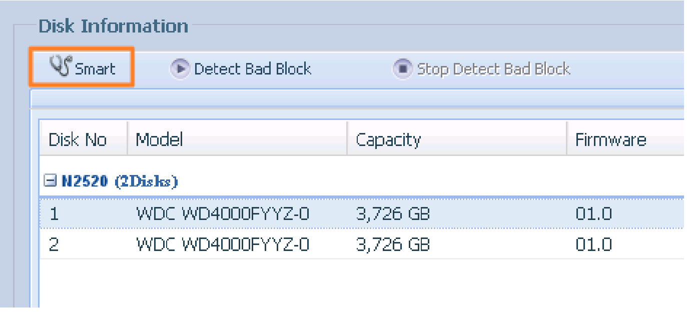
Disk Power Management: 30 Minute



Disks Information	
Item	**Description**
Disk No.	Indicates disk location.
Capacity	Shows the SATA hard disk capacity.
Model	Displays the SATA hard disk model name.
Firmware	Shows the SATA hard disk firmware version.
Bad Block scan	Yes to start scan Bad Block.

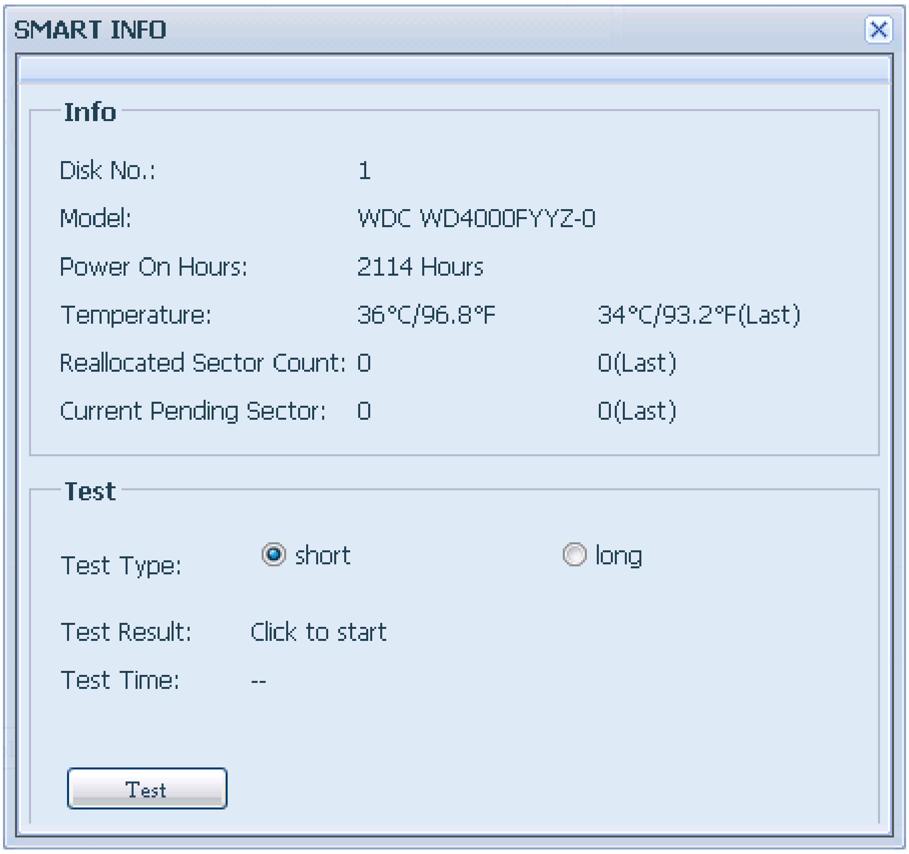
- **S.M.A.R.T. Information**

On the Disk Information screen, select a disk then click on "Smart" to list the S.M.A.R.T. info of the associated disk.


Disk Information

Disk No	Model	Capacity	Firmware
N2520 (2Disks)			
1	WDC WD4000FYYZ-0	3,726 GB	01.0
2	WDC WD4000FYYZ-0	3,726 GB	01.0

You may also perform a disk SMART test; simply click "Test" to start the SMART test. The result is only for reference and the system will not take any action from its results.


SMART INFO

Info

Disk No.: 1

Model: WDC WD4000FYYZ-0

Power On Hours: 2114 Hours

Temperature: 36°C/96.8°F 34°C/93.2°F(Last)

Reallocated Sector Count: 0 0(Last)

Current Pending Sector: 0 0(Last)

Test

Test Type: ● short ○ long

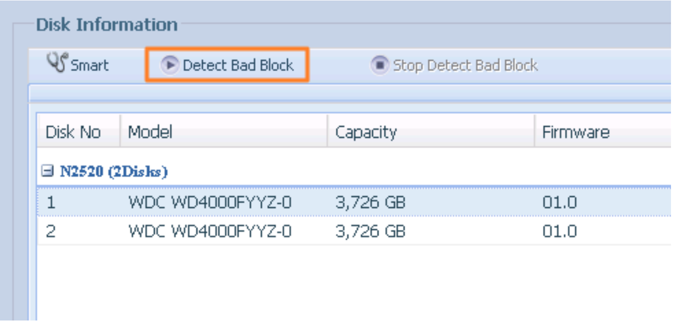
Test Result: Click to start

Test Time: --

S.M.A.R.T. Information	
Item	**Description**
Tray Number	Tray the hard disk is installed in.
Model	Model name of the installed hard disk.
Power ON Hours	Count of hours in power-on state. The raw value of this attribute shows total count of hours (or minutes, or seconds, depending on manufacturer) in power-on state.
Temperature Celsius	The current temperature of the hard disk in degrees Celsius.
Reallocated Sector Count	Count of reallocated sectors. When the hard drive finds a read/write/verification error, it marks this sector as "reallocated" and transfers data to a special reserved area (spare area). This process is also known as remapping and "reallocated" sectors are called remaps. This is why, on a modern hard disks, you cannot see "bad blocks" while testing the surface - all bad blocks are hidden in reallocated sectors. However, the more sectors that are reallocated, the more a decrease (up to 10% or more) can be noticed in disk read/write speeds.
Current Pending Sector	Current count of unstable sectors (waiting for remapping). The raw value of this attribute indicates the total number of sectors waiting for remapping. Later, when some of these sectors are read successfully, the value is decreased. If errors still occur when reading sectors, the hard drive will try to restore the data, transfer it to the reserved disk area (spare area), and mark this sector as remapped. If this attribute value remains at zero, it indicates that the quality of the corresponding surface area is low.
Test Type	Set short or long time to test.
Test Result	Result of the test.
Test Time	Total time of the test.

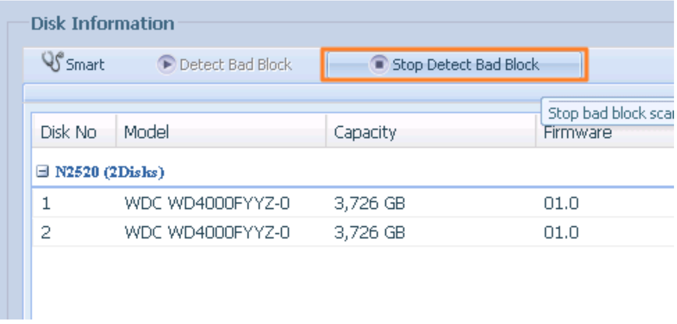
- ## Bad Block Scan

On the Disk Information screen, select a disk then click on “Detect Bad Block” to perform bad block scan of the associated disk. The result is only for reference and the system will not take any action from its results.



Disk No	Model	Capacity	Firmware
N2520 (2Disks)			
1	WDC WD4000FYYZ-0	3,726 GB	01.0
2	WDC WD4000FYYZ-0	3,726 GB	01.0

The bad block scan can be terminated by clicking on "Stop Detect Bad Block".

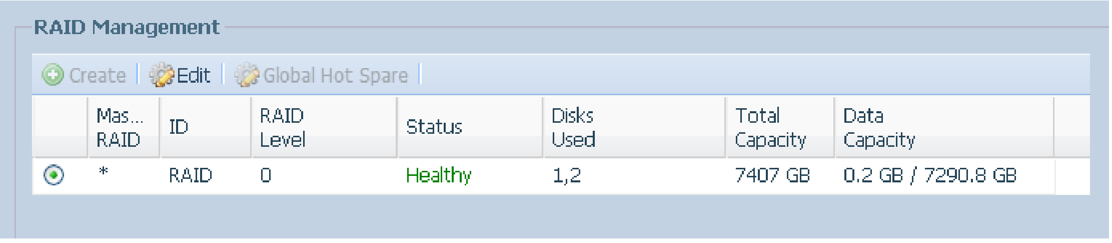


Disk No	Model	Capacity	Firmware
N2520 (2Disks)			
1	WDC WD4000FYYZ-0	3,726 GB	01.0
2	WDC WD4000FYYZ-0	3,726 GB	01.0

3.4.2 RAID Management

From the Storage category, choose the RAID Management item and the RAID Management screen appears.

This screen lists the RAID volumes currently residing in the Thecus IP storage. From this screen, you can get information about the status of your RAID volumes, as well as the capacities allocated for data.



	Mas... RAID	ID	RAID Level	Status	Disks Used	Total Capacity	Data Capacity
●	*	RAID	0	Healthy	1,2	7407 GB	0.2 GB / 7290.8 GB

RAID Management

Item	Description
Master RAID	The RAID volume currently designated as the Master RAID volume.
ID	ID of the current RAID volume. NOTE: All RAID IDs must be unique.
RAID Level	Shows the current RAID configuration.
Status	Indicates status of the RAID. Can read either ***Healthy***, ***Degraded***, or ***Damaged***.
Disks Used	Hard disks used to form the current RAID volume.
Total Capacity	Total capacity of the current RAID.
Data Capacity	Indicates the used capacity and total capacity used by user data.

- **Create a RAID**

On the RAID Information screen, press the Create button to go to the RAID Volume Creation screen. In addition to RAID disk information and status, this screen lets you make RAID configuration settings.

Using Create RAID, you can select stripe size, choose which disks are RAID disks or the Spare Disk. .

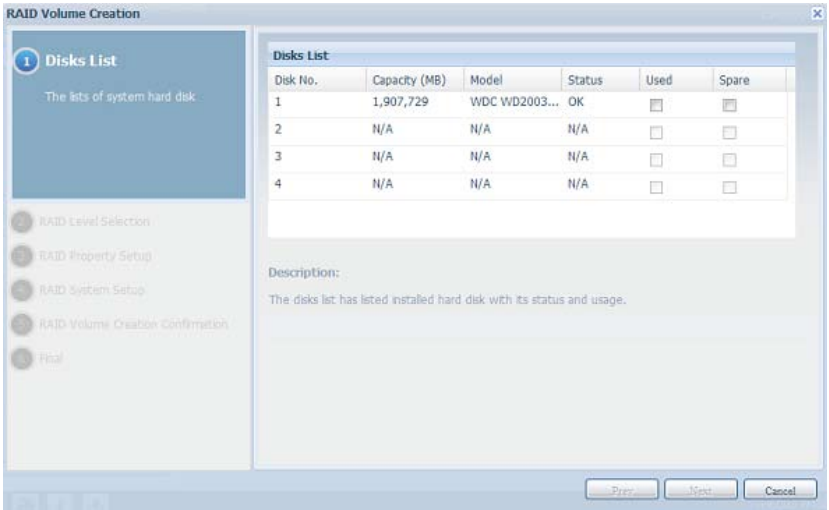
RAID Configurations

Item	Description

Disk No.	Number assigned to the installed hard disks.
Capacity (MB)	Capacity of the installed hard disks.
Model	Model number of the installed hard disks.
Status	Status of the installed hard disks.
Used	If this is checked, current hard disk is aalready part of a RAID volume.
Spare	If this is checked, current hard disk is designated as a spare for a RAID volume.
Master RAID	Check a box to designate this as the Master RAID volume. See the NOTE below for more information.
Stripe Size	This sets the stripe size to maximize performance of sequential files in a storage volume. Keep the 64K setting unless you require a special file storage layout in the storage volume. A larger stripe size is better for large files.
Data Percentage	The percentage of the RAID volume that will be used to store data.
Create	Press this button to configure a file system and create the RAID storage volume.

To create a RAID volume, follow the steps below:

1. On the RAID Information screen, clicks create.



RAID Volume Creation

1 Disks List
The lists of system hard disk

2 RAID Level Selection
3 RAID Property Setup
4 RAID System Setup
5 RAID Volume Creation Confirmation
6 Final

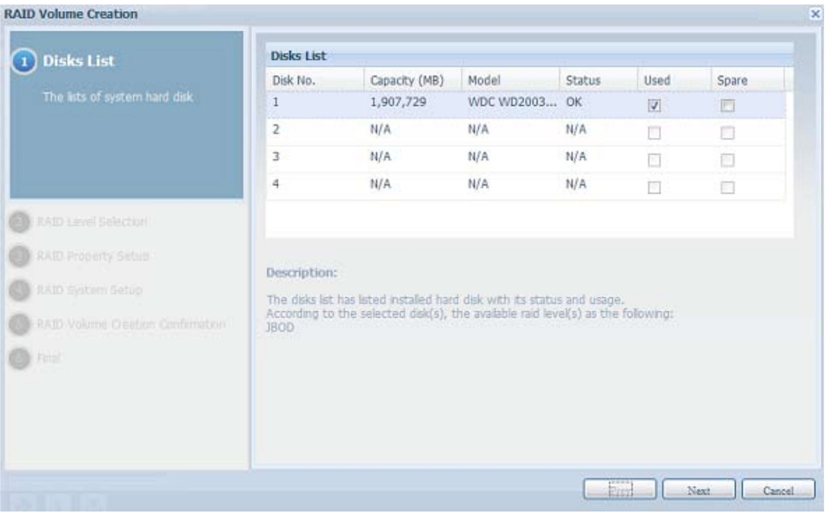
Disks List

Disk No.	Capacity (MB)	Model	Status	Used	Spare
1	1,907,729	WDC WD2003...	OK	□	□
2	N/A	N/A	N/A	□	□
3	N/A	N/A	N/A	□	□
4	N/A	N/A	N/A	□	□

Description:

The disks list has listed installed hard disk with its status and usage.

2. On the RAID Configuration screen, set the RAID storage space as JBOD, RAID 0, RAID 1, RAID 5, RAID 6 or RAID 10 (depends on model)— see Appendix B: RAID Basics for a detailed description of each.



RAID Volume Creation

1 Disks List
The lists of system hard disk

2 RAID Level Selection
3 RAID Property Setup
4 RAID System Setup
5 RAID Volume Creation Confirmation
6 Final

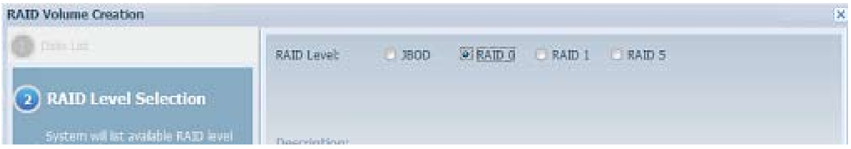
Disks List

Disk No.	Capacity (MB)	Model	Status	Used	Spare
1	1,907,729	WDC WD2003...	OK	☑	□
2	N/A	N/A	N/A	□	□
3	N/A	N/A	N/A	□	□
4	N/A	N/A	N/A	□	□

Description:

The disks list has listed installed hard disk with its status and usage.
According to the selected disk(s), the available raid level(s) as the following:
JBOD

3. Specify a RAID ID.



RAID Volume Creation

1 Disks List

2 RAID Level Selection
System will list available RAID level

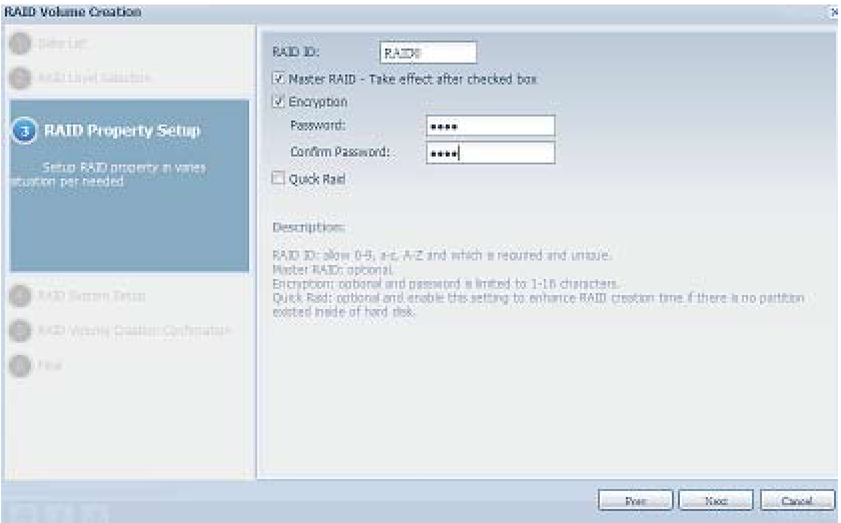
RAID Level: ○ JBOD ● RAID 0 ○ RAID 1 ○ RAID 5

Description:

4. If this RAID volume is meant to be the Master RAID volume, tick the Master RAID checkbox.

In a multiple RAID configuration, one RAID volume must be designated as the Master RAID volume. The Master RAID volume will store all installed modules. If the Master RAID is changed to another location (i.e. assigning volume 2 to be the Master RAID volume after volume 1 had been previously assigned), then all modules must be reinstalled. In addition, all system folders that were contained on the Master RAID volume will be invisible. Reassigning this volume to be the Master RAID will make these folders visible again.

5. Selected whether the RAID volume will be encrypted or not.
   The RAID volume can protect data by using RAID Volume Encryption function to prevent the risk of data exposure. To activate this function, the Encryption option needs to be enabled while the RAID is created and followed by a password input for identification. Also, an external writable USB disk plugged into any USB port on the system is required to save the password you have entered while the RAID volume is being created. See the screenshot below for details.



RAID ID: RAID0

☑ Master RAID - Take effect after checked box

☑ Encryption

Password: ••••

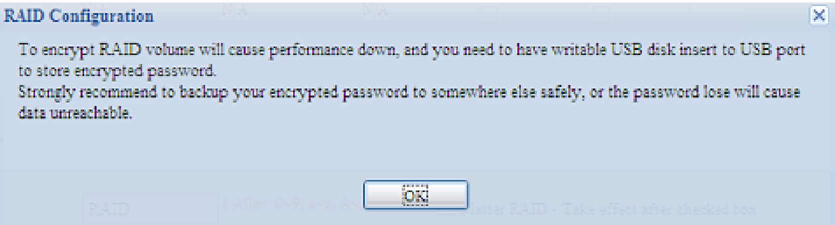
Confirm Password: ••••

□ Quick Raid

Description:

RAID ID: allow 0-9, a-z, A-Z and which is required and unique.
Master RAID: optional.
Encryption: optional and password is limited to 1-16 characters.
Quick Raid: optional and enable this setting to enhance RAID creation time if there is no partition existed inside of hard disk.

Once the Create button has been pressed with the Encryption checkbox enabled, the following message pop-up will appear for confirmation.



To encrypt RAID volume will cause performance down, and you need to have writable USB disk insert to USB port to store encrypted password.
Strongly recommend to backup your encrypted password to somewhere else safely, or the password lose will cause data unreachable.

After the RAID volume has been created, you may remove the USB disk until the next time the system boots. The RAID volume cannot be mounted if the USB disk with the encryption key isn't found in any system USB port when the volume is accessed. To activate the encrypted volume, plug the USB disk containing the encryption key and into any system USB port.

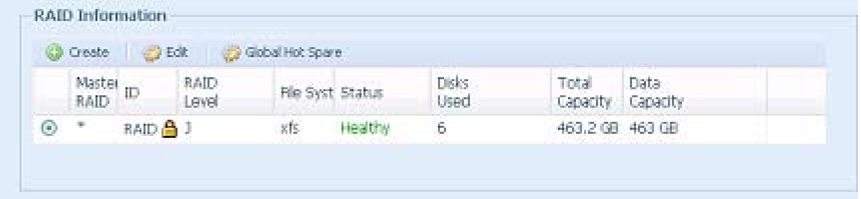
We strongly recommended copying the RAID volume encryption key to a safe place. You can find the encryption key file from the USB disk in the following format:

(RAID volume created date)_xxxxxx.key

Please keep your USB disk in a safe place and also backup the encrypted key.
There is no way to rescue data back if the key is lost.

With RAID volume encryption enabled, the system performance will go down.

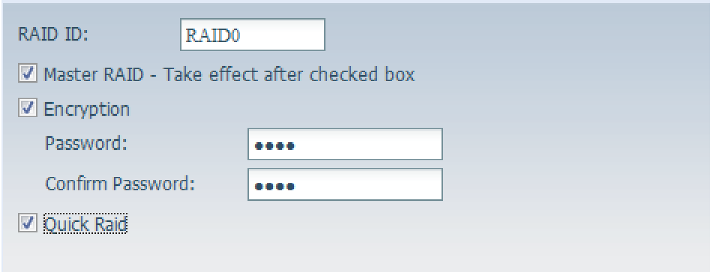
RAID volumes with encryption enabled will be displayed with a key lock symbol next to volume ID name.



RAID Information

	Master RAID	ID	RAID Level	File Syst	Status	Disks Used	Total Capacity	Data Capacity
○	*	RAID 🔒	J	xfs	Healthy	6	463.2 GB	463 GB

6. Quick RAID — Enabled the quick RAID setting is going to enhance RAID creation time.

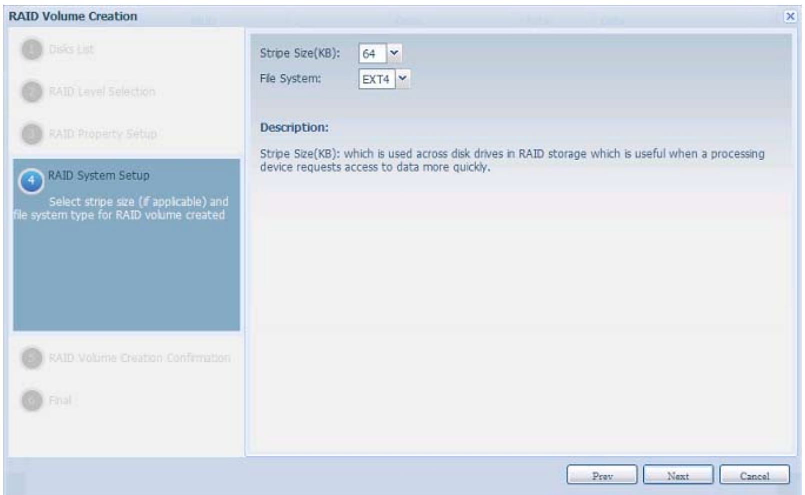


RAID ID: RAID0
☑ Master RAID - Take effect after checked box
☑ Encryption
Password: ••••
Confirm Password: ••••
☑ Quick Raid

We recommend using the "Quick RAID" setting only if the hard disks are brand new or if no existing partitions are contained.

7. Specify a stripe size — 64K is the default setting.

8. Selected the file system you would like to have for this RAID volume. .



RAID Volume Creation

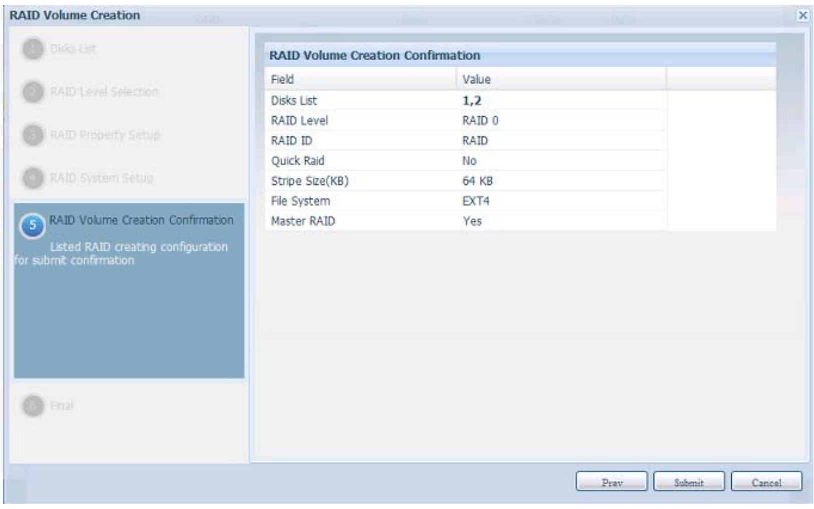
Select stripe size (if applicable) and file system type for RAID volume created

Stripe Size(KB): 64
File System: EXT4

Description:

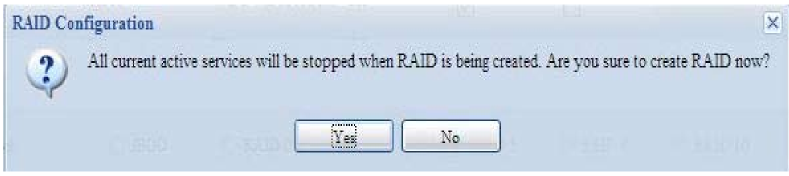
Stripe Size(KB): which is used across disk drives in RAID storage which is useful when a processing device requests access to data more quickly.

9. Press Submit to build the RAID storage volume.



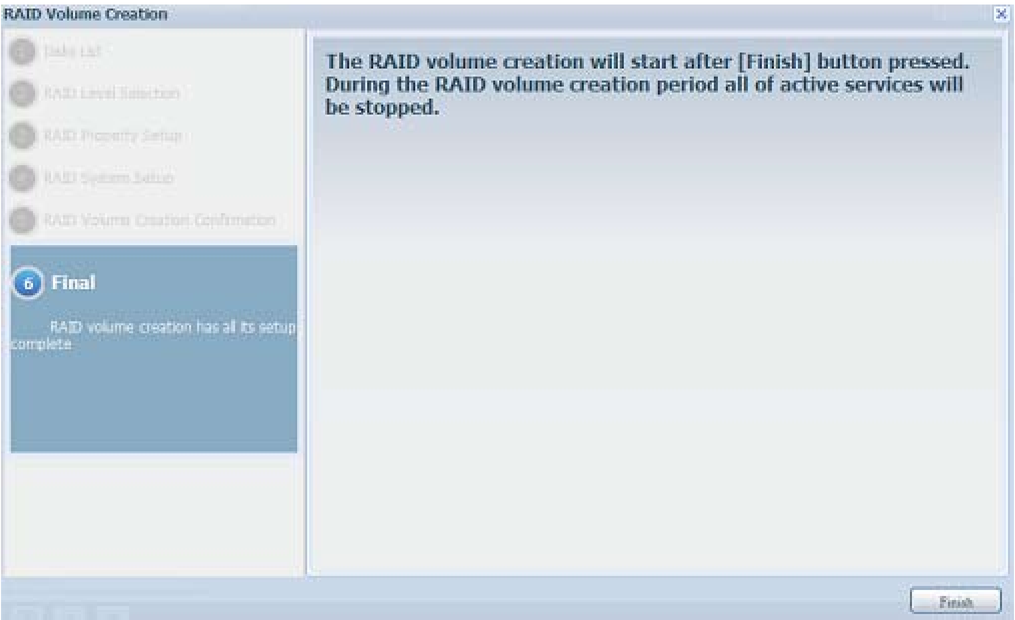
RAID Volume Creation Confirmation

Field	Value
Disks List	1,2
RAID Level	RAID 0
RAID ID	RAID
Quick Raid	No
Stripe Size(KB)	64 KB
File System	EXT4
Master RAID	Yes



All current active services will be stopped when RAID is being created. Are you sure to create RAID now?

10. Press "Yes" for RAID volume creation preparation. Then click "Finish" to start up with RAID volume building.



The RAID volume creation will start after [Finish] button pressed. During the RAID volume creation period all of active services will be stopped.

Building a RAID volume may be time consuming, depending on the size of hard drives and RAID mode. In general, if the RAID volume building process is up to "RAID Building", then the data volume is accessible.

Creating RAID destroys all data in the current RAID volume. The data will be unrecoverable.

- **RAID Level**

You can set the storage volume as JBOD, RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 (depending on model).

Level / Model	JBOD	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
N2520/N2560	•	•	•			
N4520/N4560	•	•	•	•	•	•

RAID configuration is usually required only when you first set up the device. A brief description of each RAID setting follows:

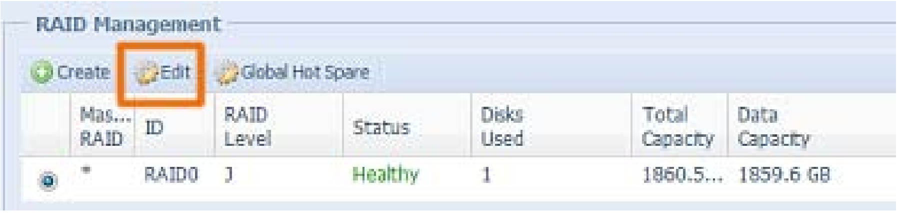
RAID Levels	
Level	**Description**
JBOD	The storage volume is a single HDD with no RAID support. JBOD requires a minimum of 1 disk.
RAID 0	Provides data striping but no redundancy. Improves performance but not data safety. RAID 0 requires a minimum of 2 disks.
RAID 1	Offers disk mirroring. Provides twice the read rate of a single disk, but same write rate. RAID 1 requires a minimum of 2 disks.
RAID 5	Data striping and stripe error correction information provided. RAID 5 requires a minimum of 3 disks. RAID 5 can sustain one failed disk.
RAID 6	Two independent parity computations must be used in order to provide protection against double disk failure. Two different algorithms are employed to achieve this purpose. RAID 6 requires a minimum of 4 disks. RAID 6 can sustain two failed disks.
RAID 10	RAID 10 has high reliability and high performance. RAID 10 is implemented as a striped array whose segments are RAID 1 arrays. It has the fault tolerance of RAID 1 and the performance of RAID 0. RAID 10 requires 4 disks. RAID 10 can sustain two failed disks.

Creating RAID destroys all data in the current RAID volume. The data will be unrecoverable.

- ## Edit RAID

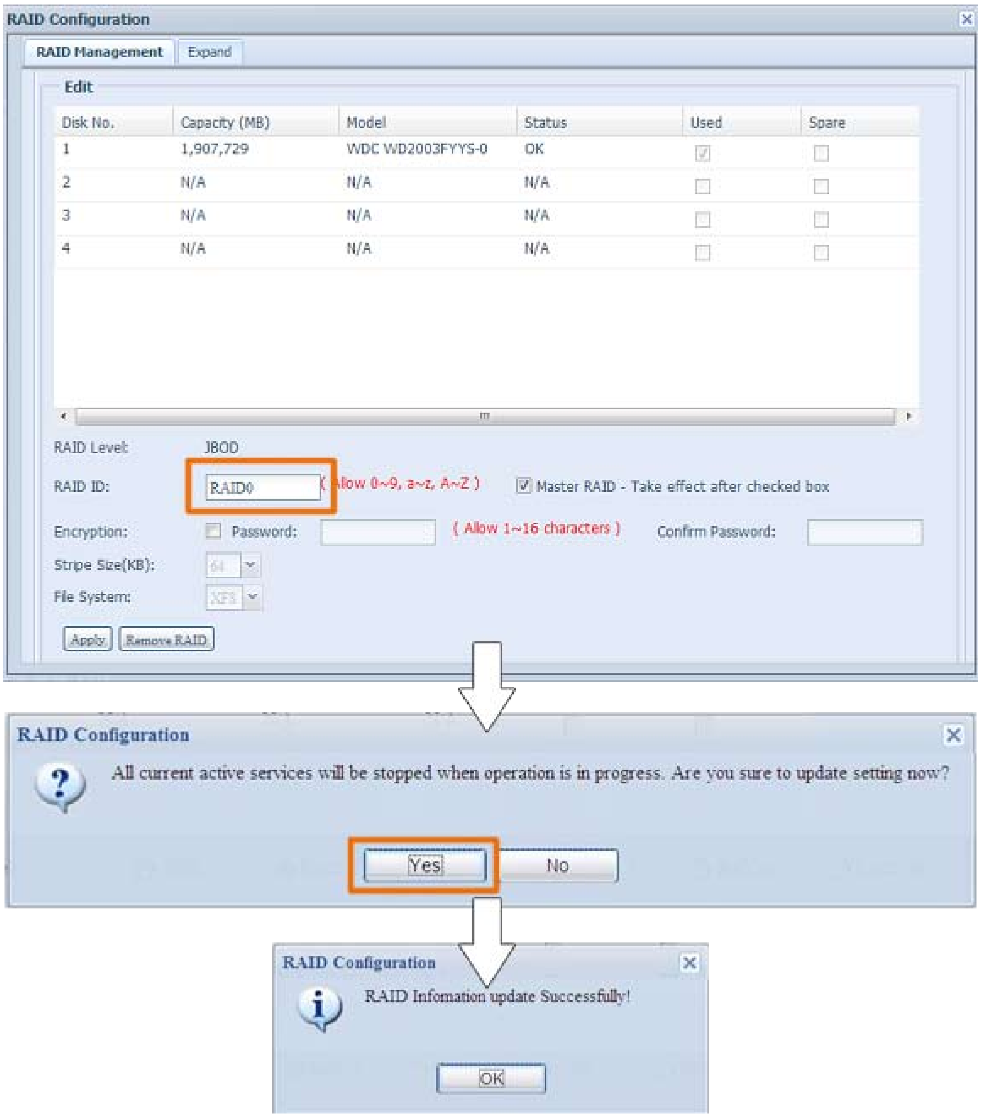
On the RAID Information screen, press the Edit button to go to the RAID Information screen.

Using Edit RAID, you can select RAID ID and the Spare Disk.



RAID Management

	Mas... RAID	ID	RAID Level	Status	Disks Used	Total Capacity	Data Capacity
○	*	RAID0	J	Healthy	1	1860.5...	1859.6 GB


RAID Configuration

Edit

Disk No.	Capacity (MB)	Model	Status	Used	Spare
1	1,907,729	WDC WD2003FYYS-0	OK	☑	□
2	N/A	N/A	N/A	□	□
3	N/A	N/A	N/A	□	□
4	N/A	N/A	N/A	□	□

RAID Level: JBOD

RAID ID: RAID0 (Allow 0~9, a~z, A~Z) ☑ Master RAID - Take effect after checked box

Encryption: □ Password: (Allow 1~16 characters) Confirm Password:

Stripe Size(KB): 64

File System: XFS

RAID Configuration

All current active services will be stopped when operation is in progress. Are you sure to update setting now?

RAID Configuration

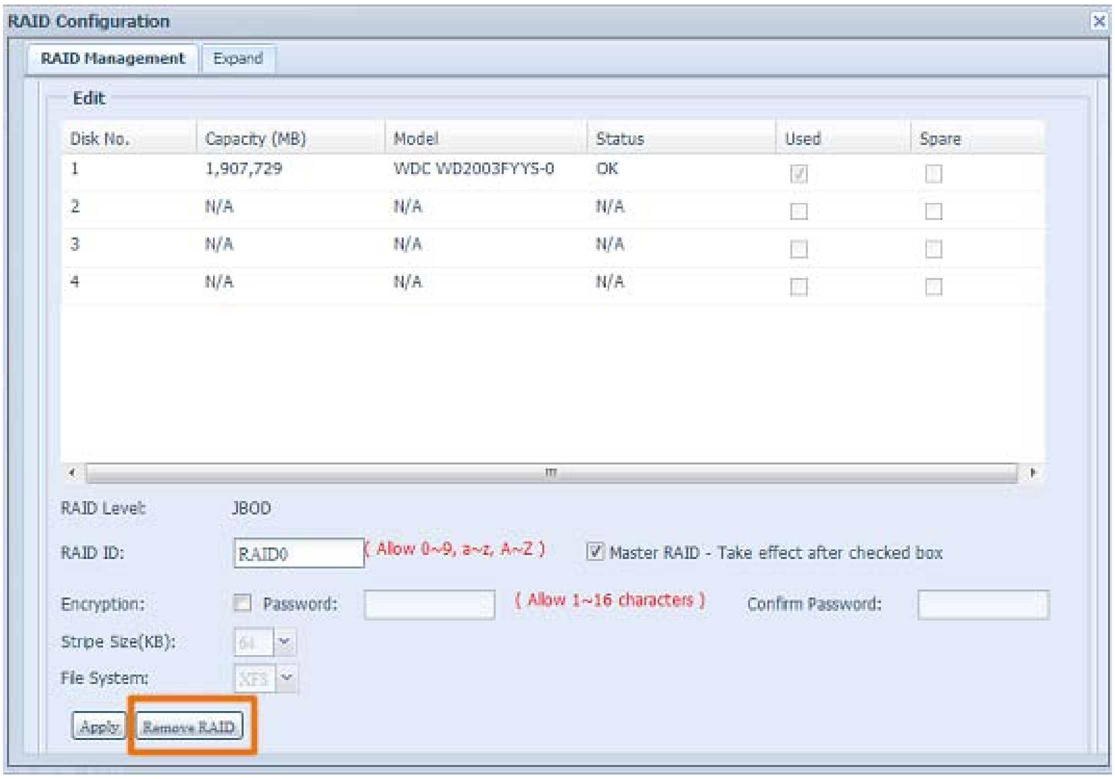
RAID Infomation update Successfully!

Remove RAID

Click to remove the RAID volume. All user data and iSCSI created in the selected RAID volume will be deleted.

To remove a RAID volume, follow the steps below:

1. On the RAID List screen, select the RAID volume by clicking on its radio button, and click RAID Information to open the RAID Configuration screen.
2. On the RAID Configuration screen, click Remove RAID.
3. A confirmation screen will appear, you will have to click "Yes" to complete the "Remove RAID" operation.



Disk No.	Capacity (MB)	Model	Status	Used	Spare
1	1,907,729	WDC WD2003FYYS-0	OK	☑	□
2	N/A	N/A	N/A	□	□
3	N/A	N/A	N/A	□	□
4	N/A	N/A	N/A	□	□

RAID Level: JBOD

RAID ID: RAID0 (Allow 0~9, a~z, A~Z) ☑ Master RAID - Take effect after checked box

Encryption: □ Password: (Allow 1~16 characters) Confirm Password:

Stripe Size(KB): 64

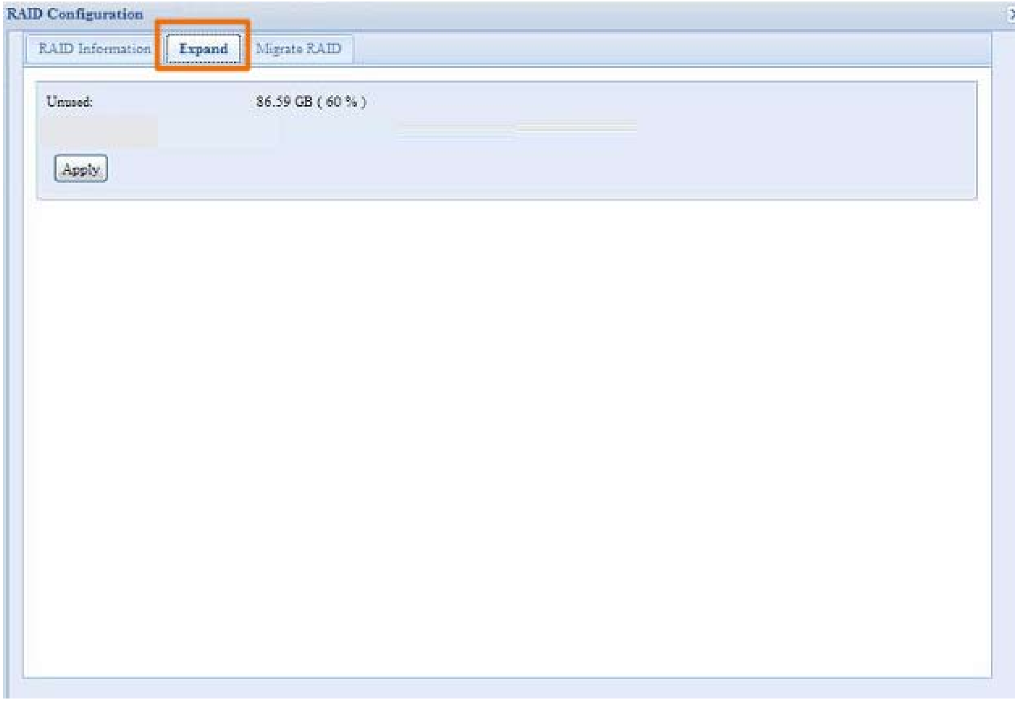
File System: XFS

Remove RAID destroys all data in the selected RAID volume. The data will be unrecoverable.

Expanding a RAID(Dose not apply to the N2520/N2560)

To expand a RAID 1, RAID 5, or RAID 6 volume, follow the steps below:

1. Replace one of the hard drives in the RAID volume and allow it to automatically rebuild.
2. Once rebuilt, you can continue to replace any remaining disks in the RAID array.
3. When you are done replacing hard drives, log on to Web Management. Navigate to Storage> RAID to open the RAID Configuration screen.
4. On the RAID Information screen, click Edit to open the RAID Configuration screen.
5. On the RAID Configuration screen, click Expand.

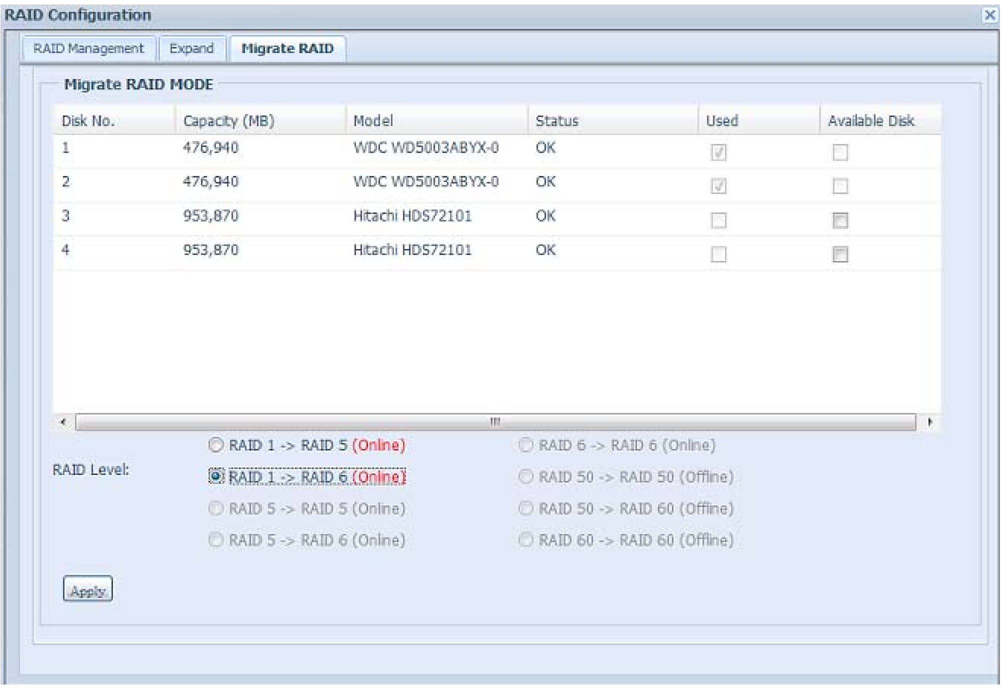

RAID Configuration

Unused: 86.59 GB (60 %)

- **Migrating a RAID(Dose not apply to the N2520/N2560)**

Once a RAID volume has been created, you may want to move it to other physical drives or change the RAID array all together. To migrate a RAID 1, RAID 5 or RAID 6 volume, follow the steps below:

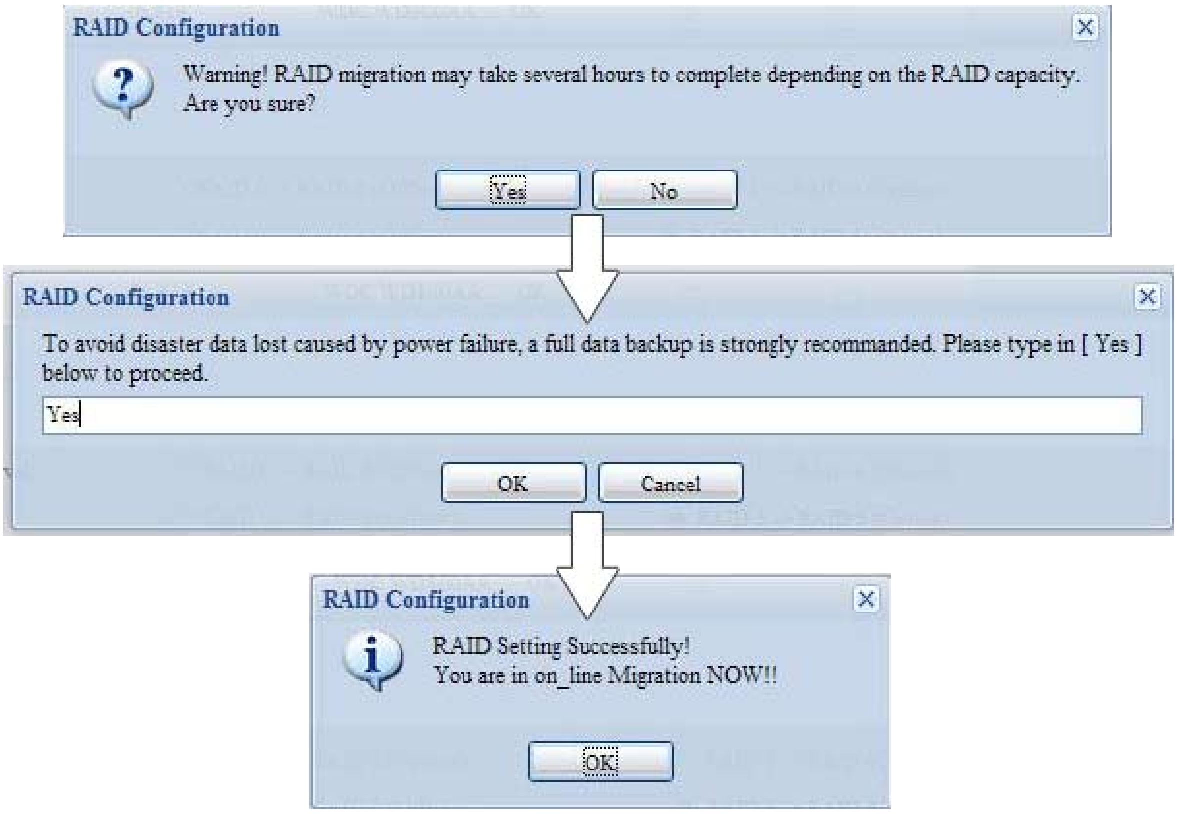
1. From the RAID Configuration screen, click Migrate RAID.
2. A list of possible RAID migration configurations will be listed. Select the desired migration scheme and click Apply.
3. The system will begin migrating the RAID volume.


RAID Configuration

Migrate RAID MODE

Disk No.	Capacity (MB)	Model	Status	Used	Available Disk
1	476,940	WDC WD5003ABYX-0	OK	☑	□
2	476,940	WDC WD5003ABYX-0	OK	☑	□
3	953,870	Hitachi HDS72101	OK	□	▨
4	953,870	Hitachi HDS72101	OK	□	▨

RAID Level:
○ RAID 1 -> RAID 5 (Online)
● RAID 1 -> RAID 6 (Online)
○ RAID 5 -> RAID 5 (Online)
○ RAID 5 -> RAID 6 (Online)
○ RAID 6 -> RAID 6 (Online)
○ RAID 50 -> RAID 50 (Offline)
○ RAID 50 -> RAID 60 (Offline)
○ RAID 60 -> RAID 60 (Offline)



RAID Configuration

Warning! RAID migration may take several hours to complete depending on the RAID capacity.
Are you sure?

RAID Configuration

To avoid disaster data lost caused by power failure, a full data backup is strongly recommanded. Please type in [Yes] below to proceed.

Yes

RAID Configuration

RAID Setting Successfully!
You are in on_line Migration NOW!!

- Migrating a RAID volume could take several hours to complete.
- The RAID migration feature is available only when it is configurable.

Here is a list of limitation with RAID level migration function:

1. During RAID level migration, it is not permitted to reboot or shutdown system.
2. For RAID migration from R1 to R5 or R1 to R6, all services will restart and "iSCSI" volume will be in read only mode but read/write of the "user data" will be possible during the operation.

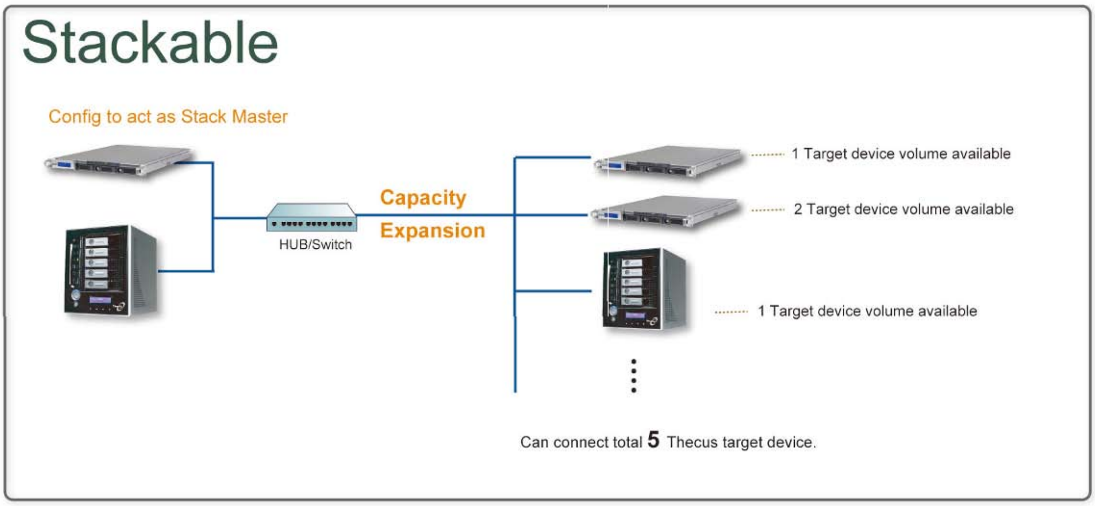
The migration scheme below is based on Thecus IP Storage product's maximum possible combination. For other model which supports less HDD, please refer to the web UI while RAID migration operates.

Below is a table listing of possible RAID migration schemes:

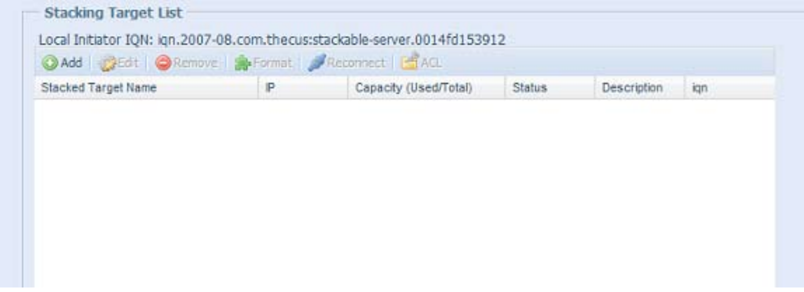
To **From**	**RAID 0**	**RAID 5**	**RAID 6**
RAID 1		[RAID 1] HDDx2 to [RAID 5] HDDx3 [RAID 1] HDDx2 to [RAID 5] HDDx4 [RAID 1] HDDx3 to [RAID 5] HDDx4	[RAID 1] HDDx2 to [RAID 6] HDDx4 [RAID 1] HDDx3 to [RAID 6] HDDx4
RAID 5	X	[RAID 5] HDDx3 to [RAID 5] HDDx4	[RAID 5] HDDx3 to [RAID 6] HDDx4

3.4.3 NAS Stacking (N4520/N4560 Only)

The Thecus IP storage's capacity can be expanded even further using the stackable function. With it, users can expand the capacity of their network storage systems up to 5 other stack target volumes which are located in different systems. These can be stacked through single network access like SMB or AFP acting as a share folder type.


Stackable
Config to act as Stack Master
HUB/Switch
Capacity
Expansion
1 Target device volume available
2 Target device volume available
1 Target device volume available
Can connect total 5 Thecus target device.

From the Control Panel, the stackable feature is located under "Storage". Please refer the figure below for reference.



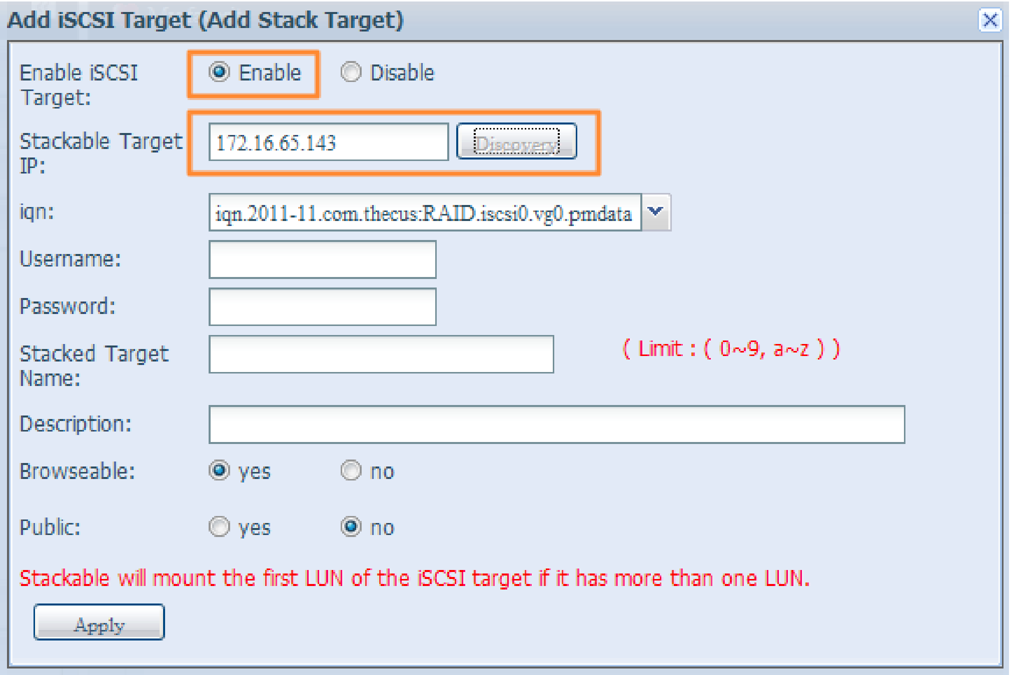
Local Initiator IQN: iqn.2007-08.com.thecus:stackable-server.0014fd153912

Stacked Target Name	IP	Capacity (Used/Total)	Status	Description	iqn

A. Add a Stack Target Volume

From the figure above, click Add to access the stackable target device configuration page. Please refer to the figure below:

With the added stack target you can "Enable" or "Disable" the stack target now or later depending on usage required.



Add iSCSI Target (Add Stack Target)

Enable iSCSI Target: ● Enable ○ Disable

Stackable Target IP: 172.16.65.143 [Discovery]

iqn: iqn.2011-11.com.thecus:RAID.iscsi0.vg0.pmdata

Username:

Password:

Stacked Target Name: (Limit : (0~9, a~z))

Description:

Browseable: ● yes ○ no

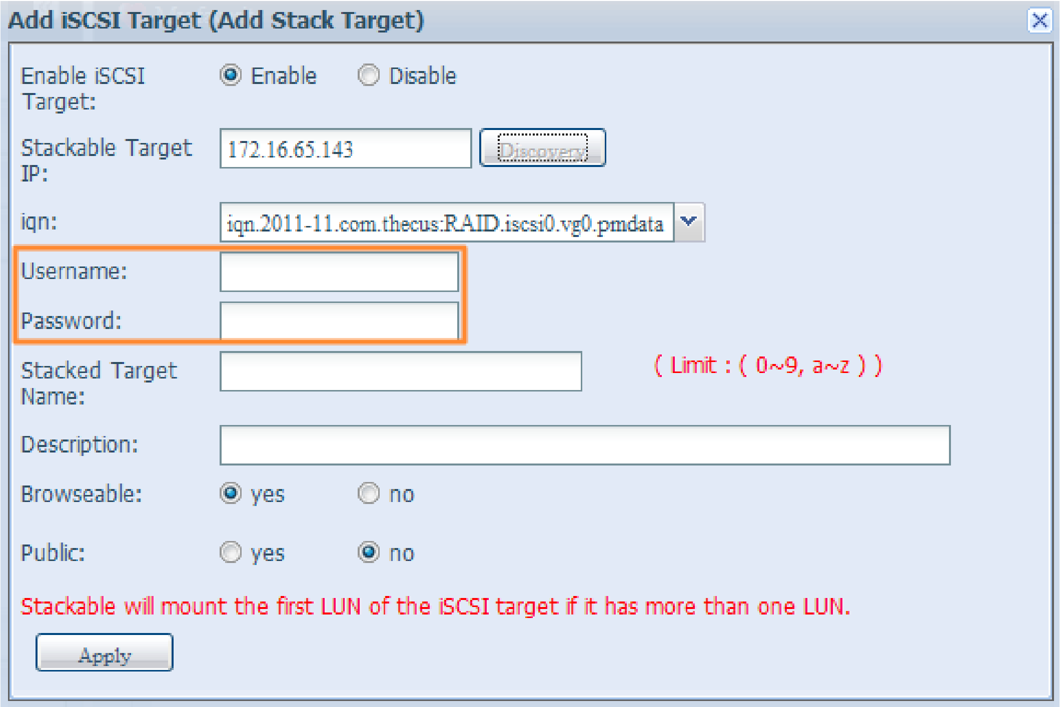
Public: ○ yes ● no

Stackable will mount the first LUN of the iSCSI target if it has more than one LUN.

[Apply]

Next, input the target IP address of the stackable device and click the Discovery button. The system will list available target volumes from the inputted IP address.

Once the volume IP has been set, you may need to input a valid user name and password to validate your access rights. If there is no user name and password needed to access target volume, then leave it blank.



Add iSCSI Target (Add Stack Target)

Enable iSCSI Target: ● Enable ○ Disable

Stackable Target IP: 172.16.65.143 [Discovery]

iqn: iqn.2011-11.com.thecus:RAID.iscsi0.vg0.pmdata

Username:

Password:

Stacked Target Name: (Limit : (0~9, a~z))

Description:

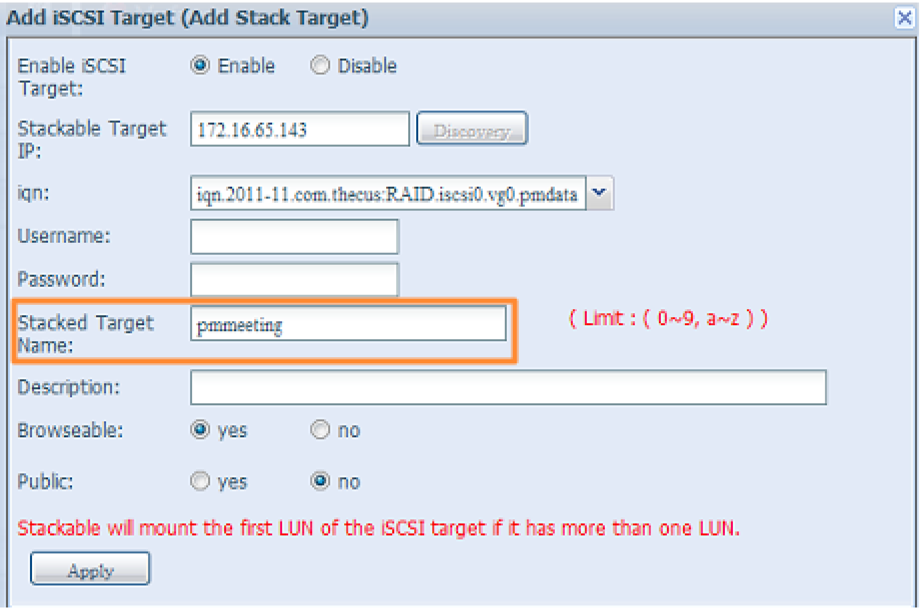
Browseable: ● yes ○ no

Public: ○ yes ● no

Stackable will mount the first LUN of the iSCSI target if it has more than one LUN.

[Apply]

The Stacked Target name will become the network share name and will be displayed through network access such as SMB. You may refer to the figure below to see the result. Please note the naming limitation.



Add iSCSI Target (Add Stack Target)

Enable iSCSI Target: ● Enable ○ Disable

Stackable Target IP: 172.16.65.143 Discovery

iqn: iqn.2011-11.com.thecus:RAID.iscsi0.vg0.pmdata

Username:

Password:

Stacked Target Name: pmmeeting (Limit : (0~9, a~z))

Description:

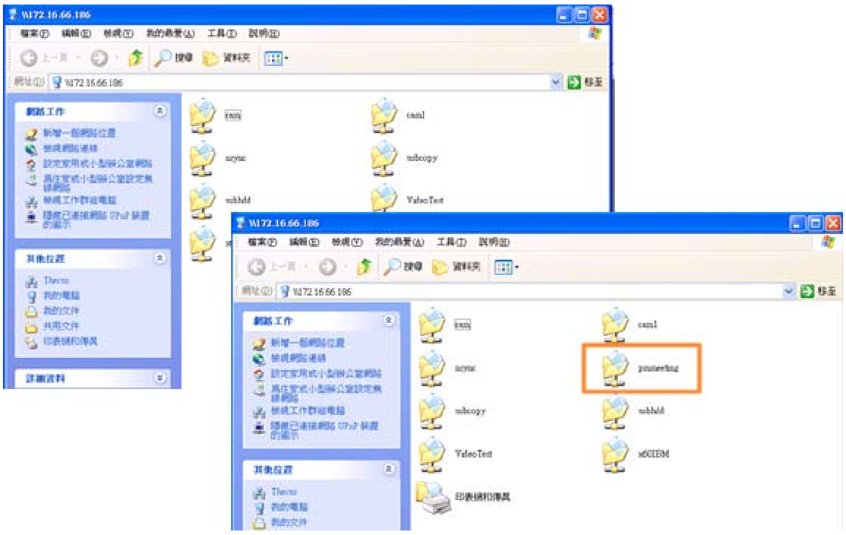
Browseable: ● yes ○ no

Public: ○ yes ● no

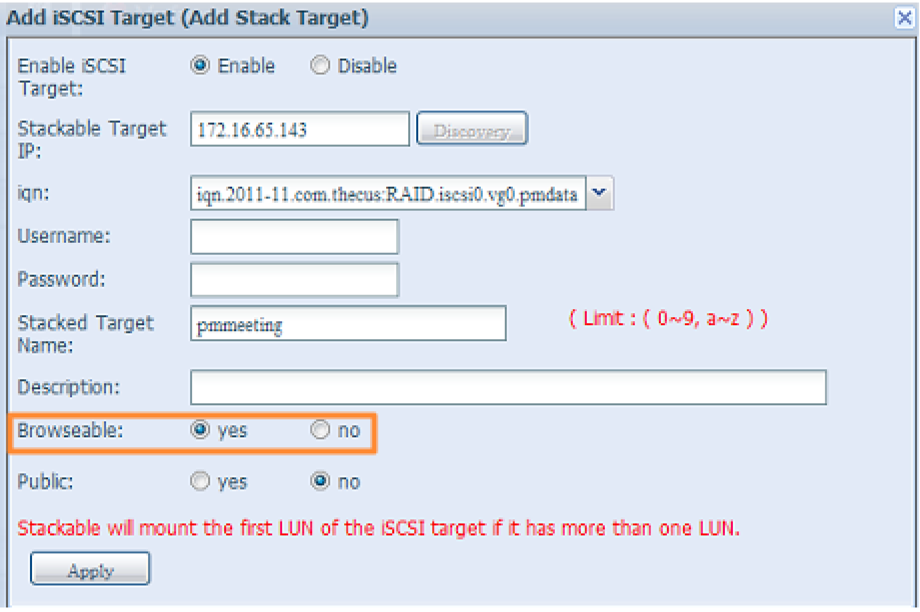
Stackable will mount the first LUN of the iSCSI target if it has more than one LUN.

Apply

From the figure above, the Stacked Target name is "pmmeeting". The figures below show the result before and after via Microsoft Network Access when settings have been completed.



The Browseable setting is the same method used for setting a system share folder. It designates whether or not this folder will be visible through web disk. You may refer to the figure below for reference when Yes and No are selected.



Add iSCSI Target (Add Stack Target)

Enable iSCSI Target: ● Enable ○ Disable

Stackable Target IP: 172.16.65.143 Discovery

iqn: iqn.2011-11.com.thecus:RAID.iscsi0.vg0.pmdata

Username:

Password:

Stacked Target Name: pmmeeting (Limit : (0~9, a~z))

Description:

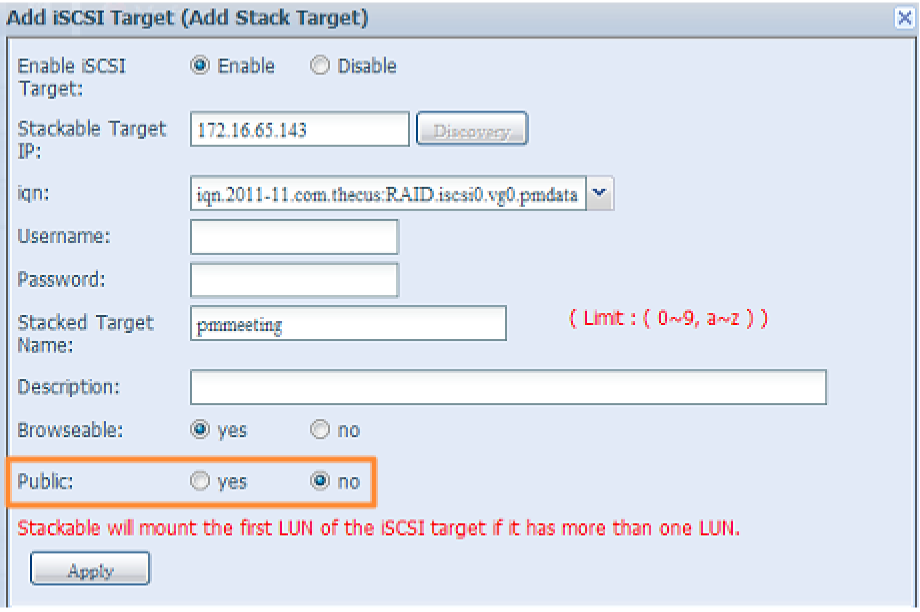
Browseable: ● yes ○ no

Public: ○ yes ● no

Stackable will mount the first LUN of the iSCSI target if it has more than one LUN.

Apply

The Public setting will be set the same way as the setting for the system share folder associated with the ACL permission is. If Public is set to Yes, all users will be able to access it, and ACL button will be grayed out. If Public is set to No, the ACL button will be available in the Stack Target List window.



Add iSCSI Target (Add Stack Target)

Enable iSCSI Target: ● Enable ○ Disable

Stackable Target IP: 172.16.65.143 Discovery

iqn: iqn.2011-11.com.thecus:RAID.iscsi0.vg0.pmdata

Username:

Password:

Stacked Target Name: pmmeeting (Limit : (0~9, a~z))

Description:

Browseable: ● yes ○ no

Public: ○ yes ● no

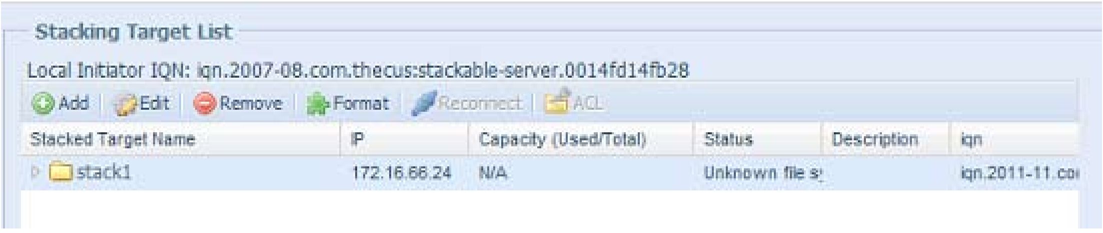
Stackable will mount the first LUN of the iSCSI target if it has more than one LUN.

Apply

Click Apply to save your changes.

B. Activate a Stack Target

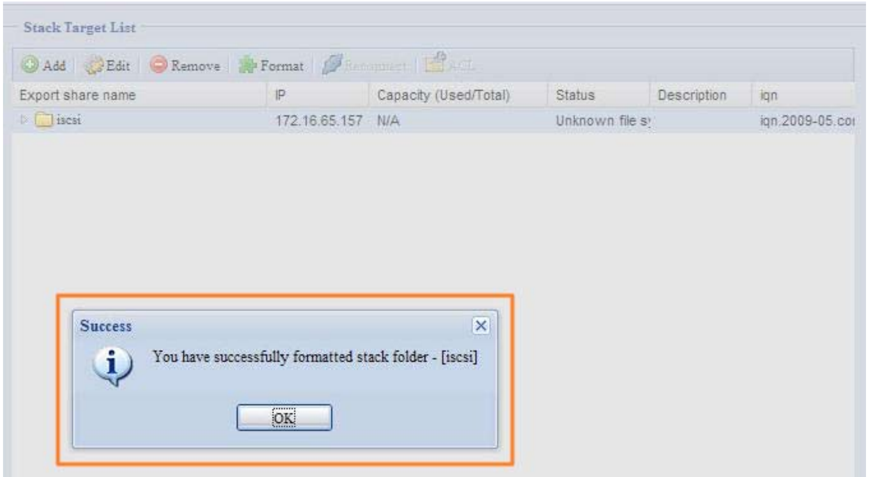
After your settings have been applied, the system will bring you back to the Stack Target List window as shown below. There is one stack target device that has been attached into this stack master.



Stacking Target List

Local Initiator IQN: iqn.2007-08.com.thecus:stackable-server.0014fd14fb28

Stacked Target Name	IP	Capacity (Used/Total)	Status	Description	iqn
stack1	172.16.66.24	N/A	Unknown file s		iqn.2011-11.co



Stack Target List

Export share name	IP	Capacity (Used/Total)	Status	Description	iqn
iscsi	172.16.65.157	N/A	Unknown file s|		iqn.2009-05.co|

Success

You have successfully formatted stack folder - [iscsi]

With this newly attached stack target device, you will see the information displayed and also have access to several options to choose from.

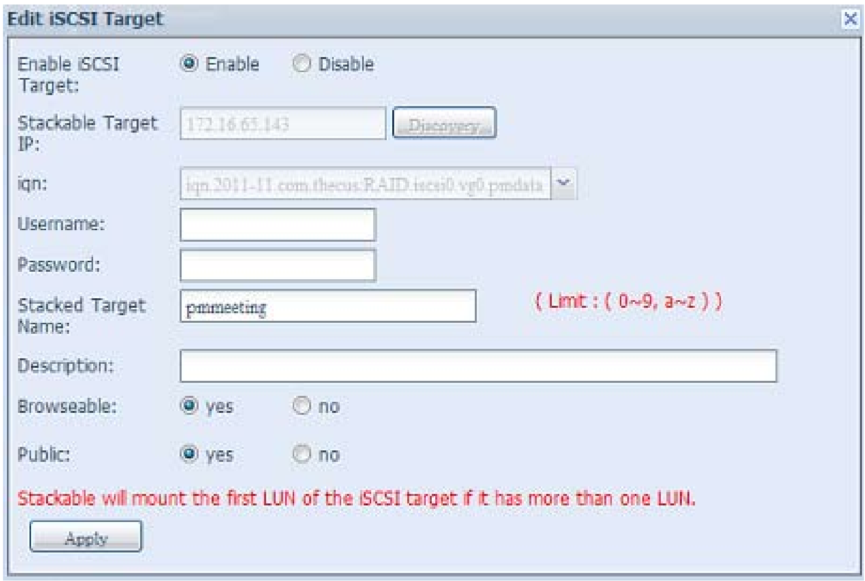
In general, if the attached stack target device has been used by another Thecus NAS as stack target volume, then the Format item will be display and system will recognize it straight away and display its capacity. Otherwise, the Format item will be available and the Capacity and Status items will show as "N/A" and "Unknown file system" respectively.

Next, click Format to proceed with formatting.

After the format is completed, the stack target volume will be created successfully. You will see the volume's capacity and status in the Stack Target List screen.

C. Edit a Stack Target

To make any changes to a stack target, click Edit for the corresponding stack target, and the system will bring up the following dialogue window:



Edit iSCSI Target

Enable iSCSI Target: ● Enable ○ Disable

Stackable Target IP: 172.16.65.143 Discovery

iqn: iqn.2011-11.com.thecus.RAID.iscsi0.vg0.pmdata

Username:

Password:

Stacked Target Name: pmmeeting (Limt : (0~9, a~z))

Description:

Browseable: ● yes ○ no

Public: ● yes ○ no

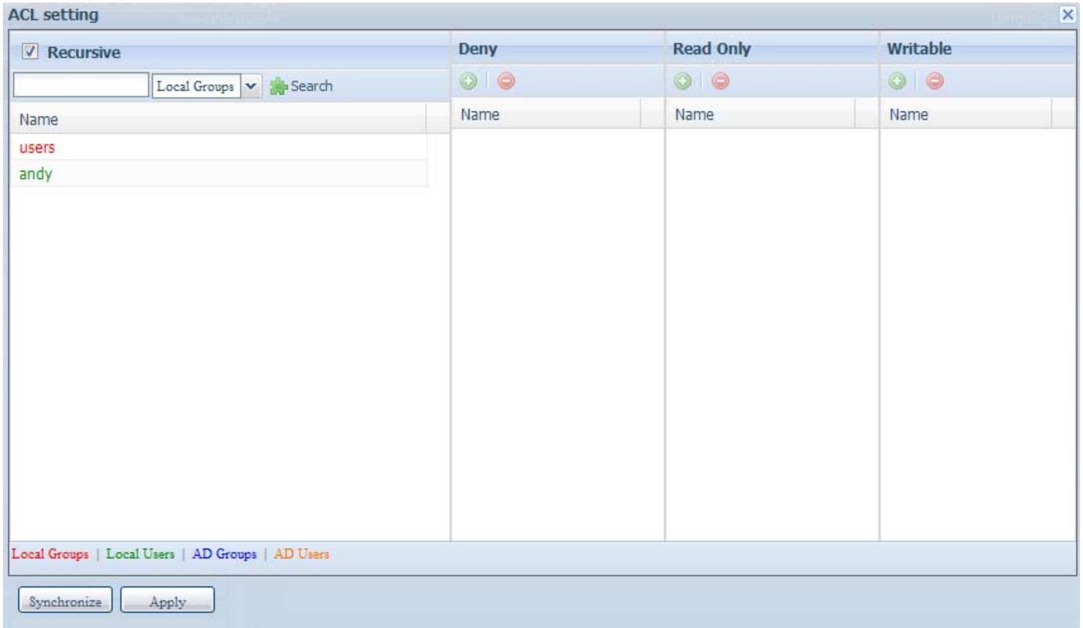
Stackable will mount the first LUN of the iSCSI target if it has more than one LUN.

After your changes have been made, click Apply to confirm any modifications. Once changes are applied, the associated information will be updated on the Stack Target List window.

D. Stack Target ACL

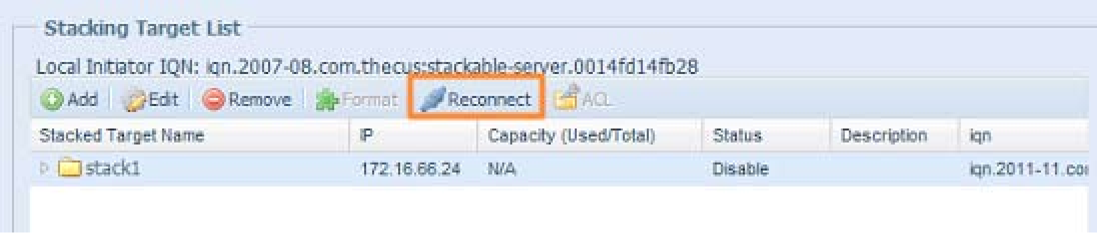
If the stack target Public setting set to Yes, then the ACL button will be grayed out. However, if Public setting is set to No, then the ACL button will be available for you to setup user access permissions for the stack target.

The ACL settings will be exactly the same as the system folder that you may have setup previously.



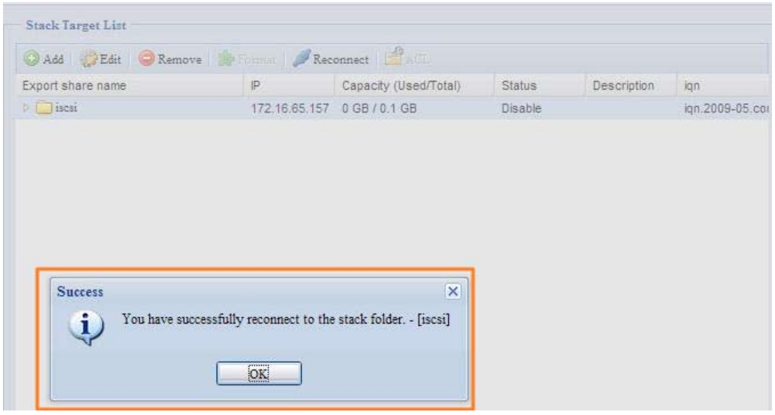
E. Reconnect a Stack Target

This is used to enable stack target devices that may have been disconnected due to a power outage or a disconnected network. When this happens, the Reconnect button will become available. To attempt to reconnect the stack target, click Reconnect.



Local Initiator IQN: iqn.2007-08.com.thecus:stackable-server.0014fd14fb28

Stacked Target Name	IP	Capacity (Used/Total)	Status	Description	iqn
stack1	172.16.66.24	N/A	Disable		iqn.2011-11.co



Export share name	IP	Capacity (Used/Total)	Status	Description	iqn
iscsi	172.16.65.157	0 GB / 0.1 GB	Disable		iqn.2009-05.co

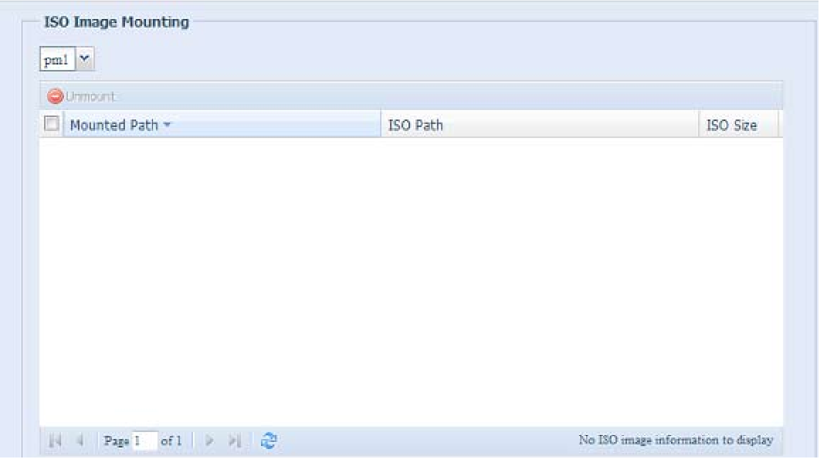
You have successfully reconnect to the stack folder. - [iscsi]

3.4.4 ISO Image Mounting (N4520/N4560 Only)

The ISO Image Mounting feature is a very useful tool from the Thecus products. With it, users can mount an ISO file and have the export name display all the details from the mounted ISO file.

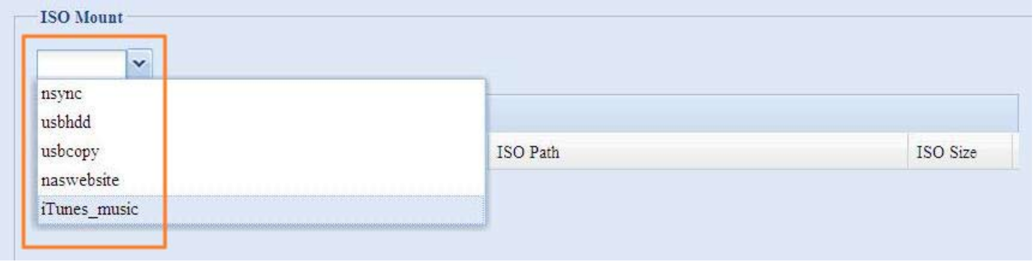
From the Control Panel, the ISO Image Mounting feature is located under "Storage". Please refer the figure below for reference.

Select the ISO Image Mounting function and the ISO Image Mounting window will appear as shown here.

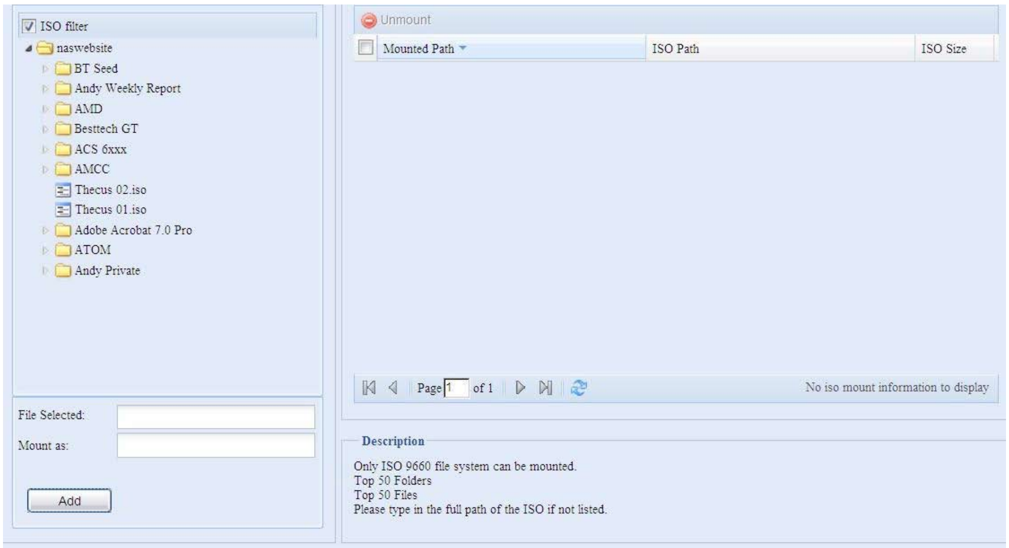


A. Add an ISO file

From the figure above, select an ISO file from the drop down share list.

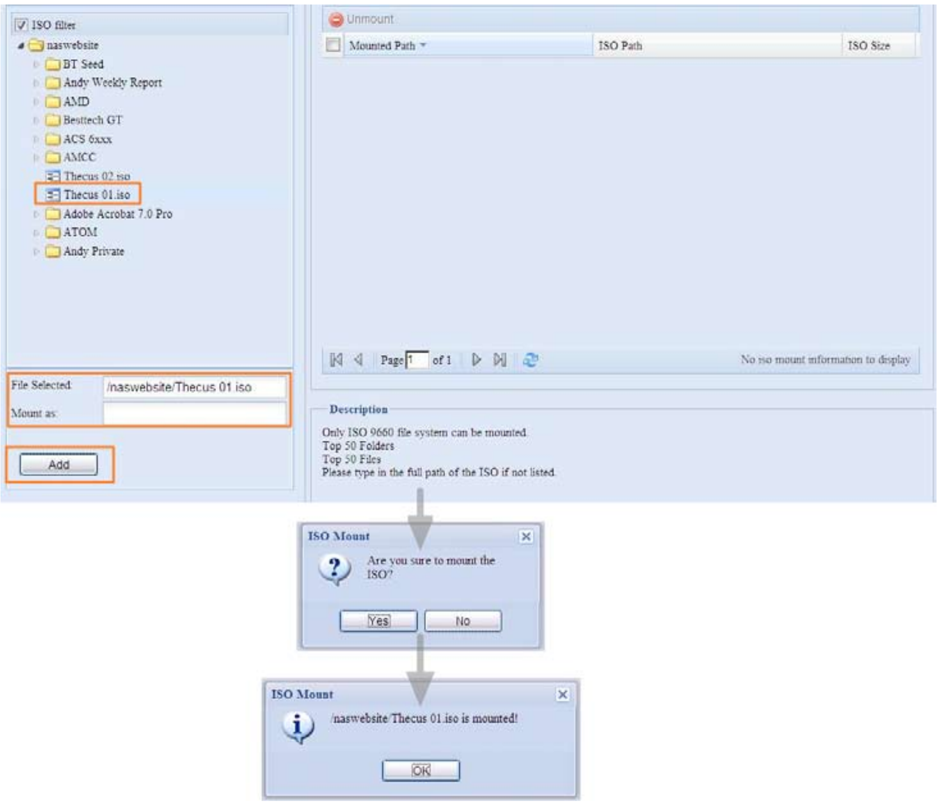


After selection, the system will bring up the Mount table screen for further settings.



Description

Only ISO 9660 file system can be mounted.
Top 50 Folders
Top 50 Files
Please type in the full path of the ISO if not listed.



File Selected: /naswebsite/Thecus 01.iso

Mount as:

□	Mounted Path	ISO Path	ISO Size

Page 1 of 1

No iso mount information to display

Description

Only ISO 9660 file system can be mounted.
Top 50 Folders
Top 50 Files
Please type in the full path of the ISO if not listed.

ISO Mount

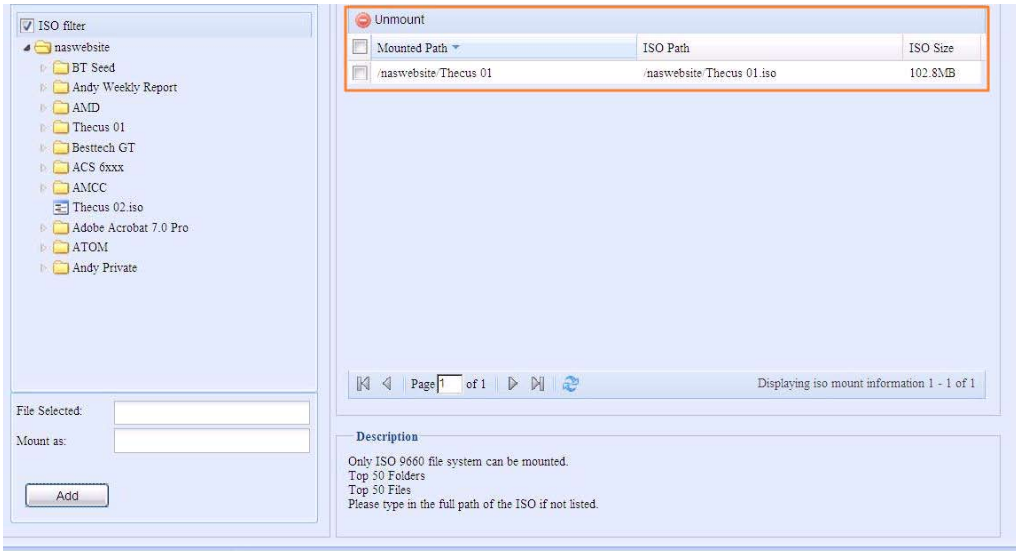
Are you sure to mount the ISO?

ISO Mount

/naswebsite/Thecus 01.iso is mounted!

To mount the new ISO file, select one file from the list of files and input the desired mounting name into the "Mount as:" field. Click "ADD" to confirm the completion of the mounting. If nothing is input in the "Mount as" ISO file export name field, the system will automatically give an export name to the ISO file. The mounting name will then be defined by the ISO file name.

After completion, the page will display all mounted ISO files.



File Selected:

Mount as:

□	Mounted Path	ISO Path	ISO Size
□	/naswebsite/Thecus 01	/naswebsite/Thecus 01.iso	102.8MB

Page 1 of 1

Displaying iso mount information 1 - 1 of 1

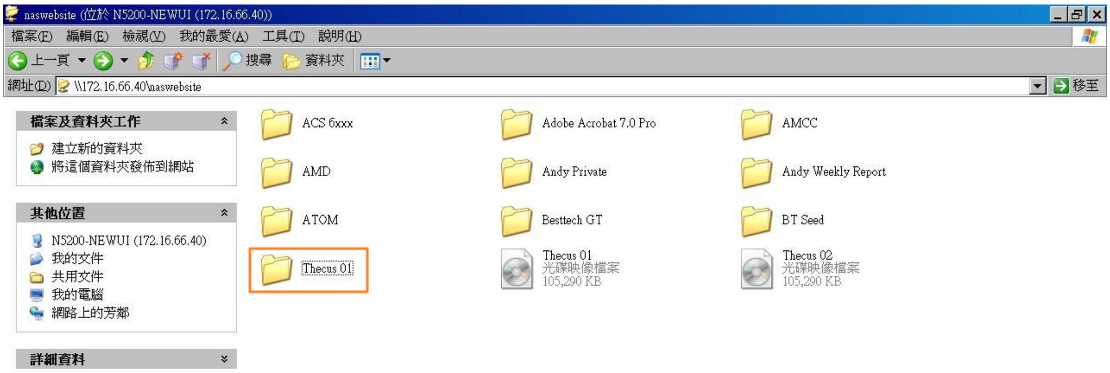
Description

Only ISO 9660 file system can be mounted.
Top 50 Folders
Top 50 Files
Please type in the full path of the ISO if not listed.

You can click "Unmount" to eliminate a mounted ISO file.

B. Using ISO

The mounted ISO file will be located in the share folder of the same name as the file. Please refer the screen shot below. Here, the ISO file "Thecus 01" wasn't assigned a mounting name, so the system automatically created a folder "Thecus 01".



3.4.5 iSCSI (N4520/N4560 Only)

You may specify the space allocated for iSCSI. See the table below to the allowed iSCSI target number per system:

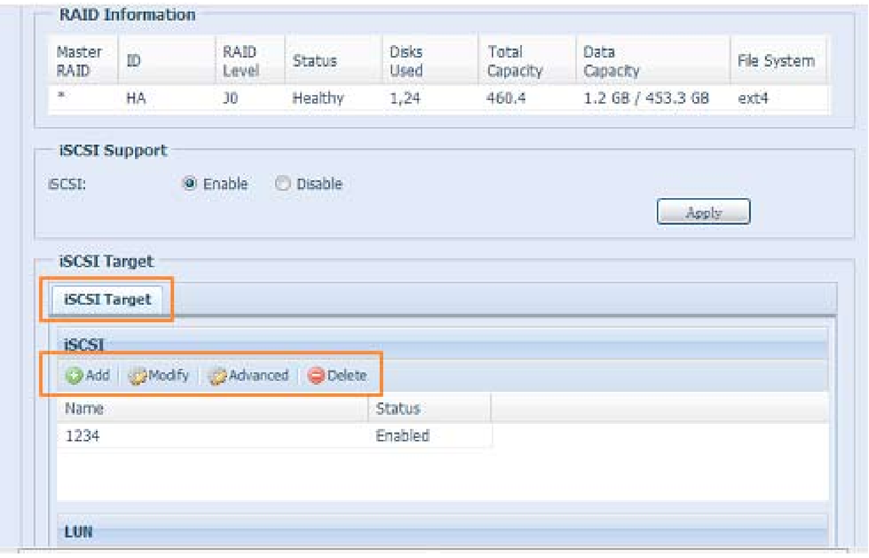
Model	N4520/N4560
Allowed iSCSI volume	15

- ### iSCSI Target

To add iSCSI target volume, click iSCSI with associated RAID volume from its drop down list and select the desired RAID volume.

iSCSI Target	
Item	**Description**
Add	Click to allocate space to iSCSI target from associated RAID volume.
Modify	Click this to modify the iSCSI Target.
Advanced	There are 3 options (iSCSI CRC/Checksum, Max Connections, Error Recovery Level) These currently allow the Admin to Enable/Disable the Thecus IP storage associated with the iSCSI setting.
Delete	Click this to delete the iSCSI Target.

Allocating Space for iSCSI Volume



RAID Information

Master RAID	ID	RAID Level	Status	Disks Used	Total Capacity	Data Capacity	File System
*	HA	J0	Healthy	1,24	460.4	1.2 GB / 453.3 GB	ext4

iSCSI Support

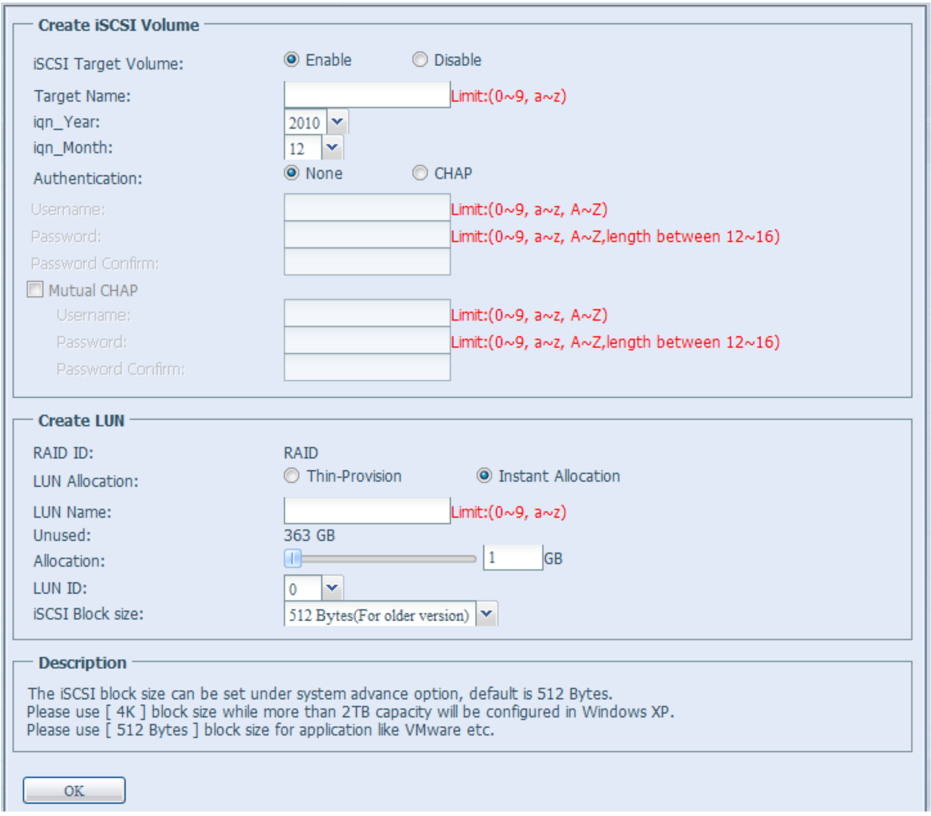
iSCSI: ● Enable ○ Disable

Name	Status
1234	Enabled

To allocate space for an iSCSI target on the current RAID volume, follow the steps below:

1. Under the iSCSI Target List, select iSCSI Target then click Add.

The Create iSCSI Volume screen appears.



Create iSCSI Volume

iSCSI Target Volume: ● Enable ○ Disable

Target Name: Limit:(0~9, a~z)

iqn_Year: 2010

iqn_Month: 12

Authentication: ● None ○ CHAP

Username: Limit:(0~9, a~z, A~Z)

Password: Limit:(0~9, a~z, A~Z,length between 12~16)

Password Confirm:

□ Mutual CHAP

Username: Limit:(0~9, a~z, A~Z)

Password: Limit:(0~9, a~z, A~Z,length between 12~16)

Password Confirm:

Create LUN

RAID ID: RAID

LUN Allocation: ○ Thin-Provision ● Instant Allocation

LUN Name: Limit:(0~9, a~z)

Unused: 363 GB

Allocation: 1 GB

LUN ID: 0

iSCSI Block size: 512 Bytes(For older version)

Description

The iSCSI block size can be set under system advance option, default is 512 Bytes.
Please use [4K] block size while more than 2TB capacity will be configured in Windows XP.
Please use [512 Bytes] block size for application like VMware etc.

Create iSCSI Volume

Item	Description
iSCSI Target Volume	Enable or Disable the iSCSI Target Volume.
Target Name	Name of the iSCSI Target. This name will be used by the Stackable NAS function to identify this export share.
iqn_Year	Select the current year from the dropdown.
Iqn_Month	Select the current month from the dropdown.
Authentication	You may choose CHAP authentication or choose None.
Username	Enter a username.
Password	Enter a password.
Password Confirm	Reenter the chosen password
Mutual CHAP	With this level of security, the target and the initiator authenticate each other.
Username	Enter a username.
Password	Enter a password.
Password Confirm	Reenter the chosen password
RAID ID	ID of current RAID volume.
LUN Allocation	Two modes can be choose from: Thin-provision: iSCSI thin-provisioning shares the available physical capacity to multiple iSCSI target volumes. It allows virtual capacity to be assigned to targets prior to adding physical space when it has run out. Instant Allocation: Allocate available physical capacity to iSCSI target volumes.
LUN Name	Name of the LUN.
Unused	Unused space on current RAID volume.
Allocation	Percentage and amount of space allocated to iSCSI volume.
LUN ID	Specific Logic unit ID number.
iSCSI Block size	The iSCSI block size can be set under system advance option, default is 512 Bytes. [4K] block size while more than 2TB capacity will be configured in Windows XP. [512 Bytes] block size for application like VMware etc.

Be sure the iSCSI target volume has been enabled or it will not list out while using Initiator to get associated iSCSI target volumes.

The iSCSI target volume creation will associate at least one LUN together. It can be assigned either "Thin-Provisioning" or "Instant Allocation".

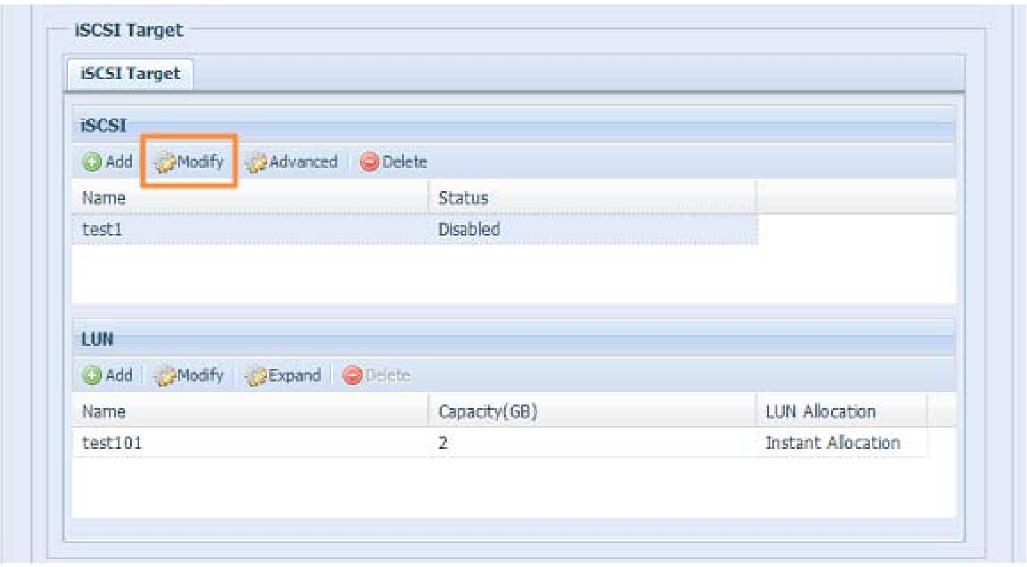
2. Enable the iSCSI Target Volume by selecting Enable.
3. Enter a Target Name. This will be used by the Stackable NAS function to identify this export share.
4. Choose the current year from the Year dropdown.
5. Choose the current month from the Month dropdown.
6. Choose to enable CHAP authentication or choose None.
7. If you've enabled CHAP authentication, enter a username and a password. Confirm your chosen password be reentering it in the Password Confirm box.
8. Choose Thin-Provision or Instant Allocation
9. Enter a LUN Name.
10. Designate the percentage to be allocated from the Allocation drag bar.
11. When iSCSI target volume has been created, the LUN ID is configurable from 0 to 254 with a default of the next available number in ascending numerical order. The LUN ID is unique and cannot be duplicated.
12. Choose [4K] block size to have iSCSI target volume over 2TB barrier or [512 Bytes] block size in some application needed.
13. Click OK to create the iSCSI volume.

- ### Modify iSCSI Volume

To modify iSCSI target on the current RAID volume, follow the steps below:

1. Under the iSCSI Target List, click Modify.

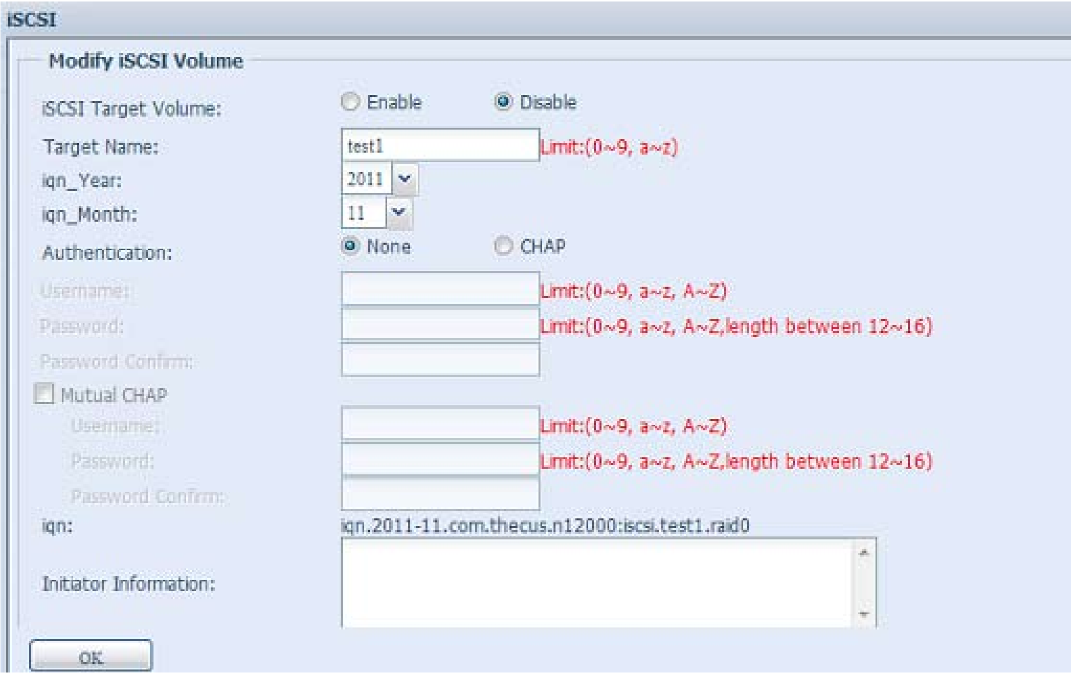
The Modify iSCSI Volume screen appears.



Name	Status
test1	Disabled

Name	Capacity(GB)	LUN Allocation
test101	2	Instant Allocation

2. Modify your settings. Press ok to change.



iSCSI

Modify iSCSI Volume

iSCSI Target Volume: ○ Enable ● Disable

Target Name: test1 Limit:(0~9, a~z)

iqn_Year: 2011

iqn_Month: 11

Authentication: ● None ○ CHAP

Username: Limit:(0~9, a~z, A~Z)

Password: Limit:(0~9, a~z, A~Z,length between 12~16)

Password Confirm:

□ Mutual CHAP

Username: Limit:(0~9, a~z, A~Z)

Password: Limit:(0~9, a~z, A~Z,length between 12~16)

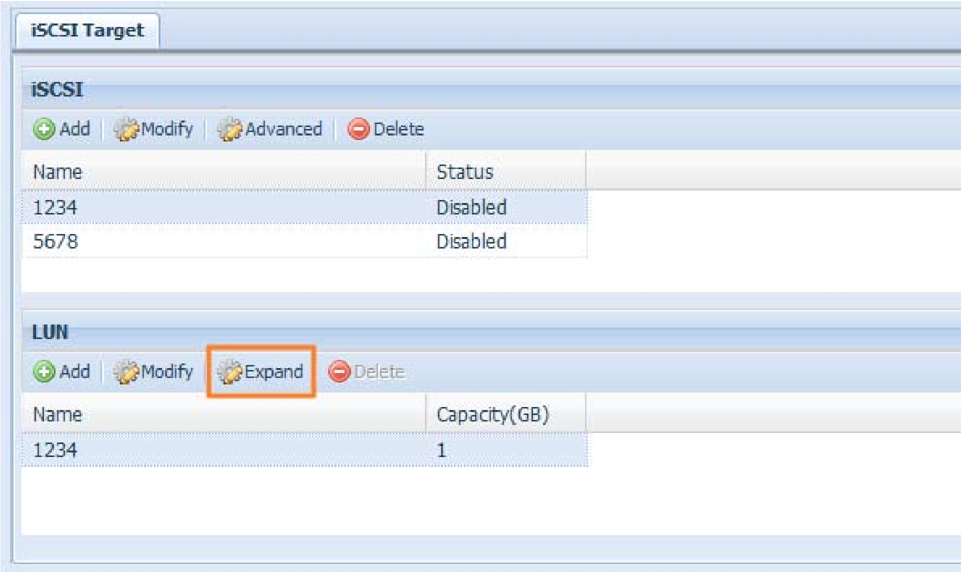
Password Confirm:

iqn: iqn.2011-11.com.thecus.n12000:iscsi.test1.raid0

Initiator Information:

- **Expand Volume**

The iSCSI volume is now able to expand its capacity from unused space (Instant Allocation mode only). From the volume list, simply select the iSCSI volume you like to expand and click the Expand button:



iSCSI Target

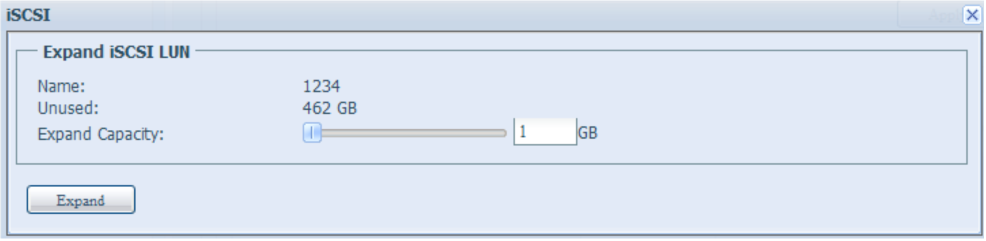
iSCSI

Name	Status
1234	Disabled
5678	Disabled

LUN

Name	Capacity(GB)
1234	1

You will then see the dialog box displayed below. Drag the Expand Capacity bar to the size you want. Then press Expand to confirm the operation.



iSCSI

Expand iSCSI LUN

Name: 1234

Unused: 462 GB

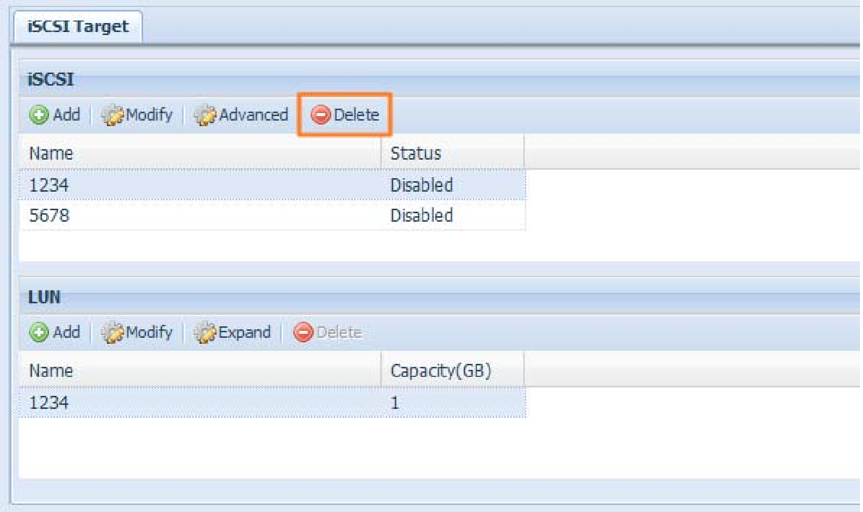
Expand Capacity: 1 GB

- ### Delete Volume

To delete volume on the current RAID volume, follow the steps below:

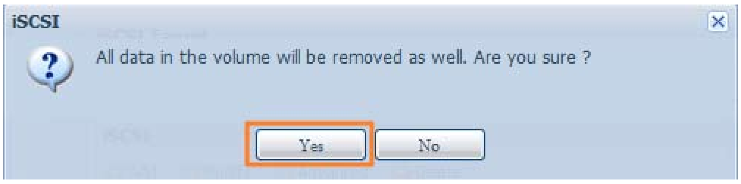
1. Under the Volume Allocation List, click Delete.

The Space Allocation screen appears.



Name	Status
1234	Disabled
5678	Disabled

Name	Capacity(GB)
1234	1



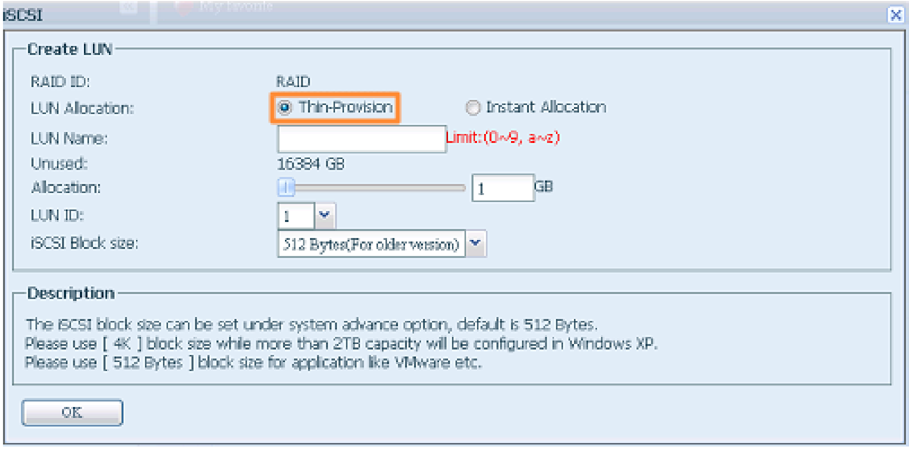
All data in the volume will be removed as well. Are you sure ?

2. Press YES. All data in the volume will be removed.

- ### iSCSI Thin-Provisioning

If iSCSI Thin-Provisioning is selected when creating an iSCSI target volume, virtual memory is assigned to the target, allowing the physical memory to reach maximum capacity and adding new disks only when needed.

To setup iSCSI thin-provisioning, simply select “Thin-Provision” mode from the “Create LUN” setting screen.

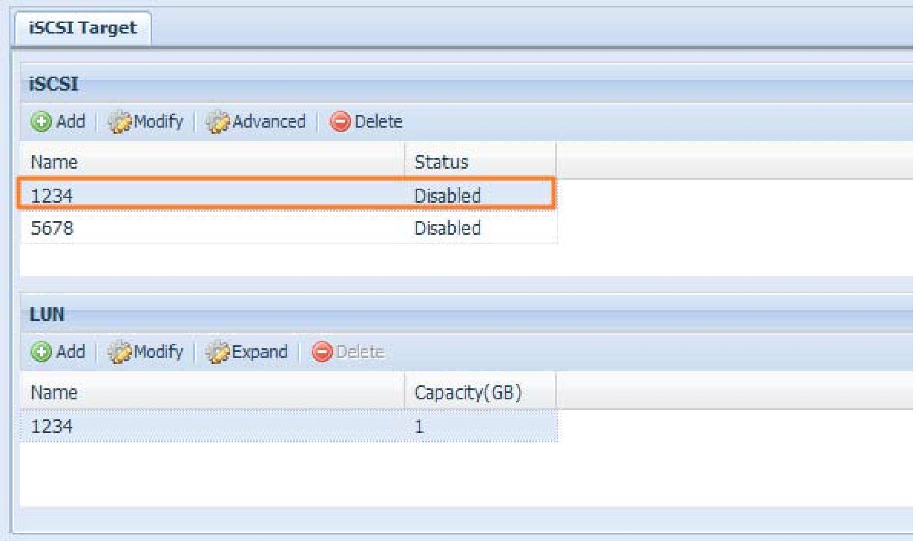


RAID ID:	RAID
LUN Allocation:	● Thin-Provision ○ Instant Allocation
LUN Name:	Limit:(0~9, a~z)
Unused:	16384 GB
Allocation:	1 GB
LUN ID:	1
iSCSI Block size:	512 Bytes(For older version)

The iSCSI block size can be set under system advance option, default is 512 Bytes.
Please use [4K] block size while more than 2TB capacity will be configured in Windows XP.
Please use [512 Bytes] block size for application like VMware etc.

Next, allocate capacity for the iSCSI thin-provision volume by dragging the Allocation bar to the desired size.

After the size has been determined, click OK to confirm. Now you will see the iSCSI thin-provisioning volume is available from the list. Please refer to the screenshot below.



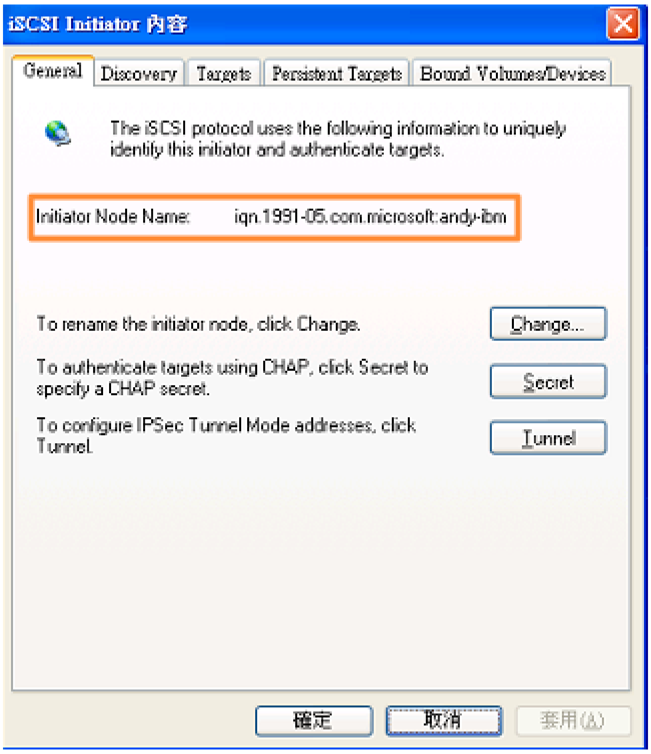
Name	Status
1234	Disabled
5678	Disabled

Name	Capacity(GB)
1234	1

If creating an iSCSI target volume under "Instant Allocation", physical memory is assign to the target, being limited by the available memory. For the iSCSI target volume created under "thin-provisioning", virtual memory is assigned to the volume, which can go up to 16384GB (16TB).

- **LUN ACL**

After iSCSI target has been created, you are one step away from using the iSCSI volume. Under "LUN ACL", you need to add "Initiator iqn" and setup ACL access privileges to determine the accessibility. Please refer the screen shot below for where "Initiator iqn" can be found.



The iSCSI protocol uses the following information to uniquely identify this initiator and authenticate targets.

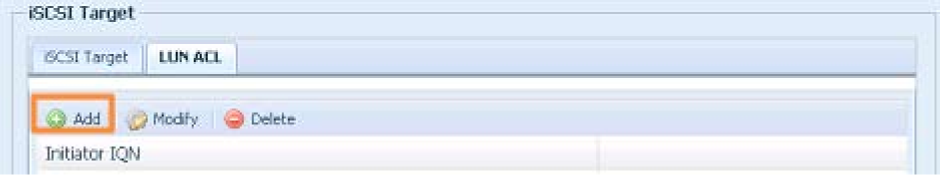
Initiator Node Name: iqn.1991-05.com.microsoft:andy-ibm

To rename the initiator node, click Change.

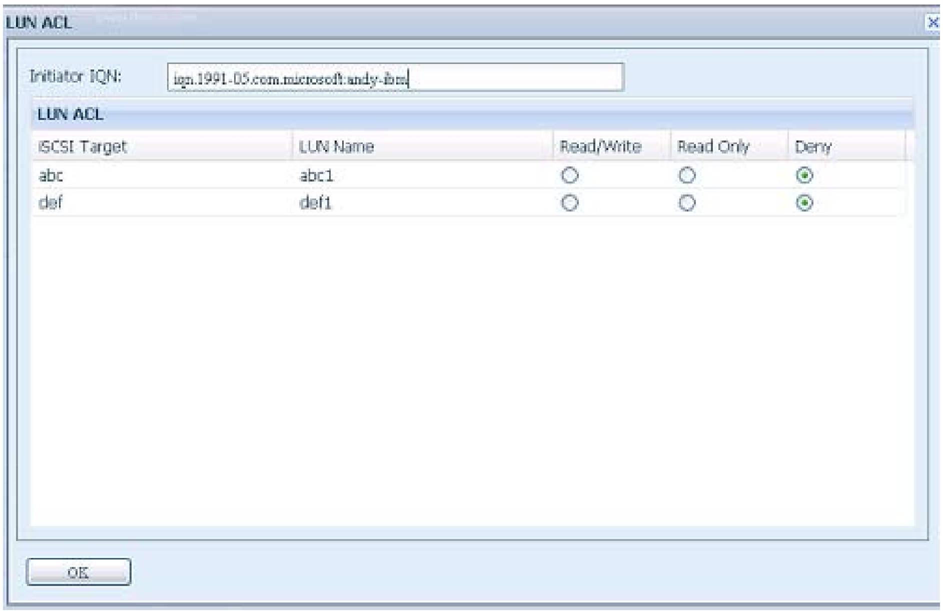
To authenticate targets using CHAP, click Secret to specify a CHAP secret.

To configure IPSec Tunnel Mode addresses, click Tunnel.

From the LUN ACL setting screen click "Add":



Next, input "Initiator iqn" and setup iSCSI target volume access privileges from the available list. Apply by clicking the OK button.



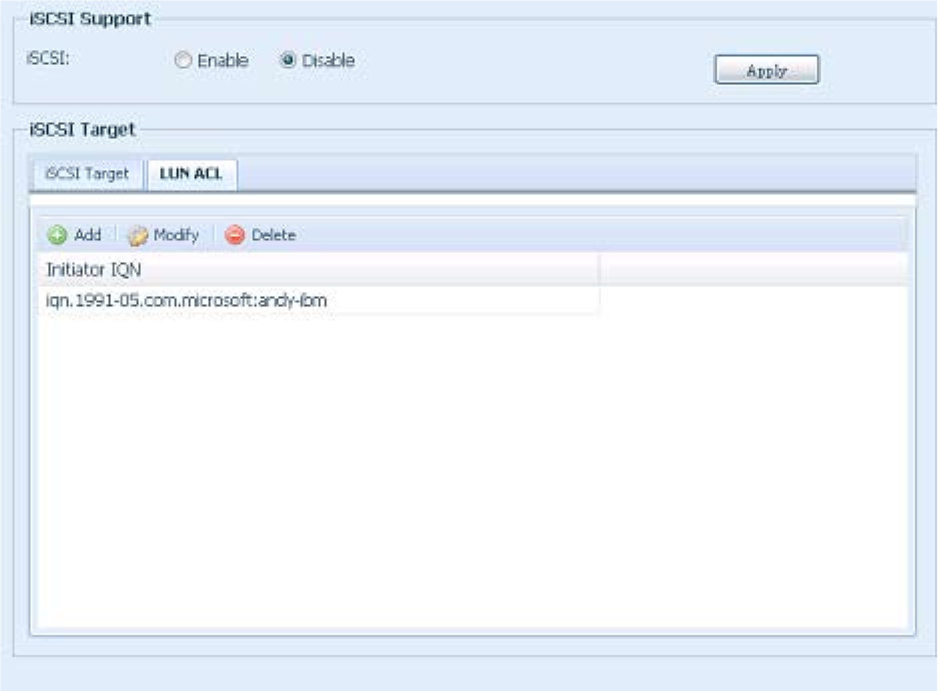
LUN ACL

Initiator IQN: iqn.1991-05.com.microsoft:andy-ibm

LUN ACL

iSCSI Target	LUN Name	Read/Write	Read Only	Deny
abc	abc1	○	○	●
def	def1	○	○	●

The accessible Initiator will be listed as shown in the screen shot displayed below.



iSCSI Support

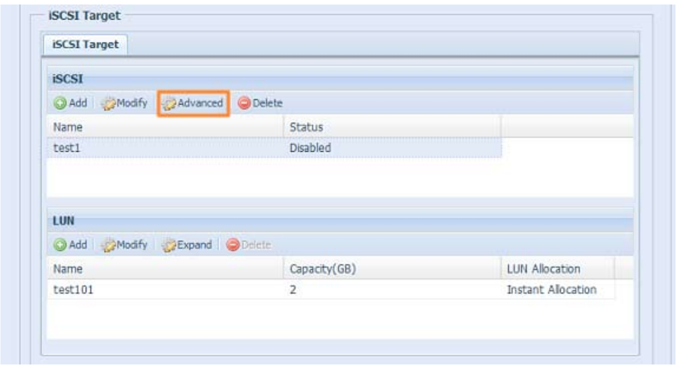
iSCSI: ○ Enable ● Disable

Initiator IQN
iqn.1991-05.com.microsoft:andy-ibm

The listed "Initiator iqn" can be modified or deleted by selecting the desired iqn and pressing Modify or Delete.

- **Advance Option**

There are 3 available options for the user to operate Thecus IP storage associated with iSCSI setting. The details are listed in the following screenshot. If the options are modified, the system will need to reboot for the changes to take place.

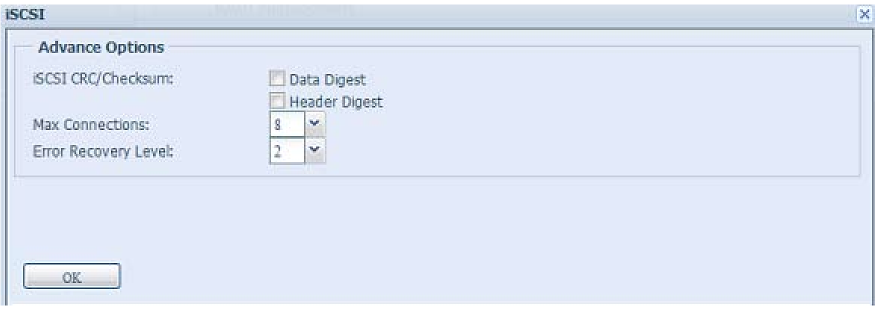


Name	Status
test1	Disabled

Name	Capacity(GB)	LUN Allocation
test101	2	Instant Allocation

iSCSI CRC/Checksum

To enable this option, the initiator can connect with "Data digest" and "Header digest".



iSCSI CRC/Checksum: □ Data Digest □ Header Digest

Max Connections: 8

Error Recovery Level: 2

Max Connections

The maximum number of iSCSI connections.

Error Recovery Level

The Error Recovery Level (ERL) is negotiated during a leading iSCSI connection login in traditional iSCSI (RFC 3720) and iSER (RFC 5046).

ERL=0: Session Recovery

ERL=0 (Session Recovery) is triggered when failures within a command, within a connection, and/or within TCP occur. This causes all of the previous connections from the failed session to be restarted on a new session by sending a iSCSI Login Request with a zero TSIHRestart all iSCSI connections on any failure.

ERL=1: Digest Failure Recovery

ERL=1, only applies to traditional iSCSI. For iSCSI/SCTP (which has its own CRC32C) and both types of iSER (so far), handling header and data checksum recovery can be disabled.

ERL=2: Connection Recovery

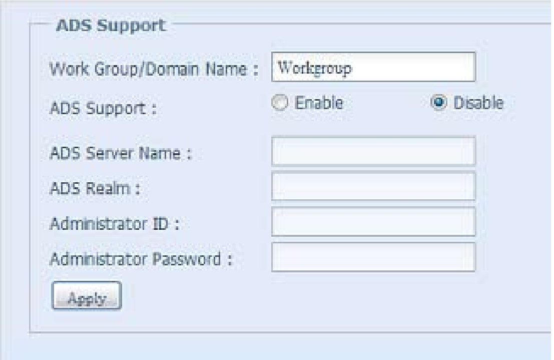
ERL=2, allows for both single and multiple communication path sessions within a iSCSI Nexus (and hence the SCSI Nexus) to actively perform realligence/retry on iSCSI ITTs from failed iSCSI connections. ERL=2 allows iSCSI fabrics to take advantage of recovery in all regards of transport level fabric failures, and in a completely OS independent fashion (i.e. below the host OS storage stack).

3.5 File Sharing/Privilege

The Thecus IP storage has built-in user database that allows administrators to manage user access using different group policies. From the File Sharing/Privilege menu, you can create, modify, and delete users, and assign them to groups that you designate.

3.5.1 ADS Support (N4520/N4560 Only)

If you have a Windows Active Directory Server (ADS) to handle the domain security in your network, you can simply enable the ADS support feature; the Thecus IP storage will connect with the ADS server and get all the information of the domain users and groups automatically. From the File Sharing/Privilege category, choose Authentication item and the ADS Support screen appears. You can change any of these items and press Apply to confirm your settings.



ADS Support

Work Group/Domain Name : Workgroup

ADS Support : ○ Enable ● Disable

ADS Server Name :

ADS Realm :

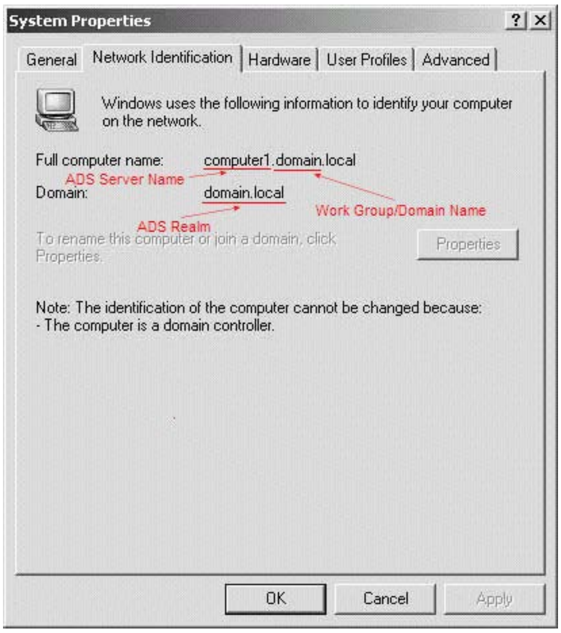
Administrator ID :

Administrator Password :

A description of each item follows:

ADS/NT Support	
Item	**Description**
Work Group / Domain Name	Specifies the SMB/CIFS Work Group / ADS Domain Name (e.g. MYGROUP).
ADS Support	Select Disable to disable authentication through Windows Active Directory Server.
ADS Server Name	Specifies the ADS server name (e.g. adservername).
ADS Realm	Specifies the ADS realm (e.g. example.com).
Administrator ID	Enter the administrators ID of Windows Active Directory, which is required for Thecus IP storage to join domain.
Administrator Password	Enter the ADS Administrator password.
Apply	To save your settings.

To join an AD domain, you can refer to the figure here and use the example below to configure the Thecus IP storage for associated filed input:



Windows uses the following information to identify your computer on the network.

Full computer name: computer1.domain.local

Domain: domain.local

To rename this computer or join a domain, click Properties.

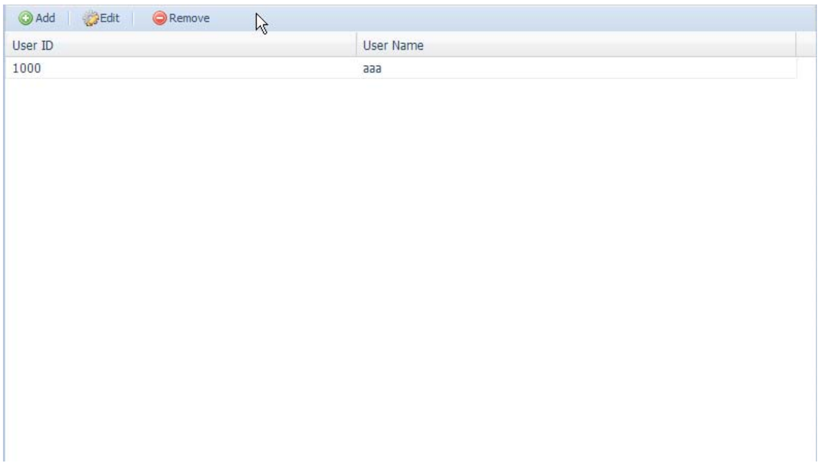
Note: The identification of the computer cannot be changed because:
- The computer is a domain controller.

AD Domain Example	
Item	**Information**
Work Group / Domain Name	domain
ADS Support	Enable
ADS Server Name	Computer1
ADS Realm	Domain.local
Administrator ID	Administrator
Administrator Password	***********

- The DNS server specified in the WAN/LAN1 configuration page should be able to correctly resolve the ADS server name.
- The time zone setting between Thecus IP storage and ADS should be identical.
- The system time difference between Thecus IP storage and ADS should be less than five minutes.
- The Administrator Password field is for the password of ADS (Active Directory Server) not Thecus IP storage.

3.5.2 Local User Configuration

From the File Sharing/Privilege category, choose the User item, and the Local User Configuration screen appears. This screen allows you to Add, Edit, and Remove local users.



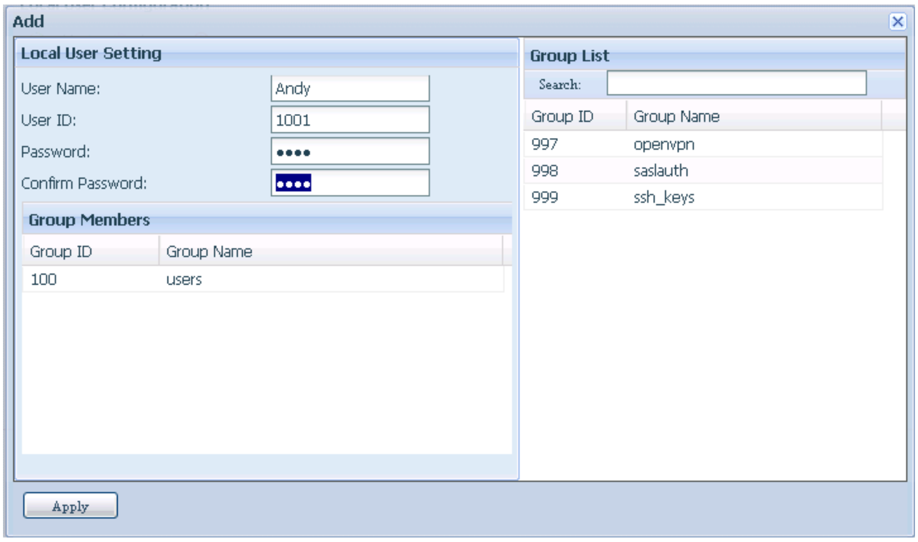
User ID	User Name
1000	aaa

Local User Configuration	
Item	**Description**
Add	Press the ***Add*** button to add a user to the list of local users.
Edit	Press the ***Edit*** button to modify a local user.
Remove	Press the ***Remove*** button to delete a selected user from the system.

- ### Add Users

1. Click on the Add button on Local User Configuration screen, and Local User Setting screen appears.
2. On the Local User Setting screen, enter a name in the User Name box.
3. Enter a User ID number or leave blank to use the system default value.
4. Enter a password in the Password box and re-enter the password in the Confirm box.
5. Select which group the user will belong to. Group Members is a list of groups this user belongs to. Group List is a list of groups this user does not belong to. Use the << or >> buttons to have this user join or leave a group.
6. Press the Apply button and the user is created.

- All users are automatically assigned to the 'users' group.


Add

Local User Setting

User Name: Andy
User ID: 1001
Password: ••••
Confirm Password: ••••

Group Members

Group ID	Group Name
100	users

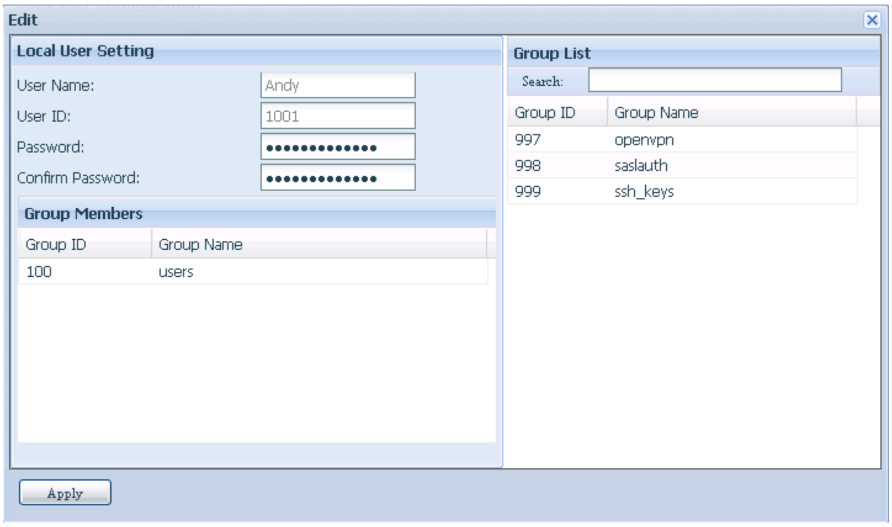
Group List

Search:

Group ID	Group Name
997	openvpn
998	saslauth
999	ssh_keys

- **Edit Users**

1. Select an existing user from the Local User Configuration screen.
2. Click on the Edit button, and the Local User Setting screen appears.
3. From here, you can enter a new password and re-enter to confirm, or use the << or >> buttons to have this user join or leave a group. Click the Apply button to save your changes.


Edit

Local User Setting

User Name: Andy
User ID: 1001
Password: •••••••••••••
Confirm Password: •••••••••••••

Group Members

Group ID	Group Name
100	users

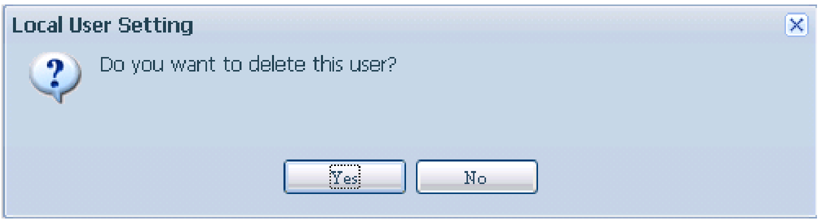
Group List

Search:

Group ID	Group Name
997	openvpn
998	saslauth
999	ssh_keys

- **Remove Users**

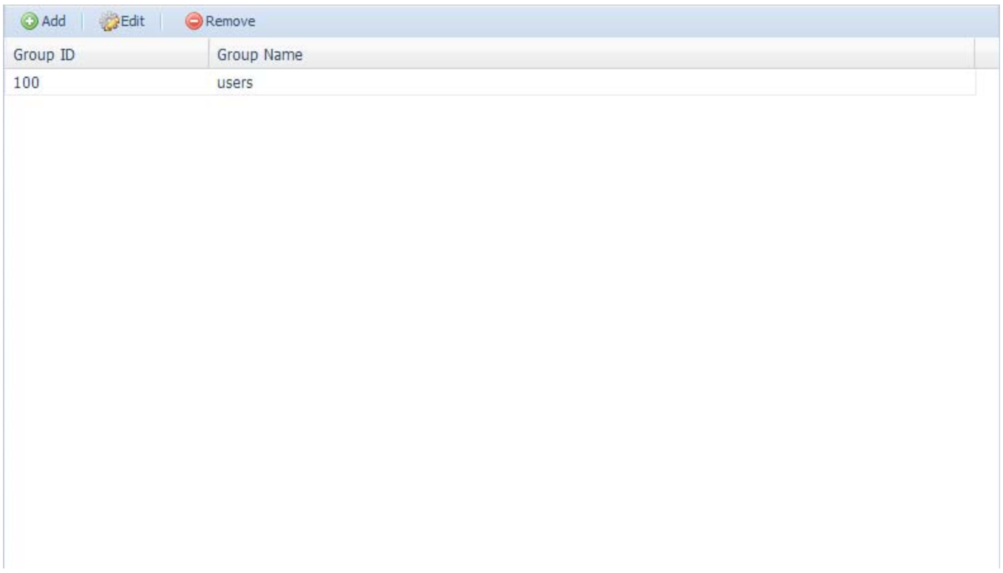
1. Select an existing user from the Local User Configuration screen.
2. Click on Remove button and the user is deleted from the system.


Local User Setting

Do you want to delete this user?

3.5.3 Local Group Configuration

From the File Sharing/Privilege category, choose the Group item, and the Local Group Configuration screen appears. This screen allows you to Add, Edit, and Remove local groups.

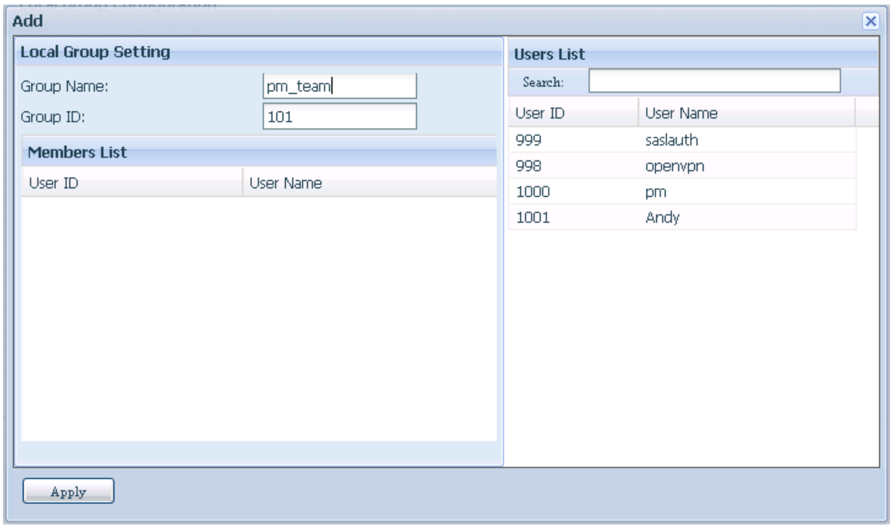


Group ID	Group Name
100	users

Local Group Configuration	
Item	**Description**
Add	Press the ***Add*** button to add a user to the list of local groups.
Edit	Press the ***Edit*** button to modify a selected group from the system.
Remove	Press the Remove button to delete a selected group from the system.

- ## Add Groups

1. On the Local Group Configuration screen, click on the Add button.
2. The Local Group Setting screen appears.
3. Enter a Group Name.
4. Enter a Group ID number. If left blank, the system will automatically assign one.
5. Select users to be in this group from the Users List by adding them to the Members List using the << button.
6. Click the Apply button to save your changes.



Group Name: pm_team

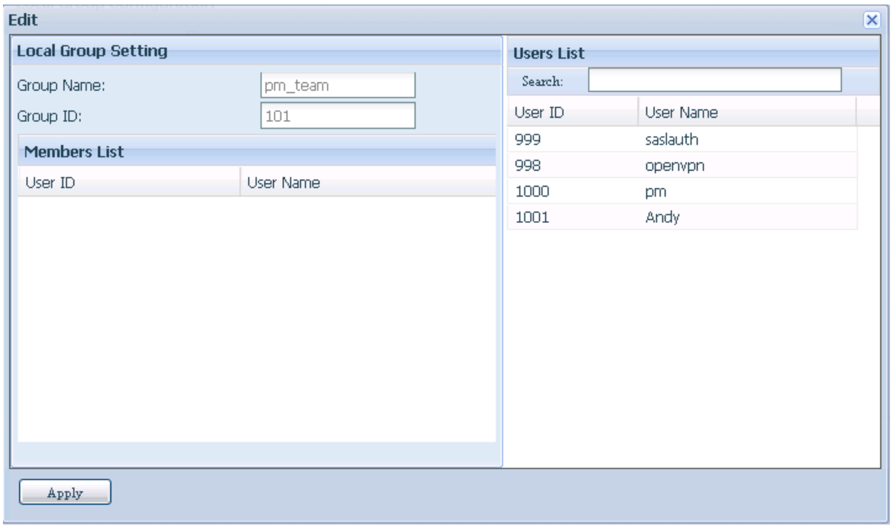
Group ID: 101

User ID	User Name

User ID	User Name
999	saslauth
998	openvpn
1000	pm
1001	Andy

- **Edit Groups**

1. On the Local Group Configuration screen, select a group name from the list.
2. Press the Edit button to modify the members in a group.
3. To add a user into a group, select the user from the Users List, and press the << button to move the user into the Members List.
4. To remove a user from a group, select the user from Members List, and press the >> button.
5. Click the Apply button to save your changes.



Edit

Local Group Setting

Group Name: pm_team

Group ID: 101

Members List

User ID	User Name

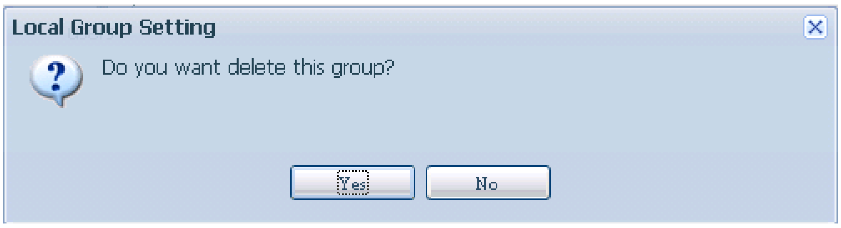
Users List

Search:

User ID	User Name
999	saslauth
998	openvpn
1000	pm
1001	Andy

- **Remove Groups**

1. On the Local Group Configuration screen, select a group name from the list.
2. Press Remove to delete the group from the system.



Local Group Setting

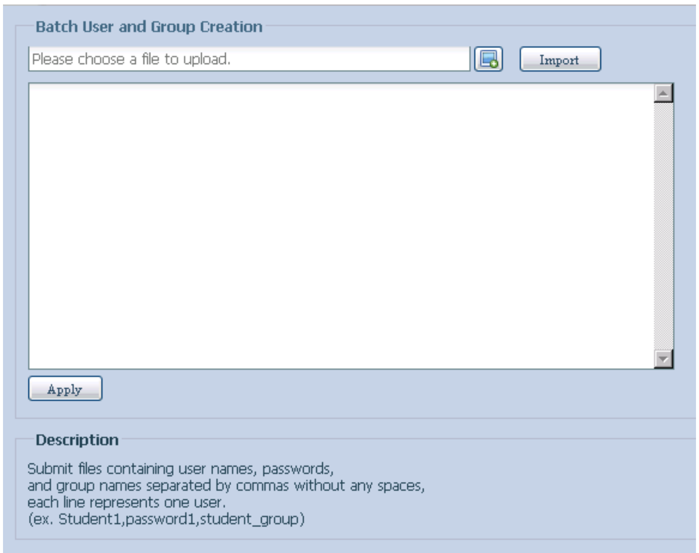
Do you want delete this group?

3.5.4 Batch Input

The Thecus IP storage can also add users and groups in batch mode. This enables you to conveniently add numerous users and groups automatically by importing a simple comma-separated plain text (*.txt) file.

From the File Sharing/Privilege category, click Batch Input and the Batch User and Group Creation dialogue will appear. To import your list of users and groups, follow these steps:

1. Click the Browse icon to locate your comma-separated text file.
   The information in the text file should follow this format:
   [USERNAME], [PASSWORD], [GROUP]
2. Click Open.
3. Click Import to begin the user list import.


Batch User and Group Creation
Please choose a file to upload.
Import
Apply
Description

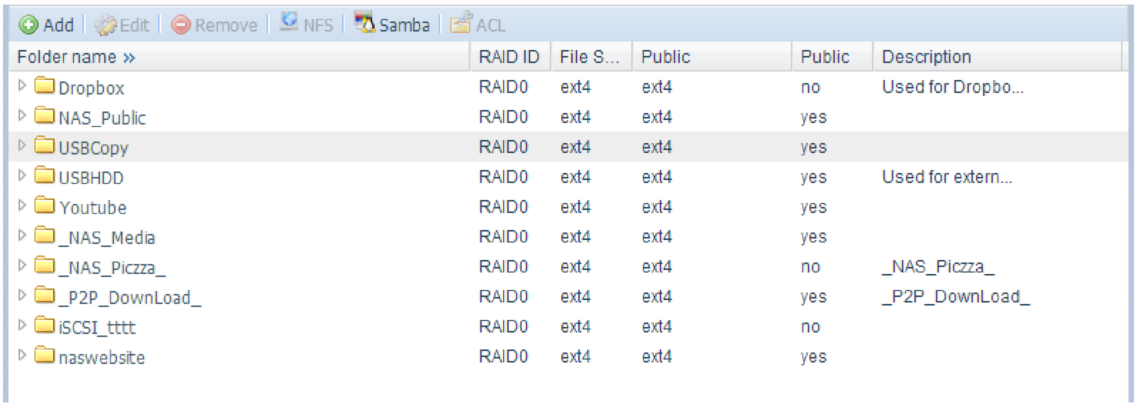
Submit files containing user names, passwords, and group names separated by commas without any spaces, each line represents one user. (ex. Student1,password1,student_group)

3.5.5 Shared Folder

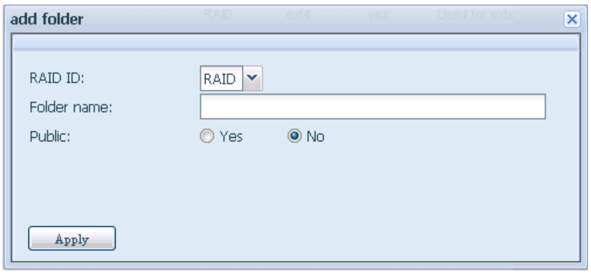
From the File Sharing/Privilege category, choose Shared Folder, and the Shared Folder screen appears. This screen allows you to create and configure folders on the Thecus IP storage volume.

- ### Adding Folders

On the Folder screen, press the Add button and the Add Folder screen appears. This screen allows you to add a folder. After entering the information, press Apply to create new folder.



Folder name »	RAID ID	File S...	Public	Public	Description
Dropbox	RAID0	ext4	ext4	no	Used for Dropbo...
NAS_Public	RAID0	ext4	ext4	yes	
USBCopy	RAID0	ext4	ext4	yes	
USBHDD	RAID0	ext4	ext4	yes	Used for extern...
Youtube	RAID0	ext4	ext4	yes	
_NAS_Media	RAID0	ext4	ext4	yes	
_NAS_Piczza_	RAID0	ext4	ext4	no	_NAS_Piczza_
_P2P_DownLoad_	RAID0	ext4	ext4	yes	_P2P_DownLoad_
iSCSI_tttt	RAID0	ext4	ext4	no	
naswebsite	RAID0	ext4	ext4	yes	



RAID ID: RAID

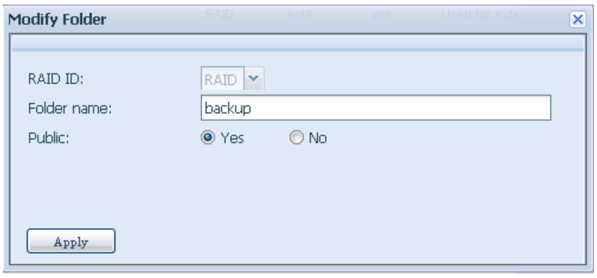
Folder name:

Public: ○ Yes ● No

Add Folder	
Item	**Description**
RAID ID	RAID volume where the new folder will reside.
Folder Name	Enter the name of the folder.
Public	Admit or deny public access to this folder.
Apply	Press ***Apply*** to create the folder.

- ### Modify Folders

On the Folder screen, press the Edit button and the Modify Folder screen appears. This screen allows you to change folder information. After entering the information, press Apply to save your changes.



Modify Folder

RAID ID: RAID

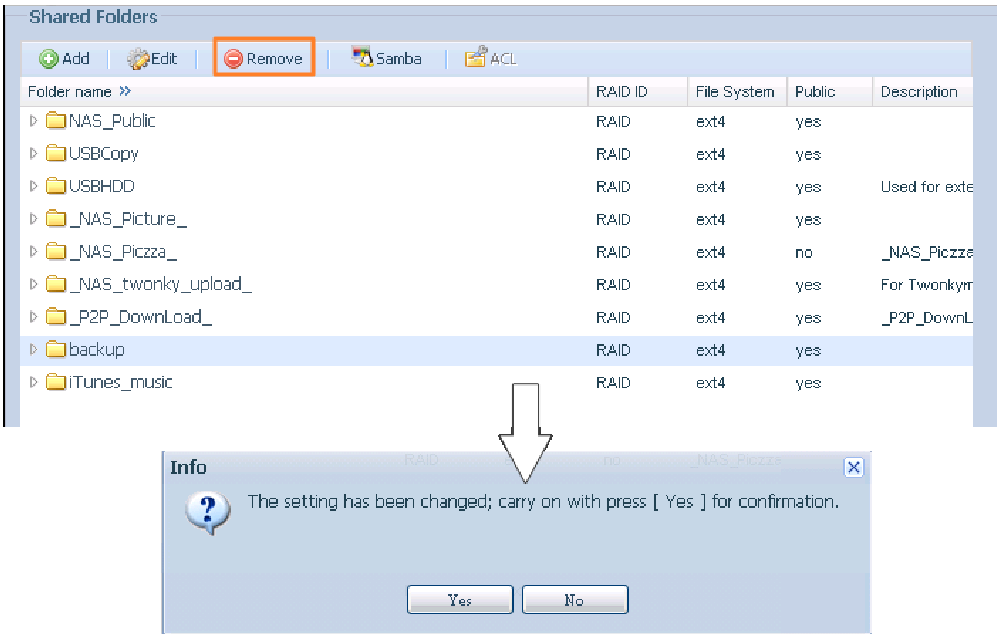
Folder name: backup

Public: ● Yes ○ No

Modify Folder	
Item	**Description**
Folder Name	Enter the name of the folder.
Public	Admit or deny public access to this folder.
Apply	Press ***Apply*** to create the folder.

- ## Remove Folders

To remove a folder, press the Remove button from the specified folder row. The system will confirm folder deletion. Press Yes to delete the folder permanently or No to go back to the folder list.



Shared Folders

Folder name	RAID ID	File System	Public	Description
NAS_Public	RAID	ext4	yes	
USBCopy	RAID	ext4	yes	
USBHDD	RAID	ext4	yes	Used for exte
_NAS_Picture_	RAID	ext4	yes	
_NAS_Piczza_	RAID	ext4	no	_NAS_Piczze
_NAS_twonky_upload_	RAID	ext4	yes	For Twonkym
_P2P_DownLoad_	RAID	ext4	yes	_P2P_DownL
backup	RAID	ext4	yes	
iTunes_music	RAID	ext4	yes	

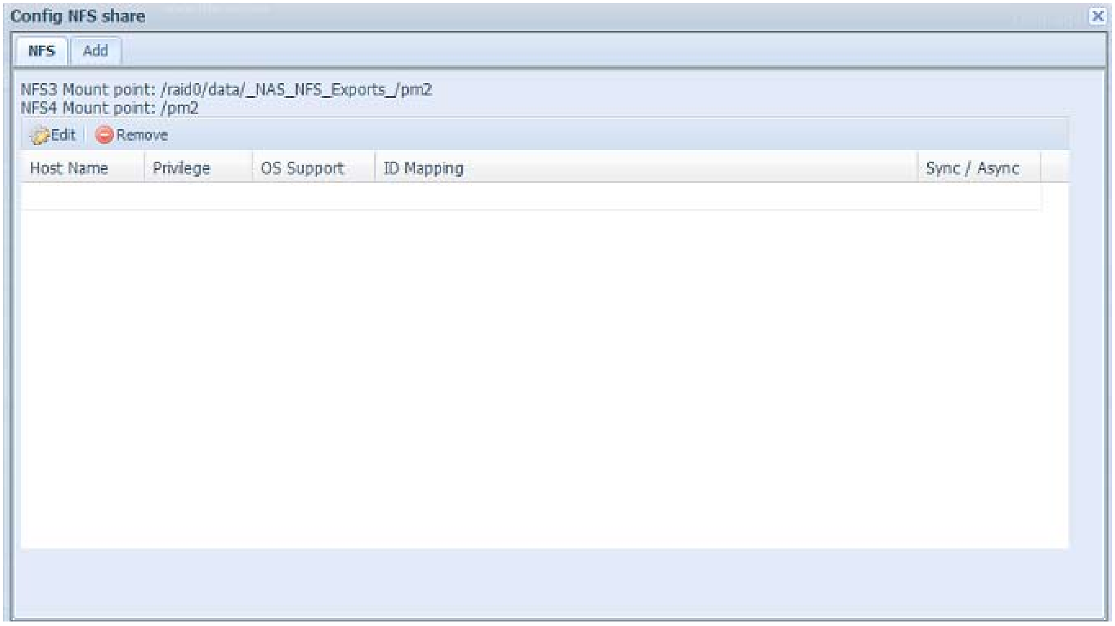
Info

The setting has been changed; carry on with press [Yes] for confirmation.

All the data stored in the folder will be deleted once the folder is deleted. The data will not be recoverable.

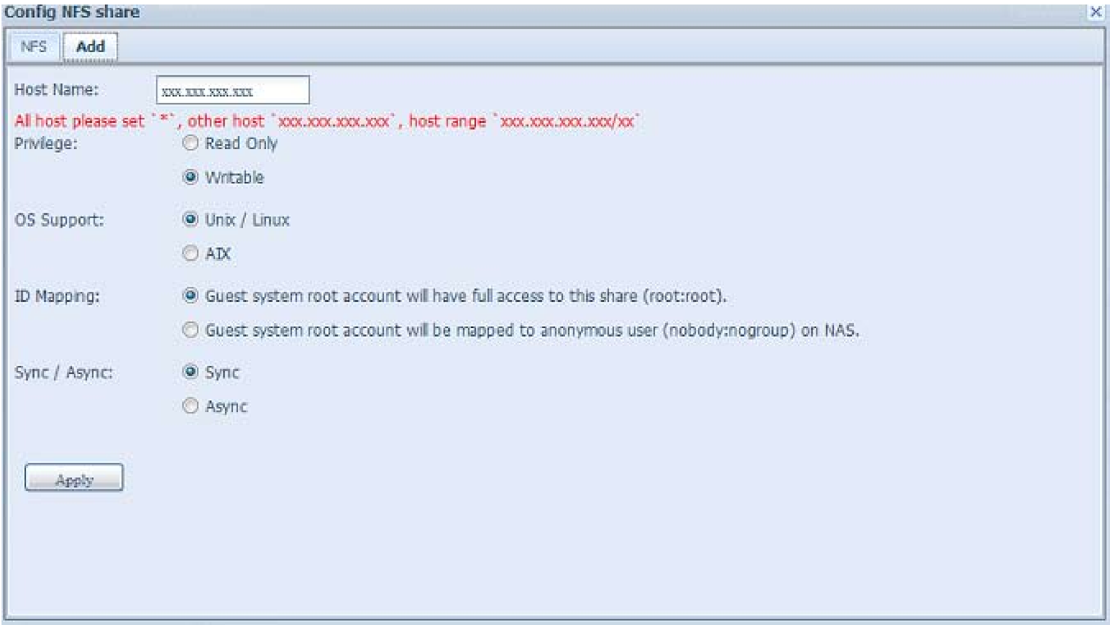
- **NFS Share**

To allow NFS access to the share folder, enable the NFS Service, and then set up hosts with access rights by clicking Add.



NFS3 Mount point: /raid0/data/_NAS_NFS_Exports_/pm2
NFS4 Mount point: /pm2

Host Name	Privilege	OS Support	ID Mapping	Sync / Async



Host Name: xxx.xxx.xxx.xxx

All host please set `*`, other host `xxx.xxx.xxx.xxx`, host range `xxx.xxx.xxx.xxx/xx`

Privilege: ○ Read Only ● Writable

OS Support: ● Unix / Linux ○ AIX

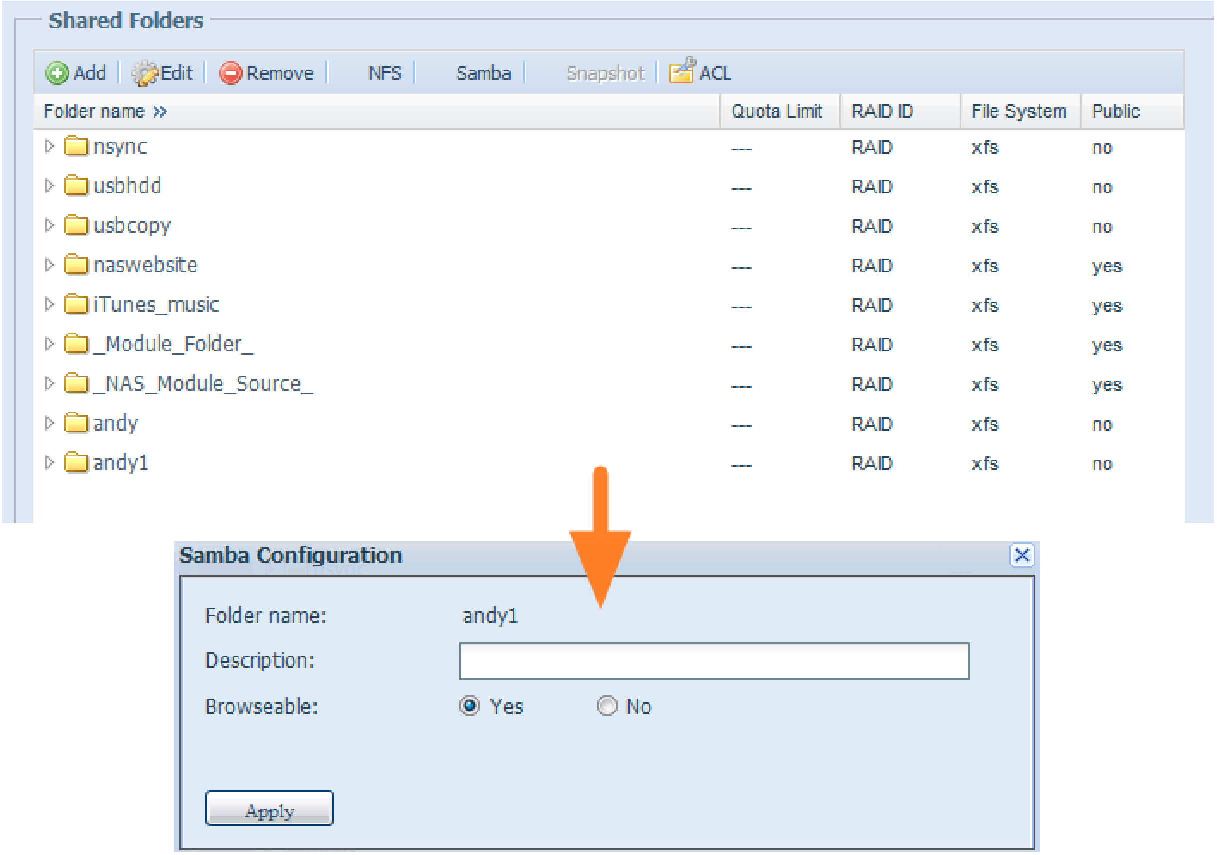
ID Mapping: ● Guest system root account will have full access to this share (root:root). ○ Guest system root account will be mapped to anonymous user (nobody:nogroup) on NAS.

Sync / Async: ● Sync ○ Async

NFS Share	
Item	**Description**
Hostname	Enter the name or IP address of the host
Privilege	Host has either read only or writeable access to the folder.
OS Support	There are two selections available: • Unix / Linux System • AIX (Allow source port > 1024) Choose the one which best fits your needs.
ID Mapping	There are three selections available: • Guest system root account will have full access to this share (root:root). • Guest system root account will be mapped to anonymous user (nobody:nogroup) on NAS. • All user on guest system will be mapped to anonymous user (nobody:nogroup) on NAS. Choose the one which best fits your needs.
Sync / Async	Choose to determine the data "Sync" at once or "Async" in arranged batch.
Apply	Click to save your changes.

- ## Samba Configuration

On the Folder screen, press the Samba button and the Samba Configuration screen appears. This screen allows you to setup samba configuration for associated folder. After entering the information, press Apply to activate input settings.



Folder name	Quota Limit	RAID ID	File System	Public
nsync	---	RAID	xfs	no
usbhdd	---	RAID	xfs	no
usbcopy	---	RAID	xfs	no
naswebsite	---	RAID	xfs	yes
iTunes_music	---	RAID	xfs	yes
_Module_Folder_	---	RAID	xfs	yes
_NAS_Module_Source_	---	RAID	xfs	yes
andy	---	RAID	xfs	no
andy1	---	RAID	xfs	no

Samba Configuration

Folder name: andy1

Description:

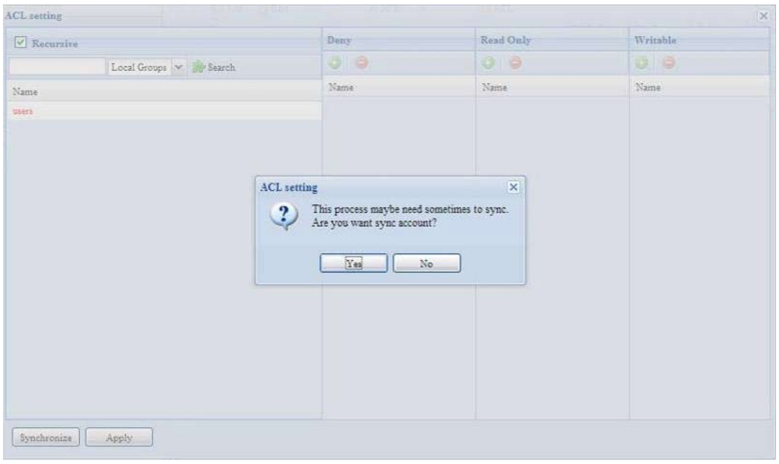
Browseable: ● Yes ○ No

Samba Configuration

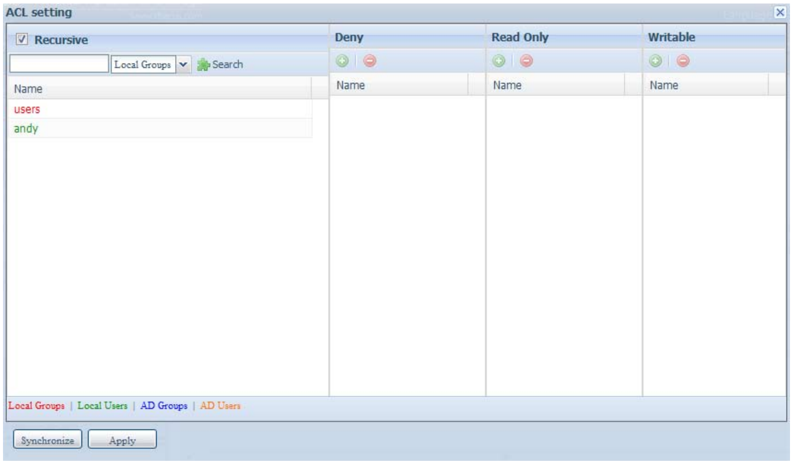
Item	Description
RAID ID	RAID volume where the new folder will reside.
Folder Name	Enter the name of the folder.
Public	Admit or deny public access to this folder.
Apply	Press ***Apply*** to create the folder.

- ## Folder and sub-folders Access Control List (ACL)

On the Folder screen, press the ACL button, and the ACL setting screen appears. This screen allows you to configure access to the specific folder and sub-folders for users and groups. Select a user or a group from the left hand column and then choose Deny, Read Only, or Writable to configure their access level. Press the Apply button to confirm your settings.



This process maybe need sometimes to sync.
Are you want sync account?



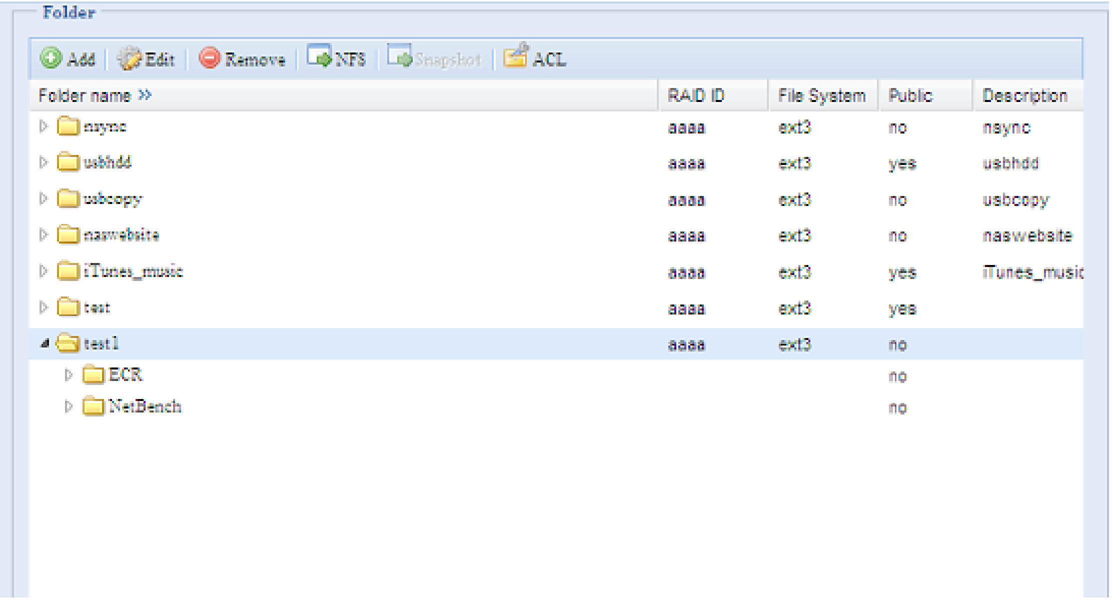
ACL setting	
Item	**Description**
Deny	Denies access to users or groups who are displayed in this column.
Read Only	Provides Read Only access to users or groups who are displayed in this column.
Writable	Provides Write access to users or groups who are displayed in this column.
Recursive	Enable to inherit the access right for all its sub-folders.

To configure folder access, follow the steps below:

1. On the ACL screen, all network groups and users are listed in the left hand column. Select a group or user from this list.
2. With the group or user selected, press one of the buttons from the three access level columns at the top. The group or user then appears in that column and has that level of access to the folder.
3. Continue selecting groups and users and assigning them access levels using the column buttons.
4. To remove a group or user from an access level column, press the Remove button in that column.
5. When you are finished, press Apply to confirm your ACL settings

If one user has belonged to more than one group with different privilege, then the priority of the privilege will be as followed:
Writable > Read Only > Deny

To setup sub-folders ACL, click on " ▹ " symbol to extract sub folders list as screen shot shows below. You may carry on with same steps as share level ACL setting.

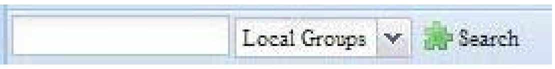


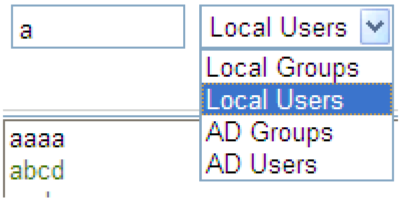
Folder name	RAID ID	File System	Public	Description
nsync	aaaa	ext3	no	nsync
usbhdd	aaaa	ext3	yes	usbhdd
usbcopy	aaaa	ext3	no	usbcopy
naswebsite	aaaa	ext3	no	naswebsite
iTunes_music	aaaa	ext3	yes	iTunes_music
test	aaaa	ext3	yes	
test1	aaaa	ext3	no	
ECR			no	
NetBench			no	

The ACL can only be set for share and sub-folders level, not for files.

The ACL screen also allows you to search for a particular user. To do this, follow the steps below:

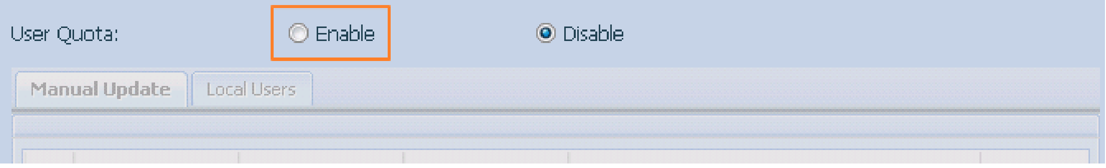
1. In the blank, enter the name of the user you would like to find.
2. From the drop down select the group you would like to search for the user in.
3. Click Search.



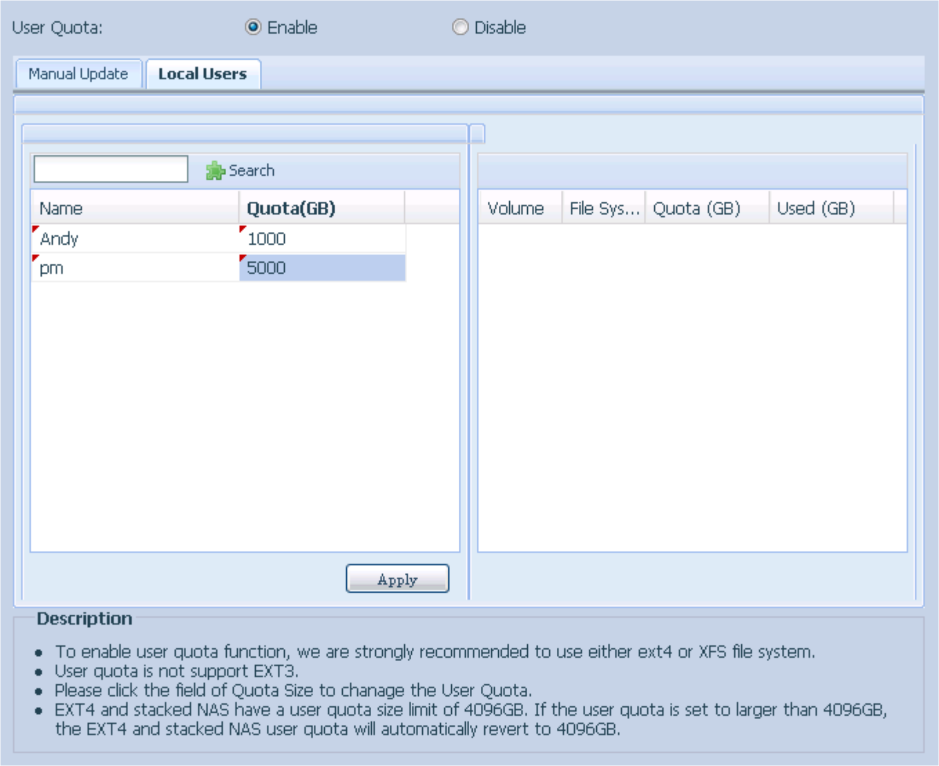


3.5.6 User Quota

The Thecus IP storage support local or AD users with storage quota limitations in each RAID volume of the system. To enable this function, simply click "Enable", then apply.


User Quota: ○ Enable ● Disable

Next, each user can be setup a global storage quota size for each RAID volume. Simply click on "Quota Size" for each user and input the desired capacity. After the setup is complete, please click on "Apply" to activate the user quota size.



User Quota: ● Enable ○ Disable

Name	Quota(GB)
Andy	1000
pm	5000

Volume	File Sys...	Quota (GB)	Used (GB)

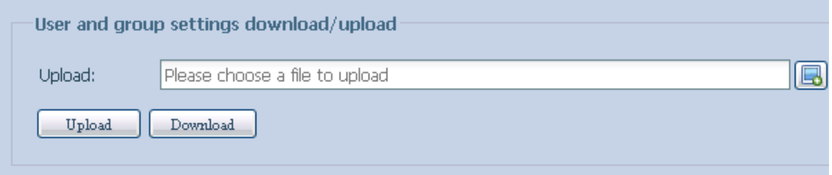
Description

- To enable user quota function, we are strongly recommended to use either ext4 or XFS file system.
- User quota is not support EXT3.
- Please click the field of Quota Size to chanage the User Quota.
- EXT4 and stacked NAS have a user quota size limit of 4096GB. If the user quota is set to larger than 4096GB, the EXT4 and stacked NAS user quota will automatically revert to 4096GB.

3.5.7 User and Group Backup

The user and group backup feature allow system users and groups to be backed up to another location and be restored if needed.

Please note, when restoring previous backup users and groups, the current users and groups list will be replaced from this restore file's contents.

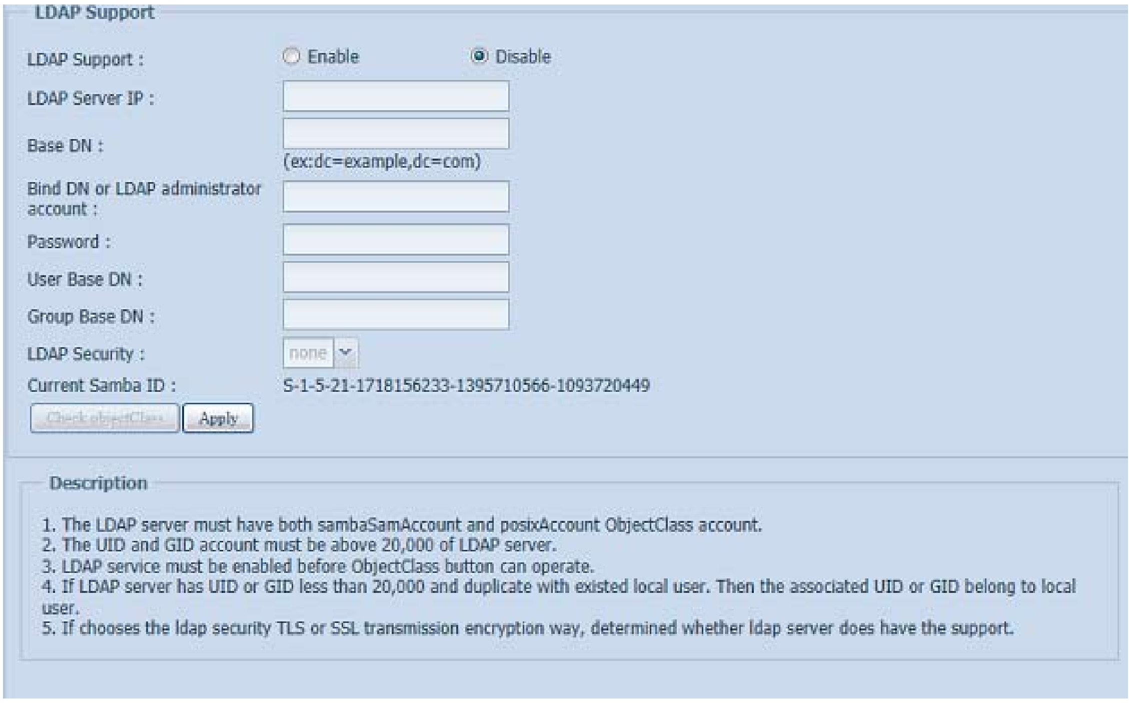


User and group settings download/upload

Upload: Please choose a file to upload

3.5.8 LDAP Support (N4520/N4560 Only)

The LDAP is another way to authenticate login users who have joined the LDAP server. You will need to fill in the LDAP server information to get LDAP authentication started. Please make sure that the LDAP server has a Samba sam and a POSIX ObjectClass account.



LDAP Support

LDAP Support : ○ Enable ● Disable

LDAP Server IP :

Base DN : (ex:dc=example,dc=com)

Bind DN or LDAP administrator account :

Password :

User Base DN :

Group Base DN :

LDAP Security : none

Current Samba ID : S-1-5-21-1718156233-1395710566-1093720449

Description

1. The LDAP server must have both sambaSamAccount and posixAccount ObjectClass account.
2. The UID and GID account must be above 20,000 of LDAP server.
3. LDAP service must be enabled before ObjectClass button can operate.
4. If LDAP server has UID or GID less than 20,000 and duplicate with existed local user. Then the associated UID or GID belong to local user.
5. If chooses the ldap security TLS or SSL transmission encryption way, determined whether ldap server does have the support.

A description of each item follows:

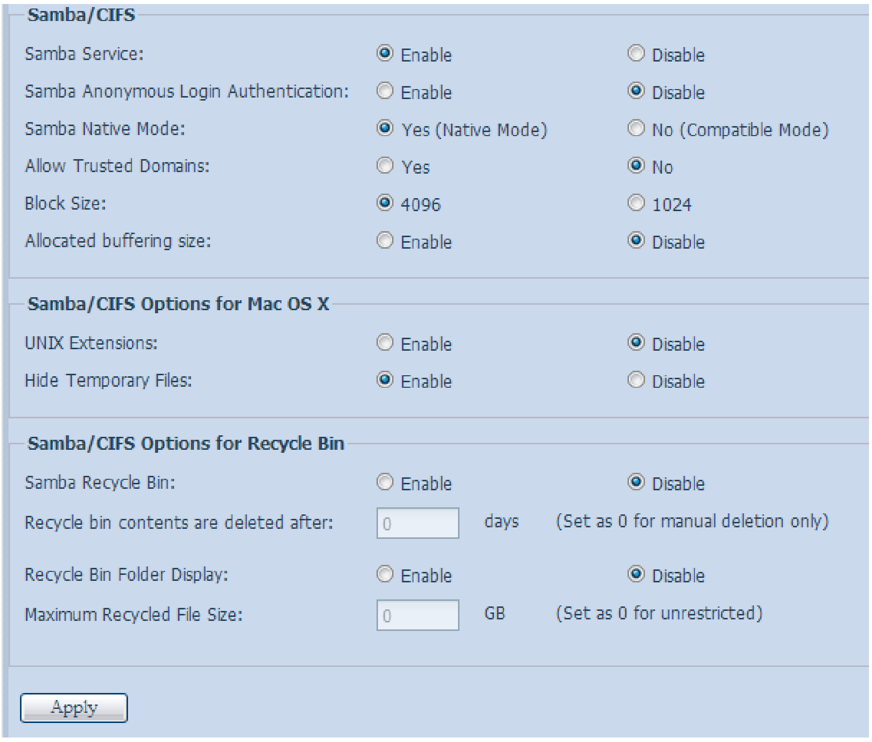
LDAP Support	
Item	**Description**
LDAP Service	Enable or Disable LDAP service.
LDAP Server IP	Input LDAP server IP address.
Base Domain	Input base domain information ex. dc=tuned, dc=com, dc=tw
Bind DN or LDAP Administrator Account	Input Administrator's name.
Password	Input Administrator's password
User Base DN	Input organization unit information where users are stored.
Group Base DN	Input organization unit information where groups are stored.
LDAP Security	Choose the LDAP security type from drop-down list
Current Samba ID	Display the current Samba ID
Check ObjectClass	Click this checkbox to ensure LDAP server has a Samba sam and a POSIX account or it may not work properly for LDAP client authentication.
Apply	Click Apply to save your changes.

3.6 Network Service

Use the Network Service category to make network service support settings.

3.6.1 Samba / CIFS

There are options allow Admin to Enable/Disable to operate Thecus IP storage associated with Samba / CIFS protocol. With the option changed, it will need to reboot system to activate.



Samba/CIFS

Samba Service:	● Enable		○ Disable
Samba Anonymous Login Authentication:	○ Enable		● Disable
Samba Native Mode:	● Yes (Native Mode)		○ No (Compatible Mode)
Allow Trusted Domains:	○ Yes		● No
Block Size:	● 4096		○ 1024
Allocated buffering size:	○ Enable		● Disable

Samba/CIFS Options for Mac OS X

UNIX Extensions:	○ Enable	● Disable
Hide Temporary Files:	● Enable	○ Disable

Samba/CIFS Options for Recycle Bin

Samba Recycle Bin:	○ Enable		● Disable
Recycle bin contents are deleted after:	0	days	(Set as 0 for manual deletion only)
Recycle Bin Folder Display:	○ Enable		● Disable
Maximum Recycled File Size:	0	GB	(Set as 0 for unrestricted)

- **Samba Service**

Used for letting the operating system of UNIX series and SMB/CIFS of Microsoft Windows operating system (Server Message Block / Common Internet File System).Do the link in network protocol. Enable or Disable SMB/CIFS protocol for Windows, Apple, Unix drive mapping

. In some environments, due to security concerns, you may wish to disable SMB/CIFS as a precaution against computer viruses.

- **Samba Anonymous Login Authentication**

To enable this option, no matter there is share folder has been created in public access. The user account and password is needed from system to access under SMB/CIFS protocol. On the other hand, no more anonymous login is allowed.

- **Samba is Native mode**

The Thecus IP storage is supported Samba mode options. In the ADS environment with "Native" mode selected then Thecus IP storage is capable to become local master position.

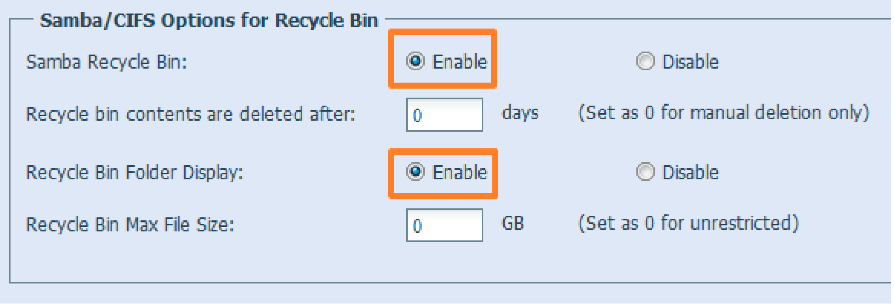
- **UNIX Extension**

The default is enable for Samba usage, with situation using Mac OSX with smb connection may have permission issue. When it happened, please setup "UNIX Extension" disable to get issue solved.

- **Samba Recycle Bin**

The Thecus IP storage is supported recycle bin via SMB/CIFS protocol.

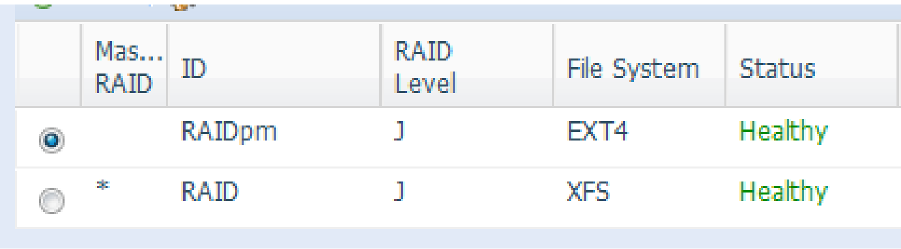
Simply enable the "Recycle Bin" function and "Recycle Folder Display" then all of deleted files/folders will reside in the "_NAS_Recycle_(Associated RDID Volume)" share folder.



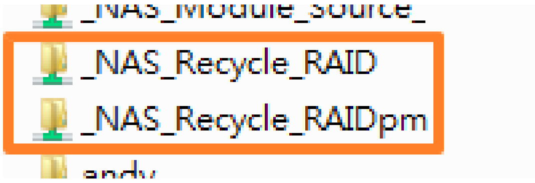
Samba/CIFS Options for Recycle Bin

Samba Recycle Bin:	● Enable	○ Disable	
Recycle bin contents are deleted after:	0	days	(Set as 0 for manual deletion only)
Recycle Bin Folder Display:	● Enable	○ Disable	
Recycle Bin Max File Size:	0	GB	(Set as 0 for unrestricted)

For example, the system has created 2 RAID volumes with ID "RAIDpm" and 'RAID'. Then it will have 2 recycle bin folder appear as "_NAS_Recycle_RAID" and "_NAS_Recycle_RAIDpm".



	Mas... RAID	ID	RAID Level	File System	Status
●		RAIDpm	J	EXT4	Healthy
○	*	RAID	J	XFS	Healthy



_NAS_Module_Source_

_NAS_Recycle_RAID

_NAS_Recycle_RAIDpm

andy

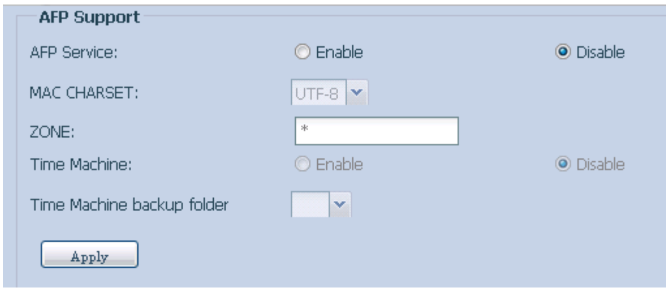
There are 2 more setting could help to manage the recycle bin for deleted folders/files.

1. Setup the "Day" to remove deleted folders/files which has resided in recycle bin permanently. Left default value "0" if desired to clean up recycle bin manually.
2. Setup the "Size" for recycle bin to allow deleted folders/files can store. Left default value "0" with no limitation.

- The deleted files/folders which have resided in recycle bin will keep its permission. On the other hand, only the admin and owner can view/read/write these folders/files.
- If deleted single file size is large than 2GB then it won't reside in the recycle bin but erase permanently.

3.6.2 AFP (Apple Network Setup)

From the Network Service category, choose the AFP item, and the AFP Support screen appears. This screen displays the configuration items for the Apple Filing Protocol. You can change any of these items and press Apply to confirm your settings.



AFP Support

AFP Service: ○ Enable ● Disable

MAC CHARSET: UTF-8

ZONE: *

Time Machine: ○ Enable ● Disable

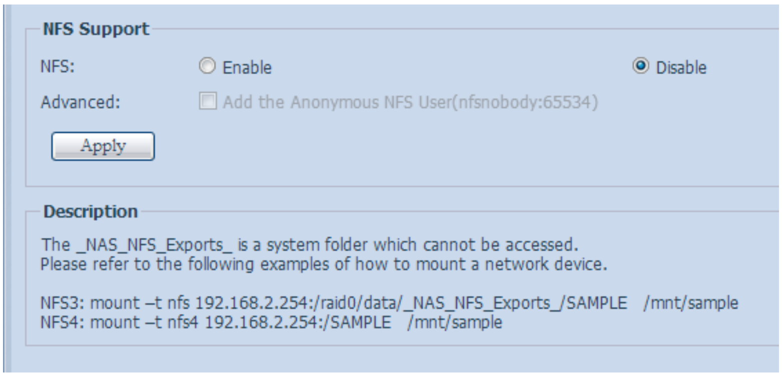
Time Machine backup folder

A description of each item follows:

Apple Network Configuration	
Item	**Description**
AFP Server	Enable or disable Apple File Service to use the Thecus IP storage with MAC OS-based systems.
MAC CHARSET	Specifies the code page from the drop down list.
Zone	Specifies Zone for Applet Talk service. If your AppleTalk network uses extended networks and is assigned with multiple zones, assign a zone name to the Thecus IP storage. If you do not want to assign a network zone, enter an asterisk (*) to use the default setting.
Time Machine	Click the enable checked box if you would like your MAC system to use the Thecus IP storage as MAC time machine backup.
Time Machine backup folder	Select from the drop down list to designate the folder for time machine backup destination.

3.6.3 NFS Setup

From the Network Service category, choose the NFS item, and the NFS Support screen appears. The Thecus IP storage can act as an NFS server, enabling users to download and upload files with their favorite NFS clients. Press Apply to confirm your settings.



NFS Support

NFS: ○ Enable ● Disable

Advanced: □ Add the Anonymous NFS User(nfsnobody:65534)

Description

The _NAS_NFS_Exports_ is a system folder which cannot be accessed.
Please refer to the following examples of how to mount a network device.

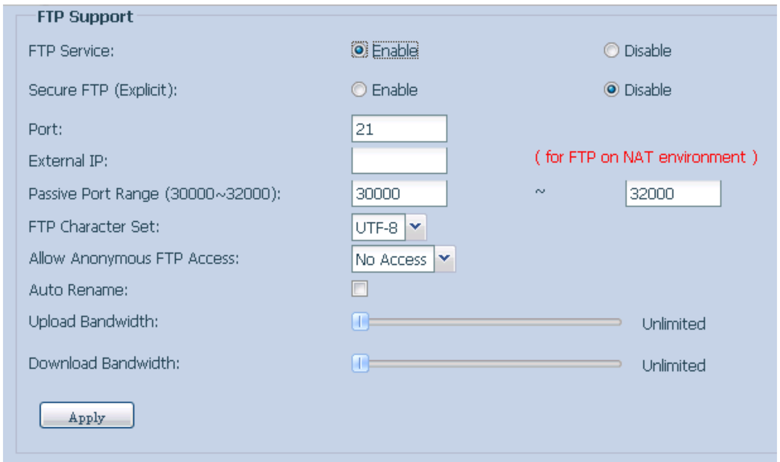
```
NFS3: mount –t nfs 192.168.2.254:/raid0/data/_NAS_NFS_Exports_/SAMPLE   /mnt/sample
NFS4: mount –t nfs4 192.168.2.254:/SAMPLE   /mnt/sample
```

A description of each item follows:

NFS Server Setting	
Item	**Description**
NFS	Enable or Disable NFS support.
Advanced	
Apply	Click ***Apply*** to save your changes.

3.6.4 FTP

The Thecus IP storage can act as an FTP server, enabling users to download and upload files with their favorite FTP programs. From the Network Service category, choose the FTP item, and the FTP screen appears. You can change any of these items and press Apply to confirm your settings.



FTP Support

FTP Service: ● Enable ○ Disable

Secure FTP (Explicit): ○ Enable ● Disable

Port: 21

External IP: (for FTP on NAT environment)

Passive Port Range (30000~32000): 30000 ~ 32000

FTP Character Set: UTF-8

Allow Anonymous FTP Access: No Access

Auto Rename: □

Upload Bandwidth: Unlimited

Download Bandwidth: Unlimited

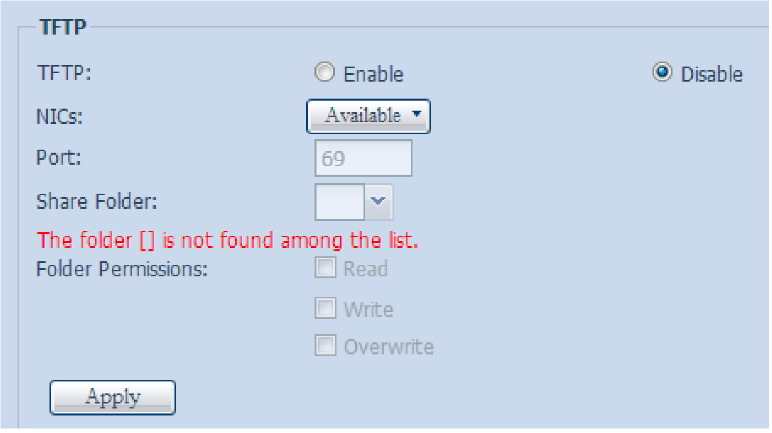
A description of each item follows:

FTP	
Item	**Description**
FTP	Enables FTP Service on the Thecus IP storage.
Security FTP	Enable or disable Security FTP, be sure the client FTP software has also security FTP setting enabled.
Port	Specifies the port number of an incoming connection on a non-standard port.
External IP	Input the public IP address of the router when the Thecus secure FTP server has been enabled. This can help to respond to the ftp client with proper communication information.
Passive Port Range (30000-32000)	Limited port range for the FTP server to use.
FTP ENCODE	If your FTP client or operating system does not support Unicode (e.g. Windows® 95/98/ME or MAC OS9/8), select the same encoding as your OS here in order to properly view the files and directories on the server. Available options are BIG5, HZ, GB2312, GB18030, ISO, EUC-JP, SHIFT-JIS and UTF-8.
Allow Anonymous FTP Access	Upload/Download: Allow anonymous FTP users to upload or download files to/from public folders. Download: Allow anonymous FTP users to download files from public folders. No access: Block anonymous FTP user access.
Auto Rename	If checked, the system will automatically rename files that are uploaded with a duplicate file name. The renaming scheme is [filename].#, where # represents an integer.
Upload Bandwidth	You may set the maximum bandwidth allocated for file uploads. Selections include Unlimited, 1 ~ 32 MB/s.
Download Bandwidth	You may set the maximum bandwidth allocated for file downloads. Selections include Unlimited, 1 ~ 32 MB/s.

To access the share folder on the Thecus IP storage, use the appropriate user login and password set up on the Users page. Access control to each share folder is set up on the ACL page (Storage Management > Share Folder > ACL).

3.6.5 TFTP (N4520/N4560 Only)

Thecus IP storage can act as a TFTP server, enabling users to download and upload files with their favorite TFTP programs. From the Network Service category, choose the TFTP item, and the TFTP screen appears. You can change any of these items and press Apply to confirm your settings.



TFTP

TFTP: ○ Enable ● Disable

NICs: Available

Port: 69

Share Folder:

The folder [] is not found among the list.

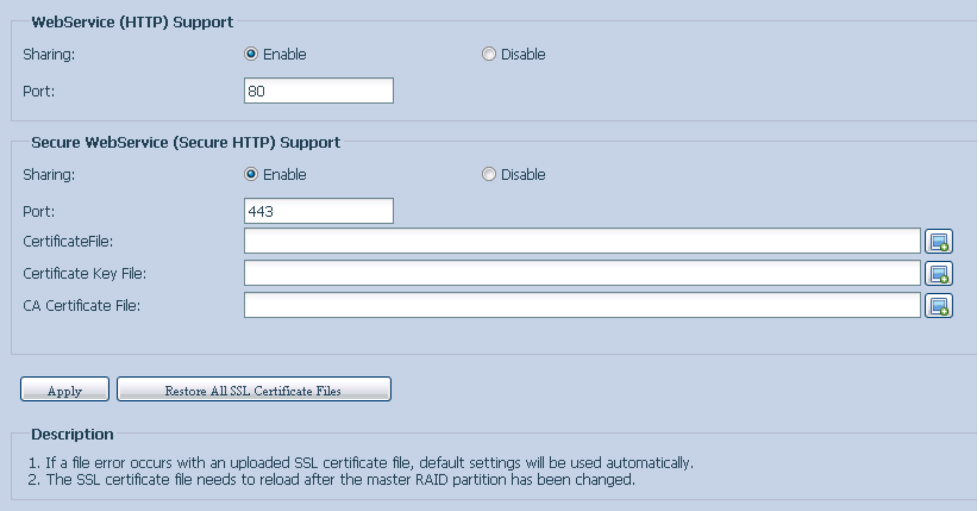
Folder Permissions: □ Read □ Write □ Overwrite

A description of each item follows:

TFTP	
Item	**Description**
TFTP	Enables TFTP Service on the Thecus IP storage.
NICs	Checked WAN/LAN1 or LAN2 to enable port use
Port	Specifies the port number of an incoming connection on a non-standard port.
Share Folder	Select the file stored folder, it cannot be empty.
Folder Permission	Select the folder permission

3.6.6 WebService

From the Network Service category, choose the WebService item, and the WebService Support screen appears. This screen displays the service support parameters of the system. You can change any of these items and press Apply to confirm your settings.



WebService (HTTP) Support

Sharing: ● Enable ○ Disable

Port: 80

Secure WebService (Secure HTTP) Support

Sharing: ● Enable ○ Disable

Port: 443

CertificateFile:

Certificate Key File:

CA Certificate File:

Description

1. If a file error occurs with an uploaded SSL certificate file, default settings will be used automatically.
2. The SSL certificate file needs to reload after the master RAID partition has been changed.

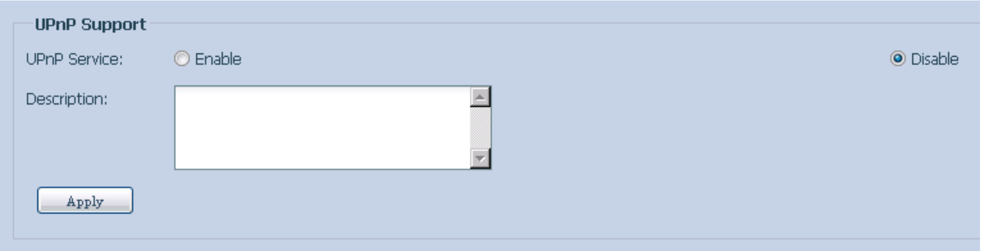
A description of each item follows:

Web Service	
Item	**Description**
HTTP (WebDisk) Support	Enable or disable WebDisk support. Enter the port number if this option is enabled. The port number is default 80.
HTTPs (Secure WebDisk) Support	Enable or disable secure WebDisk support. Enter the port if this option is enabled.
Certificate Type	Select "User" if there is available Certification ID ex. Apply from VeriSign. Or using system default by select "System".
Certificate File	Upload Certificate File if choose Certificate type "User".
Certificate Key File	Upload Certificate Key File if choose Certificate type "User".
CA Certificate File	Upload CA Certificate File if choose Certificate type "User".
Restore All SSL Certificate Files	Click to set back to default certification details.
Apply	Click "Apply" to confirm the changes.

Disable HTTP support and Enable Secure HTTP support to guarantee secure access.

3.6.7 UPnP Service

This device supports UPnP Media server, which allows users to play media files with UPnP client (ex. DMA devices). Enable or disable Universal Plug and Play protocol. UPnP helps to find the IP address of Thecus IP storage.



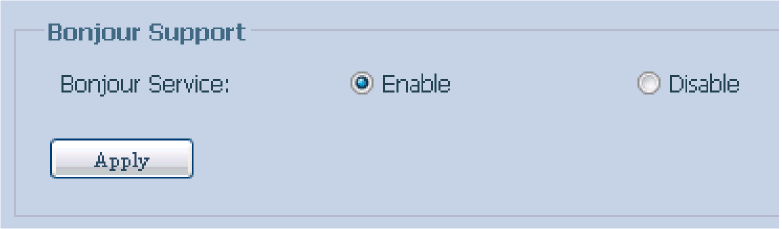
UPnP Support

UPnP Service: ○ Enable ● Disable

Description:

3.6.8 Bonjour Setting

Bonjour, is Apple Inc.'s trade name for its implementation of Zeroconf, a service discovery protocol. Bonjour locates devices such as printers, as well as other computers, and the services that those devices offer on a local network using multicast Domain Name System service records. This definitive guide walks you through Bonjour zero-configuration networking with a complete description of the protocols and technologies used to create Bonjour enabled applications and devices.



Bonjour Support

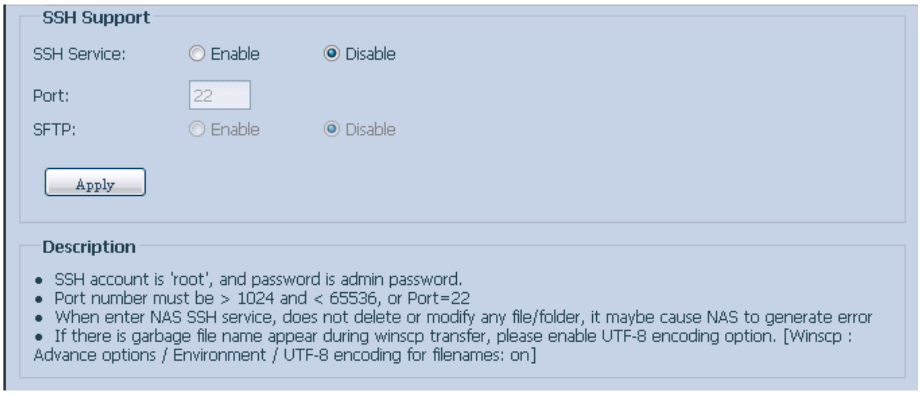
Bonjour Service: ● Enable ○ Disable

3.6.9 SSH

The device is now SSH protocol supported. It allows user to use SSH and have console to manipulate as needed. The SSH default login user name is "root" with full privilege and password is admin's password. The default admin password is "admin" so once the admin password has changed then SSH login need to change the password too.

A description for each item as following:

SSH	
Item	**Description**
SSH Service	Enable or disable SSH service.
Port	The port number is default 22.
SFTP	Enable or disable SFTP protocol under SSH service.
Apply	Click "Apply" to confirm the changes.



SSH Support

SSH Service: ○ Enable ● Disable

Port: 22

SFTP: ○ Enable ● Disable

Description

- SSH account is 'root', and password is admin password.
- Port number must be > 1024 and < 65536, or Port=22
- When enter NAS SSH service, does not delete or modify any file/folder, it maybe cause NAS to generate error
- If there is garbage file name appear during winscp transfer, please enable UTF-8 encoding option. [Winscp : Advance options / Environment / UTF-8 encoding for filenames: on]

3.6.10 DDNS

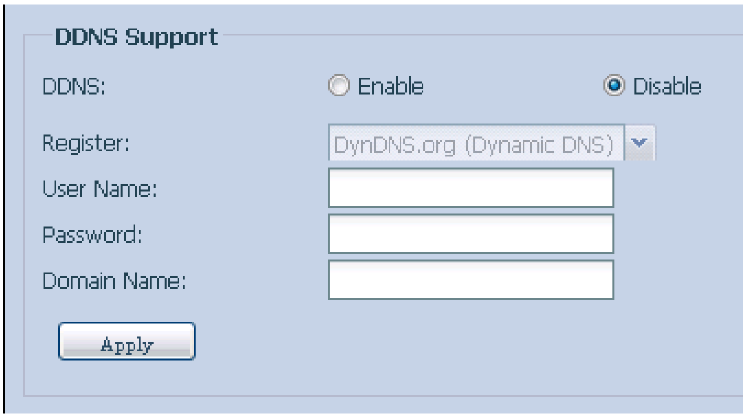
To set up a server on the Internet and enable the users to connect to it easily, a fixed and easy-to remember host name is often required. However, if the ISP provides only dynamic IP address, the IP address of the server will change from time to time and is difficult to recall. You can enable the DDNS service to solve the problem.

After enabling the DDNS service of the NAS, whenever the NAS restarts or the IP address is changed, the NAS will notify the DDNS provider immediately to record the new IP address. When the user tries to connect to the NAS by the host name, the DDNS will transfer the recorded IP address to the user.

The NAS supports the DDNS providers:

DyDNS.org(Dynamic DNS),DyDNS.org(Custom DNS),DyDNS.org(Static DNS),

www.zoneedit.com,www.no-ip.com.



DDNS Support

DDNS: ○ Enable ● Disable

Register: DynDNS.org (Dynamic DNS)

User Name:

Password:

Domain Name:

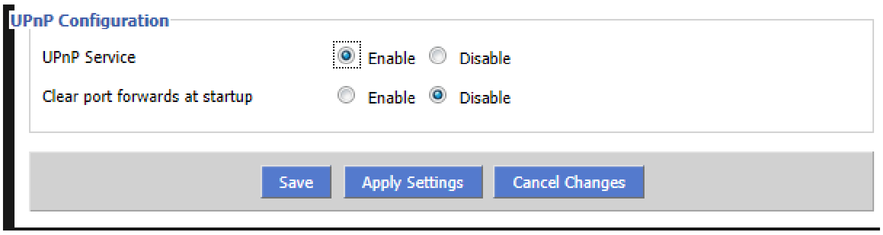
A description for each item as following:

DDNS	
Item	**Description**
DDNS Service	Enable or disable DDNS service.
Register	Choose the service provider from the drop down list.
User name	Input user name with DDNS registry.
Password	Input password with DDNS registry.
Domain name	Input domain name with DDNS registry.
Apply	Click "Apply" to confirm the changes.

3.6.11 UPnP Port Management

One of the most convent way to allow users to access required services such as FTP, SSH, web disk and http etc. from Internet environment is setting UPnP port management.

To set up this UPnP port forwarding feature, please be sure that the router has "UPnP Service" Enabled. The following is an example from one of the router manufacture with UPnP Configuration page.

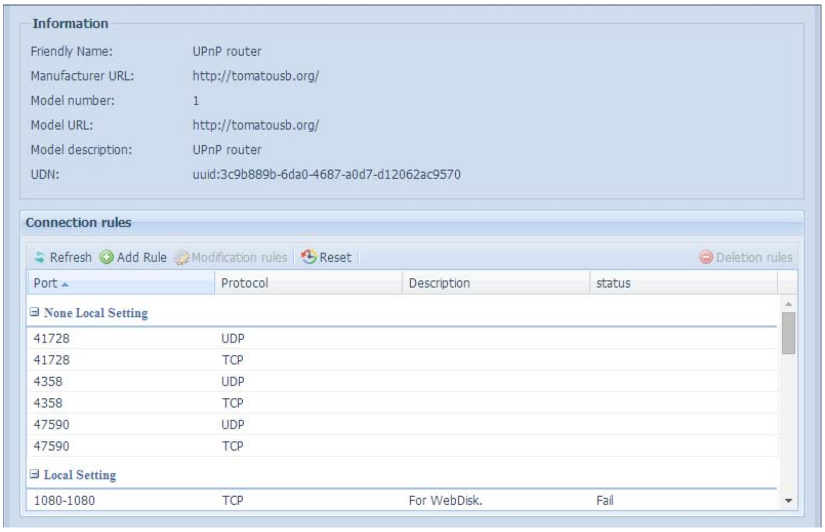


UPnP Configuration

UPnP Service ● Enable ○ Disable

Clear port forwards at startup ○ Enable ● Disable

After the router has enabled "UPnP Service" then you will have information come from associated router to UPnP port management as shown in the screen shot below.



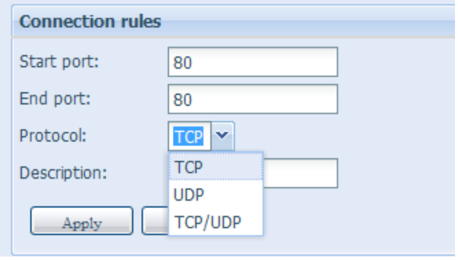
Information

Friendly Name:	UPnP router
Manufacturer URL:	http://tomatousb.org/
Model number:	1
Model URL:	http://tomatousb.org/
Model description:	UPnP router
UDN:	uuid:3c9b889b-6da0-4687-a0d7-d12062ac9570

Connection rules

Port	Protocol	Description	status
⊟ None Local Setting			
41728	UDP		
41728	TCP		
4358	UDP		
4358	TCP		
47590	UDP		
47590	TCP		
⊟ Local Setting			
1080-1080	TCP	For WebDisk.	Fail

And click "Add Rule" to add more port mapping from Internet to access desired services or press "Refresh" to get most updated list.



Connection rules

Start port: 80

End port: 80

Protocol: TCP

Description:

A description for each item as following:

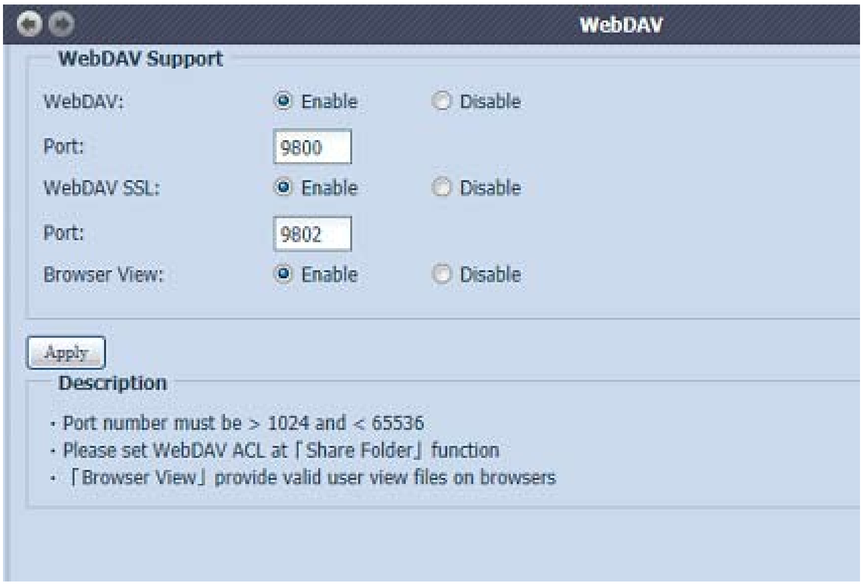
UPnP Port Management	
Item	**Description**
Start port	Specific port number starts with.
End port	Specific port number ended
Protocol	Choose the protocol for port forwarding needed.
Description	Specific the port services if applicable.
Apply	Click "Apply" to confirm the changes.
Cancel	Click "Cancel" to abort the changes

Some of the routers do not allow the input of port number below 1024. So it may have resulted "setting fails".

3.6.12 WebDAV

The WebDAV is an extended protocol of http(s) which allows remote access to your NAS system.

To begin using WebDAV and WebDAV SSL, simply click enable and provide the port number. The default port number is 9800, under normal circumstances this will not need to be changed.



WebDAV Support

WebDAV: ● Enable ○ Disable

Port: 9800

WebDAV SSL: ● Enable ○ Disable

Port: 9802

Browser View: ● Enable ○ Disable

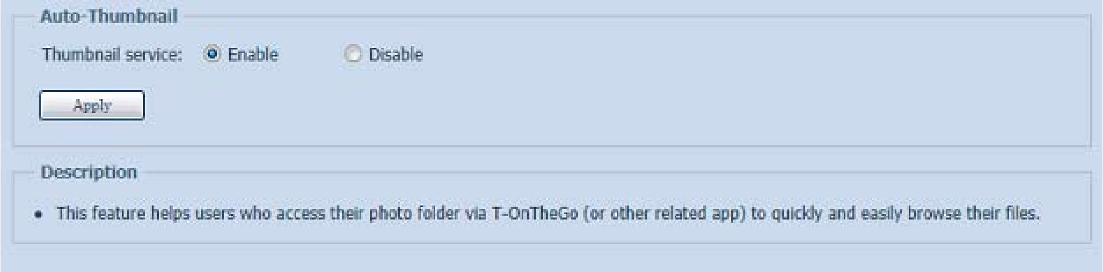
Description

- Port number must be > 1024 and < 65536
- Please set WebDAV ACL at「Share Folder」function
- 「Browser View」provide valid user view files on browsers

WebDAV Configuration	
Item	**Description**
WebDAV Service	Press the ***Enable*** button to activate WebDAV service and specify the port number if it needs to change from the default value. P.S. Port number is limited to greater than 1024 and less than 65536
WebDAV SSL Service	Press the ***Enable*** button to activate WebDAV SSL service and specify the port number if it needs to be changed from the default value. P.S. The ort number is limited to greater than 1024 and less than 65536
Browser View	Press the **Enable** button and viewing the share folder list through the browser will be allowed
Apply	Click ***Apply*** to save your changes.

3.6.13 Auto Thumbnail

The auto thumbnail is a function on the GUI that can be used with the Thecus T-OnTheGo mobile application. It helps to resize a photo while when it is on written the NAS system. Enable this service allows you to speed up photo viewing on your Mobile device.


Auto-Thumbnail

Thumbnail service: ● Enable ○ Disable

Description

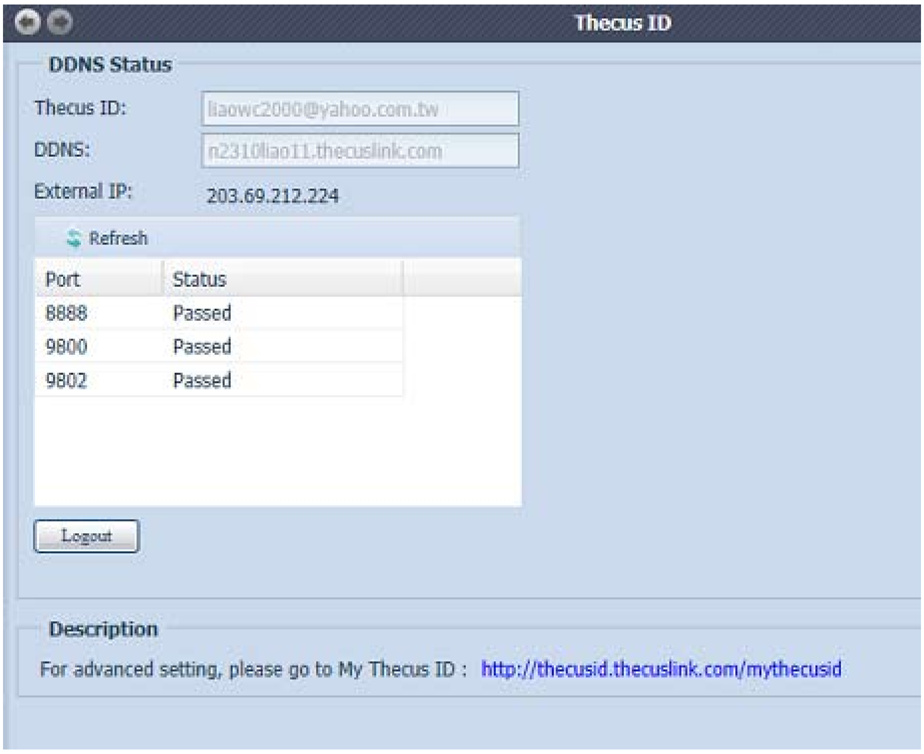
- This feature helps users who access their photo folder via T-OnTheGo (or other related app) to quickly and easily browse their files.

Auto Thumbnail Configuration	
Item	**Description**
Auto Thumbnail Service	Press the ***Enable*** button to activate the auto thumbnail service.
Apply	Click ***Apply*** to save your changes.

3.6.14 ThecusID

Creating a Thecus ID will give you full access to all that Thecus has to offer. After creating a Thecus ID, you'll receive a free* DDNS (i.e"yourname.thecuslink.com".) You can use your DDNS to easily access your NAS, make use of the mobile T-OnTheGo™ app, and share links to files with your friends. In the future, free cloud backup of your NAS configuration file will also be provided.

From here, it will display the current Thecus ID and DDNS information for the associated Thecus NAS system and also the port connection status. You can click logout if remote access is no longer needed.



Thecus ID: liaowc2000@yahoo.com.tw

DDNS: n2310liao11.thecuslink.com

External IP: 203.69.212.224

Port	Status
8888	Passed
9800	Passed
9802	Passed

For advanced setting, please go to My Thecus ID : http://thecusid.thecuslink.com/mythecusid

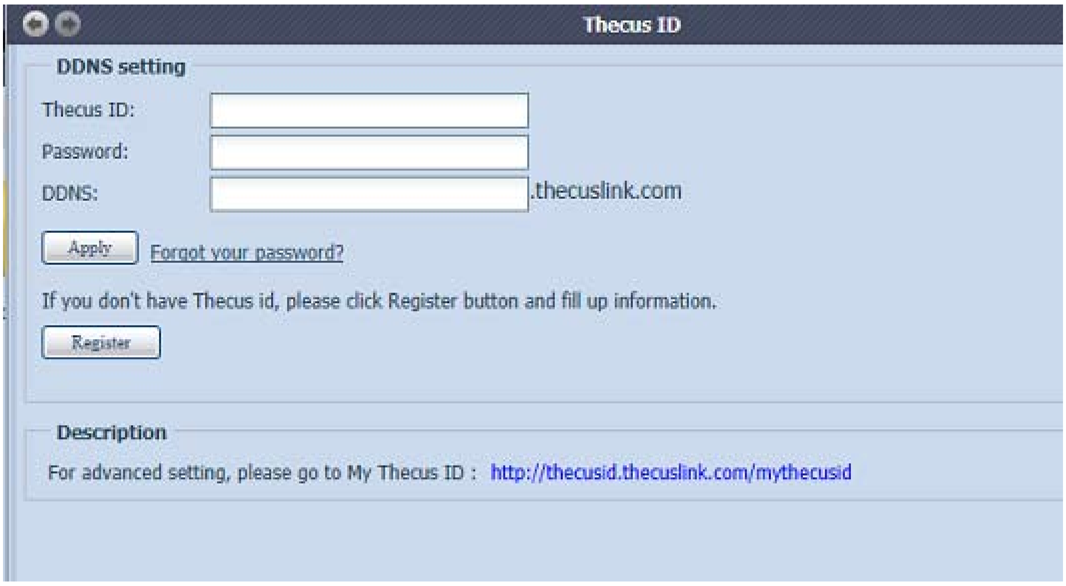
If your Thecus NAS system is not currently logged in, or if DDNS has not yet been applied, then it can be done here.

- **Login Thecus NAS system:**

Simply input your existing Thecus ID and DDNS for this Thecus NAS then press apply.

- **Create free DDNS for your Thecus NAS:**

With registered Thecus ID, you could create DDNS for your Thecus NAS by fill in valid Thecus ID and password. Then input desired DDNS name to complete DDNS creation.



Thecus ID

DDNS setting

Thecus ID:

Password:

DDNS: .thecuslink.com

Apply Forgot your password?

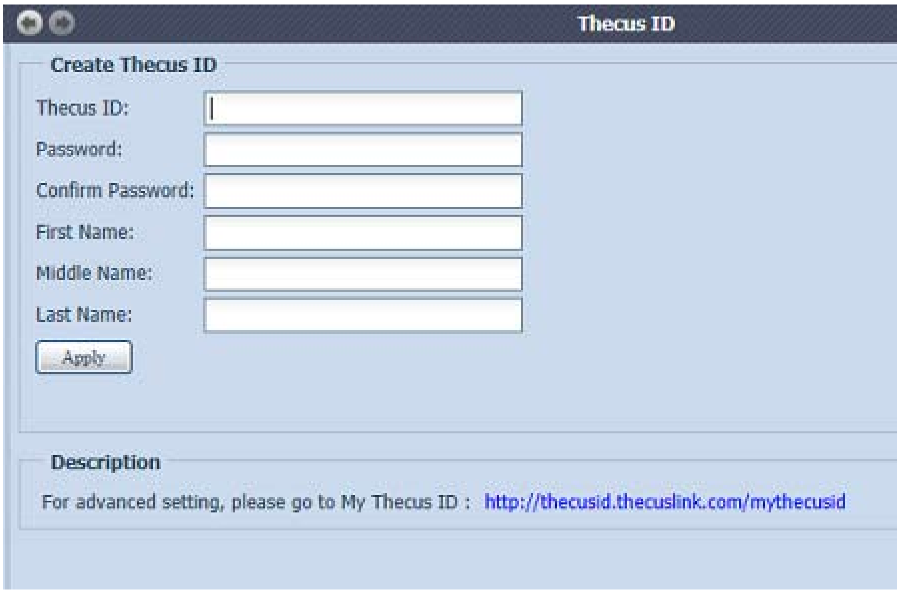
If you don't have Thecus id, please click Register button and fill up information.

Register

Description

For advanced setting, please go to My Thecus ID : http://thecusid.thecuslink.com/mythecusid

If you don't have a Thecus ID, click "Register" and the screen below will appear. Please fill in the required information and click Apply.



Thecus ID

Create Thecus ID

Thecus ID:

Password:

Confirm Password:

First Name:

Middle Name:

Last Name:

Apply

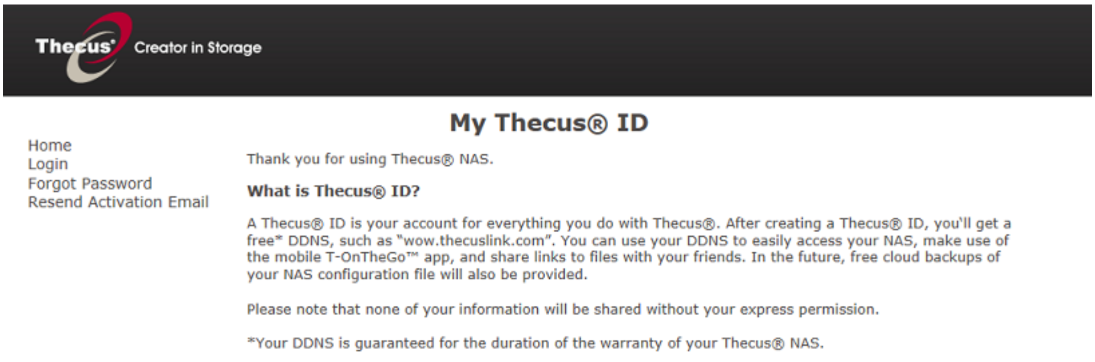
Description

For advanced setting, please go to My Thecus ID : http://thecusid.thecuslink.com/mythecusid

Register Thecus ID	
Item	**Description**
Thecus ID	Input a valid email address. It will require confirmation to activate your Thecus ID.
Password	Input the password for your Thecus ID
Confirm Password	Re-input the password for your Thecus ID.
First Name	Input your First name
Middle Name	Input your Middle name
Last Name	Input your Last name
Apply	Click ***Apply*** to save your changes.

Once your ThecusID has been registered, you will be given access to a webpage providing more information (i.e. connection test, re-send password, etc.).

http://thecusid.thecuslink.com/mythecusid/index.php



My Thecus® ID

Thank you for using Thecus® NAS.

What is Thecus® ID?

A Thecus® ID is your account for everything you do with Thecus®. After creating a Thecus® ID, you'll get a free* DDNS, such as "wow.thecuslink.com". You can use your DDNS to easily access your NAS, make use of the mobile T-OnTheGo™ app, and share links to files with your friends. In the future, free cloud backups of your NAS configuration file will also be provided.

Please note that none of your information will be shared without your express permission.

*Your DDNS is guaranteed for the duration of the warranty of your Thecus® NAS.

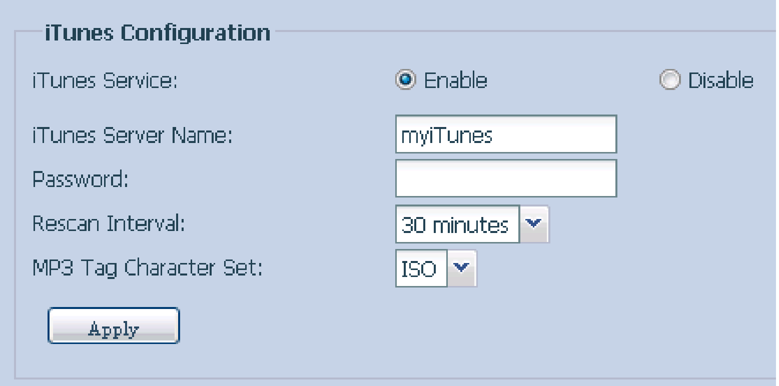
3.7 Application Server

The Thecus IP storage supports built-in application such as iTunes server as well as add-on official or third -party applications.

3.7.1 iTunes® Server (Built in)

With the built-in iTunes server capability, Thecus IP storage enables digital music to be shared and played anywhere on the network!

From the Application Server category, choose the iTunes item, and then the iTunes Configuration screen appears. You may enable or disable the iTunes Service from here. Once enabled, enter the proper information for each field and press Apply to save your changes.



iTunes Configuration

iTunes Service: ● Enable ○ Disable

iTunes Server Name: myiTunes

Password:

Rescan Interval: 30 minutes

MP3 Tag Character Set: ISO

See the following table for a detailed description of each field:

iTunes Configuration	
Item	**Description**
iTunes Service	Enable or disable the iTunes Service.
iTunes Server Name	Name used to identify Thecus IP storage to iTunes clients.
Password	Enter a password to control access to your iTunes music.
Rescan Interval	Rescan interval in seconds.
MP3 Tag Encode	Specify tag encoding for MP3 files stored in Thecus IP storage. All ID3 tags will be sent out in UTF-8 format.

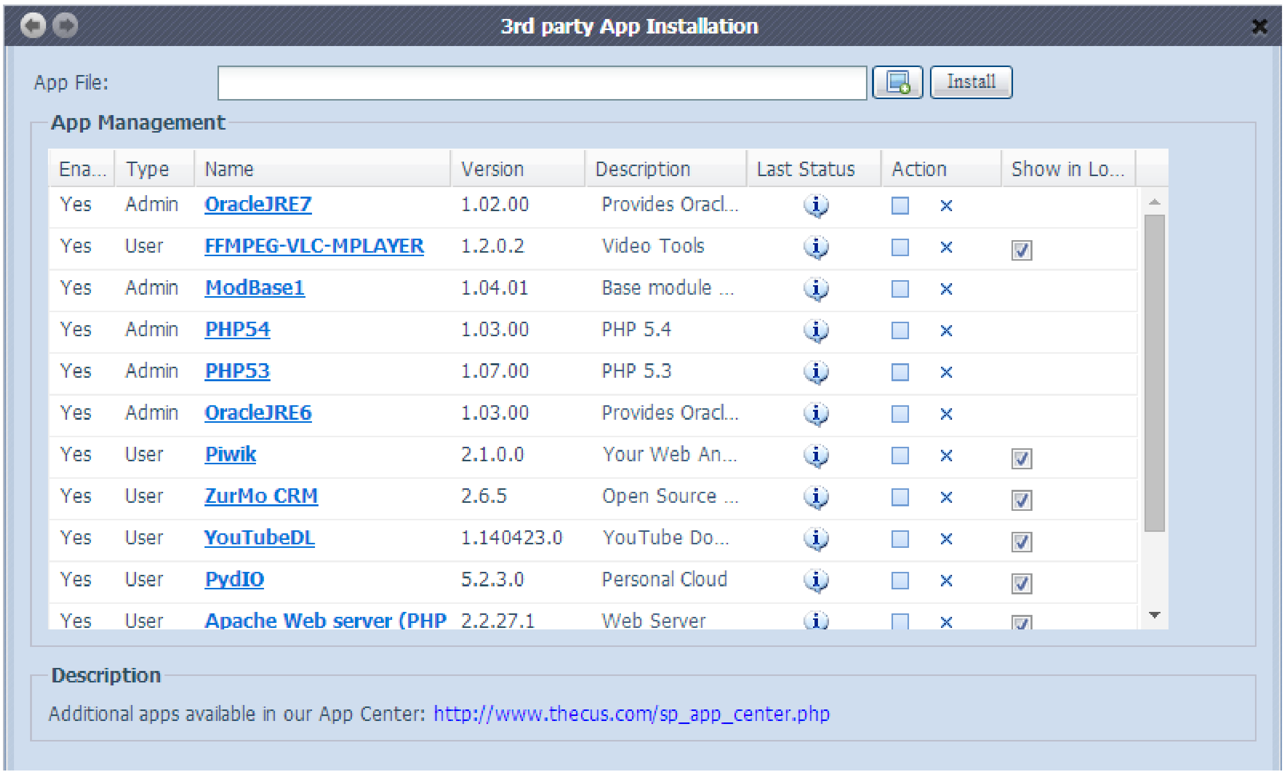
Once the iTunes service is enabled, Thecus IP storage will make all music located in the Music folder available for iTunes-equipped computers on the network.

3.7.2 Add-on Official Applications

There are several default pre-loaded official applications such as WebDisk, Piczza (Photo server) and Transmission-Kit (BT download manager) that can be found from the Application Server category.

3.7.3 3rd party App Installation

From the Application Server Category, choose the Module Installation item and the Module Management screen appears. Here is the entry for all of third party user module could install from.



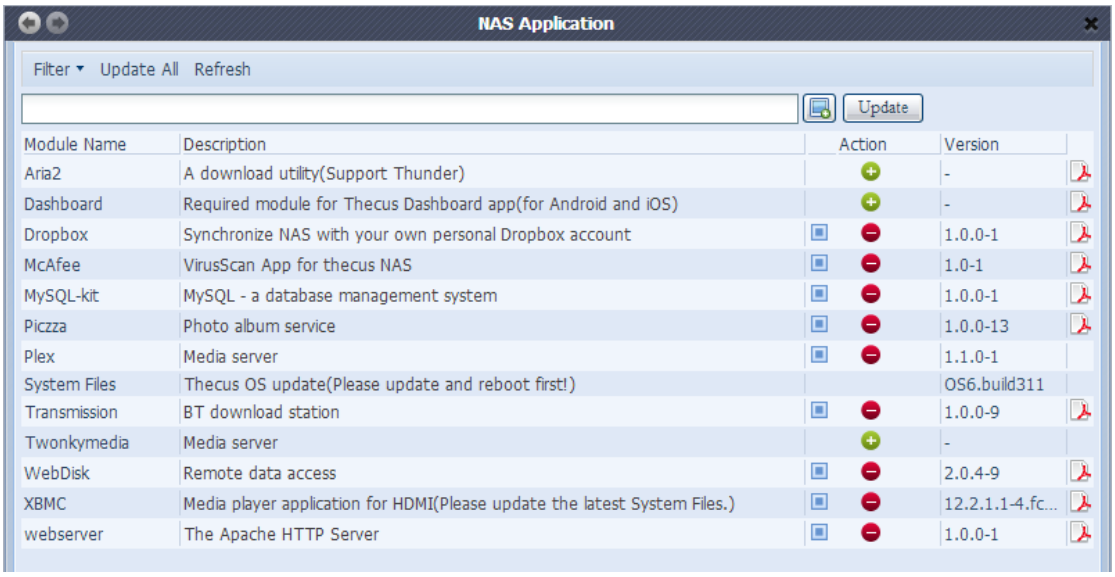
Ena...	Type	Name	Version	Description	Last Status	Action		Show in Lo...
Yes	Admin	OracleJRE7	1.02.00	Provides Oracl...	ⓘ	□	×	
Yes	User	FFMPEG-VLC-MPLAYER	1.2.0.2	Video Tools	ⓘ	□	×	☑
Yes	Admin	ModBase1	1.04.01	Base module ...	ⓘ	□	×	
Yes	Admin	PHP54	1.03.00	PHP 5.4	ⓘ	□	×	
Yes	Admin	PHP53	1.07.00	PHP 5.3	ⓘ	□	×	
Yes	Admin	OracleJRE6	1.03.00	Provides Oracl...	ⓘ	□	×	
Yes	User	Piwik	2.1.0.0	Your Web An...	ⓘ	□	×	☑
Yes	User	ZurMo CRM	2.6.5	Open Source ...	ⓘ	□	×	☑
Yes	User	YouTubeDL	1.140423.0	YouTube Do...	ⓘ	□	×	☑
Yes	User	PydIO	5.2.3.0	Personal Cloud	ⓘ	□	×	☑
Yes	User	Apache Web server (PHP	2.2.27.1	Web Server	ⓘ	□	×	☑

Description

Additional apps available in our App Center: http://www.thecus.com/sp_app_center.php

3.7.4 NAS Application

Click on NAS Application from the Application Server category, it will list the current system software and official application status.



Module Name	Description	Action		Version	
Aria2	A download utility(Support Thunder)		⊕	-	📄
Dashboard	Required module for Thecus Dashboard app(for Android and iOS)		⊕	-	📄
Dropbox	Synchronize NAS with your own personal Dropbox account	▣	⊖	1.0.0-1	📄
McAfee	VirusScan App for thecus NAS	▣	⊖	1.0-1	📄
MySQL-kit	MySQL - a database management system	▣	⊖	1.0.0-1	📄
Piczza	Photo album service	▣	⊖	1.0.0-13	📄
Plex	Media server	▣	⊖	1.1.0-1	
System Files	Thecus OS update(Please update and reboot first!)			OS6.build311	
Transmission	BT download station	▣	⊖	1.0.0-9	📄
Twonkymedia	Media server		⊕	-	
WebDisk	Remote data access	▣	⊖	2.0.4-9	📄
XBMC	Media player application for HDMI(Please update the latest System Files.)	▣	⊖	12.2.1.1-4.fc...	📄
webserver	The Apache HTTP Server	▣	⊖	1.0.0-1	📄

3.8 Backup

There are a number of ways to back up data with the Thecus IP storage.

3.8.1 Rsync Target Server

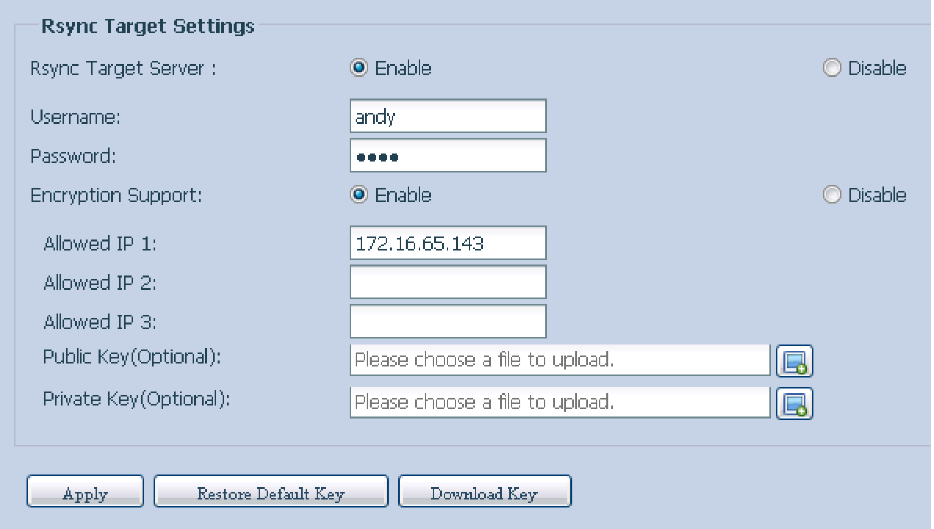
When it comes to backing up your data, it's very important to have flexibility. Data guard provides you with many options, including full backup for all shares, custom backup for selected shares and iSCSI volume backup. Being based on the Linux operating system, it is also much more stable and experiences much less frequent data loss during transfer than other remote backup systems.

-For this tutorial you will need to use Rsync Target Server (Step 1) and Data Guard (Step 2+3) under Backup for this client/server backup feature. It also can be named for function "Remote Replication".

Step 1 – Enabling Rsync on your target (backup) NAS

-Log in to your target (backup) NAS through the UI in your web browser

-Go to Rsync Target Server under Backup in the menu of the UI



Rsync Target Settings

Rsync Target Server :	● Enable	○ Disable
Username:	andy	
Password:	••••	
Encryption Support:	● Enable	○ Disable
Allowed IP 1:	172.16.65.143	
Allowed IP 2:		
Allowed IP 3:		
Public Key(Optional):	Please choose a file to upload.	
Private Key(Optional):	Please choose a file to upload.	

1. Enable Rsync Target Server
2. Add a username and password (they can be different than your NAS's username and password)
3. Select Apply

> You will need this user name and password while the data is going to remotely backup to this Rsync target server.

Now Rsync is turned on your NAS, which means it can be used as a target for Rsync backup, in other words, only the backup NAS needs to be activated in this way.

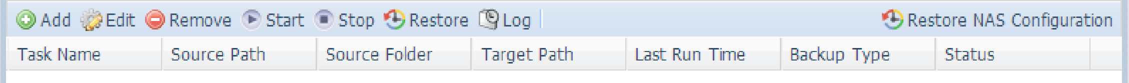
3.8.2 Data Guard (Remote Backup)

Step 2 – Setting up your backup task and schedule on your source NAS

-Log in to your other NAS (your source NAS) through the UI in your web browser

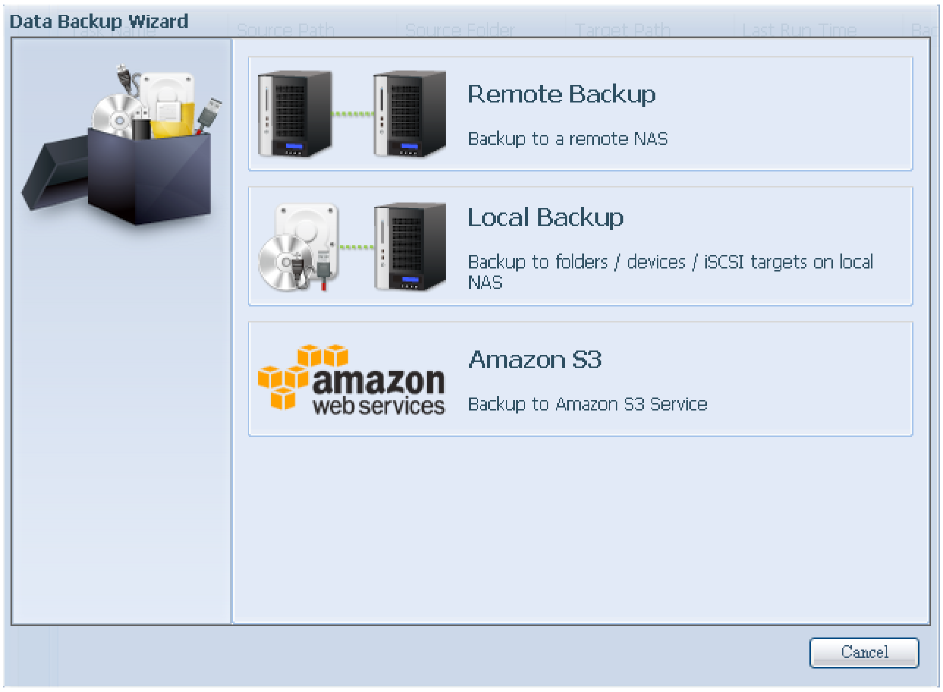
-Go to Data Guard under Backup in the System Management category of the UI

-From the Data Guard function list, choose Add

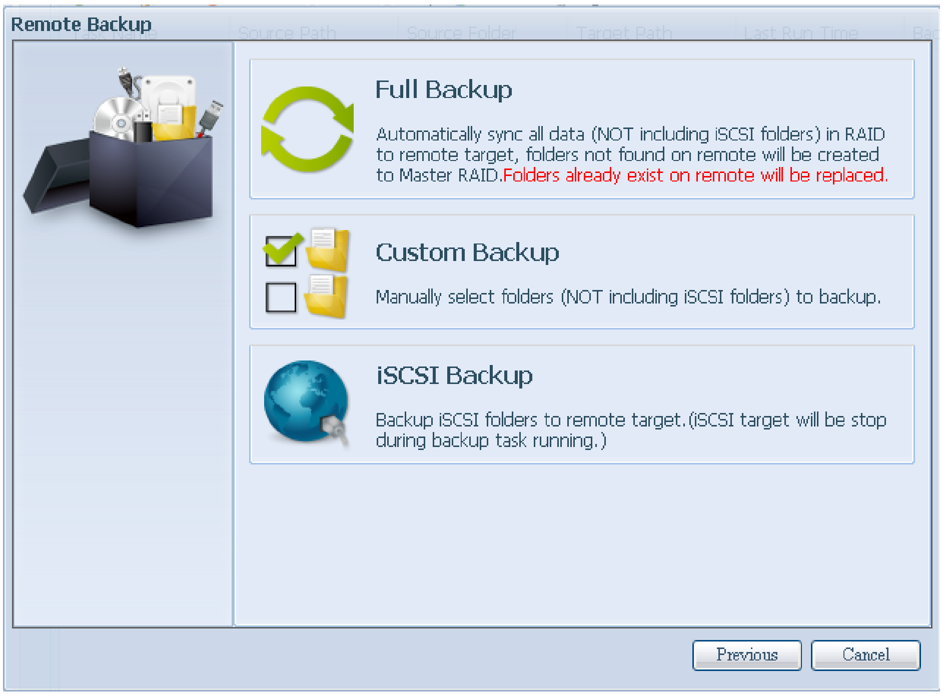


Remote Data backup	
Item	**Description**
Add	Add new task.
Edit	Edit select task.
Remove	Remove select task
Start	If associated task has been setup in schedule and like to start at once, click on to start task right away.
Stop	Stop the associated running task. The other scenario is if a task has been setup in real-time then clicking “Stop” can terminate the running process. Simple click ‘Start” to re-start the real-time operation.
Restore	Restore the associated task
Log	Click to view the associated task in process details.
Restore NAS Configuration	Click to restore system configuration from selected destination to source unit. More details will describe in sections.

The data backup setup wizard appears as below, click on ‘Remote Backup”:



Then 3 different selections appear and can be chosen from:



Remote Backup

Full Backup

Automatically sync all data (NOT including iSCSI folders) in RAID to remote target, folders not found on remote will be created to Master RAID.Folders already exist on remote will be replaced.

Custom Backup

Manually select folders (NOT including iSCSI folders) to backup.

iSCSI Backup

Backup iSCSI folders to remote target.(iSCSI target will be stop during backup task running.)

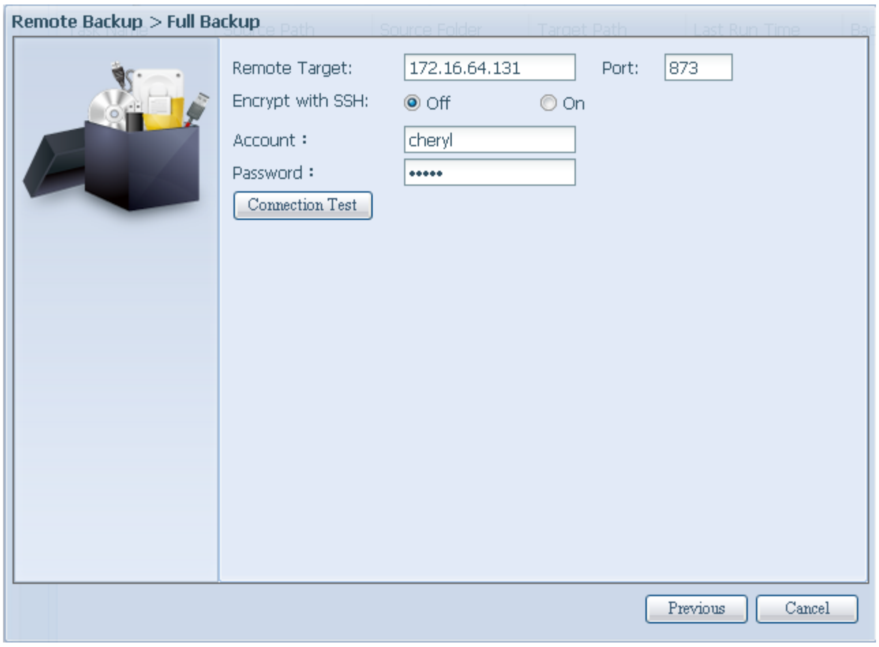
Remote Data backup	
Item	**Description**
Full Backup	The “Full backup” will have all shares from source backup to destination. It could also create shares automatically from destination if it is not existent. This only applies if the target server is the same model as the source.
Custom Backup	The “Custom backup” allows user to choose desired shares backup to destination.
iSCSI Backup	The “iSCSI backup” can backup iSCSI volume as single file to destination.

- **Full Backup**

Click on full backup and the setup screen appear as below. Fill in the remote target IP (Destination) and port (need to be changed only if this port is already in use).

If encryption is required then enable it. Please make sure the associated target server also has encryption enabled.

Carry on with inputting valid remote target server account name and password.



Remote Backup > Full Backup

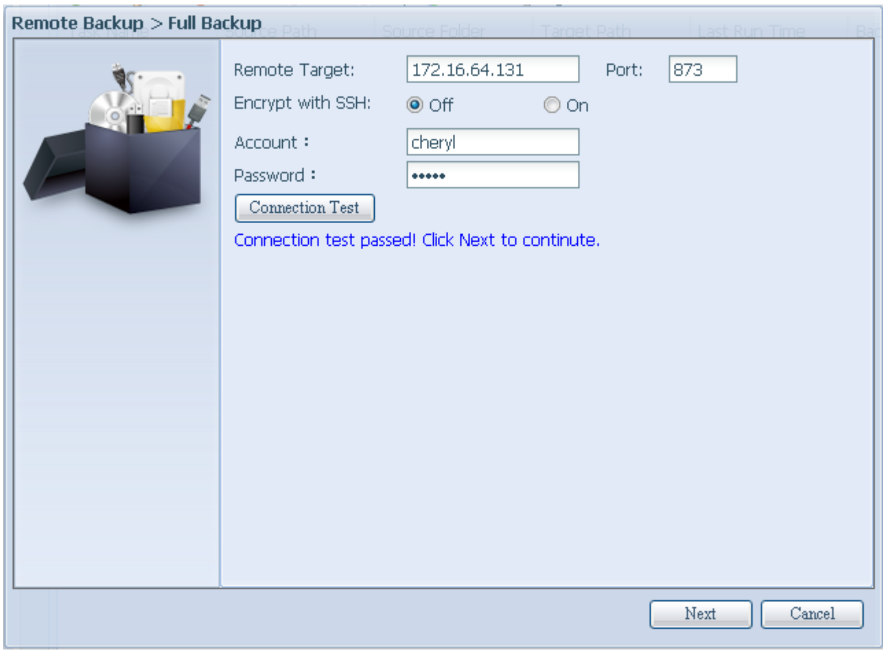
Remote Target: 172.16.64.131 Port: 873

Encrypt with SSH: ● Off ○ On

Account : cheryl

Password : •••••

After the settings are complete, please click on "Connection Test". The source unit will try to connect with the associated target system. If a connection can be built up successfully then "Connection passed" will be prompted, otherwise "Failed" will appear.



Remote Backup > Full Backup

Remote Target: 172.16.64.131 Port: 873

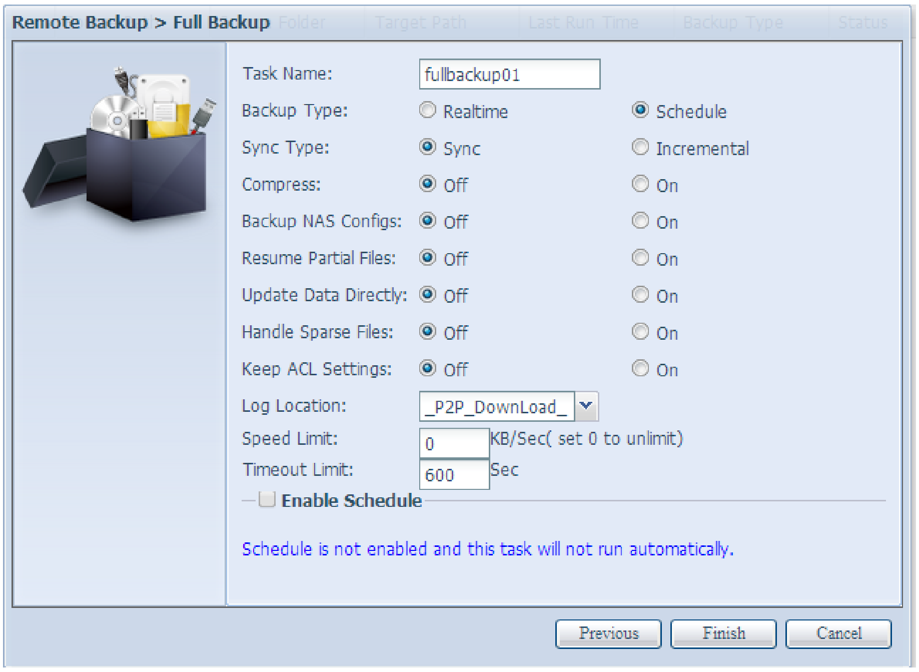
Encrypt with SSH: ● Off ○ On

Account : cheryl

Password : •••••

Connection test passed! Click Next to contitute.

Click "Next" and more setting will appear.



Remote Backup > Full Backup

Task Name:	fullbackup01	
Backup Type:	○ Realtime	● Schedule
Sync Type:	● Sync	○ Incremental
Compress:	● Off	○ On
Backup NAS Configs:	● Off	○ On
Resume Partial Files:	● Off	○ On
Update Data Directly:	● Off	○ On
Handle Sparse Files:	● Off	○ On
Keep ACL Settings:	● Off	○ On
Log Location:	_P2P_DownLoad_	
Speed Limit:	0 KB/Sec(set 0 to unlimit)	
Timeout Limit:	600 Sec	

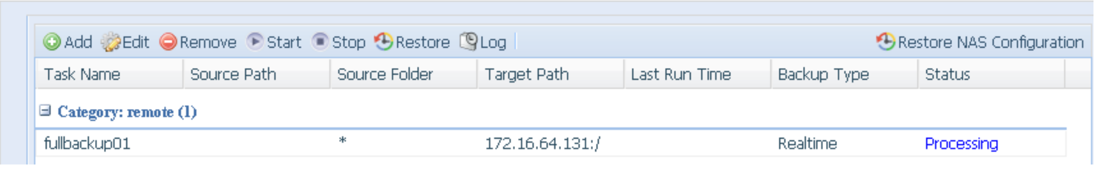
□ **Enable Schedule**

Schedule is not enabled and this task will not run automatically.

-Fill out all the necessary details and choose your parameters

Add Rsync Backup Task	
Item	**Description**
Task Name	This is how this task will appear in the task list.
Backup Type	Real time: It will backup folders/files from source to target on the fly. On the other hand, any changes from the source will back up to the target right away. Schedule: The task will start only according to the schedule.
Sync Type	Sync mode: Makes your source match your target completely; deleting and adding files on your target as they are deleted and added on your source. Incremental Mode : Makes your source match your target and keep all old files; adding files on your target as they are added on your source, but NOT deleting files on your target as they are deleted on your source.
Compress	With this option, compress the file data as it is sent to the destination machine, which reduces the amount of data being transmitted – something that is useful over a slow connection.
Backup NAS Config	Enabling this will back up the source unit system configurations to the designed path on the target system.
Resume Partial File	
Handle Sparse File	Try to handle sparse file efficiently so they take up less space on the destination.
Keep ACL Setting	It will backup not just data itself but also ACL configuration with associated folders/files.
Log Location	Choose the folder to save the log details while the task is executed.
Speed Limit	Input the bandwidth control for data backup operation.
Timeout Limit	Setup the timeout when trying to build up a connection in between the source and the target system.
Enable Schedule	If backup is set as "Schedule", please input the related period and time.

After the required fields are filled and the parameters are setup, click 'Finish" to complete. The data guard task will appear in the list as shown below.



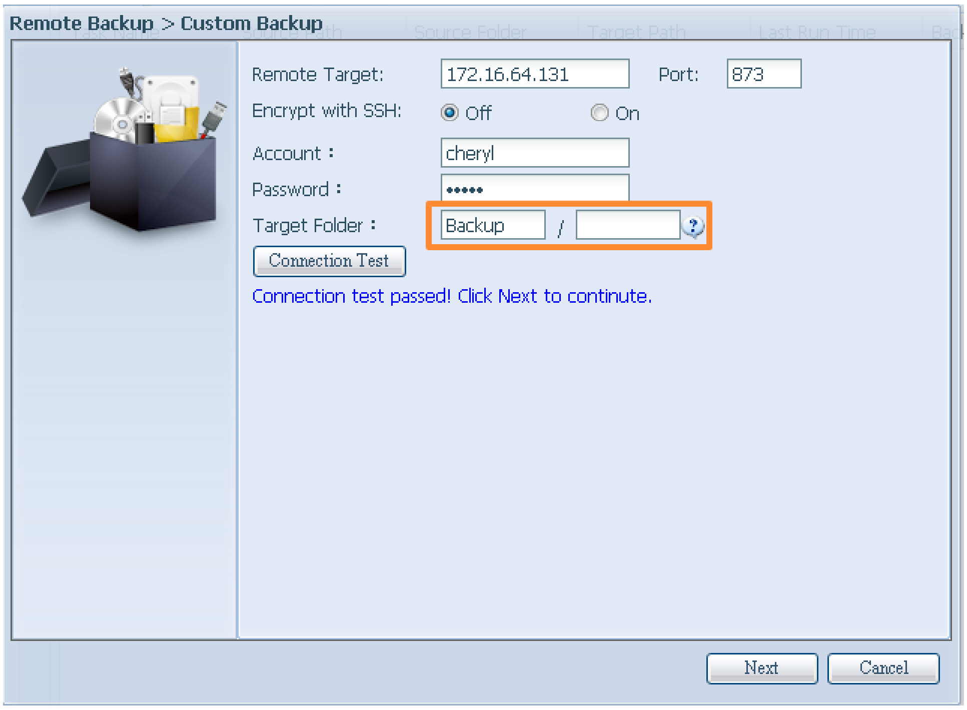
Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
Category: remote (1)						
fullbackup01	*		172.16.64.131:/		Realtime	Processing

From the task list, you can now see the newly added task "fullback01". The backup is setup as "real time". From the status field, "Processing" can be read as the back-up is performed on the fly.

- ## Custom Backup

The custom backup setting is similar to the full backup. The only differences are explained below:

1. Inputs the share folder name of target sever where the source is going to backup. The sub-folder can be left as blank.



Remote Backup > Custom Backup

Remote Target: 172.16.64.131 Port: 873

Encrypt with SSH: ● Off ○ On

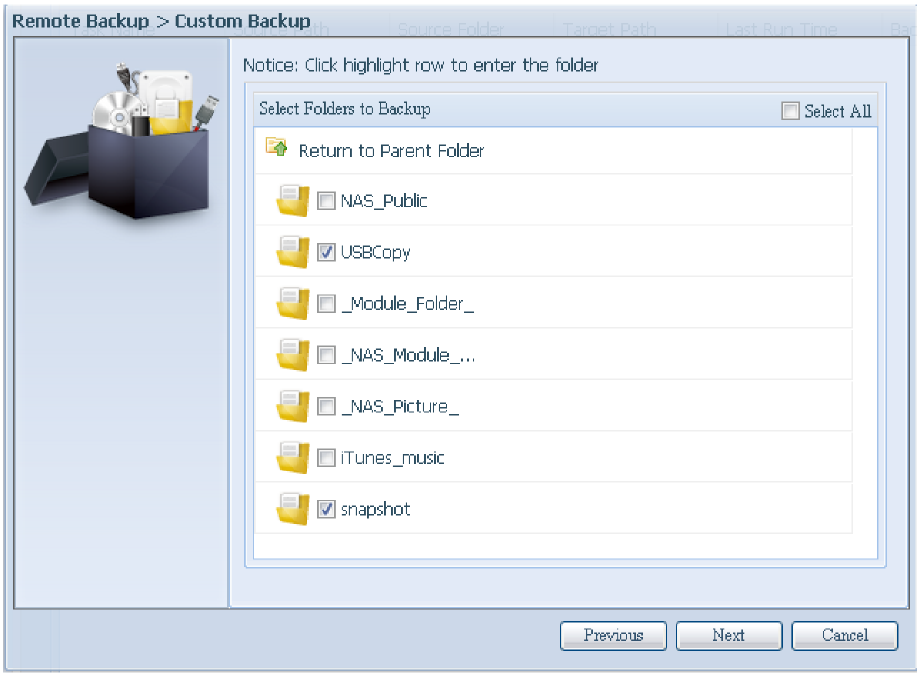
Account : cheryl

Password : •••••

Target Folder : Backup /

Connection test passed! Click Next to contintute.

2. Select the source share folder(s) which are desired to be backed up to the target server. You can also click on "Select All" from top right corner check box.



Remote Backup > Custom Backup

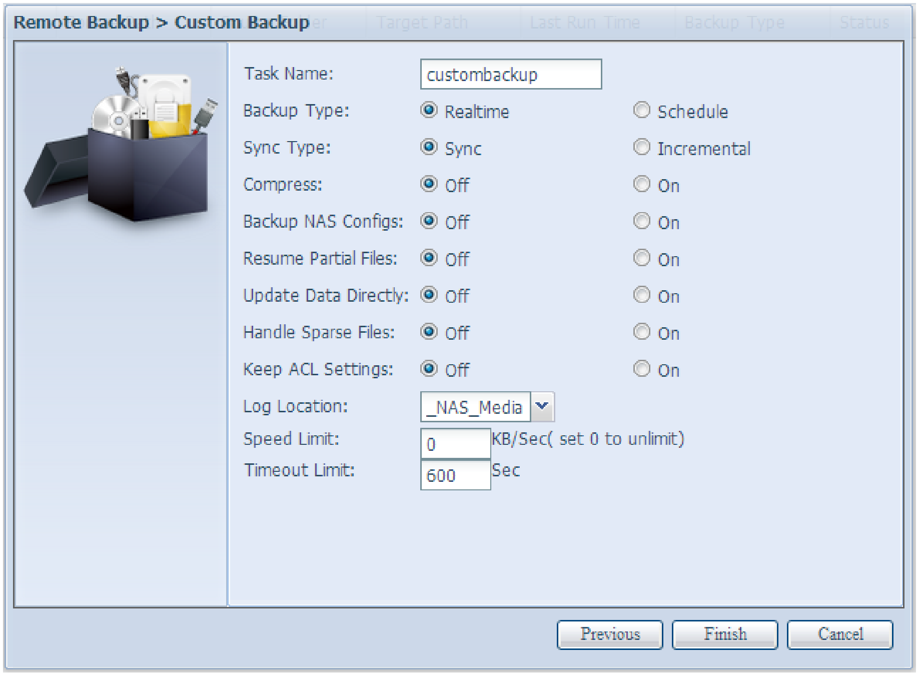
Notice: Click highlight row to enter the folder

Select Folders to Backup □ Select All

Return to Parent Folder

- □ NAS_Public
- ☑ USBCopy
- □ _Module_Folder_
- □ _NAS_Module_...
- □ _NAS_Picture_
- □ iTunes_music
- ☑ snapshot

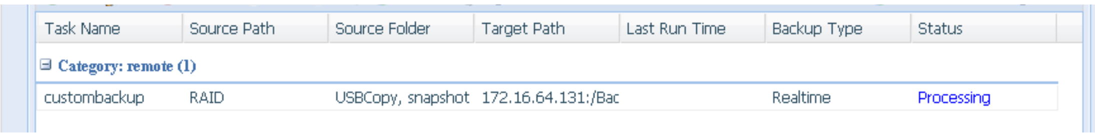
3. Click "Next" and more setting appears. These are the as the settings for "Full backup"



Remote Backup > Custom Backup

Task Name:	custombackup	
Backup Type:	● Realtime	○ Schedule
Sync Type:	● Sync	○ Incremental
Compress:	● Off	○ On
Backup NAS Configs:	● Off	○ On
Resume Partial Files:	● Off	○ On
Update Data Directly:	● Off	○ On
Handle Sparse Files:	● Off	○ On
Keep ACL Settings:	● Off	○ On
Log Location:	_NAS_Media	
Speed Limit:	0 KB/Sec(set 0 to unlimit)	
Timeout Limit:	600 Sec	

4. Click "Finish" and the data guard task will appear in the list as shown below.



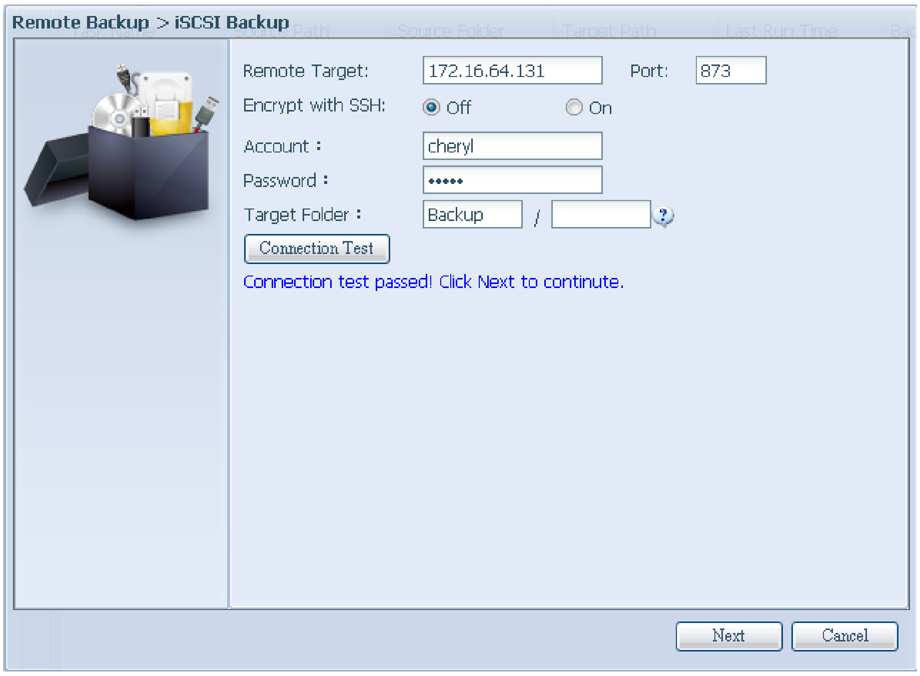
Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
⊟ Category: remote (1)						
custombackup	RAID	USBCopy, snapshot	172.16.64.131:/Bac		Realtime	Processing

From the task list, you can now see the newly added "customback01". This backup is setup as "schedule".

- ## iSCSI Backup

If the source unit contains iSCSI volume, it can be backed up to the target unit as a single file. The procedure is the same as for the previous “Full backup” and “Custom backup”, select “iSCSI backup” from data guard wizard.

1. Inputs the share folder name of the target sever where the source is going to backup. The sub-folder can be left as blank.



Remote Backup > iSCSI Backup

Remote Target: 172.16.64.131 Port: 873

Encrypt with SSH: ● Off ○ On

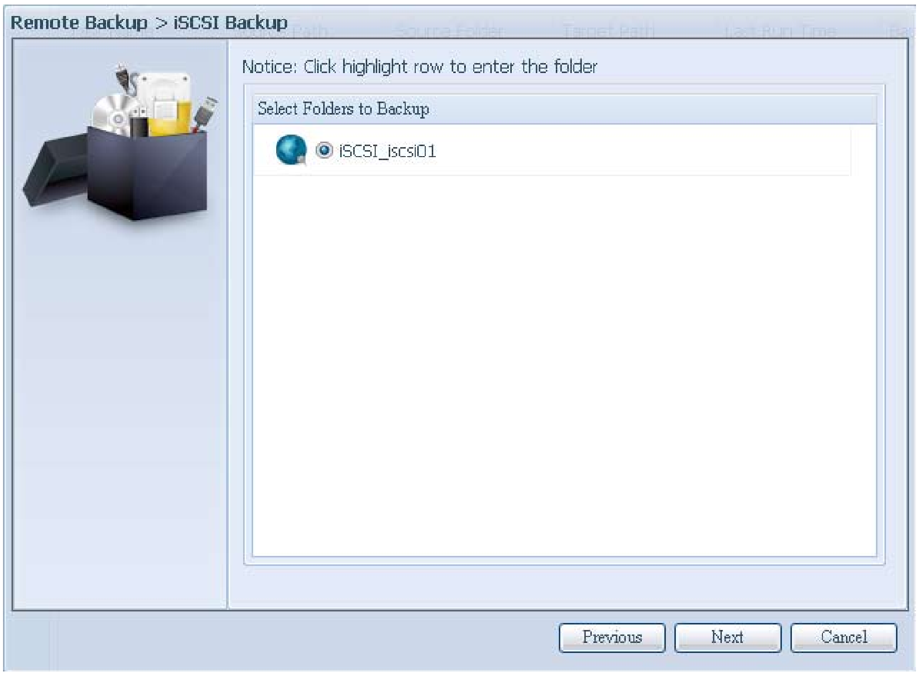
Account : cheryl

Password : •••••

Target Folder : Backup /

Connection test passed! Click Next to continute.

2. Select the iSCSI target volume which you wish to back up to the target server.



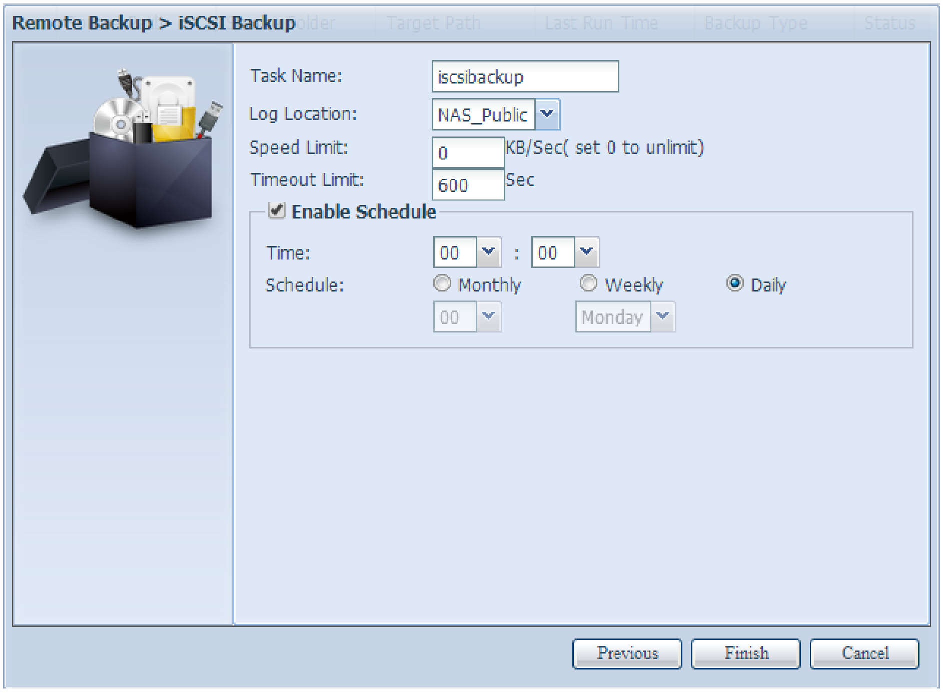
Remote Backup > iSCSI Backup

Notice: Click highlight row to enter the folder

Select Folders to Backup

● iSCSI_iscsi01

3. Click “Next” and more settings will appear. It is slightly differing from “Full backup” and “Custom backup”. Only “Schedule” backup is supported with less options.



Remote Backup > iSCSI Backup

Task Name: iscsibackup

Log Location: NAS_Public

Speed Limit: 0 KB/Sec(set 0 to unlimit)

Timeout Limit: 600 Sec

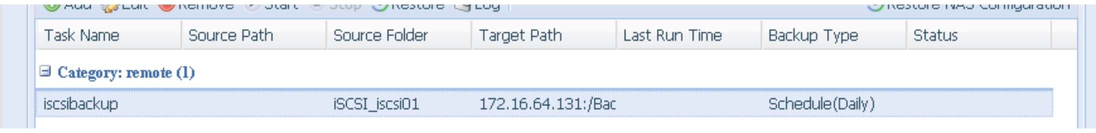
☑ Enable Schedule

Time: 00 : 00

Schedule: ○ Monthly ○ Weekly ● Daily

00 Monday

4. Click "Finish" and the data guard task will appear in the list as shown below.

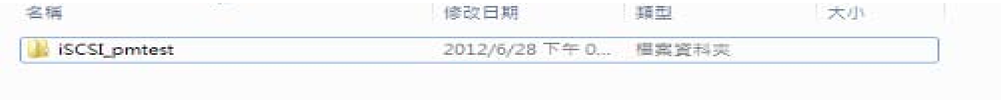


Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
⊟ Category: remote (1)						
iscsibackup		iSCSI_iscsi01	172.16.64.131:/Bac		Schedule(Daily)	

From the task list, you can now see the newly added "iscsiback". This backup is setup as "schedule".

The source folder name will use iSCSI_+target volume name. So here it is displayed as "iSCSI_pmtest". pmtest is the iSCSI target name when the iSCSI target was created.

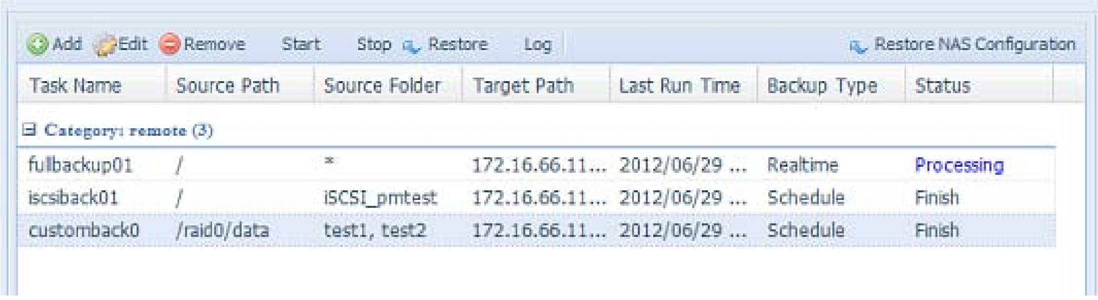
The iSCSI backup can see the result as below. The task "iSCSI_pmtest" has backup to target 172.16.66.131 and share folder NAS_Public with file "iSCSI_pmtest".



名稱	修改日期	類型	大小
iSCSI_pmtest	2012/6/28 下午 0...	檔案資料夾	

• Restore

To restore a backup from the backup task, simply select a task from the task list then click "Restore" from the function bar. The restore task will start to have the associated files/folders from the target server restored to the source.

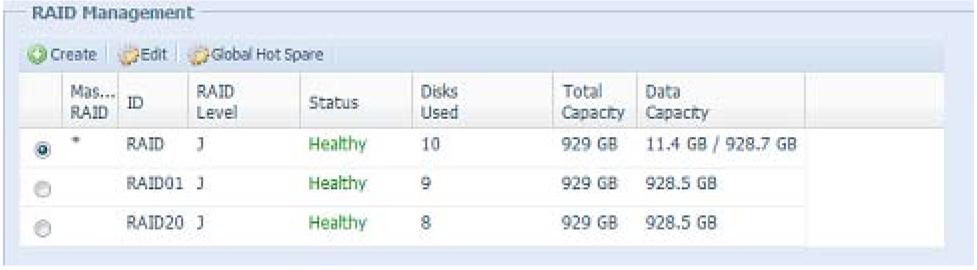


Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
⊟ Category: remote (3)						
fullbackup01	/	*	172.16.66.11...	2012/06/29 ...	Realtime	Processing
iscsiback01	/	iSCSI_pmtest	172.16.66.11...	2012/06/29 ...	Schedule	Finish
custombacK0	/raid0/data	test1, test2	172.16.66.11...	2012/06/29 ...	Schedule	Finish

• Restore NAS Configuration

This is a useful feature if the system configuration needs to be restored to a brand new unit. Let's go thru the following example to see how it works.

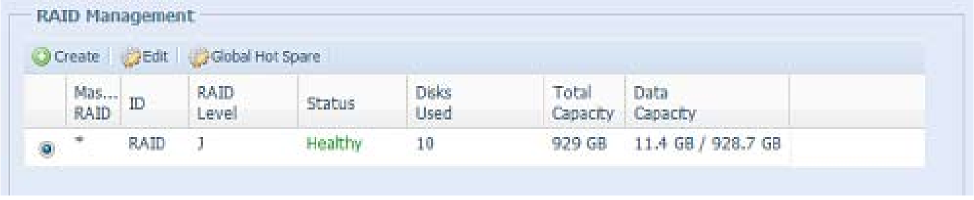
The original source system has 3 RAID volume, "RAID", 'RAID10" and "RAID20", and has backed up the system configurations to the target server.



RAID Management

	Mas... RAID	ID	RAID Level	Status	Disks Used	Total Capacity	Data Capacity
●	*	RAID	J	Healthy	10	929 GB	11.4 GB / 928.7 GB
○		RAID01	J	Healthy	9	929 GB	928.5 GB
○		RAID20	J	Healthy	8	929 GB	928.5 GB

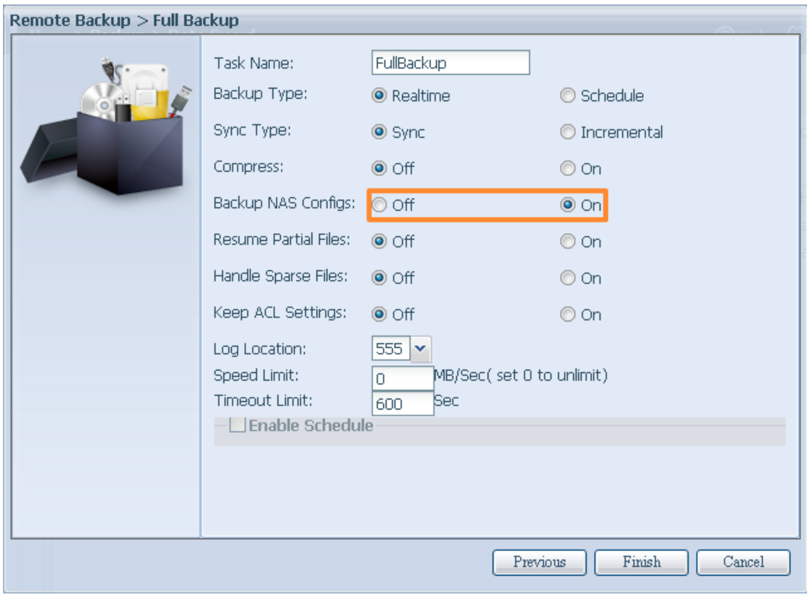
The brand new source unit only has a 1 RAID volume 'RAID".



RAID Management

	Mas... RAID	ID	RAID Level	Status	Disks Used	Total Capacity	Data Capacity
●	*	RAID	J	Healthy	10	929 GB	11.4 GB / 928.7 GB

1. When adding a new backup task with "Full backup" or "Custom backup" and enabling the option "Backup NAS Config" as shows below, the source unit system configurations are then backed up to the designed path on the target system every time the task is executed.



Remote Backup > Full Backup

Task Name: FullBackup

Backup Type: ● Realtime ○ Schedule

Sync Type: ● Sync ○ Incremental

Compress: ● Off ○ On

Backup NAS Configs: ○ Off ● On

Resume Partial Files: ● Off ○ On

Handle Sparse Files: ● Off ○ On

Keep ACL Settings: ● Off ○ On

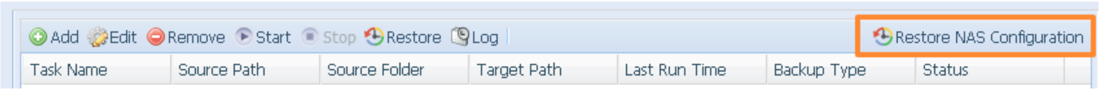
Log Location: 555

Speed Limit: 0 MB/Sec(set 0 to unlimit)

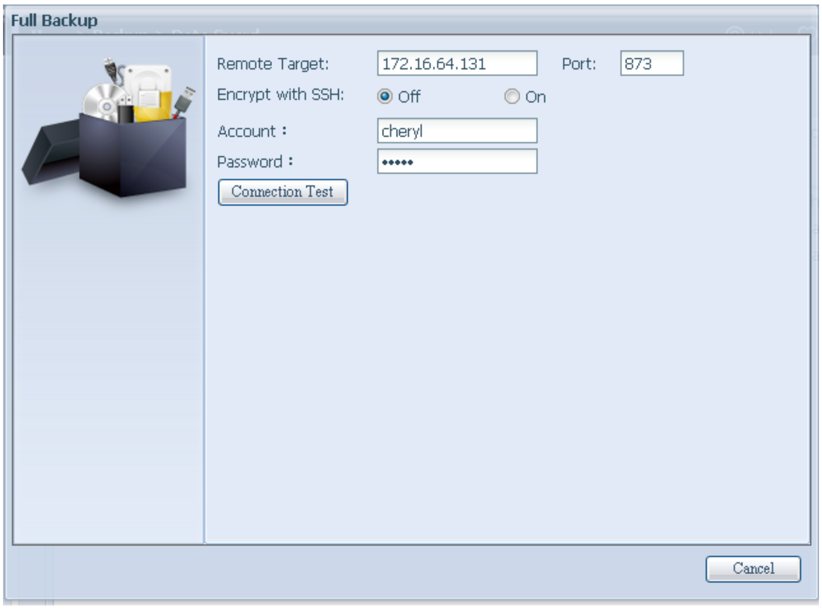
Timeout Limit: 600 Sec

□ Enable Schedule

2. Click on "Restore NAS Configuration" and the screen shown below will appear. Input the target server's IP address where the system configuration has been backed up, and necessary authentication info. Confirm by doing a "Connection Test" to make sure the communication between the source and the target server works.



Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status



Full Backup

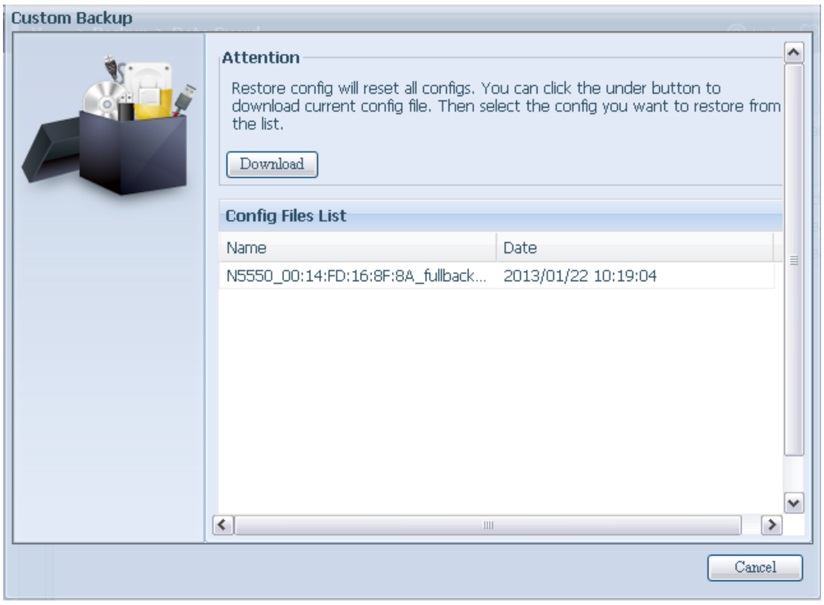
Remote Target: 172.16.64.131 Port: 873

Encrypt with SSH: ● Off ○ On

Account : cheryl

Password : •••••

3. Click "Next" and a screen will appear as shown below. It has the listed available system configuration backup files. Select the one you want and click next. You also have the option to download the current system configuration before restoring from the backup file.



Custom Backup

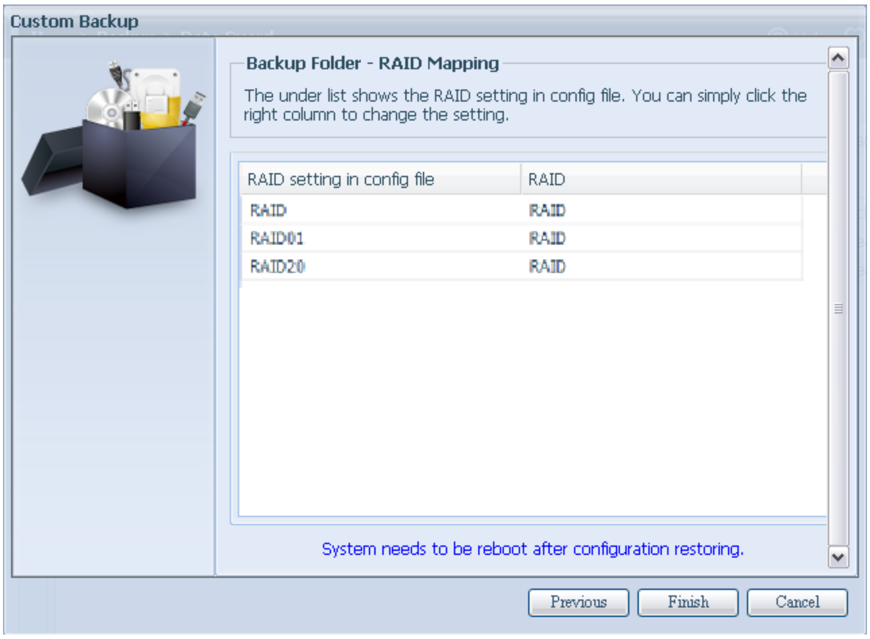
Attention

Restore config will reset all configs. You can click the under button to download current config file. Then select the config you want to restore from the list.

Config Files List

Name	Date
N5550_00:14:FD:16:8F:8A_fullback...	2013/01/22 10:19:04

4. After clicking "Next", a screen will appear as shown below. Listed on the left hand side, you will see the configuration backup details which contain the 3 RAID volumes. On the right hand side, you will see a list of single "RAID" volume. You may roll back to previous page to recall the example we have taken.



Custom Backup

Backup Folder - RAID Mapping

The under list shows the RAID setting in config file. You can simply click the right column to change the setting.

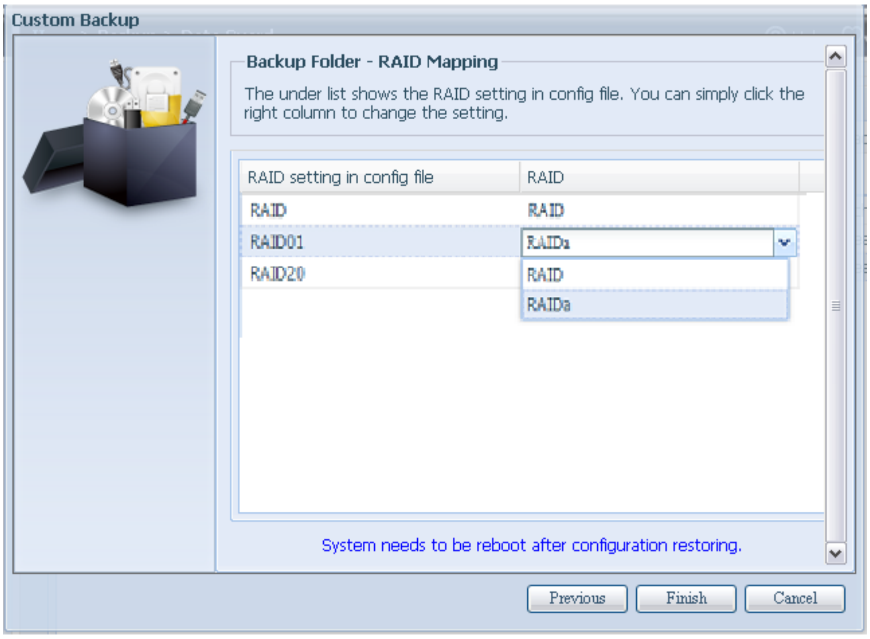
RAID setting in config file	RAID
RAID	RAID
RAID01	RAID
RAID20	RAID

System needs to be reboot after configuration restoring.

5. The backup configuration has different numbers of RAID volume than the current system (3 vs 1). It can be kept as the RAID volume mapping arranged by the system, then carry on to click "Finish". This means that all 3 RAID volumes configuration such as share folder etc. will all restore to the current unit in the RAID volume "RAID".
6. In other circumstances, if the current unit contains 2 RAID volumes, then it can be chosen from the left hand side of system backup configuration RAID volume list which RAID volume to map to the current system.

Let's see the following screen to make it clearer.

The current system has 2 RAID volumes, "RAID" and "RAIDa". Select the RAID volume from the backup configuration volume list which is going to be mapped to the RAID volume of the current system. Simply click on the right hand side of "RAIDa" and a drop down list will appear. Now you can choose which volume to map with. In this case the "RAID01" volume from the system backup configuration will be mapped to the volume "RAIDa" of the current unit. Once again, it means all the shares that were created in the volume "RAID01" will be restored to volume "RAIDa" of the current system.



Custom Backup

Backup Folder - RAID Mapping

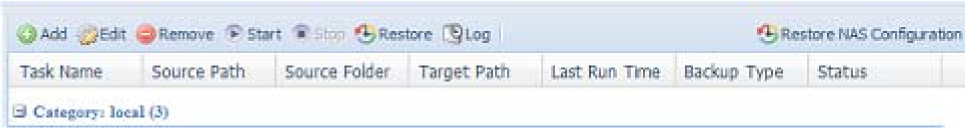
The under list shows the RAID setting in config file. You can simply click the right column to change the setting.

RAID setting in config file	RAID
RAID	RAID
RAID01	RAIDa
RAID20	

System needs to be reboot after configuration restoring.

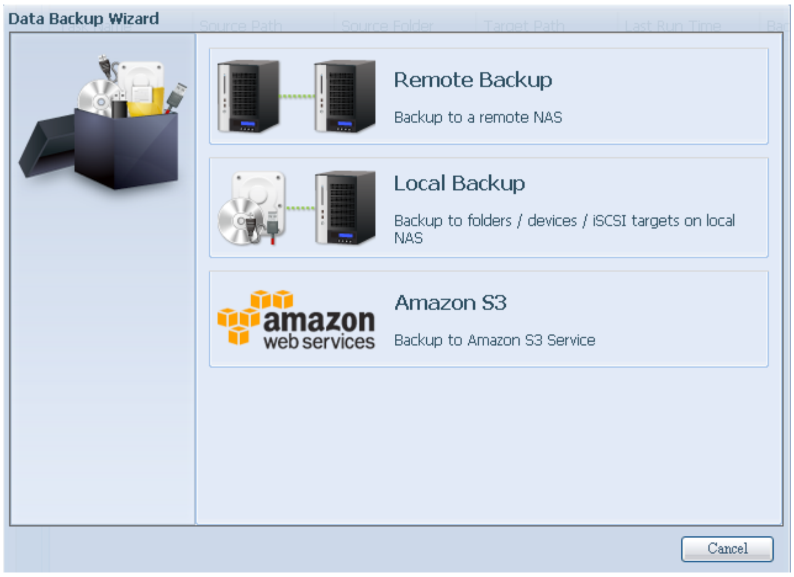
3.8.3 Data Guard (Local Backup)

The Thecus product provides complete backup solution between Thecus NAS systems as well as between folders of local systems.

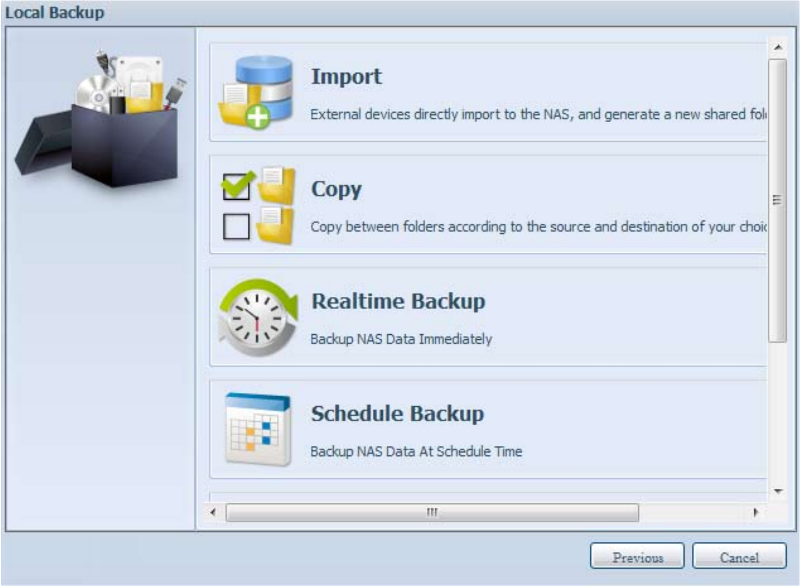


Remote Data backup	
Item	**Description**
Add	Add a new task.
Edit	Edit selected task.
Remove	Remove selected task.
Start	Click on start to start a scheduled scan task right away.
Stop	Stop the associated running task. Also can be used if a task has been setup as real-time, clicking "Stop" can terminate the running process. Simply click 'Start" to re-start the real-time operation.
Restore	Restore the associated task.
Log	Click to view the associated task process details.
Restore NAS Configuration	Click to restore the system configurations from a selected destination to a source unit.

From the Data Guard function list, select Add. The data backup setup wizard appears as below, click on "Local Backup":

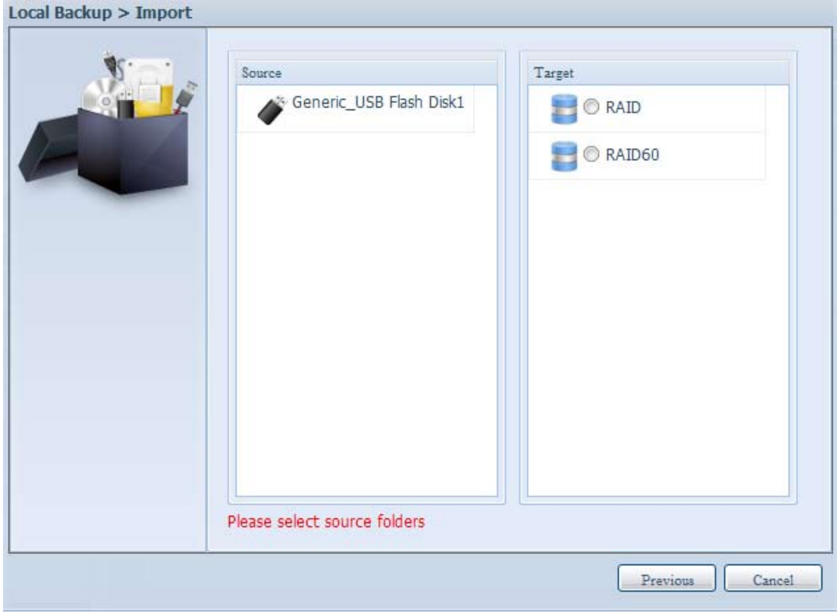


The local backup has 6 different selection you can choose from.


Local Backup
Import
External devices directly import to the NAS, and generate a new shared fol
Copy
Copy between folders according to the source and destination of your choi
Realtime Backup
Backup NAS Data Immediately
Schedule Backup
Backup NAS Data At Schedule Time
Previous
Cancel

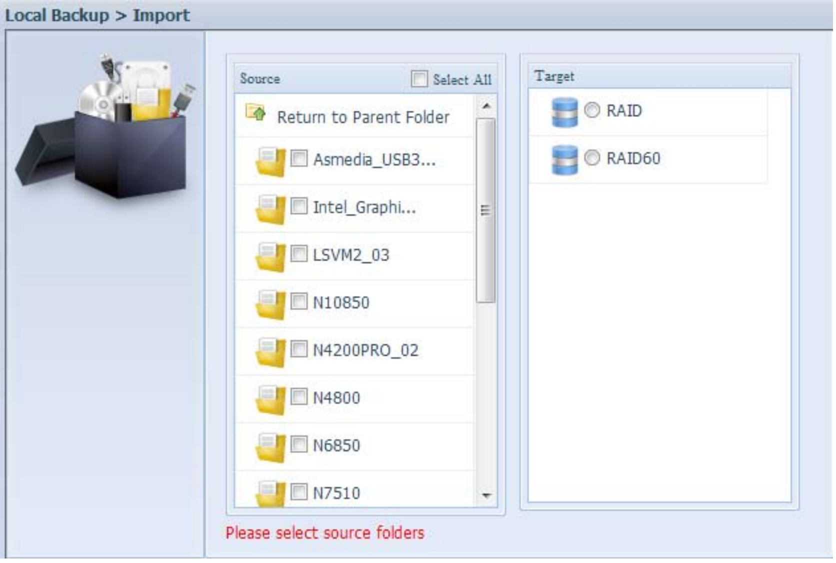
Local Data backup	
Item	**Description**
Import	This is associated with external devices which are added to the system such as USB disk. You can select a folder from an external device and import it to the NAS as a share folder.
Copy	Copy folder to folder or NAS folder to external device or external device to NAS folder. This backup is within folder level.
Realtime Backup	The task will be executed on the fly between the source and the target. In other word, any changes made at the source will sync to the destination immediately.
Schedule Backup	The task will be executed on schedule between the source and the target.
iSCSI Backup	The iSCSI volume will be backup to the destination as a single file.
iSCSI Import	The iSCSI file can be imported from the iSCSI backup back to the destination as an iSCSI volume.

1. Import: click on "Import" and a screen will appear as below.
   If there is an external device installed on system such as USB disk, then it will be listed in the Source pane.



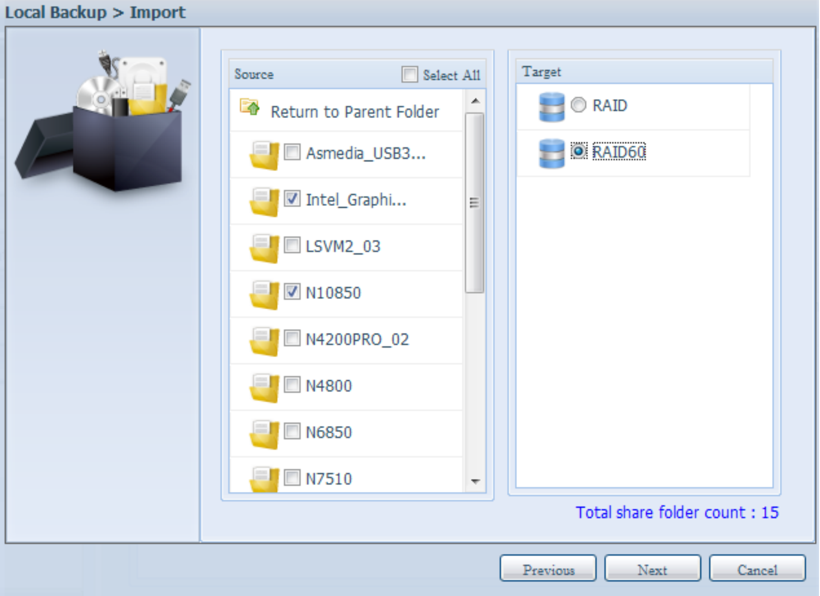
Please select source folders

Click on the associated external device and the contain folders will be listed. Select the folders that are going to be imported to the NAS and select the available RAID volume which is listed in Target pane.

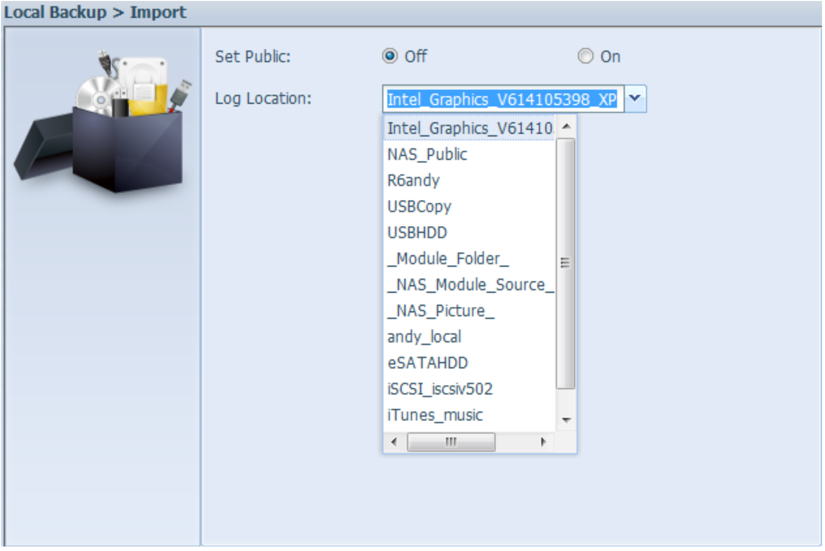


Please select source folders

In here, we have selected the "Intel Graphi…" and "N10850" folders from the external device and imported them to the NAS under the RAID60volume.

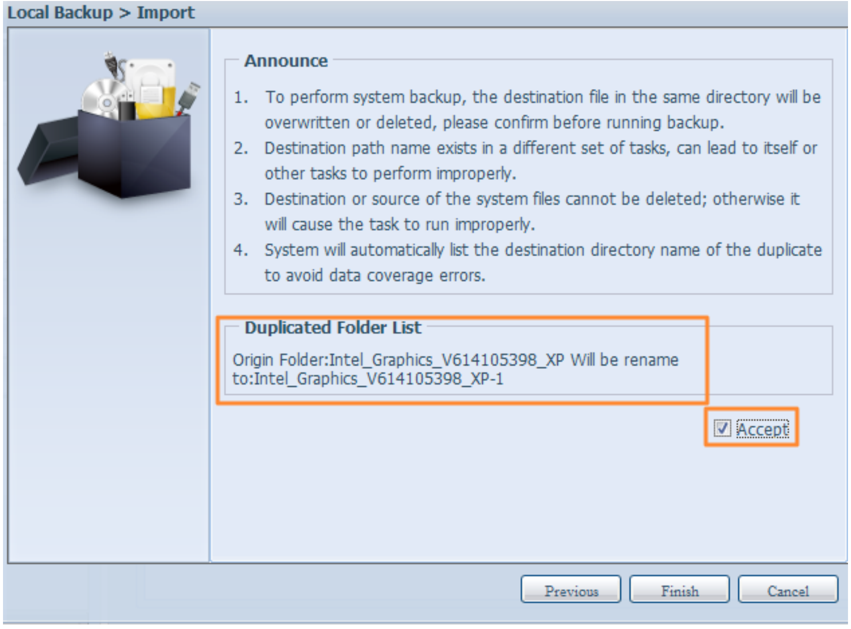


Next, please select the path from the drop down list to save the log. Also, give the access permission whether these selected folders will be "Public" or not after the import.



Read the notes and check the "Accept" box for confirmation. If a share name already exists for the import, then the import will be rename automatically to "existing share name -1".

For esample, if the NAS RAID volume "RAID60" already has a folder named "Intel_Graphics_V614105398_XP", the import folder will then be rename to: "Intel_Graphics_V614105398_XP-1".



Local Backup > Import

Announce

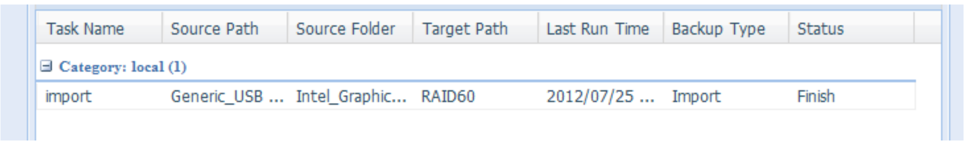
1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.

Duplicated Folder List

Origin Folder:Intel_Graphics_V614105398_XP Will be rename to:Intel_Graphics_V614105398_XP-1

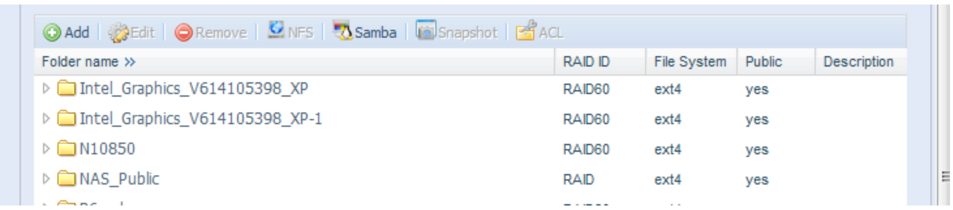
☑ Accept

Now, you will see in the data guard task list that you have created a task .



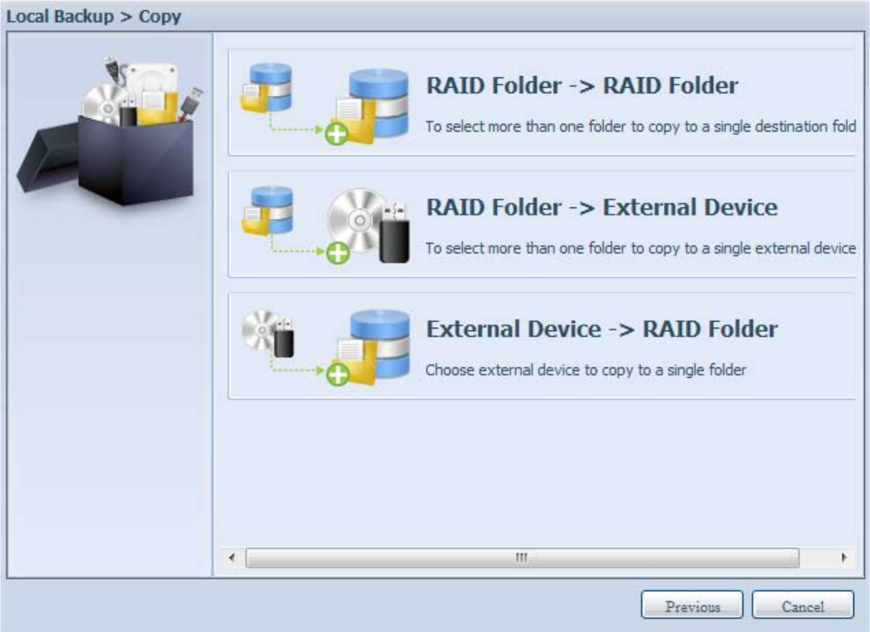
Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
⊟ Category: local (1)						
import	Generic_USB ...	Intel_Graphic...	RAID60	2012/07/25 ...	Import	Finish

And that the system has created 2 new share folders from the task just created.



Folder name »	RAID ID	File System	Public	Description
Intel_Graphics_V614105398_XP	RAID60	ext4	yes	
Intel_Graphics_V614105398_XP-1	RAID60	ext4	yes	
N10850	RAID60	ext4	yes	
NAS_Public	RAID	ext4	yes	

2. Copy: click on “Copy” and this screen appears.
   3 different options can be selected, folder to folder, folder to external device or external device to folder.



Local Backup > Copy

RAID Folder -> RAID Folder

To select more than one folder to copy to a single destination fold

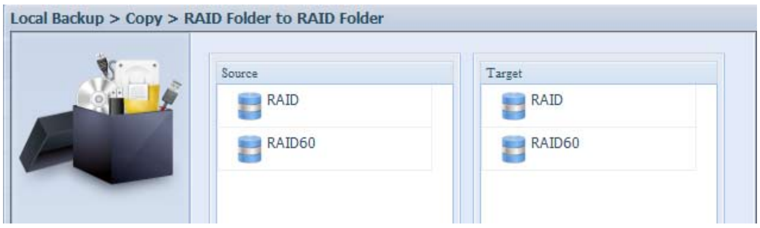
RAID Folder -> External Device

To select more than one folder to copy to a single external device

External Device -> RAID Folder

Choose external device to copy to a single folder

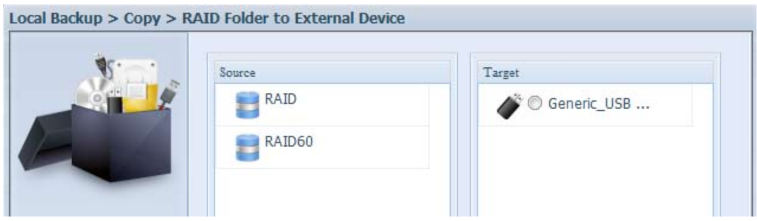
- **Folder to Folder**



Local Backup > Copy > RAID Folder to RAID Folder

Source	Target
RAID	RAID
RAID60	RAID60

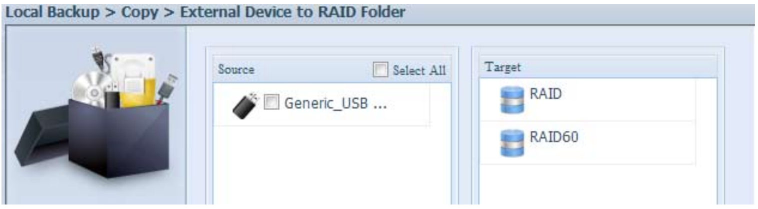
- **Folder to external device**



Local Backup > Copy > RAID Folder to External Device

Source	Target
RAID	○ Generic_USB ...
RAID60	

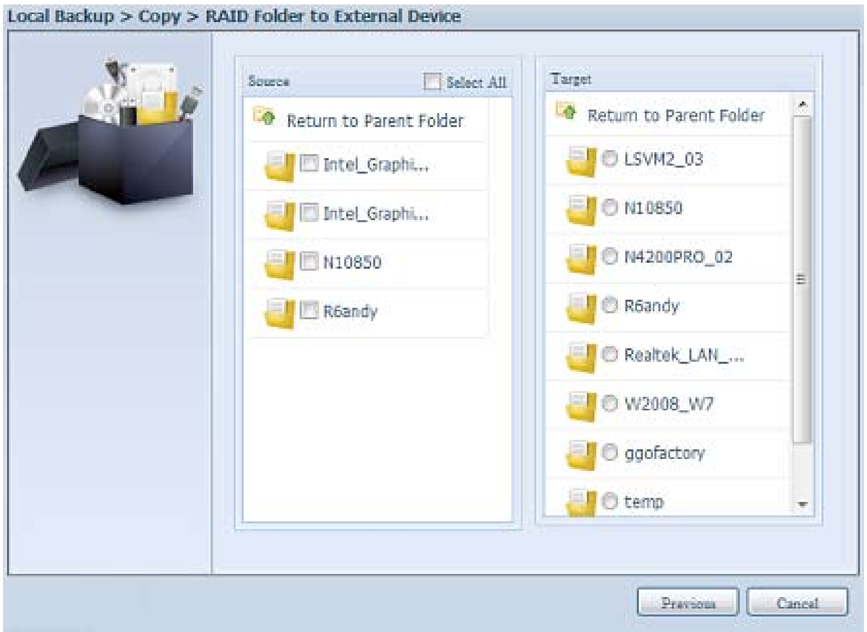
- **External device to Folder**



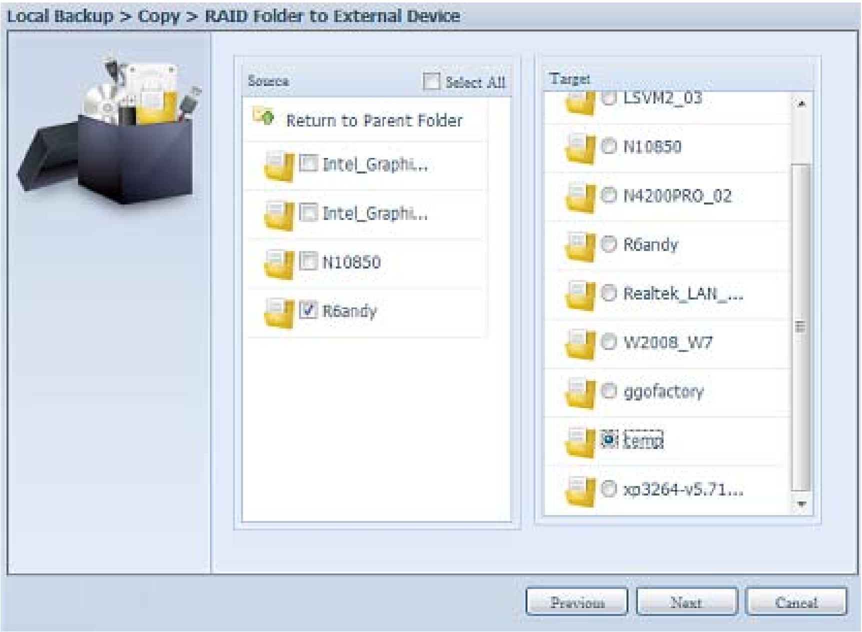
Local Backup > Copy > External Device to RAID Folder

Source □ Select All	Target
□ Generic_USB ...	RAID
	RAID60

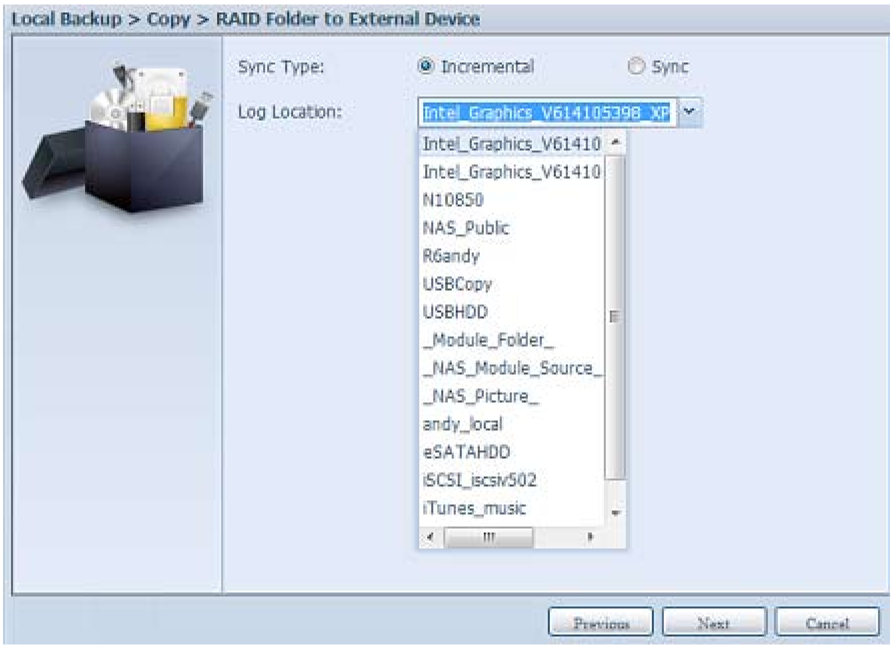
Let's take "Folder to External device" as an example. In the source pane, select the desired RAID volume and its associated folder list will appear; same method in the target pane for the associated external device.



Select a folder from the source pane which is going to be copy over, then select in target pane it's destination.



Choosing the sync type, "Incremental" or 'Sync", and select the log path from the drop menu list.

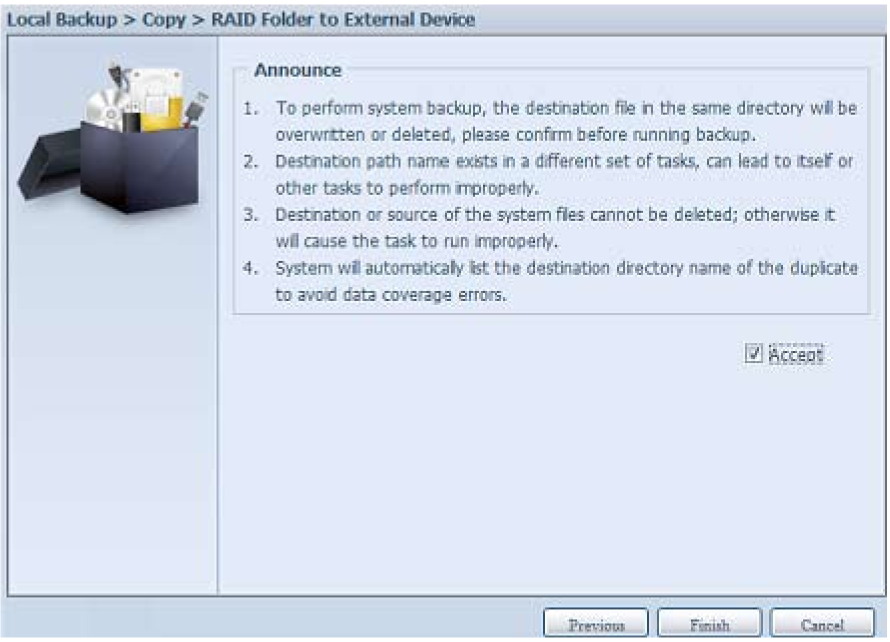


Local Backup > Copy > RAID Folder to External Device

Sync Type: ● Incremental ○ Sync

Log Location: Intel_Graphics_V614105398_XP

Read the notes and check the "Accept" box for confirmation.



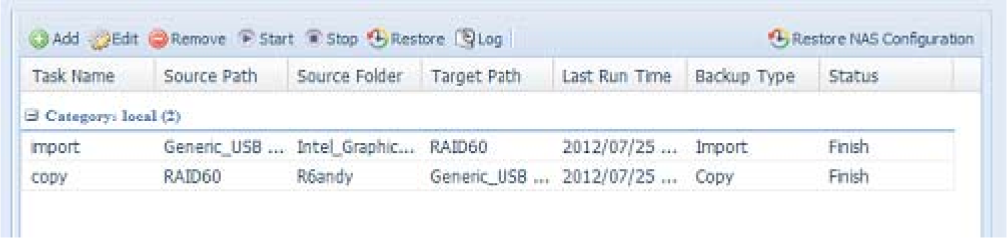
Local Backup > Copy > RAID Folder to External Device

Announce

1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.

☑ Accept

Now, you will see in the data guard task list that you have created a task.

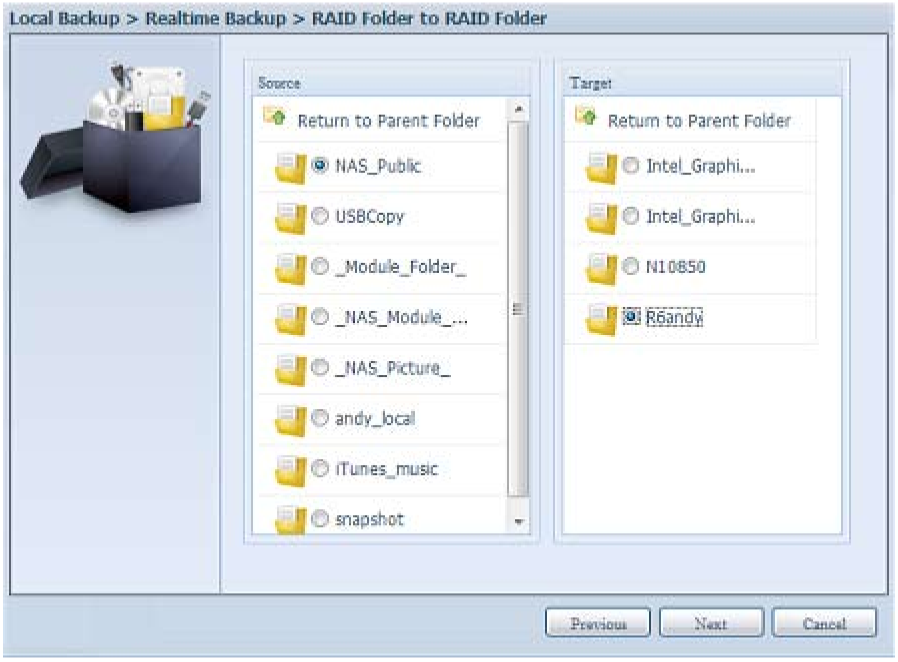


Category: local (2)

Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
import	Generic_USB ...	Intel_Graphic...	RAID60	2012/07/25 ...	Import	Finish
copy	RAID60	R6andy	Generic_USB ...	2012/07/25 ...	Copy	Finish

3. Realtime Backup: click on "Realtime Backup" and this screen will appear.
   2 different options can be selected from, folder to folder, folder to external device.

   Let's take "Folder to Folder" backup for example. Select from the source pane the folder "NAS_Public", then select its destination in the target panefolder "R6andy".



Local Backup > Realtime Backup > RAID Folder to RAID Folder

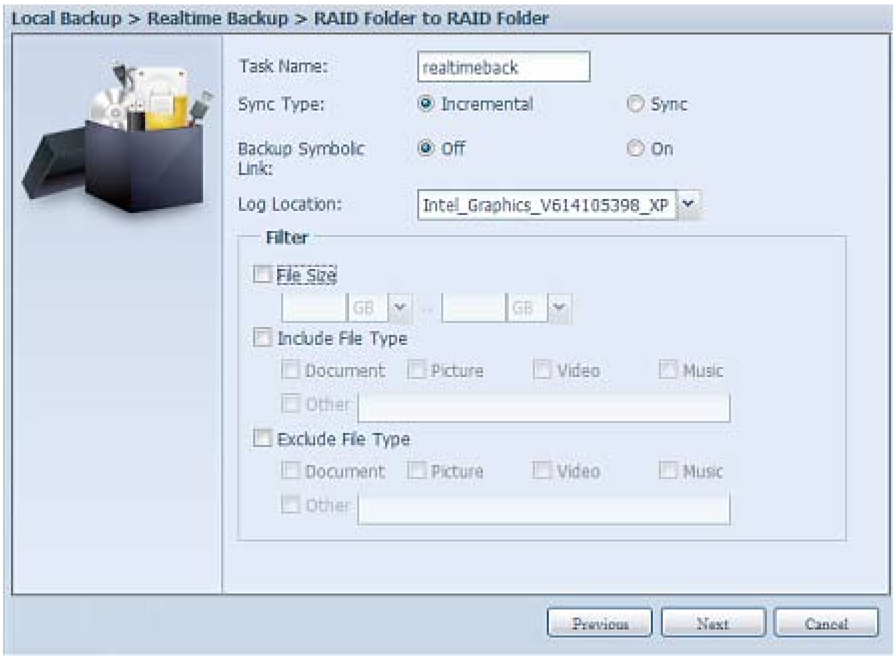
Source

- Return to Parent Folder
- ● NAS_Public
- ○ USBCopy
- ○ _Module_Folder_
- ○ _NAS_Module_...
- ○ _NAS_Picture_
- ○ andy_local
- ○ iTunes_music
- ○ snapshot

Target

- Return to Parent Folder
- ○ Intel_Graphi...
- ○ Intel_Graphi...
- ○ N10850
- ● R6andy

Next, fill in the task name and related settings.



Local Backup > Realtime Backup > RAID Folder to RAID Folder

Task Name: realtimeback

Sync Type: ● Incremental ○ Sync

Backup Symbolic Link: ● Off ○ On

Log Location: Intel_Graphics_V614105398_XP

Filter

□ File Size

GB ~ GB

□ Include File Type

□ Document □ Picture □ Video □ Music

□ Other

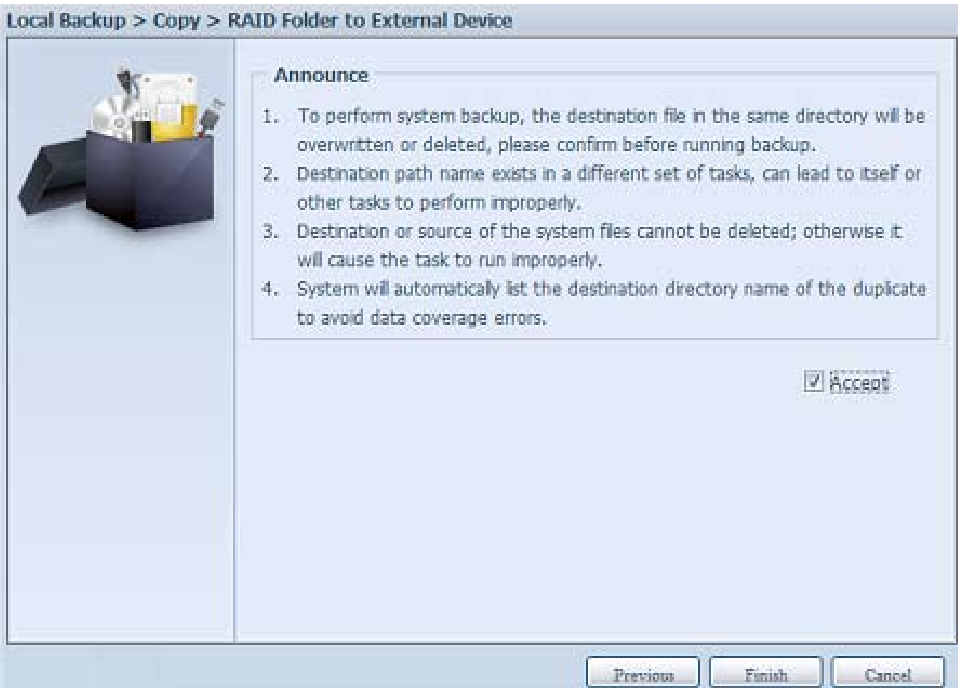
□ Exclude File Type

□ Document □ Picture □ Video □ Music

□ Other

Realtime Backup	
Item	**Description**
Task Name	Input the task name, length limited to 4~12 characters.
Sync Type	Select "Incremental" or "Synchronize".
Backup Symbolic Link	Choose to backup symbolic link which is included in the source.
Filter	The filter can be set to be executed only in certain circumstances. If none of them has been selected, it will do the real time backup from the source to the destination in full. File size: From xx ~ xxx If xx=1 and xxx blank then only file size > xx will execute real time backup. If xx=1 and xxx=2 then only size in between xx and xxx will execute real time backup. If xx blank and xxx=2 then only file size < xxx will execute real time backup. Include File Type: Only the associated file format will do the real time backup. Exclude File Type: The excluded file format won't be included in the real time backup. For document file format: doc, xls, pdf, docx, xlsx, txt, ppt, pptx, html, htm For picture file format: jpg, bmp, tif, png, pbm, tga, xar, xbm For video file format: avi, mpg, mp4, mkv, fli, flv, rm, ram For music file format: mp3, wav, wma, acc, dss, msv, dvf, m4p, 3gp, amr, awb User defined can be input in other box.

Read the notes and check the "Accept" box for confirmation.



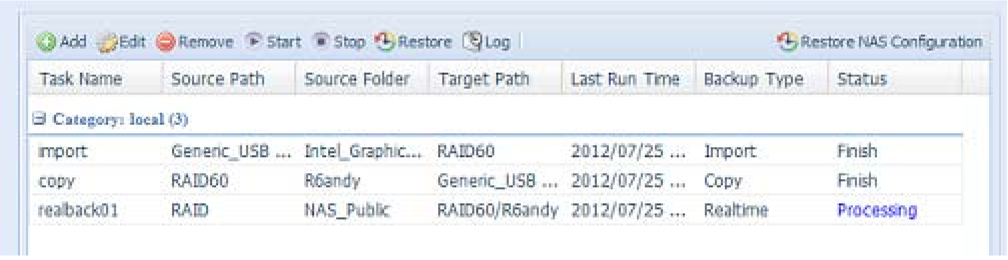
Local Backup > Copy > RAID Folder to External Device

Announce

1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.

☑ Accept

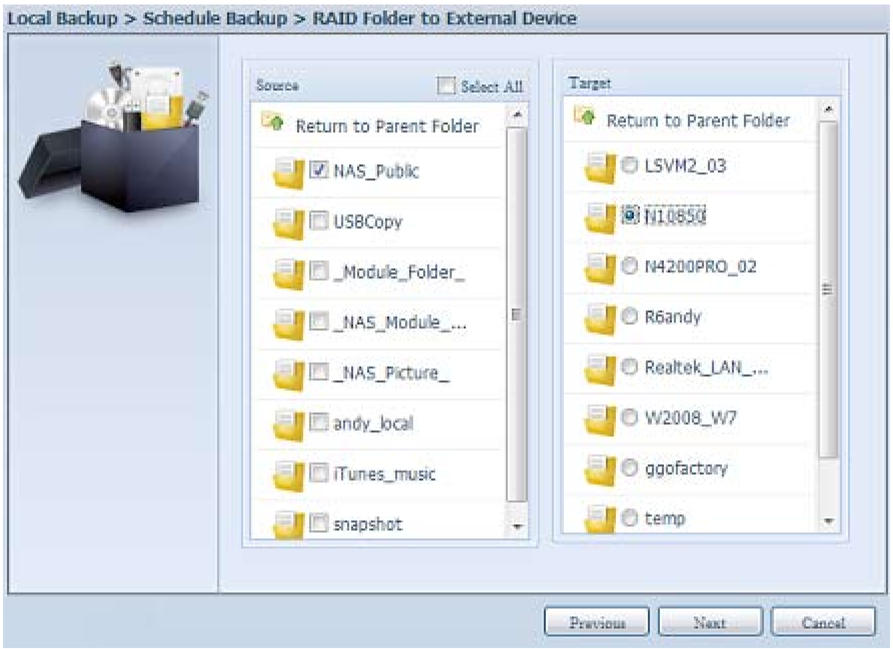
Now, you can see in the data guard task list that your created task is listed. The task status will say "Processing" untill the "Stop" button is pressed.



Category: local (3)

Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
import	Generic_USB ...	Intel_Graphic...	RAID60	2012/07/25 ...	Import	Finish
copy	RAID60	R6andy	Generic_USB ...	2012/07/25 ...	Copy	Finish
realback01	RAID	NAS_Public	RAID60/R6andy	2012/07/25 ...	Realtime	Processing

4. Schedule Backup: click on "Schedule Backup" and this screen will. 2 different choices can be selected from, folder to folder, folder to external device.
   Let's use "Folder to External device" backup for our example. From the NAS volume RAID in the Source pane select the folder "NAS_Public", then in the target pane select the external USB disk folder "N10850".



Local Backup > Schedule Backup > RAID Folder to External Device

Source □ Select All

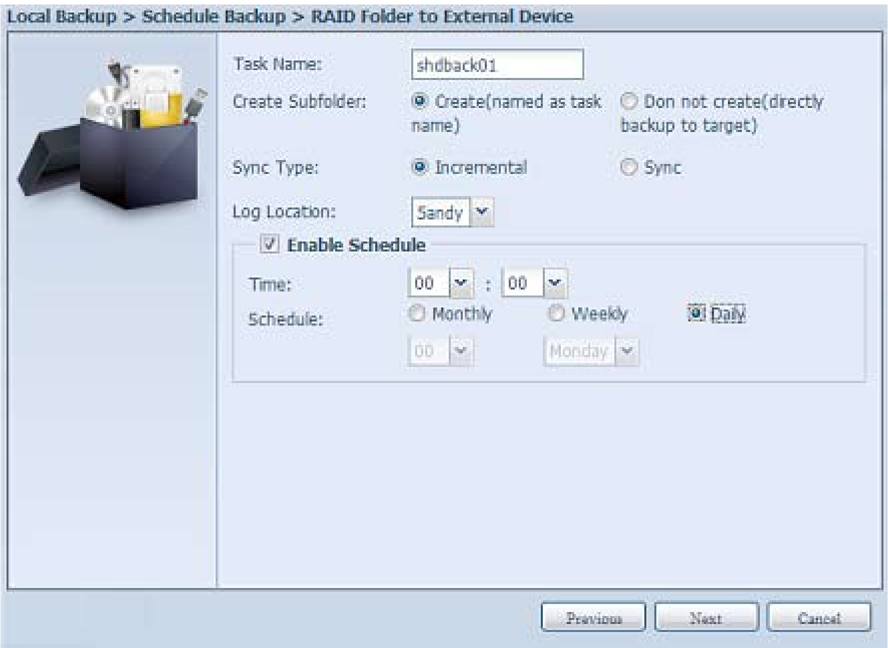
- Return to Parent Folder
- ☑ NAS_Public
- □ USBCopy
- □ _Module_Folder_
- □ _NAS_Module_...
- □ _NAS_Picture_
- □ andy_local
- □ iTunes_music
- □ snapshot

Target

- Return to Parent Folder
- ○ LSVM2_03
- ● N10850
- ○ N4200PRO_02
- ○ R6andy
- ○ Realtek_LAN_...
- ○ W2008_W7
- ○ ggofactory
- ○ temp

Next, fill in the task name and related settings.

Schedule Backup	
Item	Description
Task Name	Input the task name, length limited to 4~12 characters.
Create Sub-folder	If you choose to create a sub-folder, then it will use the task name as folder name then copy the source under it. Or it will copy the source to the same level as the destination.
Sync Type	Select "Incremental" or "Synchronize".
Log Location	Select from the drop down list where the task log will be stored.
Enable Schedule	Click to enable. If it is not checked, the task won't start unless you select the associate task and click "Start" from the task list page.
Time	Specify the time for the backup to start.
Schedule	Can choose daily, weekly or monthly.



Local Backup > Schedule Backup > RAID Folder to External Device

Task Name: shdback01

Create Subfolder: ● Create(named as task name) ○ Don not create(directly backup to target)

Sync Type: ● Incremental ○ Sync

Log Location: Sandy

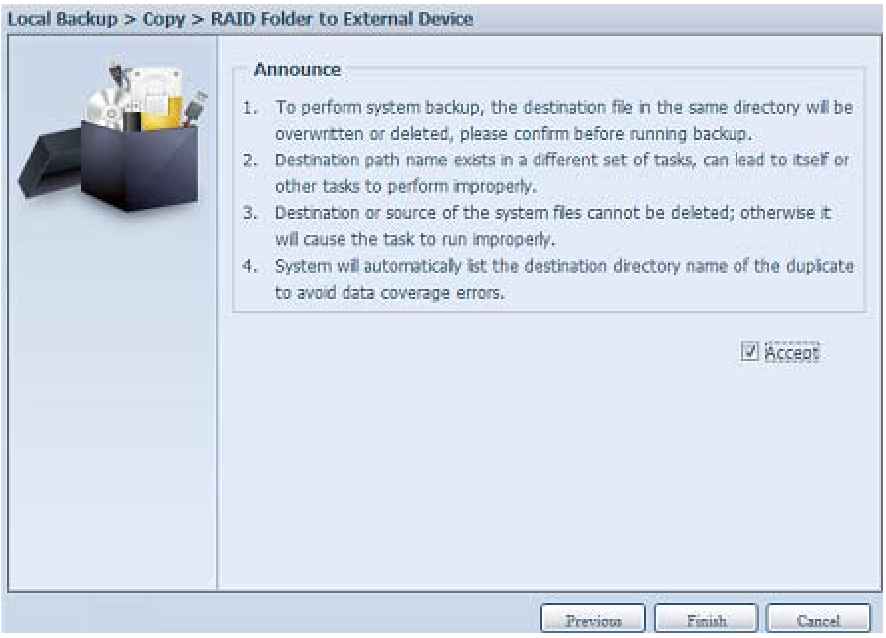
☑ Enable Schedule

Time: 00 : 00

Schedule: ○ Monthly ○ Weekly ● Daily

00 Monday

Read the notes and check the "Accept" box for confirmation.



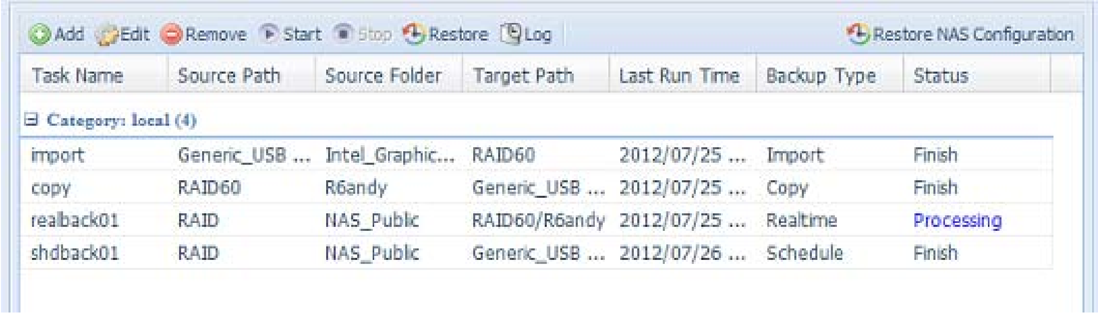
Local Backup > Copy > RAID Folder to External Device

Announce

1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.

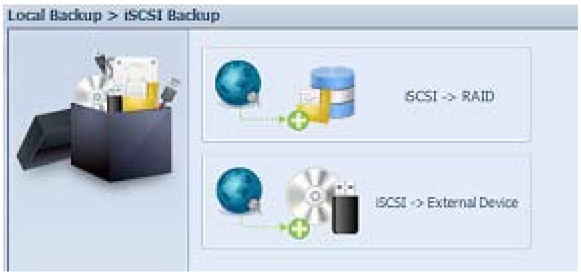
☑ Accept

Now, you will see in the data guard task list that you have created a task.



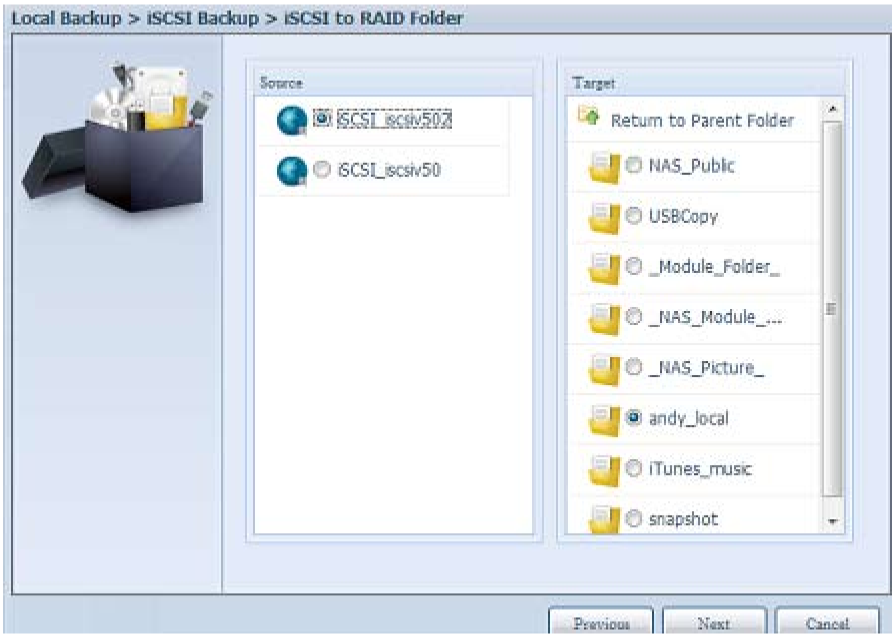
Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
⊟ Category: local (4)						
import	Generic_USB ...	Intel_Graphic...	RAID60	2012/07/25 ...	Import	Finish
copy	RAID60	R6andy	Generic_USB ...	2012/07/25 ...	Copy	Finish
realback01	RAID	NAS_Public	RAID60/R6andy	2012/07/25 ...	Realtime	Processing
shdback01	RAID	NAS_Public	Generic_USB ...	2012/07/26 ...	Schedule	Finish

5. iSCSI Backup: click on "iSCSI Backup" and screen appear as below.
It can be backup to two different storage pool, iSCSI to folder, iSCSI to external device.



Let's take example to have "iSCSI to Folder" backup, from existed iSCSI volume "iSCSI_iscsiv502" to volume RAID folder "andy_local".

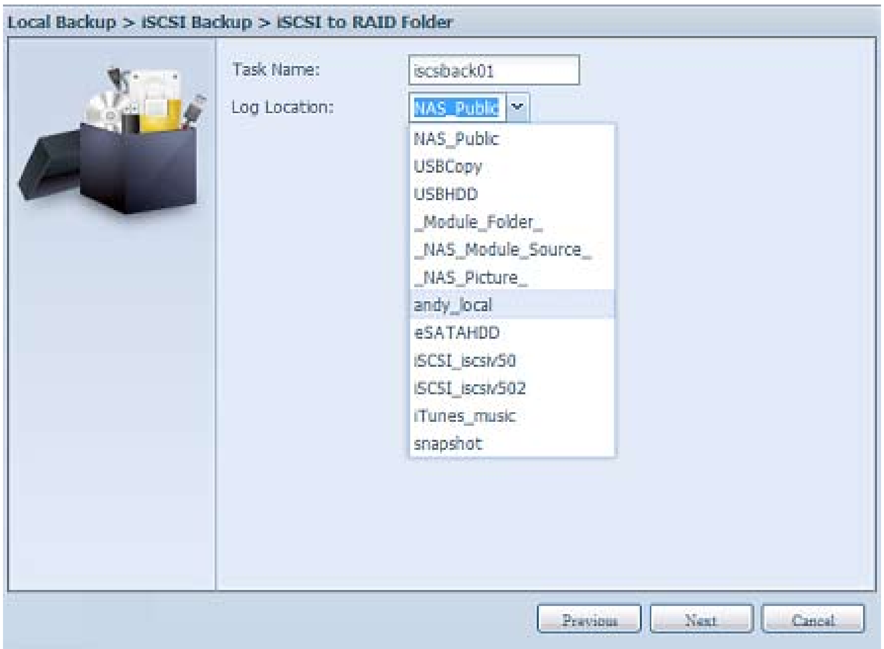
The source pane listed "iSCSI_iscsiv502" and "iSCSI_iscsiv50" where are iscsi volume has existed in this system with name "iSCSI_+iscsi target volume name".



Source:
- ● iSCSI_iscsiv502
- ○ iSCSI_iscsiv50

Target:
- ○ NAS_Public
- ○ USBCopy
- ○ _Module_Folder_
- ○ _NAS_Module_...
- ○ _NAS_Picture_
- ● andy_local
- ○ iTunes_music
- ○ snapshot

Next, provide the task name and where the task log will store.

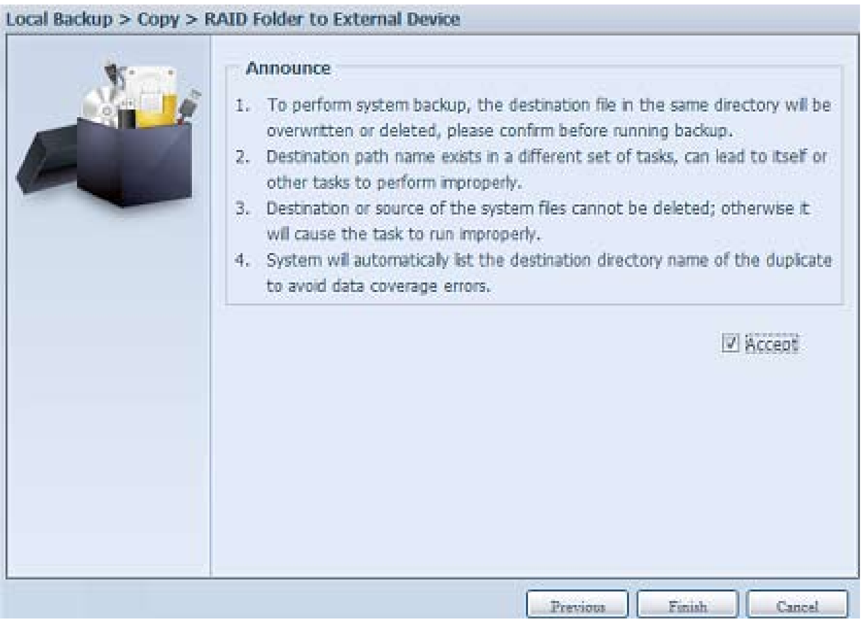


Task Name: iscsback01

Log Location: NAS_Public

- NAS_Public
- USBCopy
- USBHDD
- _Module_Folder_
- _NAS_Module_Source_
- _NAS_Picture_
- andy_local
- eSATAHDD
- iSCSI_iscsiv50
- iSCSI_iscsiv502
- iTunes_music
- snapshot

Reading the note and check on "Accept" for confirmation.



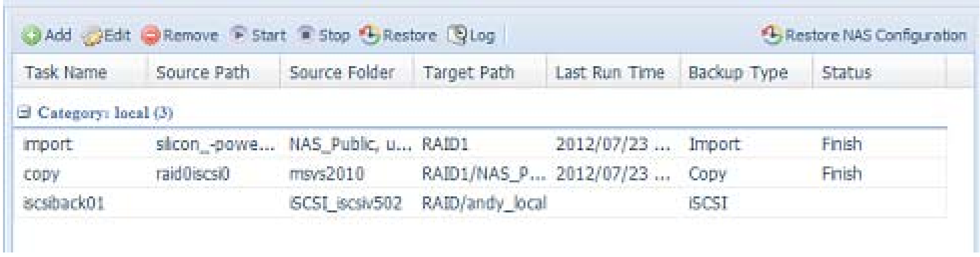
Local Backup > Copy > RAID Folder to External Device

Announce

1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.

☑ Accept

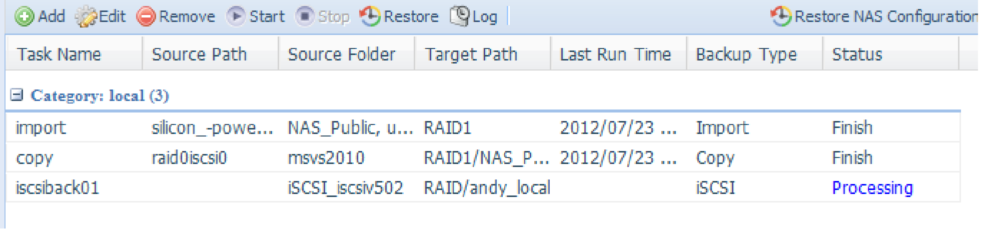
task list will have created task listed. To start the iSCSI volume backup, select the task and click "Start" from task bar.



⊟ Category: local (3)

Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
import	silicon_-powe...	NAS_Public, u...	RAID1	2012/07/23 ...	Import	Finish
copy	raid0iscsi0	msvs2010	RAID1/NAS_P...	2012/07/23 ...	Copy	Finish
iscsiback01		iSCSI_iscsiv502	RAID/andy_local		iSCSI	

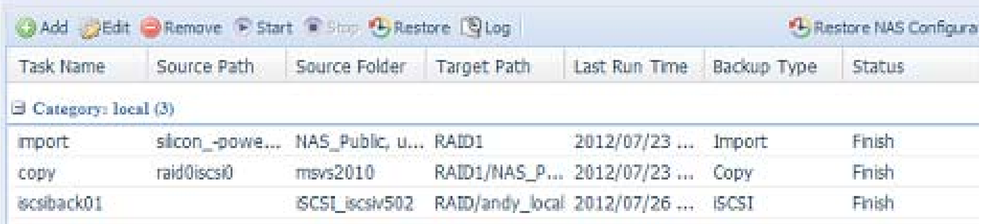
Once "Start" click, the associated iSCSI volume will not allow to I/O during backup processing. And the task status will change to 'Processing'.



⊟ Category: local (3)

Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
import	silicon_-powe...	NAS_Public, u...	RAID1	2012/07/23 ...	Import	Finish
copy	raid0iscsi0	msvs2010	RAID1/NAS_P...	2012/07/23 ...	Copy	Finish
iscsiback01		iSCSI_iscsiv502	RAID/andy_local		iSCSI	Processing

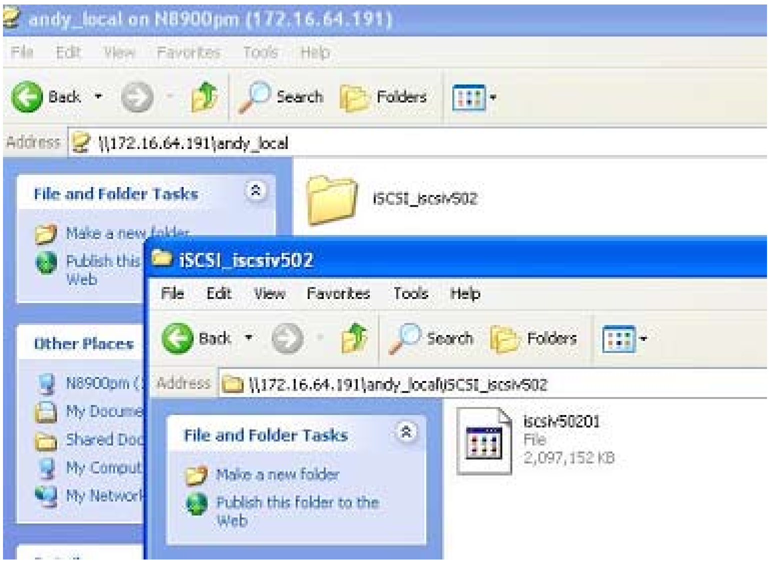
States change to "Finish" after task complete.



⊟ Category: local (3)

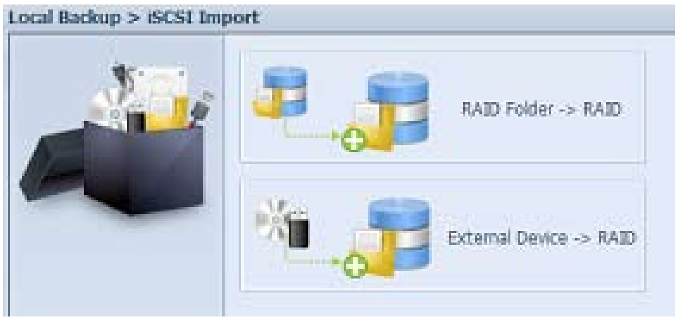
Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
import	silicon_-powe...	NAS_Public, u...	RAID1	2012/07/23 ...	Import	Finish
copy	raid0iscsi0	msvs2010	RAID1/NAS_P...	2012/07/23 ...	Copy	Finish
iscsiback01		iSCSI_iscsiv502	RAID/andy_local	2012/07/26 ...	iSCSI	Finish

From the RAID volume folder 'andy_local', it has backup iSCSI volume file stored. This backup iSCSI volume file is needed while it required import to storage. Next topic will describe about this.

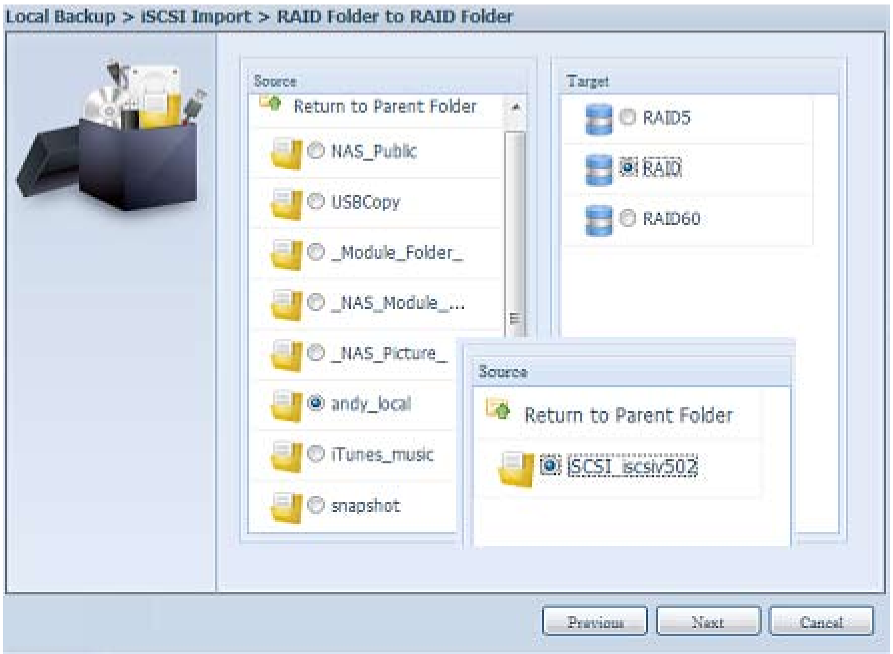


6. iSCSI Import: click on "iSCSI Import" and screen appear as below.

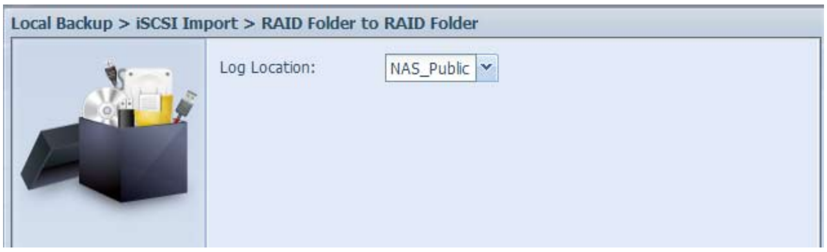
It can be imported from two different storage pools, folder to iSCSI or external device to iSCSI. It is depend on where iSCSI volume has backup to.



Let's take example to import "RAID folder to iSCSI" which is the iSCSI volume we have backup earlier to RAID volume folder andy_local than import to volume RAID.



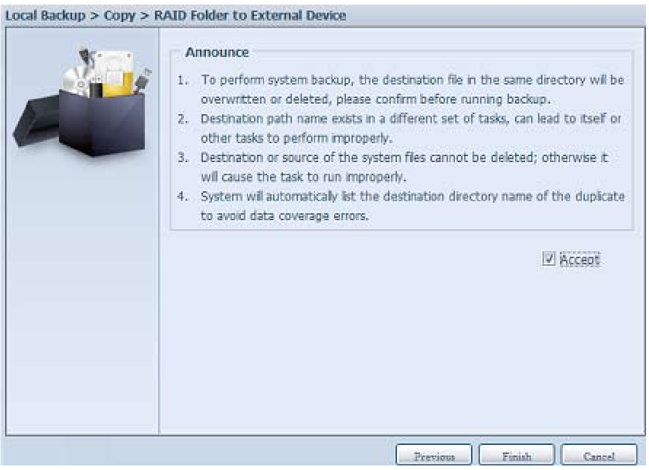
Next, provide where the task log will store.



Local Backup > iSCSI Import > RAID Folder to RAID Folder

Log Location: NAS_Public

Reading the note and check on "Accept" for confirmation.



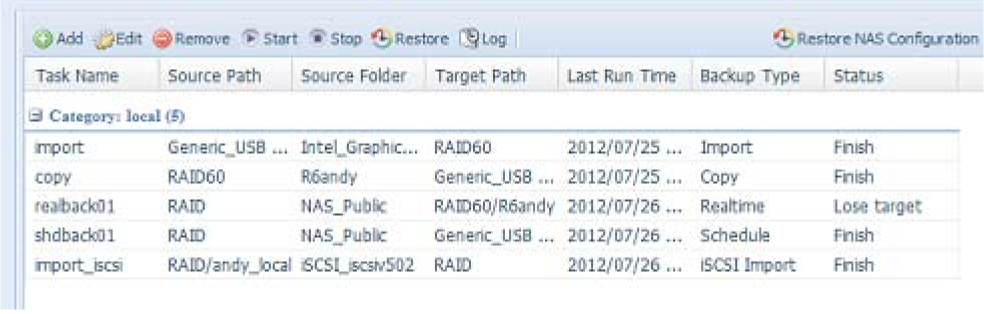
Local Backup > Copy > RAID Folder to External Device

Announce

1. To perform system backup, the destination file in the same directory will be overwritten or deleted, please confirm before running backup.
2. Destination path name exists in a different set of tasks, can lead to itself or other tasks to perform improperly.
3. Destination or source of the system files cannot be deleted; otherwise it will cause the task to run improperly.
4. System will automatically list the destination directory name of the duplicate to avoid data coverage errors.

☑ Accept

Now, from the data guard task list will have created task listed.



Category: local (5)

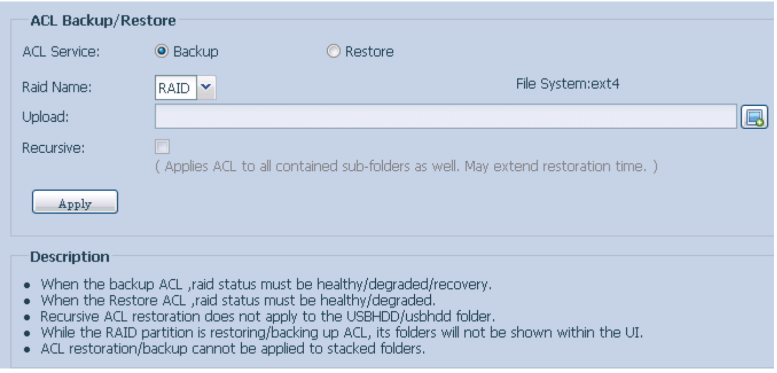
Task Name	Source Path	Source Folder	Target Path	Last Run Time	Backup Type	Status
import	Generic_USB ...	Intel_Graphic...	RAID60	2012/07/25 ...	Import	Finish
copy	RAID60	R6andy	Generic_USB ...	2012/07/25 ...	Copy	Finish
realback01	RAID	NAS_Public	RAID60/R6andy	2012/07/26 ...	Realtime	Lose target
shdback01	RAID	NAS_Public	Generic_USB ...	2012/07/26 ...	Schedule	Finish
import_iscsi	RAID/andy_local	iSCSI_iscsiv502	RAID	2012/07/26 ...	iSCSI Import	Finish

3.8.4 ACL Backup and Restore

The ACL backup and restore feature enables the system ACL (Access Control List) to be backed up on the RAID volume based to other location and restored if needed.

Let's look at the example bellow to see how it works.

We have one system with a RAID volume "RAID", select "Backup" to backup this RAID volume's ACL to other location. The current RAID volume "RAID" has share folder as listed on right hand screen shot.



ACL Backup/Restore

ACL Service: ● Backup ○ Restore

Raid Name: RAID File System:ext4

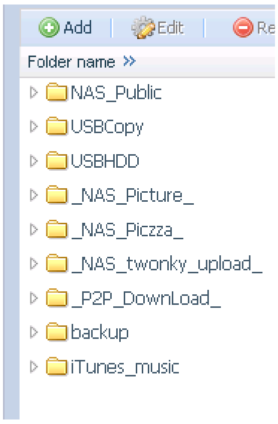
Upload:

Recursive: □ (Applies ACL to all contained sub-folders as well. May extend restoration time.)

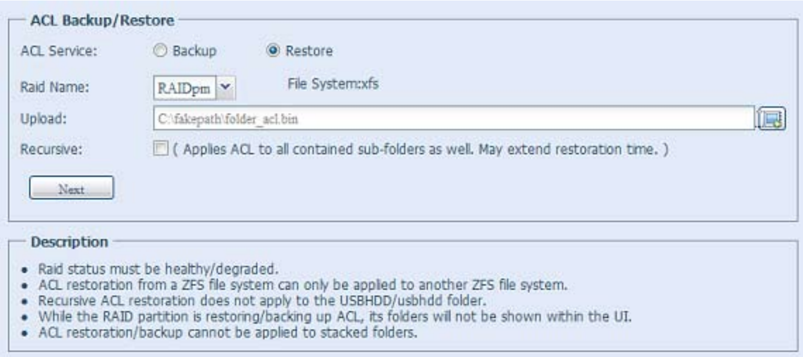
Apply

Description

- When the backup ACL ,raid status must be healthy/degraded/recovery.
- When the Restore ACL ,raid status must be healthy/degraded.
- Recursive ACL restoration does not apply to the USBHDD/usbhdd folder.
- While the RAID partition is restoring/backing up ACL, its folders will not be shown within the UI.
- ACL restoration/backup cannot be applied to stacked folders.



For the ACL restore, it can be restored in the same system or used in another unit. For example, let's restore the ACL backup file to another unit. This unit has a RAID volume "RAIDpm" with share folders as listed on right hand screen shot.



ACL Backup/Restore

ACL Service: ○ Backup ● Restore

Raid Name: RAIDpm File System:xfs

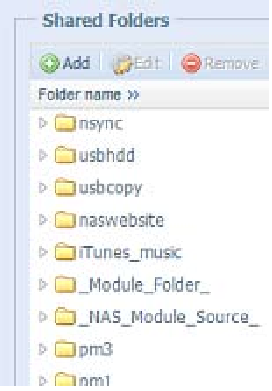
Upload: C:\fakepath\folder_acl.bin

Recursive: □ (Applies ACL to all contained sub-folders as well. May extend restoration time.)

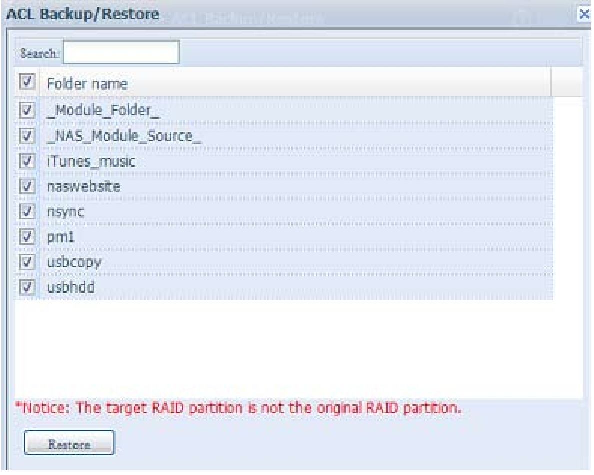
Next

Description

- Raid status must be healthy/degraded.
- ACL restoration from a ZFS file system can only be applied to another ZFS file system.
- Recursive ACL restoration does not apply to the USBHDD/usbhdd folder.
- While the RAID partition is restoring/backing up ACL, its folders will not be shown within the UI.
- ACL restoration/backup cannot be applied to stacked folders.



After inputting the ACL backup file and clicking the "Next" button, the system will show another screen to list the matched folders in between the backup file and this RAID volume. Just select the desired folders for the ACL restore.



ACL Backup/Restore

Search:

☑ Folder name
☑ _Module_Folder_
☑ _NAS_Module_Source_
☑ iTunes_music
☑ naswebsite
☑ nsync
☑ pm1
☑ usbcopy
☑ usbhdd

*Notice: The target RAID partition is not the original RAID partition.

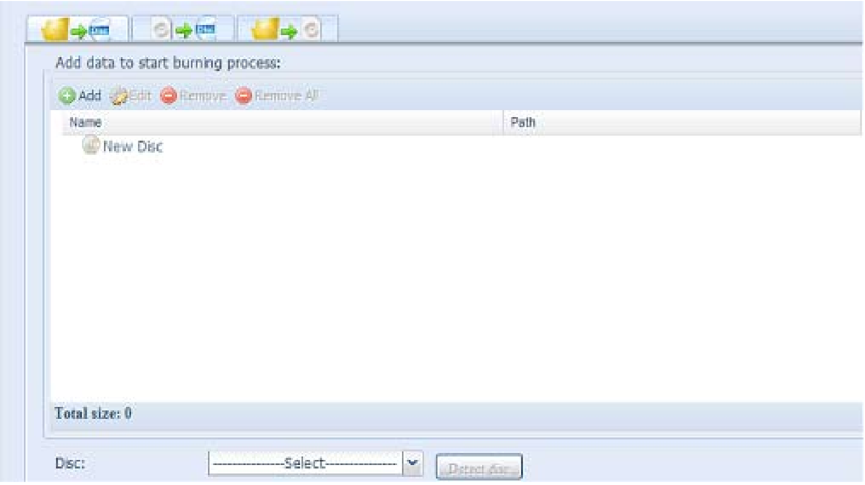
Restore

- The ACL backup will only back to share folder level; it does not apply to its sub-layer.
- If recursive has been checked during the ACL restoration, it will apply to all of its sub-folders with the same permission.

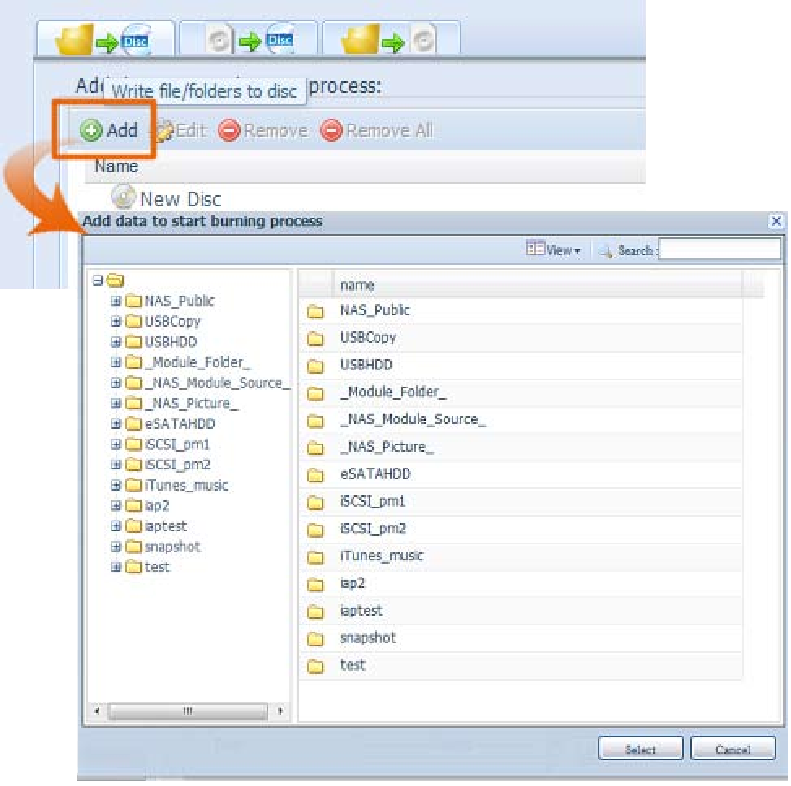
3.8.5 Data Burn

The data burn is featured to support 3 different modes of data burning for files/folders to and from image file and physical optical disk.

The 3 different modes are “Write Files/folders to disc”, “Write image to disk” and “Write files/folders to image”.

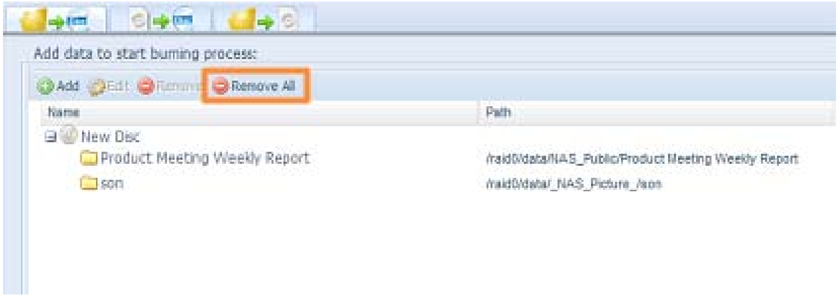

Add data to start burning process:
Add
Edit
Remove
Remove All
Name
Path
New Disc
Total size: 0
Disc:
---------------Select---------------
Detect disc

1. Write Files/folders to disc



a. Click the Add button and the NAS share list appears.

b. Select files/folders which you would like to burn. All of the selected folders/files will be seen under the disc label name “New Disc”. The disc label name can be changed by clicking on it and press “Edit” from menu bar. The selected folders/files also can be removed by clicking on them and then pressing “remove” or “remove all” for all selected items.

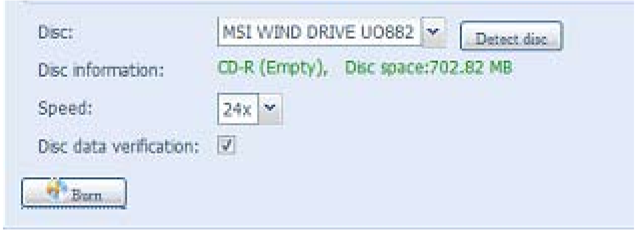


Add data to start burning process:

Name	Path
New Disc	
Product Meeting Weekly Report	/raid0/data/NAS_Public/Product Meeting Weekly Report
son	/raid0/data/_NAS_Picture_/son

c. Select from the installed USB burning devices. Please click the "detect disc" button to check the status once the disc is inserted.

d. Select the burning speed from the drop down list.



Disc: MSI WIND DRIVE UO882

Disc information: CD-R (Empty), Disc space:702.82 MB

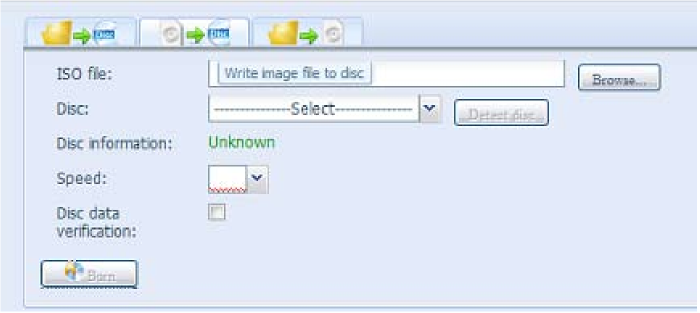
Speed: 24x

Disc data verification: ☑

e. Select whether disc data verification is required or not.

f. Click "Burn" to start disc burning.

2. Write image file to disc.



ISO file: Write image file to disc

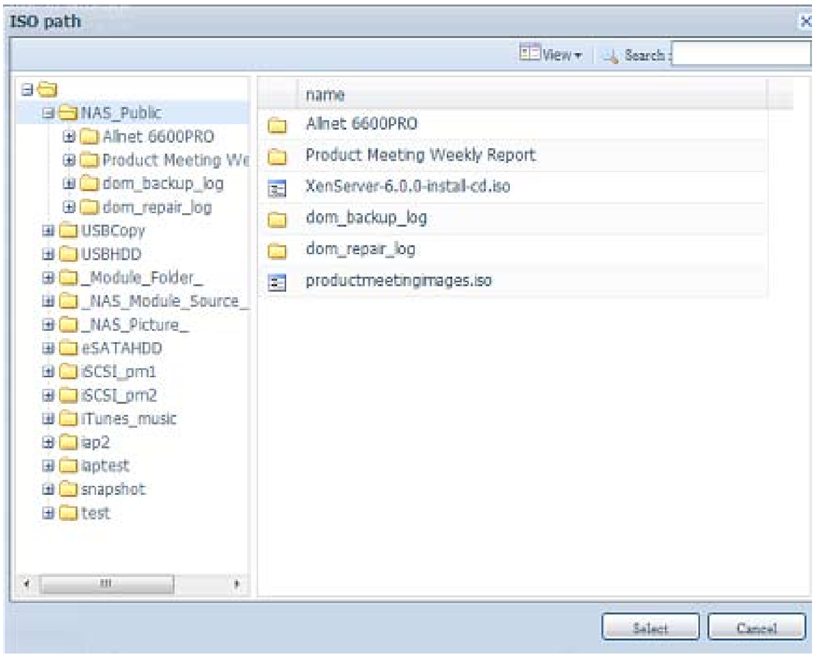
Disc: ---------------Select---------------

Disc information: Unknown

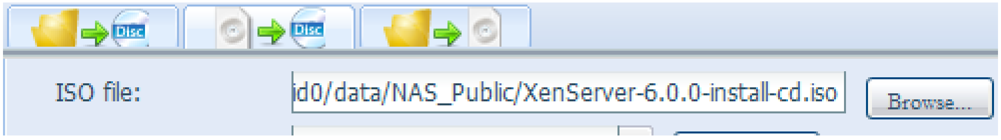
Speed:

Disc data verification: □

a. Click "Browser" and the NAS share list will appear to locate the desired image file to burn.



b. Select the ISO file.



ISO file: id0/data/NAS_Public/XenServer-6.0.0-install-cd.iso

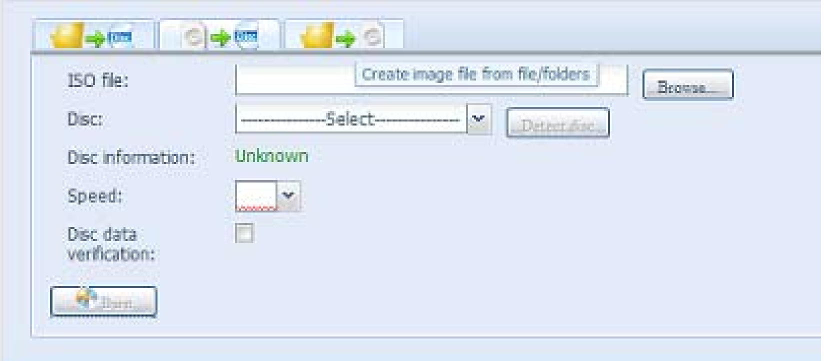
c. Select from the installed USB burning devices. Please click the "detect disc" button to check the status once the disc is inserted.

d. Select the burning speed from the drop down list.

e. Select whether disc data verification is required or not.

f. Click "Burn" to start disc burning.

3. Create image file from files/folders



ISO file:

Disc: ------------Select------------

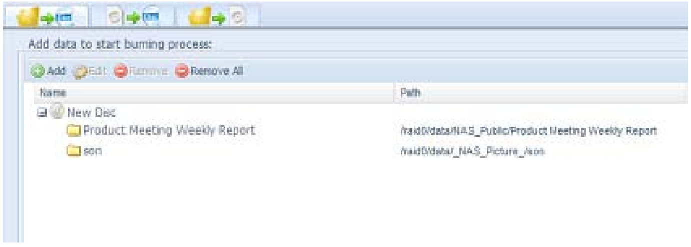
Disc information: Unknown

Speed:

Disc data verification: □

a. Click the Add button and the NAS share list will appear.

b. Select the files/folders which you would like to burn. All of the selected folders/files will appear under the disc label name "New Disc". The disc label name can be changed by clicking on it and pressing "Edit" from the menu bar. The selected folders/files also can be removed by clicking on them and pressing "remove" or "remove all" for all the selected items.



Add data to start burning process:

Name	Path
New Disc	
Product Meeting Weekly Report	/raid0/data/NAS_Public/Product Meeting Weekly Report
son	/raid0/data/_NAS_Picture_/son

c. Input the path where the ISO file is going to be stored, you can press the "Browse" button to have the share list appear.

d. Input the ISO file name for burned image file.

e. Click "Burn" to start the ISO file burning.

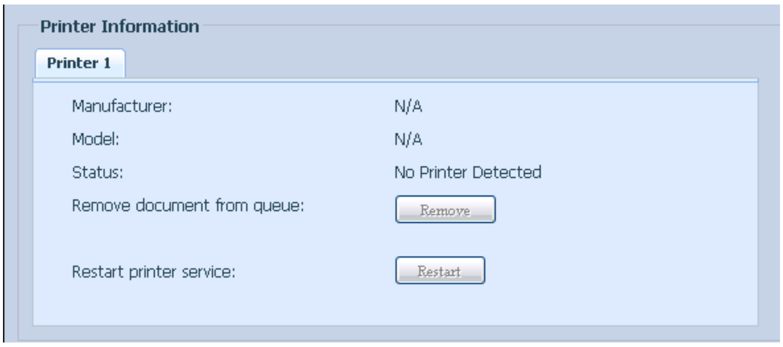
The data burn does not support rewriteable media if it has been burned with left space. On the other hand, the used rewriteable media will be erased first then carry on with burning.

3.9 External Devices

The Thecus IP storage supports printer server and UPS via USB interface. The integrated Print Server allows you to share a single USB printer with all users on the network. For the UPS, Thecus IP storage support via USB, Series and Network interface. The following section shows you how.

3.9.1 Printers

From the External Devices menu, choose the Printer item, and the Printer Information screen appears. This screen provides the following information about the USB printer connected to the USB port.



Manufacturer: N/A

Model: N/A

Status: No Printer Detected

Remove document from queue:

Restart printer service:

Printer Information	
Item	**Description**
Manufacturer	Displays the name of the USB printer manufacturer.
Model	Displays the model of the USB printer.
Status	Displays the status of the USB printer.
Remove document from Queue	Click to remove all documents from printer queue
Restart Printer service	Click to restart printer service

If a corrupt print job is sent to a printer, printing may suddenly fail. If your print jobs seem to be locked up, pressing the Remove All Documents button to clear the print queue may resolve the issue.

You can configure Thecus IP storage to act as a printer server. That way, all PCs connected to the network can utilize the same printer.

Windows XP SP2

To set up the Printer Server in Windows XP SP2, follow the steps below:

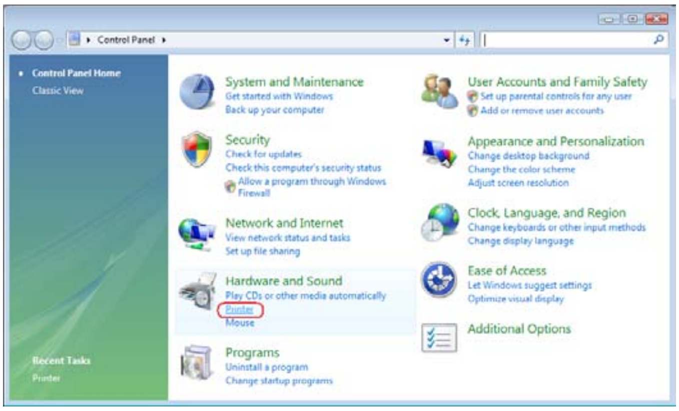
1. Connect the USB printer to one of the USB ports (preferably the rear USB ports; front USB ports can be used for external HDD enclosures).
2. Go to Start > Printers and Faxes.
3. Click on File > Add Printer.
4. The Add Printer Wizard appears on your screen. Click Next.
5. Select the "A network printer, or a printer attached to another computer" option.
6. Select "Connect to a printer on the Internet or on a home or office network", and enter "http:// Thecus IP storage IP_ADDRESS:631/printers/usb-printer" into the URL field.
7. Your Windows system will ask you to install drivers for your printer. Select the correct driver for your printer.
8. Your Windows system will ask you if you want to set this printer as "Default Printer". Select Yes and all your print jobs will be submitted to this printer by default. Click Next.
9. Click Finish.

Note that if a multi-function (all-in-one) printer is attached to the Thecus IP Storage, usually only the printing and fax functions will work. Other features, such as scanning, will probably not function.

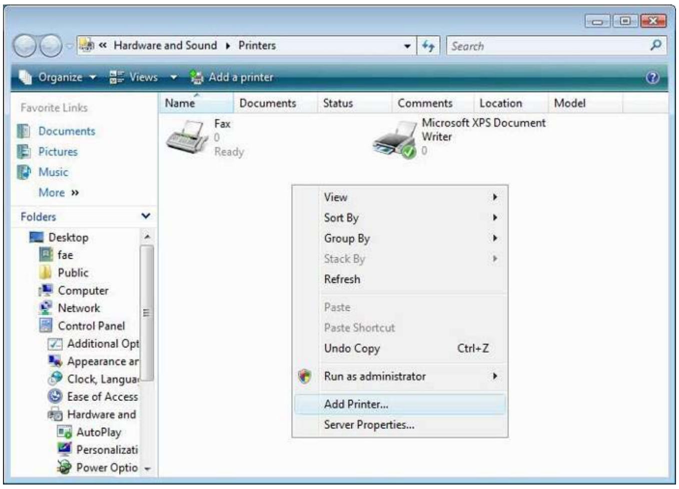
Windows Vista

To set up the Printer Server in Windows Vista, follow the steps below:

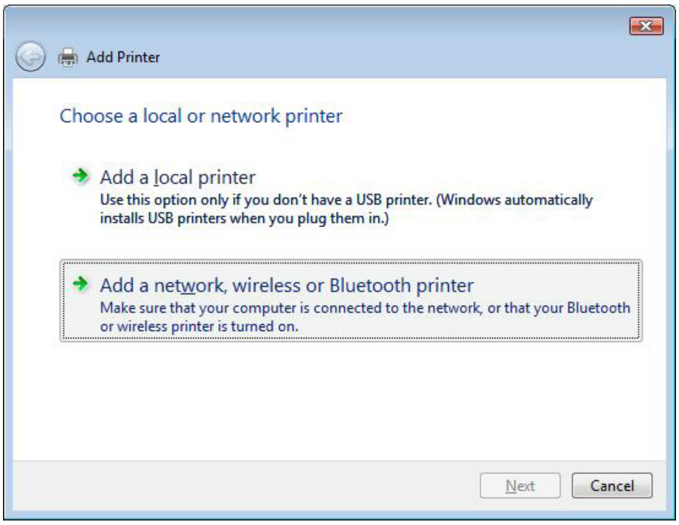
1. Open Printer Folder from the Control Panel.



2. Click the right mouse button in anywhere on the Printers folder and then select Add Printer.



3. Select Add a network, wireless or Bluetooth printer.



Choose a local or network printer

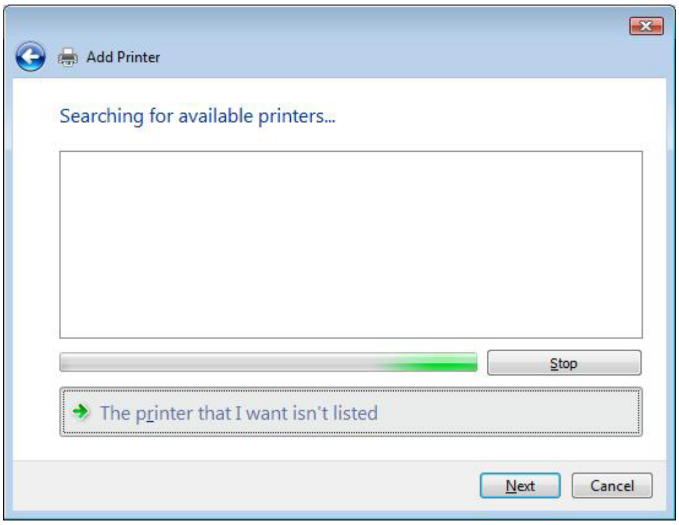
Add a local printer

Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer

Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

4. Select The printer that I want isn't listed.

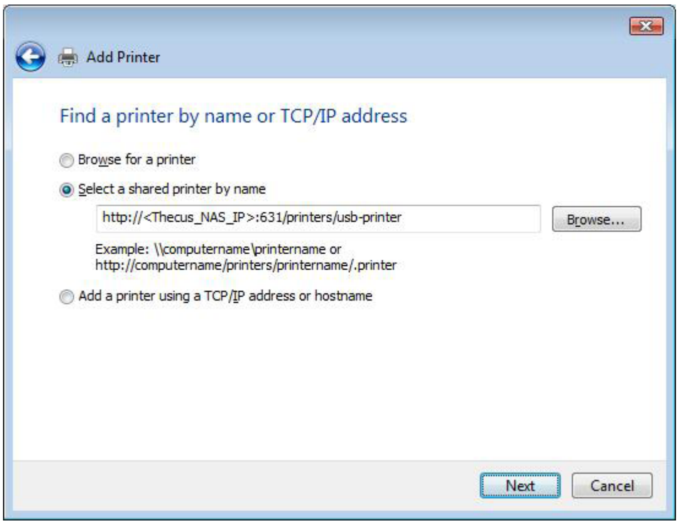


Searching for available printers...

The printer that I want isn't listed

You can press The printer that I want isn't listed to go into next page without waiting for Searching for available printers to finish.

5. Click Select a shared printer by name.



Add Printer

Find a printer by name or TCP/IP address

○ Browse for a printer

● Select a shared printer by name

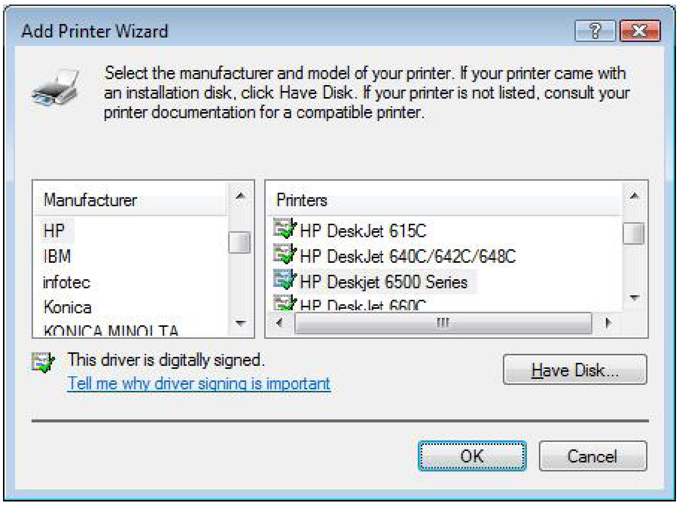
http://<Thecus_NAS_IP>:631/printers/usb-printer

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

Type http://<Thecus_NAS>:631/printers/usb-printer in the box, where <Thecus_NAS_IP> is the IP address of Thecus IP storage. Click Next.

6. Select or install a printer and then press OK.



Add Printer Wizard

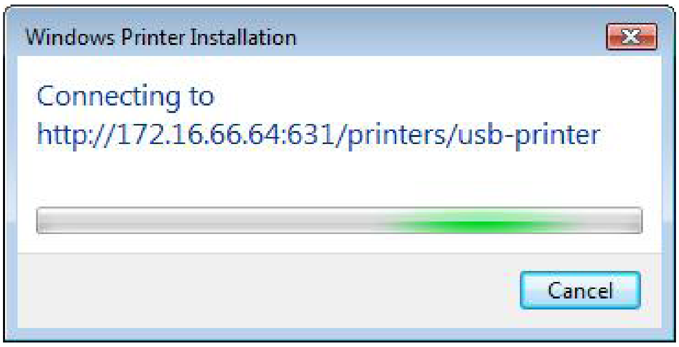
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer
HP
IBM
infotec
Konica
KONICA MINOLTA

Printers
HP DeskJet 615C
HP DeskJet 640C/642C/648C
HP Deskjet 6500 Series
HP DeskJet 660C

This driver is digitally signed.
Tell me why driver signing is important

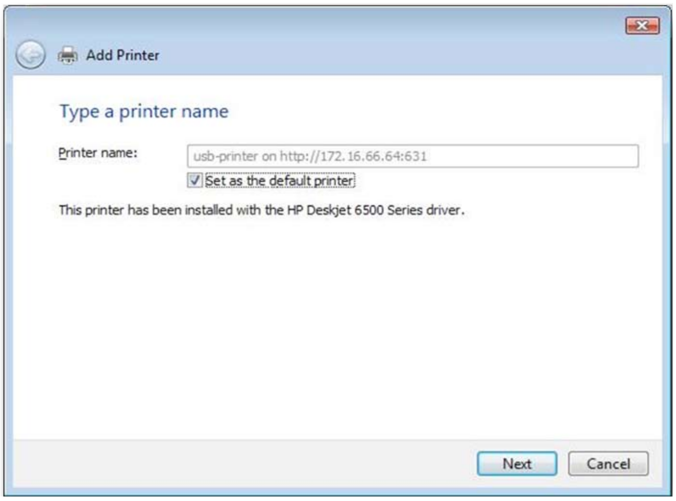
7. Windows will attempt to connect to the printer.



Windows Printer Installation

Connecting to
http://172.16.66.64:631/printers/usb-printer

8. You can choose to set this printer as the default printer by checking the Set as the default printer box. Click Next to continue.



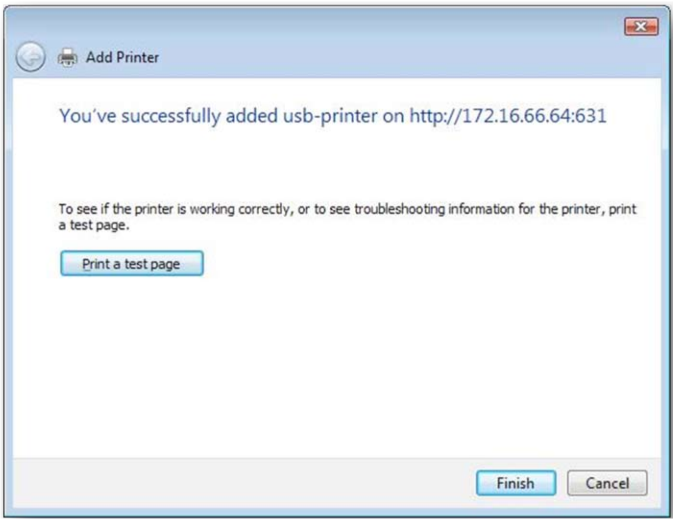
Type a printer name

Printer name: usb-printer on http://172.16.66.64:631

☑ Set as the default printer

This printer has been installed with the HP Deskjet 6500 Series driver.

9. Done! Click Finish.

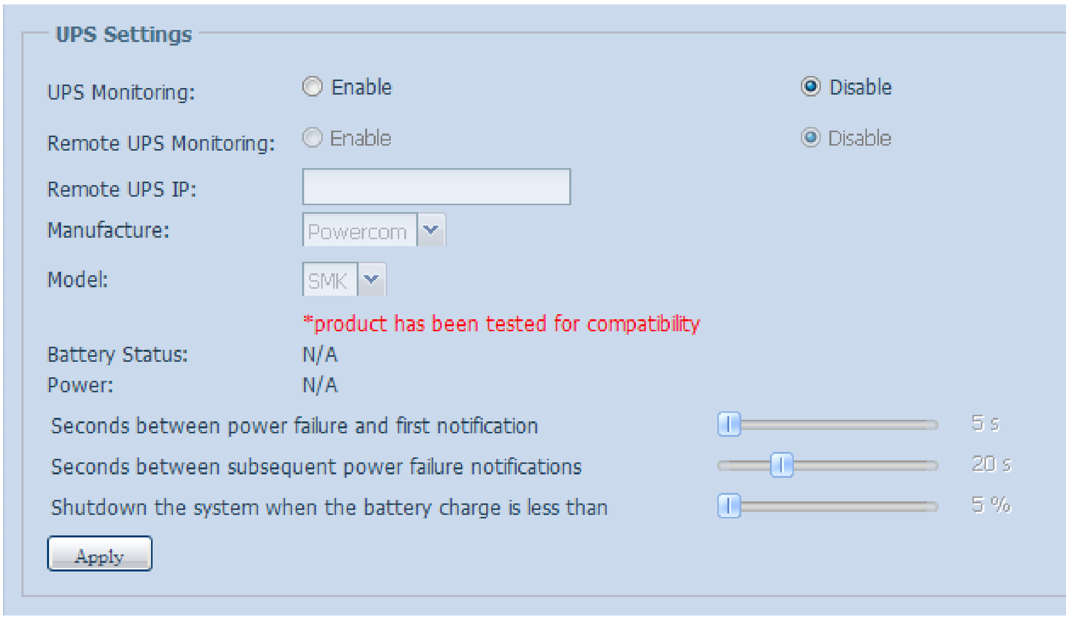


You've successfully added usb-printer on http://172.16.66.64:631

To see if the printer is working correctly, or to see troubleshooting information for the printer, print a test page.

3.9.2 Uninterrupted Power Source

From the External Devices menu, choose the Uninterrupted Power Source item and the UPS Setting screen appears. Make any changes you wish, and press Apply to confirm changes.



UPS Settings

UPS Monitoring: ○ Enable ● Disable

Remote UPS Monitoring: ○ Enable ● Disable

Remote UPS IP:

Manufacture: Powercom

Model: SMK

*product has been tested for compatibility

Battery Status: N/A

Power: N/A

Seconds between power failure and first notification 5 s

Seconds between subsequent power failure notifications 20 s

Shutdown the system when the battery charge is less than 5 %

See the following table for a detailed description of each item.

UPS Setting	
Item	**Description**
UPS Monitoring	Enable or disable UPS monitoring.
Remote UPS Monitoring	Enable or disable Remote UPS monitoring.
Remote UPS IP	Input the IP address of the NAS that the UPS device is connected to via USB or RS232.Input the IP address of your network UPS.
Manufacturer	Choose the UPS manufacturer from the dropdowns.
Model	Choose the UPS model number from the dropdowns.
Battery Status	Current status of the UPS battery
Power	Current status of the power being supplied to the UPS
Seconds between power failure and first notification	Delay between power failure and first notification in seconds.
Seconds between subsequent power failure notifications	Delay between subsequent notifications in seconds.
Shutdown the system when the battery charge is less than	Amount of UPS battery remaining before system should auto-shutdown.
Apply	Press ***Apply*** to save your changes.

❖ Appendix A: Customer Support

If you are still experiencing problems with your Thecus IP storage, or require a Return Merchandise Authorization (RMA), feel free to contact technical support via our Technical Support Website:

http://www.thecus.com/sp_tech.php

Customers in the US should send all technical support enquiries to the US contact window included in the following web page:

http://www.thecus.com/sp_tech.php

For Sales Information you can e-mail us at:

sales@thecus.com

Thank you for choosing Thecus!

❖ Appendix B: RAID Basics

• Overview

A Redundant Array of Independent Disks (RAID) is an array of several hard disks that provide data security and high performance. A RAID system accesses several hard disks simultaneously, which improves I/O performance over a single hard disk. Data security is enhanced by a RAID, since data loss due to a hard disk failure is minimized by regenerating redundant data from the other RAID hard disks.

• Benefits

RAID improves I/O performance, and increases data security through fault tolerance and redundant data storage.

• Improved Performance

RAID provides access to several hard disk drives simultaneously, which greatly increases I/O performance.

• Data Security

Hard disk drive failure unfortunately is a common occurrence. A RAID helps prevent against the loss of data due to hard disk failure. A RAID offers additional hard disk drives that can avert data loss from a hard disk drive failure. If a hard drive fails, the RAID volume can regenerate data from the data and parity stored on its other hard disk drives.

• RAID Levels

The Thecus IP storage supports standard RAID levels 0, 1, 5, 6, 10 and JBOD. You choose a RAID level when you create a system volume. The factors for selecting a RAID level are:

- Your requirements for performance
- Your need for data security
- Number of hard disk drives in the system, capacity of hard disk drives in the system

The following is a description of each RAID level:

RAID 0

RAID 0 is best suited for applications that need high bandwidth but do not require a high level of data security. The RAID 0 level provides the best performance of all the RAID levels, but it does not provide data redundancy.

RAID 0 uses disk striping and breaking up data into blocks to write across all hard drives in the volume. The system can then use multiple hard drives for faster read and write. The stripe size parameter that was set when the RAID was created determines the size of each block. No parity calculations complicate the write operation.

RAID 1

RAID 1 mirrors all data from one hard disk drive to a second one hard disk drive, thus providing complete data redundancy. However, the cost of data storage capacity is doubled.

This is excellent for complete data security.

RAID 5

RAID 5 offers data security and it is best suited for networks that perform many small I/O transactions at the same time, as well as applications that require data security such as office automation and online customer service. Use it also for applications with high read requests but low write requests.

RAID 5 includes disk striping at the byte level and parity information is written to several hard disk drives. If a hard disk fails the system uses parity stored on each of the other hard disks to recreate all missing information.

RAID 6

RAID 6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (dual parity)

Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain two simultaneous drive failures.

This is a perfect solution for mission critical applications.

RAID 10

RAID 10 is implemented as a striped array whose segments are RAID 1 arrays. RAID 10 has the same fault tolerance as RAID level 1.

RAID 10 has the same overhead for fault-tolerance as mirroring alone. High I/O rates are achieved by striping RAID 1 segments.

Under certain circumstances, RAID 10 array can sustain up to 2 simultaneous drive failures

Excellent solution for applications that would have otherwise gone with RAID 1 but need an additional performance boost.

JBOD

Although a concatenation of disks (also called JBOD, or "Just a Bunch of Disks") is not one of the numbered RAID levels, it is a popular method for combining multiple physical disk drives into a single virtual one. As the name implies, disks are merely concatenated together, end to beginning, so they appear to be a single large disk.

As the data on JBOD is not protected, one drive failure could result total data loss.

Stripe Size

The length of the data segments being written across multiple hard disks. Data is written in stripes across the multiple hard disks of a RAID. Since multiple disks are accessed at the same time, disk striping enhances performance. The stripes can vary in size.

Disk Usage

When all disks are of the same size, and used in RAID, Thecus IP storage disk usage percentage is listed below:

RAID Level	Percentage Used
RAID 0	100%
RAID 1	1/n x 100%
RAID 5	(n-1)/n x 100%
RAID 6	(n-2)/n x 100%
RAID 10	50%
JBOD	100%

n: HDD number

❖ Appendix C: Active Directory Basics

• Overview

With Windows 2000, Microsoft introduced Active Directory (ADS), which is a large database/ information store. Prior to Active Directory the Windows OS could not store additional information in its domain database. Active Directory also solved the problem of locating resources; which previously relied on Network Neighborhood, and was slow. Managing users and groups were among other issues Active Directory solved.

• What is Active Directory?

Active Directory was built as a scalable, extensible directory service that was designed to meet corporate needs. A repository for storing user information, accounts, passwords, printers, computers, network information and other data, Microsoft calls Active Directory a "namespace" where names can be resolved.

ADS Benefits

ADS lets Thecus IP storage integrate itself with the existing ADS in an office environment. This means the Thecus IP storage is able to recognize your office users and passwords on the ADS server. Other major benefits ADS support provides include:

1. Easy integration of Thecus IP storage into the existing office IT infrastructure
   The Thecus IP storage acts as a member of the ADS. This feature significantly lowers the overhead of the system administrator. For example, corporate security policies and user privileges on an ADS server can be enforced automatically on Thecus IP storage.
2. Centralized user/password database
   The Thecus IP storage does not maintain its own copy of the user/password database. This avoids data inconsistency between Thecus IP storage and other servers. For example, without ADS support, an administrator might need to remove a specific user privilege on Thecus IP storage and each individual server. With ADS support, the change on an ADS server is known to all of its ADS members.

❖ Appendix D: Licensing Information

• Overview

This product included copyrighted third-party software licensed under the terms of GNU General Public License. Please see THE GNU General Public License for extra terms and conditions of this license.

Source Code Availability

Thecus Technology Corp. has exposed the full source code of the GPL licensed software. For more information on how you can obtain our source code, please visit our web site, http://www.thecus.com.

• Copyrights

- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- This product includes software developed by Mark Murray.
- This product includes software developed by Eric Young (eay@cryptsoft.com).
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
- This product includes PHP, freely available from (http://www.php.net/).
- This product includes software developed by the University of California, Berkeley and its contributors.
- This product includes software developed by Winning Strategies, Inc.
- This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).
- This product includes software developed by Softweyr LLC, the University of California, Berkeley, and its contributors.
- This product includes software developed by Bodo Moeller.
- This product includes software developed by Greg Roelofs and contributors for the book, "PNG: The Definitive Guide," published by O'Reilly and Associates.
- This product includes software developed by the NetBSD Foundation, Inc. and its contributors.
- This product includes software developed by Yen Yen Lim and North Dakota State University.
- This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.
- This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.
- This product includes software developed by the Nick Simicich.
- This product includes software written by Tim Hudson (tjh@cryptsoft.com).
- This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

• CGIC License Terms

Basic License

CGIC, copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Thomas Boutell and Boutell.Com, Inc.

Permission is granted to use CGIC in any application, commercial or noncommercial, at no cost. HOWEVER, this copyright paragraph must appear on a "credits" page accessible in the public online and offline documentation of the program. Modified versions of the CGIC library should not be distributed without the attachment of a clear statement regarding the author of the modifications, and this notice may in no case be removed. Modifications may also be submitted to the author for inclusion in the main CGIC distribution.

GNU General Public License

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

• PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software

Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another Language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all de-

rivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS