USER AND MAINTENANCE GUIDE

CS3160 Cloud Storage Node

Doc. Rev. 1.2

POSSIBILITIES START HERE kontron

CS3160 CLOUD STORAGE NODE - USER AND MAINTENANCE GUIDE

Disclaimer

Kontron would like to point out that the information contained in this manual may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the manual or any product characteristics set out in the manual. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this manual only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

Kontron Ag

Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
www.kontron.com

Revision History

Revision	Brief Description of Changes	Date of Issue
1.0	Initial Issue	2016-Sept-21
1.1	Added Safety Caution Messages	2016-Nov-02
1.2	Added Safety Caution Messages	2016-Dec-06

Customer Service

Visit our website at www.kontron.com.

Customer Comments

If you have any difficulties using this guide, discover an error, or just want to provide some feedback, please send a message to Kontron. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user guide on our website. Thank you

Symbols

The following symbols may be used in this manual

⚠DANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
⚠CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	NOTICE indicates a property damage message.
	Electric Shock! This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material. Please refer also to the "High-Voltage Safety Instructions" portion below in this section.
	ESD Sensitive Device! This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.
	HOT Surface! Do NOT touch! Allow to cool before servicing.
	This symbol indicates general information about the product and the user manual. This symbol also indicates detail information about the specific product configuration.
	This symbol precedes helpful hints and tips for daily use.

Table of Contents

List of Tables

List of Figures

Electrostatic Discharge

ESD Sensitive Device!

The CS3160 Storage is sensitive to electrostatic discharge (ESD). Users must take the appropriate precautions when handling ESD-sensitive devices.

Limited Warranty

Kontron grants the original purchaser of Kontron's products a TWO YEAR LIMITED HARDWARE WARRANTY as described in the following. However, no other warranties that may be granted or implied by anyone on behalf of Kontron are invalid unless the consumer has the express written consent of Kontron.

Kontron warrants their own products, excluding software, to be free from manufacturing and material defects for a period of 24 consecutive months from the date of purchase. This warranty is not transferable nor extendible to cover any other users or long- term storage of the product. It does not cover products which have been modified, altered or repaired by any other party than Kontron or their authorized agents. Furthermore, any product which has been, or is suspected of being damaged as a result of negligence, improper use, incorrect handling, servicing or maintenance, or which has been damaged as a result of excessive current/voltage or temperature, or which has had its serial number(s), any other markings or parts thereof altered, defaced or removed will also be excluded from this warranty.

If the customer's eligibility for warranty has not been voided, in the event of any claim, he may return the product at the earliest possible convenience to the original place of purchase, together with a copy of the original document of purchase, a full description of the application the product is used on and a description of the defect. Pack the product in such a way as to ensure safe transportation (see our safety instructions).

Kontron provides for repair or replacement of any part, assembly or sub-assembly at their own discretion, or to refund the original cost of purchase, if appropriate. In the event of repair, refunding or replacement of any part, the ownership of the removed or replaced parts reverts to Kontron, and the remaining part of the original guarantee, or any new guarantee to cover the repaired or replaced items, will be transferred to cover the new or repaired items. Any extensions to the original guarantee are considered gestures of goodwill, and will be defined in the "Repair Report" issued by Kontron with the repaired or replaced item.

Kontron will not accept liability for any further claims resulting directly or indirectly from any warranty claim, other than the above specified repair, replacement or refunding. In particular, all claims for damage to any system or process in which the product was employed, or any loss incurred as a result of the product not functioning at any given time, are excluded. The extent of Kontron liability to the customer shall not exceed the original purchase price of the item for which the claim exists.

Kontron issues no warranty or representation, either explicit or implicit, with respect to its products reliability, fitness, quality, marketability or ability to fulfill any particular application or purpose. As a result, the products are sold "as is," and the responsibility to ensure their suitability for any given task remains that of the purchaser. In no event will Kontron be liable for direct, indirect or consequential damages resulting from the use of our hardware or software products, or documentation, even if Kontron were advised of the possibility of such claims prior to the purchase of the product or during any period since the date of its purchase.

Please remember that no Kontron employee, dealer or agent is authorized to make any modification or addition to the above specified terms, either verbally or in any other form, written or electronically transmitted, without the company's consent.

Safety Warnings

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

NOTICE	Read this manual thoroughly before attempting to set up your CS3160.
NOTICE	Your CS3160 is a complicated electronic device. DO NOT attempt to repair it under any circumstances. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
NOTICE	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.
NOTICE	Your CS3160 can operate normally under temperatures between 5°C and 40°C, with relative humidity of 20% – 85%. Using the CS3160 under extreme environmental conditions could damage the unit.
⚠CAUTION	This unit usually has more than one power supply cord. Disconnect all power supply cords before servicing to avoid electric shock.
⚠CAUTION	Installation of this product must be in accordance with national wiring codes and conform to local regulations. Different types of line cord sets may be used for connections to the mains supply circuit and must comply with the electrical code requirements of the country of use.
⚠CAUTION	The AC power supply plug is intended to serve as a power disconnect device. The socket outlet must be installed near the equipment and must be easily accessible.
⚠CAUTION	Disconnect all power by turning off the power and unplugging the power cords before installing or removing a chassis or working near power supplies. Débranchez toute l'alimentation en mettant l'appareil hors tension et en débranchant les cordons d'alimentation avant d'installer ou de retirer un châssis ou de travailler près de sources d'alimentation.
NOTICE	Ensure that the CS3160 is provided with the correct supply voltage. Plugging the CS3160 to an incorrect power source could damage the unit.
NOTICE	Do NOT expose the CS3160 to dampness, dust, or corrosive liquids.
NOTICE	Do NOT place the CS3160 on any uneven surfaces.
NOTICE	DO NOT place the CS3160 in direct sunlight or expose it to other heat sources.

DO NOT use chemicals or aerosols to clean the CS3160. Unplug the power cord and all connected cables before cleaning.

NOTICE

DO NOT place any objects on the CS3160 or obstruct its ventilation slots to avoid overheating the unit.

⚠WARNING

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.

⚠WARNING

Risk of explosion if battery is replaced by an incorrect type.

Il y a risque d'explosion si la batterie est remplacée par une batterie de type incorrect.

Dispose of used batteries according to the instructions.

Mettre au rebut les batteries usagées conformément aux instructions.

1/ Introduction

1.1. Overview

Thank you for choosing the Kontron Storage - CS3160 Server. The CS3160 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 the CS3160 to take over file management functions, increase application and data sharing and provide faster data response.

The CS3160:

- Offers data mobility with a disk roaming feature that lets you swap working hard drives for use in other CS3160, securing the continuity of data in the event of hardware failure;
- Allows data consolidation and sharing between Windows (SMB/CIFS), UNIX/Linux, and Apple OS X environments;
- Is a user-friendly GUI that supports multiple languages.

1.2. Product Highlights

1.2.1. File Server

First and foremost, the CS3160 allows you to store and share files over an IP network. With a Network Attached Storage (NAS) device, you can centralize your files and share them easily over your network. With the easy-to-use web-based interface, users on your network can access these files in a snap.

To learn about the Web User Interface, go to Section 4.2.

1.2.2. FTP Server

With the built-in FTP Server, friends, clients, and customers can upload and download files to your CS3160 over the Internet with their favorite FTP programs. You can create user accounts so that only authorized users have access.

To set up the FTP Server, refer to Section 4.8.4.

1.2.3. iTunes Server

With the built-in iTunes server capability, the CS3160 enables digital music to be shared and played anywhere on the network!

To set up the iTunes Server, refer to Section 4.9.1.

1.2.4. Printer Server

With the CS3160 Printer Server, you can easily share an IPP printer with other PCs connected to your network.

To set up the Printer Server, refer to Section 4.11.1.

1.2.5. Multiple RAID

The CS3160 supports multiple RAID volumes on one system. So, you can create RAID 0 for your non-critical data, and create RAID 1,5,6,50 or 60 (depend on model) for mission-critical data. Create the RAID levels depending on your needs.

To configure RAID modes on the CS3160, refer to 4.6.2.

1.2.6. iSCSI Capability

The CS3160 is not only a file server, but it also supports iSCSI initiators. Your server can access the CS3160 as a direct-attached-storage over the LAN or Internet. There is no easier way to expand the capacity of your current application servers. All the storage needs can be centrally managed and deployed. This brings ultimate flexibility to users.

To set up an iSCSI volume, refer to 4.6.7.

1.2.7. Superior Power Management

The CS3160 supports schedule power on/off. With this feature, administrator can set at what time to turn on or off the system. This feature is a big plus for people who want to conserve energy. Wake-On-LAN enables administrator to remotely turn on the system without even leaving their own seat.

To schedule system on and off, refer to 4.4.4.

1.3. Package Contents

The CS3160 storage should contain the following common items:

- System Unit x1
- QIG (Quick Installation Guide) x1
- CD-Title (Acronis backup CD & Universal CD)
- Ethernet Cable x1
- Accessory bag x1
- HDD Compatibility list Card x1
- Multiple Languages Warranty Card x1
- Power cord x2

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

1.4. Front Panel

The Kontron CS3160 front panel has the device's controls, indicators, and hard disk trays:

Figure 1: Front panel

Figure 2: Front panel buttons, indicators and ports

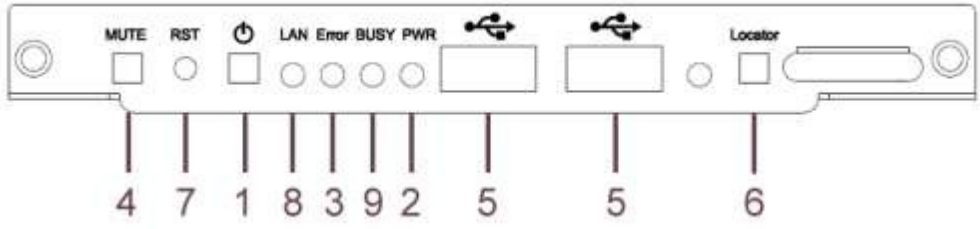


Table 1: Front panel

Item	Description
1. Power Button	Power on/off CS3160
2. Power LED	Solid green: System is power on.
3. System error LED	Solid RED: System error.
4. Mute button	Mute the system fan alarm.
5. USB Port	USB 2.0 port for compatible USB devices, such as USB disks and USB printers
6. Locator button / LED	Press the button, the back led will light up to identify the rack position of the system
7. RST	Reboot system.
8. LAN	Blinking green: network activity Solid green: network link
9. BUSY	Blinking orange: system startup or system maintenance; data currently inaccessible
10. LCD	Displays current system status and messages LCD screen saver will be enabled after screen is idle for more than 3 minutes LCD screen will be turn off after idle for more than 6 minutes
11. Up Button ▲	Push to scroll up when using the OLED display
12. Down Button ▼	Push to enter USB copy operation screen
13. Enter Button ↵☐	Push to enter OLED operate password for basic system setting
14. Escape Button ESC	Push to leave the current OLED menu

1.5. Rear Panel

The CS3160 rear panel features ports and connectors.

Figure 3: Rear panel

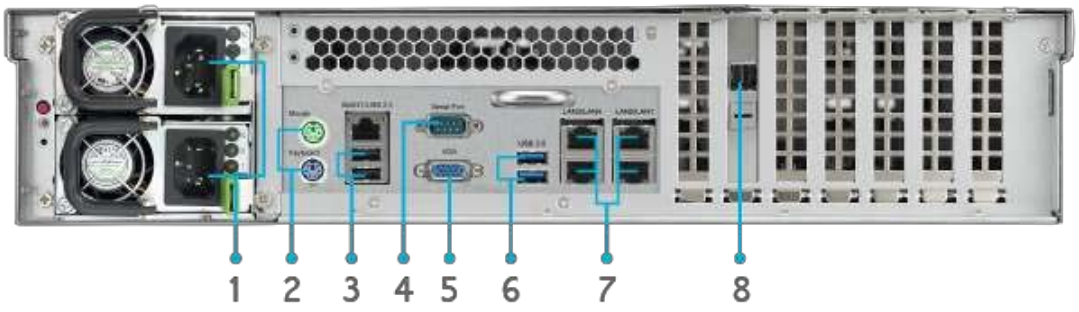


Table 2: Rear panel

Item	Description
1. Power Connector	Connect the included power cords to these connectors
2. PS/2 connector	The color-coded PS/2 connection ports (purple for keyboard and green for mouse)
3. USB Port	USB 2.0 port for compatible USB devices, such as USB disks, and USB printers
4. Serial Port	This port is for external UPS device
5. VGA Port	For Video out
6. USB Port	USB 3.0 port for compatible USB devices.
7. LAN1\LAN2\ LAN3\ LAN4 Port	LAN1\LAN2\ LAN3\ LAN4 port for connecting to an Ethernet network through a switch or router
8. SFF-8644 SAS Wide Port	Support Capacity expansion via Kontron JBOD device

2/ Hardware Installation

2.1. Overview

Your CS3160 is designed for easy installation. To help you get started, the following chapter will help you quickly get your CS3160 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:

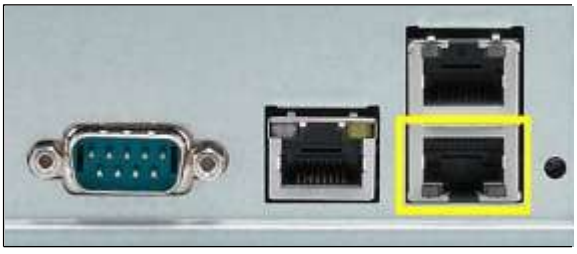
1. Read and understand the Safety Warnings outlined in the beginning of the manual.
2. If possible, wear an anti-static wrist strap during installation to prevent static discharge from damaging the sensitive electronic components on the CS3160.
3. Be careful not to use magnetized screwdrivers around the electronic components of the CS3160.

2.3. Cable Connections

To connect the CS3160 to your network, follow the steps below:

1. Connect an Ethernet cable from your network to the WAN/LAN1 port on the back panel of the CS3160.

Figure 4: CS3160 WAN/LAN1 port

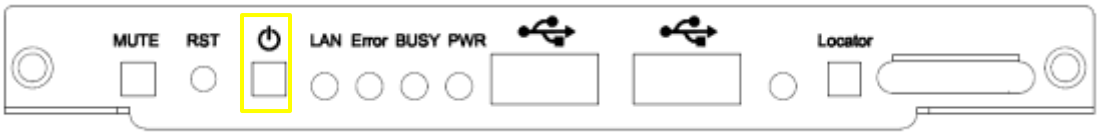


2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket.

Figure 5: CS3160 power socket

3. Press the power button on the Front Panel to boot up the CS3160.

Figure 6: CS3160 power button



3/ First Time Setup

3.1. Overview

Once the hardware is installed, physically connected to your network, and powered on, you can configure the CS3160 so that it is accessible to your network users. There are two ways to set up your CS3160: using the Thecus Setup Wizard or the LCD display. Follow the steps below for initial software setup.

3.2. Thecus Setup Wizard

The handy Thecus Setup Wizard makes configuring the CS3160 a snap. To configure the CS3160 using the Setup Wizard, perform the following steps:

1. Insert the installation CD into your CD-ROM drive (the host PC must be connected to the network).
2. The Setup Wizard should launch automatically. If not, please browse your CD-ROM drive and double click on Setup.exe.

Figure 7: Setup wizard

For MAC OS X users, double click on Thecus Setup Wizard .dmg file.

3. The Setup Wizard will start and automatically detect all CS3160 devices on your network. If none are found, please check your connection and refer to Chapter 6/ for assistance.

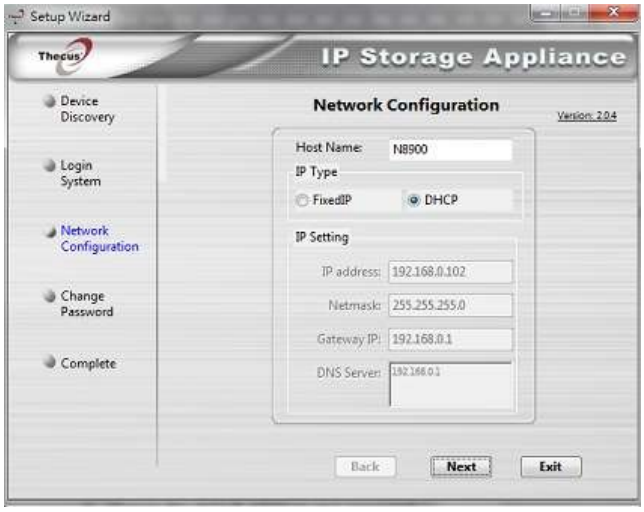
Figure 8: Device selection

4. Select the CS3160 that you like to configure.
5. Login with the administrator account and password. The default account and password are both “admin”.

Figure 9: Login screen

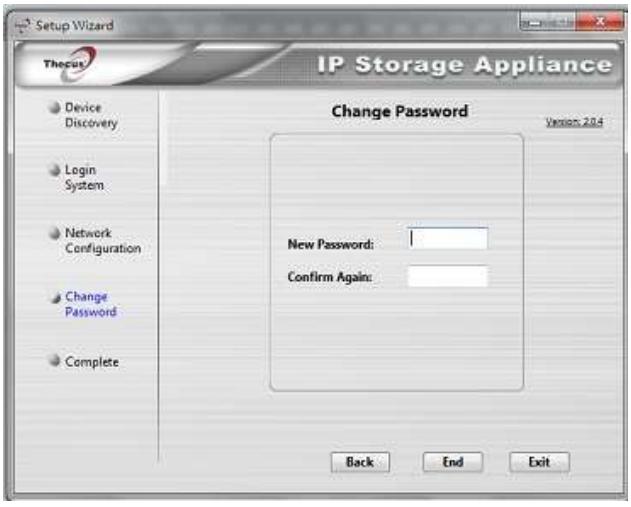
6. Name your CS3160 and configure the network IP address. If your switch or router is configured as a DHCP Server, configuring the CS3160 to automatically obtain an IP address is recommended. You may also use a static IP address and enter the DNS Server address manually.

Figure 10: Network configuration



7. Change the default administrator password.

Figure 11: Password change



8. Finished! Access the CS3160 Web Administrator Interface by pressing the ***Start Browser*** button. You can also configure another CS3160 at this point by clicking the ***Setup Other Device*** button. Press ***Exit*** to exit the wizard.

Figure 12: Setup complete

The Thecus Setup Wizard is designed for installation on systems running Windows XP/2000/vista/7 or Mac OSX or later. Users with other operating systems will need to install the Thecus Setup Wizard on a host machine with one of these operating systems before using the unit.

3.3. LCD Operation

The CS3160 storage is equipped with an LCD on the front for easy status display and setup. There are four buttons on the front panel to control the LCD functions.

3.3.1. LCD Controls

Use the **Up** (▲), **Down** (▼), **Enter** (↵) and **Escape** (**ESC**) keys to select various configuration settings and menu options for CS3160 configuration.

The following table illustrates the keys on the front control panel:

Table 3: LCD controls

Icon	Function	Description
▲	Up Button	Select the previous configuration settings option.
▼	Down Button	USB copy confirmation display.
↵	Enter	Enter the selected menu option, sub-menu, or parameter setting.
ESC	Escape	Escape and return to the previous menu.

There are two modes of operation for the LCD: **Display Mode** and **Management Mode**.

3.3.2. Display Mode

During normal operation, the LCD will be in **Display Mode**.

Table 4: Display mode

Item	Description
Host Name	Current host name of the system.
WAN/LAN1	Current WAN/LAN1 IP setting.
LAN2	Current LAN2 IP setting.
Link Aggregation	Current Link Aggregation status
System Fan1	Current system fan1 status.
System Fan2	Current system fan2 status.
CPU Fan	Current CPU fan status
2009/05/22 12:00	Current system time.
Disk Info	Current status of disk slot has been installed
RAID	Current RAID status.

The CS3160 will rotate these messages every one-two seconds on the LCD display.

3.3.3. USB Copy

The USB Copy function enables you to copy files stored on USB devices such as USB disks and digital cameras to the CS3160 by press button. To use USB copy, follow the steps below:

1. Plug your USB device into an available USB port on the Front end.
2. In **Display Mode**, press the **Down Button** (▼).
3. The LCD will display "**USB Copy?**"
4. Press **Enter** (↵) and the CS3160 will start copying USB disks connected to the front USB port.
5. All of data will be copied into system folder named "USB copy".

3.3.4. Management Mode

During setup and configuration, the LCD will be in **Management Mode**.

To enter into Management Mode, press **Enter (↵)** and an "*Enter Password*" prompt will show on the LCD.

At this time, the administrator has to enter the correct LCD password. System will check whether the correct LCD password has been entered. The default LCD password is "0000". If correct password is entered, you will enter into the **Management Mode** menu.

Table 5: Management mode

Item	Description
WAN/LAN1 Setting	IP address and netmask of your WAN/LAN1 ports.
LAN2 Setting	IP address and netmask of your LAN2 ports.
Link Agg. Setting	Select **Load Balance, 802.3ad** or **Failover**.
Change Admin Passwd	Change administrator's password for LCD operation.
Reset to Default	Reset system to factory defaults.
Exit	Exit **Management Mode** and return to **Display Mode**.

You can also change your LCD password using the Web Administration Interface by navigating to **System Management > Administrator Password**.

For more on the Web Administration Interface, see **Chapter 4/**.

3.4. USB Copy

The USB Copy function enables you to copy files stored on USB devices such as USB disks and digital cameras to the Kontron storage with a press of a button. To use USB copy, follow the steps below:

1. Plug your USB device into an available USB port on the Front Panel.
2. In **Display Mode**, press the **Enter** (↵).
3. The LCD will display "**USB Copy?**"
4. Press **Enter** (↵) and the Kontron storage will start copying USB disks connected to the front USB port. The LCD will display the USB copy progress and results.

3.5. Typical Setup Procedure

From the Web Administration Interface, you can begin to setup your CS3160 for use on your network. Setting up the CS3160 typically follows the five steps outlined below.

For more on how to use the Web Administration Interface, see Section 4.2.

3.5.1. Step 1: Network Setup

From the Web Administration Interface, you can configure the network settings of the CS3160 for your network. You can access the **Network** menu from the menu bar.

For details on how to configure your network settings, refer to Section 4.5.

3.5.2. Step 2: RAID Creation

Next, administrators can configure their preferred RAID setting and build their RAID volume. You can access RAID settings from the menu bar of the Web Administration Interface by navigating to **Storage Management > RAID Management**.

For more information on configuring RAID, see Section 4.6.2.

Don't know which RAID level to use? Find out more about the different RAID levels from Appendix B: RAID basics.

3.5.3. Step 3: Create Local Users or Setup Authentication

Once the RAID is ready, you can begin to create local users for the CS3160, or choose to setup authentication protocols such as Active Directory (AD).

For more on managing users, go to Section 4.7.

For more information on configuring Active Directory, see Section 4.7.1.

For information about the benefits of Active Directory, see Appendix D: Active Directory Basics.

3.5.4. Step 4: Create Folders and Set Up ACLs

Once users are introduced into your network, you can begin to create various folders on the CS3160 and control user access to each using Folder Access Control Lists.

More information on managing folders, see Section 4.6.5.

To find out about configuring Folder Access Control Lists, see Section 4.6.5.5.

3.5.5. Step 5: Start Services

Finally, you can start to setup the different services of the CS3160 for the users on your network. You can find out more about each of these services by clicking below:

- Samba / CIFS
- AFP (Apple Network Setup)
- NFS Setup)
- FTP
- iTunes® Server
- Printers

4/ System Administration

4.1. Overview

The CS3160 provides an easily accessible Web Administration Interface. With it, you can configure and monitor the CS3160 anywhere on the network.

4.2. Web Administration Interface

Make sure your network is connected to the Internet. To access the CS3160 Web Administration Interface:

1. Type the CS3160 IP address into your browser. (Default IP address is http://192.168.1.100)

Figure 13: Web administration interface

Your computer's network IP address must be on the same subnet as the CS3160. If the CS3160 has default IP address of 192.168.1.100, your managing PC IP address must be 192.168.1.x, where x is a number between 1 and 254, but not 100.

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

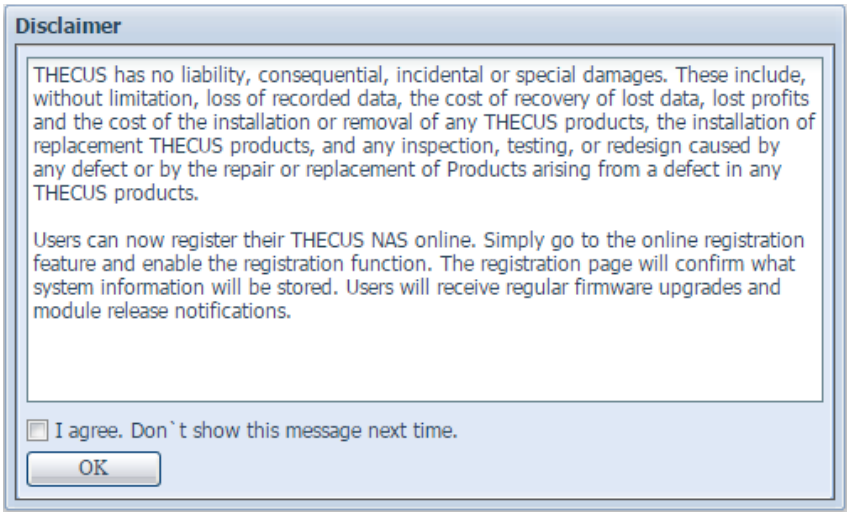
   User Name: admin

   Password: admin

   - If you changed your password in the setup wizard, use the new password.

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.

Figure 14: Disclaimer

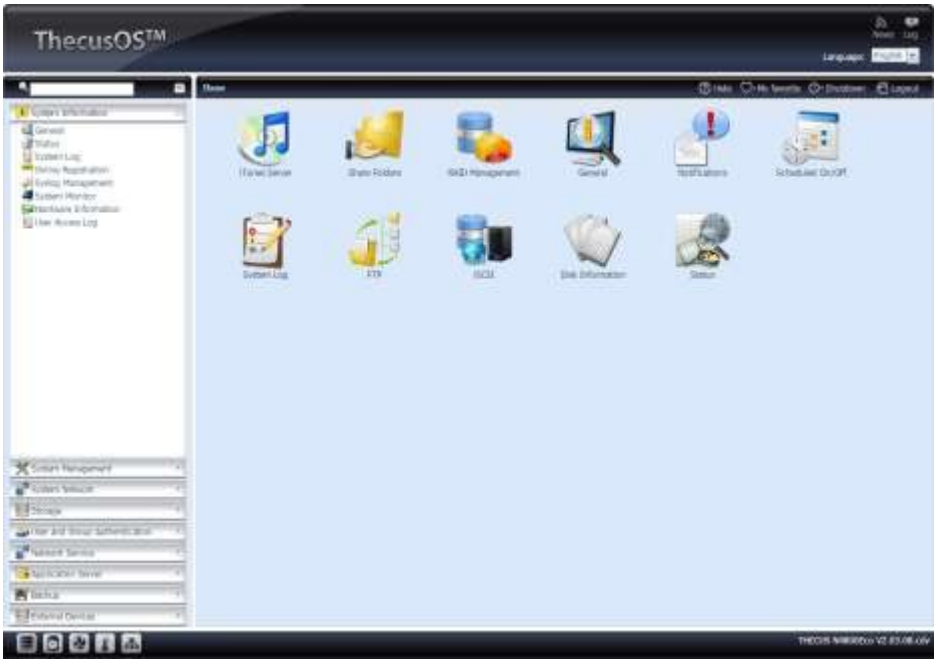


Following the disclaimer page, you will see the Web Administration Interface. From here, you can configure and monitor virtually every aspect of the CS3160 from anywhere on the network.

4.2.1. My Favorite

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

Figure 15: System favorite functions



Administrators can add or remove favorite functions to My Favorites by right clicking the mouse on the menu tree.

Another way the administrators can add favorite functions is by clicking the "Add Favorite" icon in each function screen. See the figure below with the red circled icon.

Figure 16: My favorite

To return to the favorite screen, simply click "Home" located at the left hand corner of the main screen.

Figure 17: Home

4.2.1.1. Menu Bar

The Menu Bar is where you will find all of the information screens and system settings of the CS3160. The various settings are placed in the following groups on the menu bar:

Figure 18: Menu bar

Table 6: Description of Menu bar items

Item	Description
System Information	Current system status of the CS3160.
System Management	Various CS3160 system settings and information.
System Network	Information and settings for network connections, as well as various services of the CS3160.
Storage	Information and settings for storage devices installed into the CS3160.

User and Group Authentication	Allows configuration of users and groups.
Network Service	Use the Network Service menu to make network service support settings.
Application Server	App and iTunes Server set-up of the CS3160.
Backup	Category of Backup Features setup of the CS3160.
External Devices	The CS3160 supports printer server and UPS via USB interface.

Moving your cursor over any of these items will display the dropdown menu selections for each group.

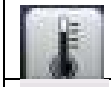
In the following sections, you will find detailed explanations of each function, and how to configure your CS3160.

4.2.1.2. Message Bar

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

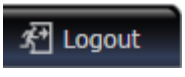
Figure 19: Message bar

Table 7: Message bar

Item	Status	Description
	RAID Information	Display the status of created RAID volume. Click to go to RAID information 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.
	FAN	Display system FAN Status. Click to go to System Status page as short cut.
	Temperature	Display system temperature, click to go to System Status page as shot cut.
	Network	Green: Connection to the network is normal. Red: abnormal connection to the network

4.2.2. Logout

Figure 20: Logout



Click to logout Web Administration Interface.

4.2.3. Language Selection

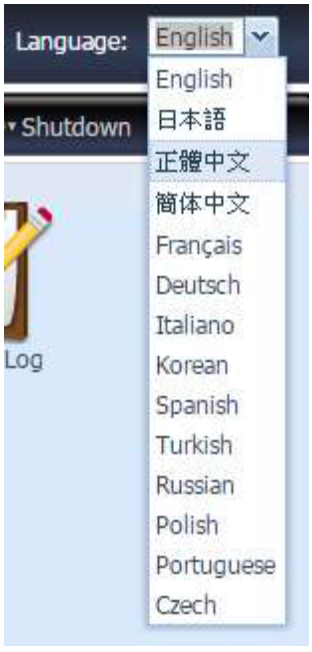
The CS3160 supports multiple Languages, including:

- English
- Japanese

- Traditional Chinese
- Simplified Chinese
- French
- German
- Italian
- Korean
- Spanish
- Turkish
- Russian
- Polish
- Portuguese
- Czech

On the menu bar, click **Language** and the selection list appears. This user interface will switch to the selected language for the CS3160.

Figure 21: Language selection



4.3. System Information

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

The menu bar allows you to see various aspects of the CS3160. From here, you can discover the status of the CS3160, and also other details.

4.3.1. General

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

Figure 22: System information

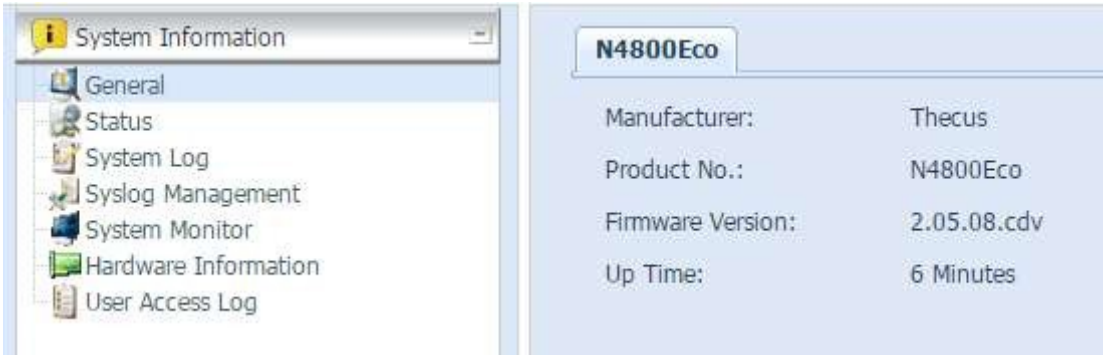


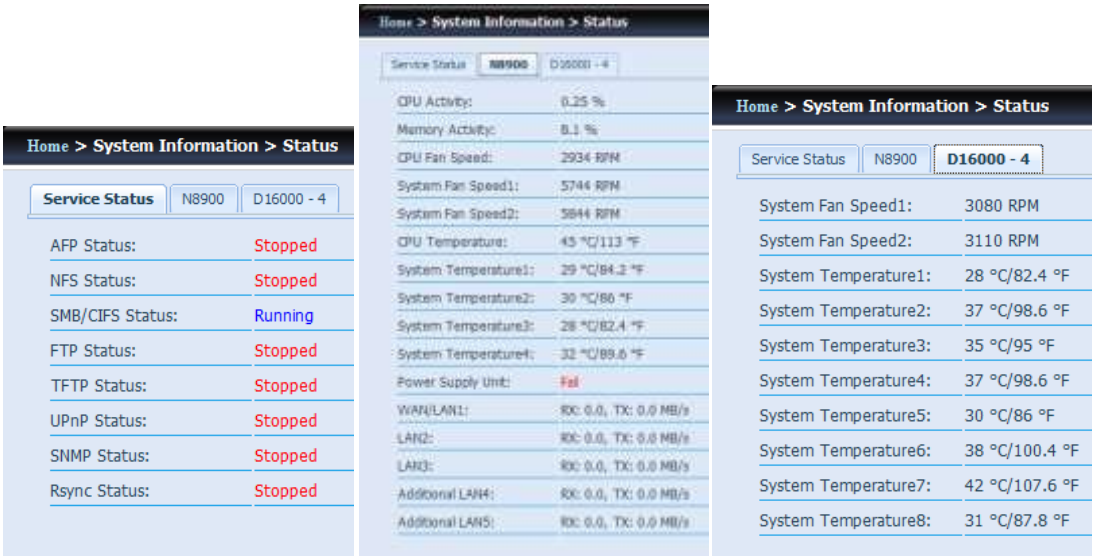
Table 8: System information

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.

4.3.2. Status

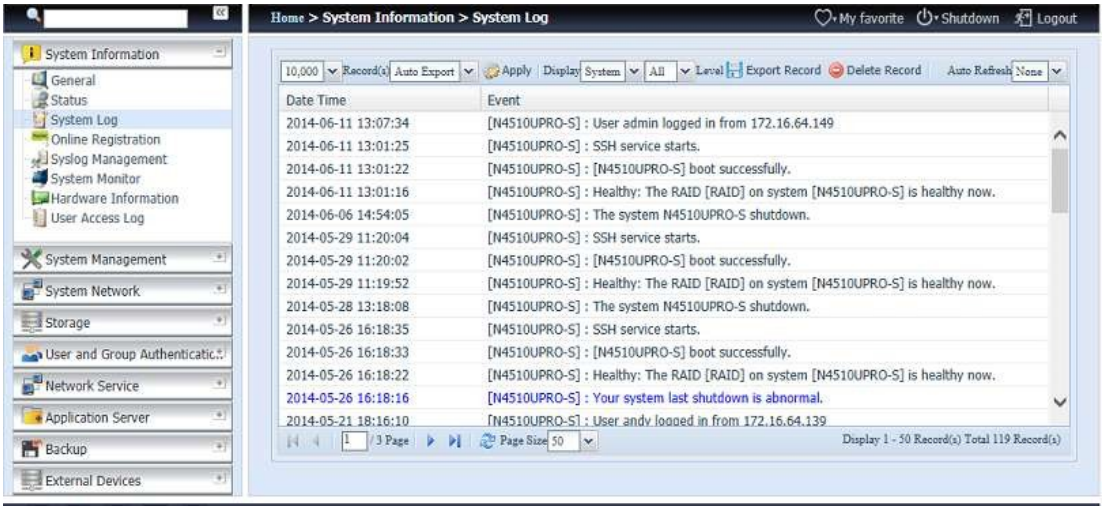
From the **System Information** menu, choose the **Status** item, **System Service Status** and HW Status screens appear. These screens provide basic system and service status information.

Figure 23: Status



4.3.3. Logs

Figure 24: Logs

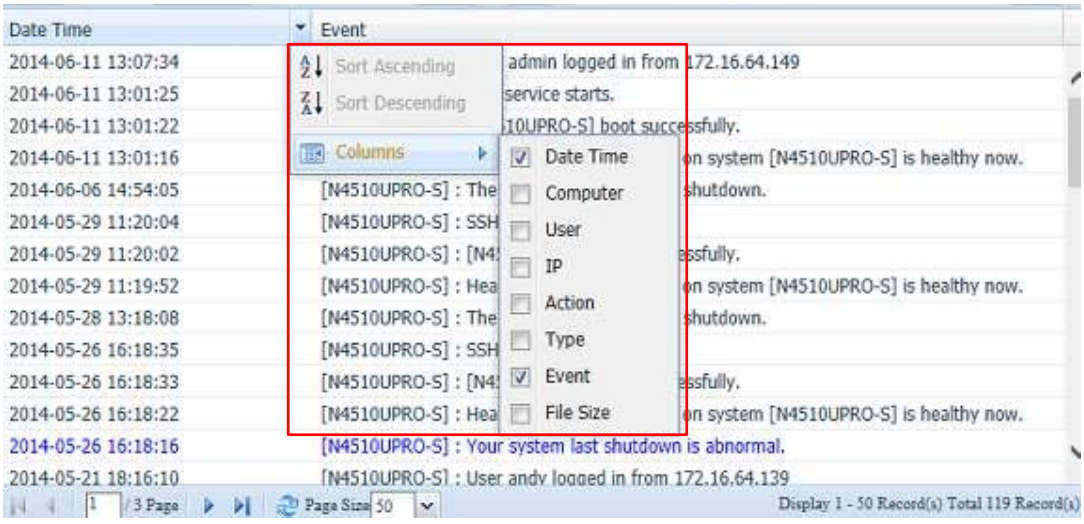


From the **System Information** menu, choose the **System Logs** option and the System Logs screen will appear. This screen shows a history of system usage and important events such as disk status, network information, and system booting.

Table 9: 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. WARNING: Shows only warning messages. ERROR: Shows only error messages.
Export Records	Export all logs to an external file.
Delete Records	Clear all log files.
Auto Refresh	Specify the auto refresh time interval.
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.

Figure 25: Columns



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

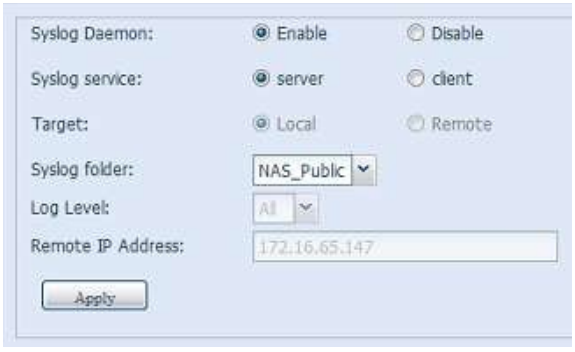
4.3.4. Syslog Management

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.

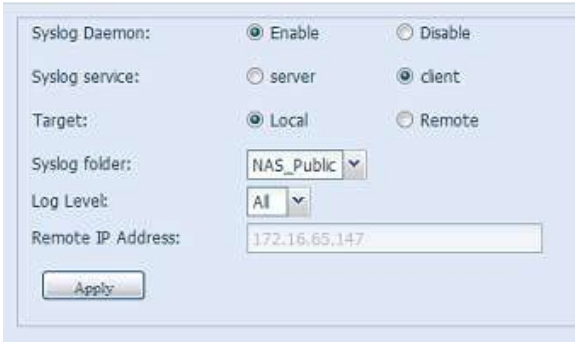
Configuration with syslog server:

Figure 26: Syslog server



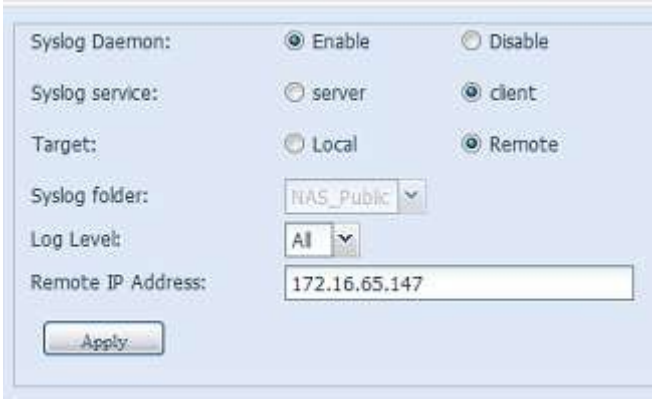
Configuration with syslog client and target to store locally:

Figure 27: Syslog client, target to store locally



Configuration with syslog client and target to store remotely:

Figure 28: Syslog client, target to store remotely



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

Table 10: Syslog

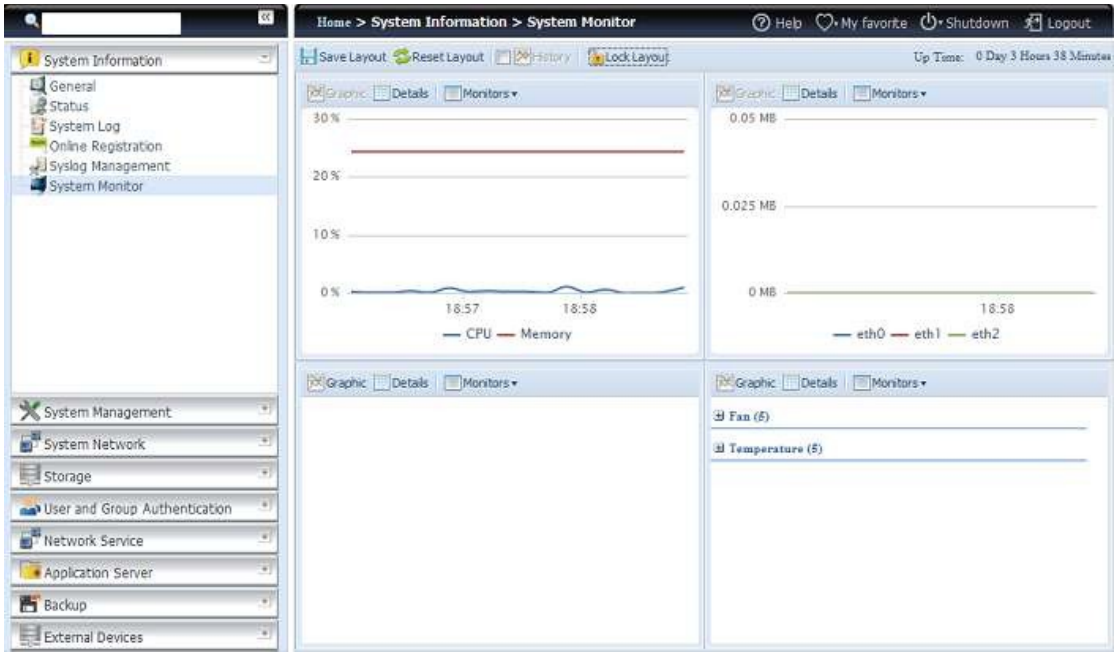
Item	Description
Syslog Daemon	Enable/Disable syslog daemon.
Syslog service	If Server has been selected then associated syslog folder will be used to store all system logs from other NAS devices which has assigned this system for syslog server as well as syslog of this server unit. It can be seen from 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 “messages” 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.

4.3.5. System Monitor

The system monitor is capable to monitor system status including CPU/memory utilization, fan/temperature status, 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.

Figure 29: System monitor

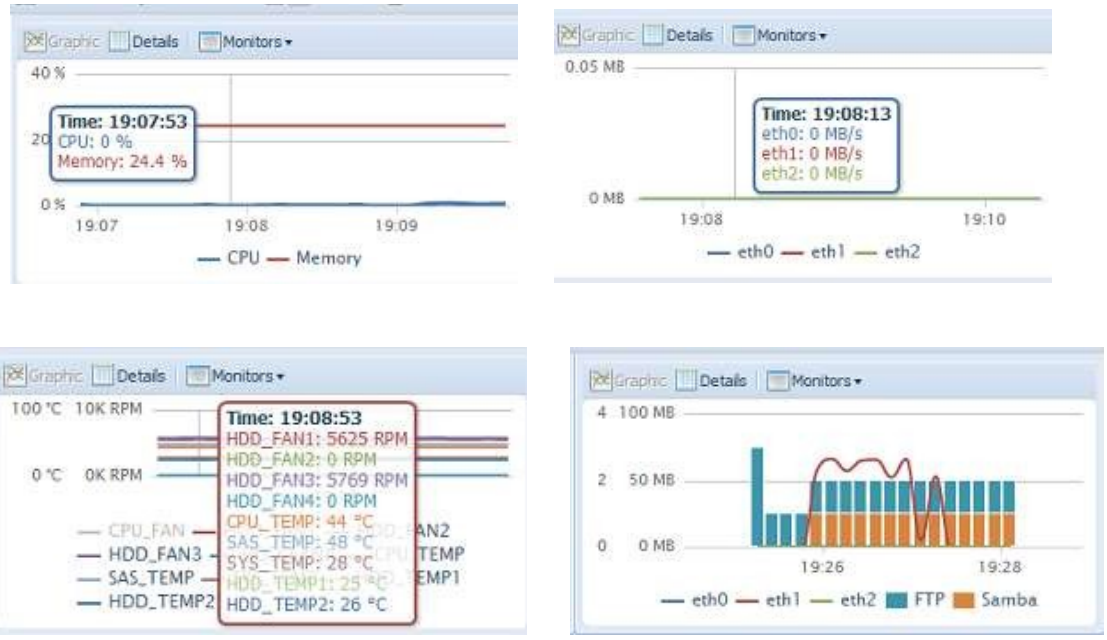


It is divided into 4 sections. Each section can be modified to monitor specific items by using the drop down list from the “Monitors” tab, simply click on the items you would like to monitor. From each section, you can also choose to display the information graphically by selecting “Graphic” or by plain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

Figure 30: Example



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

Figure 31: User list

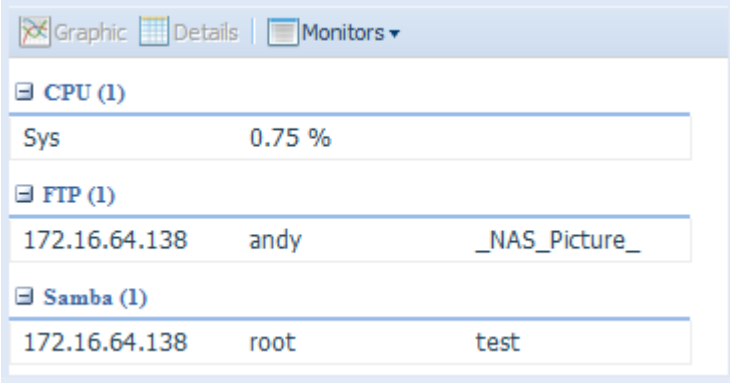


Table 11: System monitor

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 

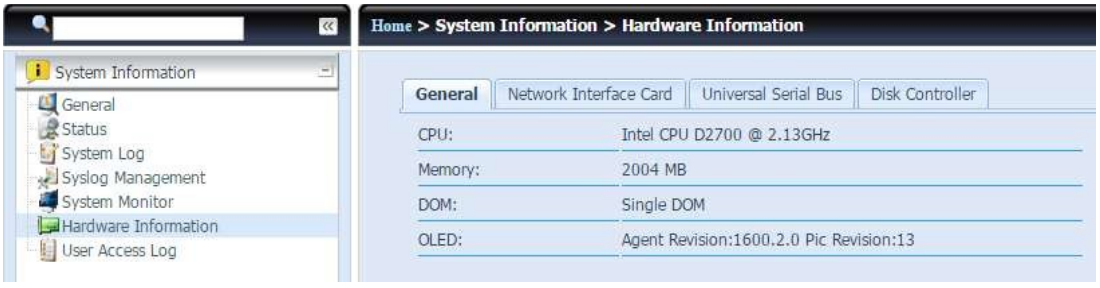
and system monitor will display the history with different period for selection.

Figure 32: History

4.3.6. Hardware Information

From the System Information category, choose the Hardware Information item and the system will display the related HW details for the associated model.

Figure 33: Hardware information



4.3.7. User Access Log

Figure 34: User access log

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

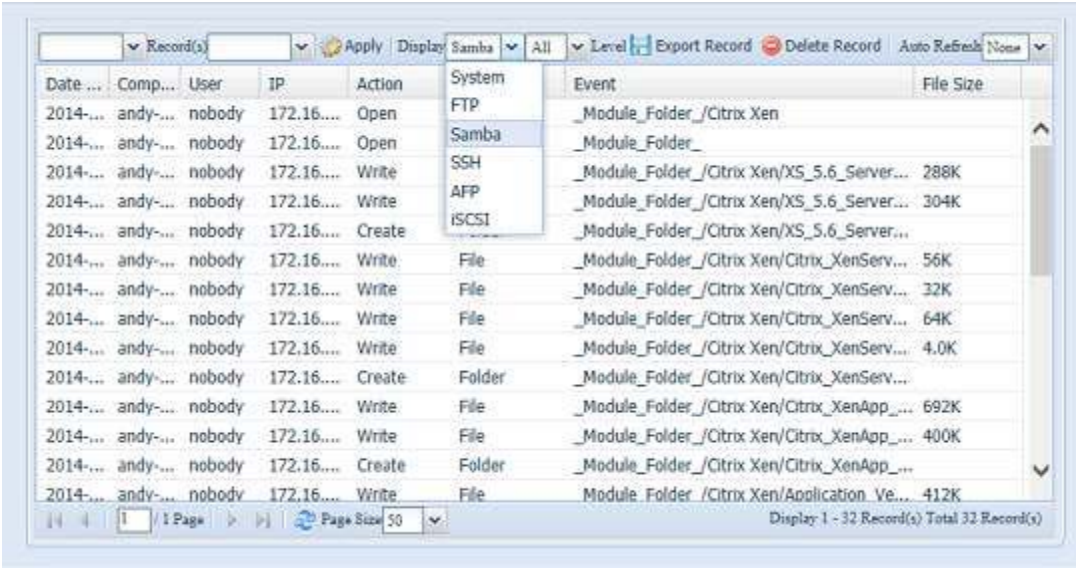
Table 12: User access log

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.

Figure 35: Display dropdown list



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.

Figure 36: Export step 1

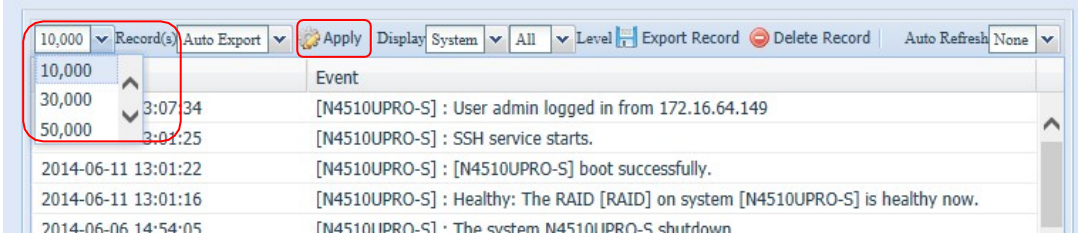
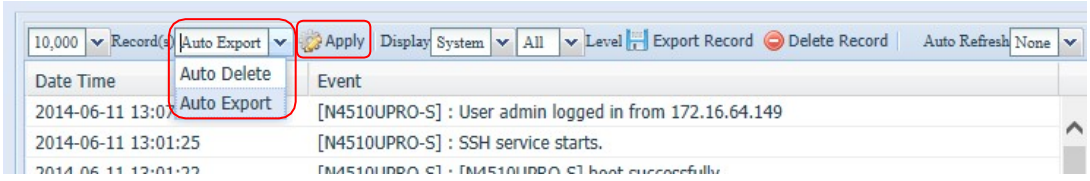
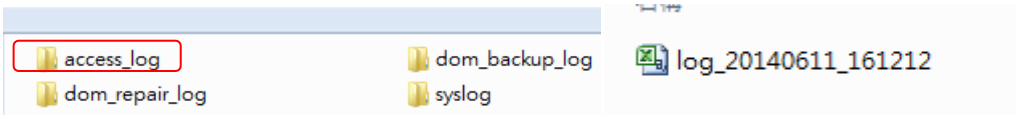


Figure 37: Export step 2



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

Figure 38: Log file



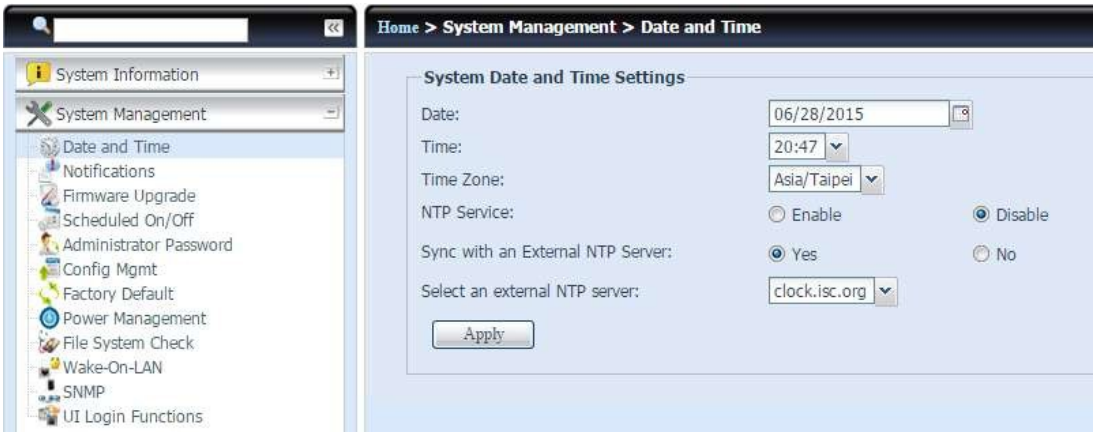
4.4. System Management

The System Management menu gives you a wealth of settings that you can use to configure your CS3160 system administration and functions. You can set up system time, system notifications, and even upgrade firmware from this menu.

4.4.1. Date and Time: Setting System Time

From the System Management menu, choose the Date and Time item and the System Date and Time Settings screen appears. Set the desired Date, Time, and Time Zone. You can also elect to synchronize the system time on the CS3160 with an NTP (Network Time Protocol) Server.

Figure 39: Setting system time



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

Table 13: 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 the CS3160 to synchronize with an NTP server of your choice.
Select an external NTP server	Choice an external NTP server.
Apply	Click Apply to save changes.

If an NTP server is selected, please make sure your CS3160 has been setup to access the NTP server.

4.4.2. Notification Configuration

From the System Management menu, choose the Notifications item, and the Notifications Configuration screen appears. This screen lets you have the CS3160 notify you in case of any system malfunction. Press Apply to confirm all settings. See following table for a detailed description of each item.

Figure 40: Notification configuration

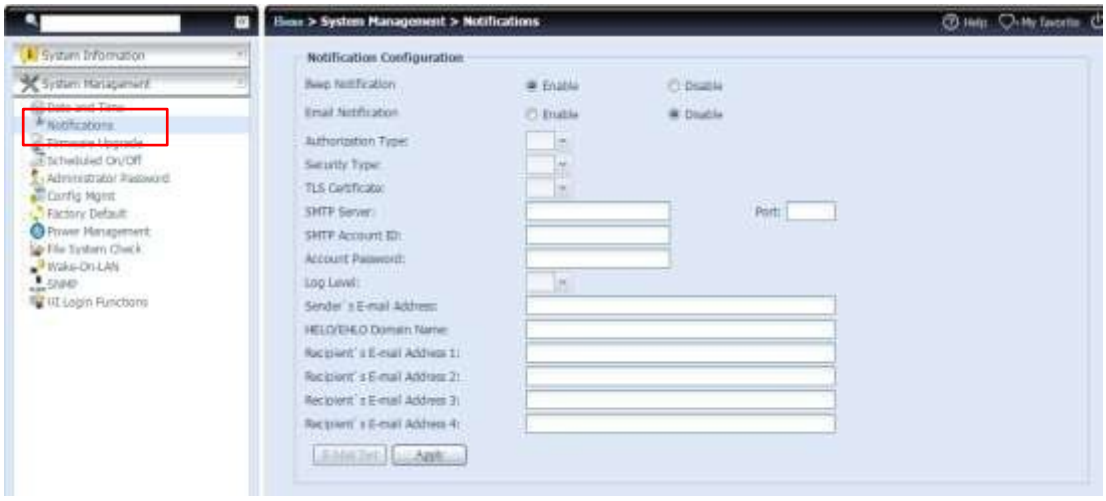


Table 14: Notification configuration

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.
Security Type	Select Security Type: SSL or StartTLS
TLS Certificate	On/off TLS Certificate.
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	Enter the 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.

Consult with your mail server administrator for email server information.

4.4.3. Firmware Upgrade

From the menu, choose the Firmware Upgrade item and the Firmware Upgrade screen appears.

Figure 41: Firmware upgrade

4.4.3.1. Manual Update

Follow the steps below to upgrade your firmware manually:

1. Use the **Browse** button  to find the firmware file.
2. Press **Apply**.
3. The buzzer will beep and the Busy LED will blink until the upgrade is complete.

The buzzer only beeps if it is enabled in the System Notification menu.

Check Kontron's website for the latest firmware release and release notes.

Downgrading firmware is not permitted.

NOTICE

Do not turns off the system during the firmware upgrade process. This will lead to a catastrophic result that may render the system inoperable.

4.4.3.2. Auto Update

If checked, the system will automatically detect and download new firmware (either a Major or Latest Update). The firmware will be installed when the system is shut down or rebooted.

Follow the steps below to upgrade your firmware automatically:

1. Check the Major Update or the Latest Update.
2. Press **Apply**.

Table 15: Auto update

Item	Description
Major Update	The system will download and upgrade to the latest essential firmware available.
Latest Update	The system will download and upgrade to the latest firmware available

4.4.4. Schedule Power On/Off

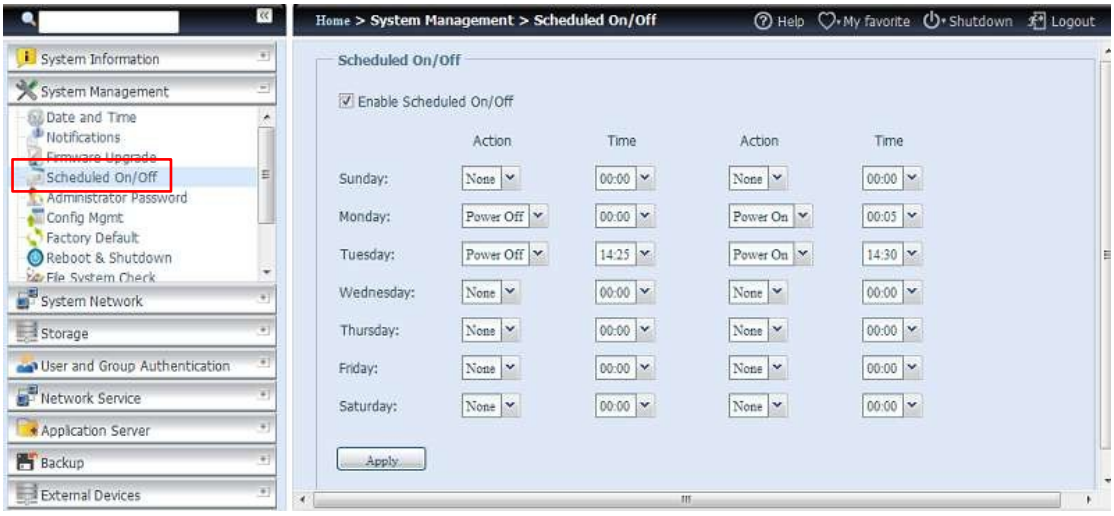
Using the CS3160 System Management, you can save energy and money by scheduling the CS3160 to turn itself on and off during certain times of the day.

From the System Management menu, choose the Schedule Power On/Off item and the Schedule Power On/Off screen appears.

To designate a schedule for the CS3160 to turn on and off, first enable the feature by checking the Enable Schedule Power On/Off checkbox.

Then, simply choose an on and off time for each day of the week. Finally, click Apply to save your changes.

Figure 42: Schedule power on/off



- 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

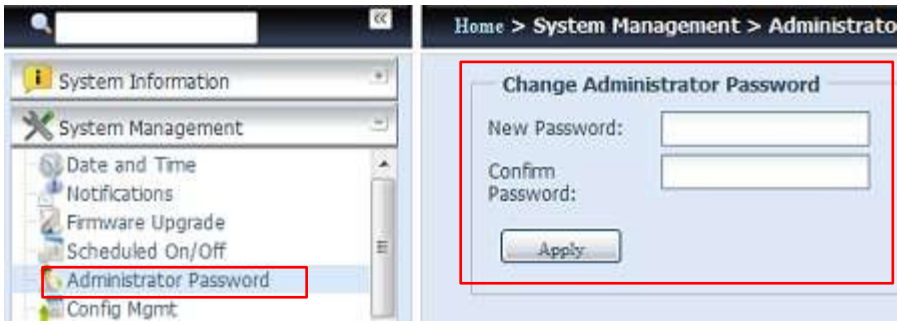
System will turn off at 8:00 AM on Monday. System will turn off at 16:00 PM on Monday, if it was on. If the system was already off at 16:00 PM on Monday, system will stay off.

4.4.5. Administrator Password

From the menu, 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.

There is also a password to enter the LCD setting that you can setup here. 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.

Figure 43: Administrator password



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

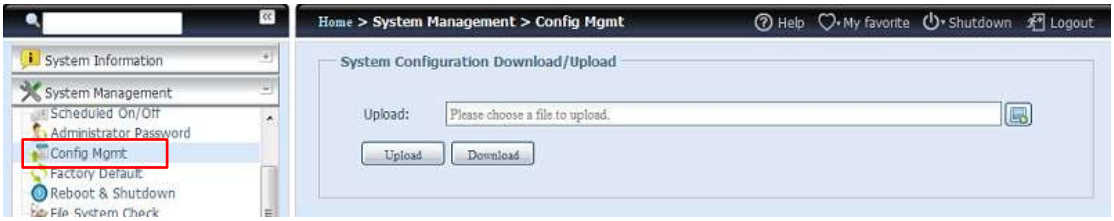
Table 16: Change administrator and LCD entry password

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.

4.4.6. Config Mgmt

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

Figure 44: Config Mgmt



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

Table 17: Config Mgmt

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.

4.4.7. Factory Default

From the menu, choose the Factory Default item and the Reset to Factory Default screen appears. Press Apply to reset the CS3160 to factory default settings.

Figure 45: Factory default

NOTICE

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.

4.4.8. Power Management

From the menu, choose Power Management item, and the Shutdown/Reboot System screen appears.

4.4.8.1. Shutdown/Reboot System

Press **Reboot** to restart the system or **Shutdown** to turn the system off.

Figure 46: Shutdown/reboot system

4.4.8.2. Automatic Resume

The setting determines how the CS3160 behaves when the poweris restored after an unexpected power loss.

Table 18: Automatic resume

Item	Description
No	The CS3160 remains power off until power on manually.
Yes	The CS3160 power on automatically when the power restores..
Previous Status	If the CS3160 was on, it will power on when the power restores. If the CS3160 was off, it will remains power off when the power restores.
Apply	Press this to save your changes.

The Automatic Resume feature will only be enabled when power is lost for at least 10 seconds.

4.4.9. File System Check

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

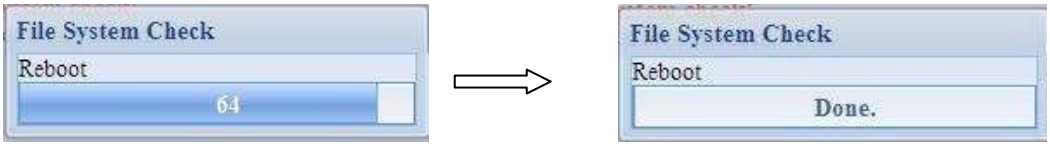
Figure 47: File system check

To perform a file system check, click **Apply**. Once clicked, the following prompt will appear:

Figure 48: Prompt

Click Yes to reboot the system.

Figure 49: Execution



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.

Figure 50: RAID volumes

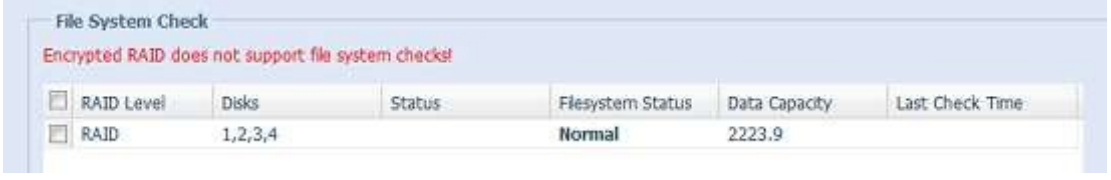


Figure 51: RAID selection

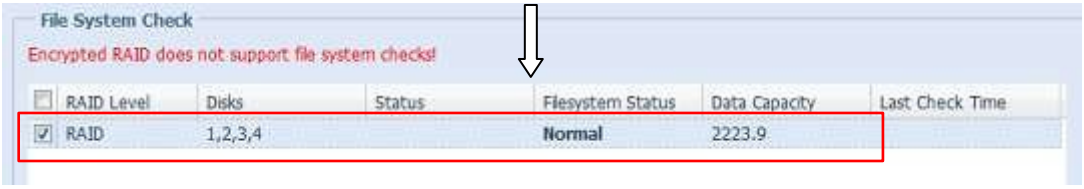
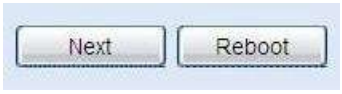
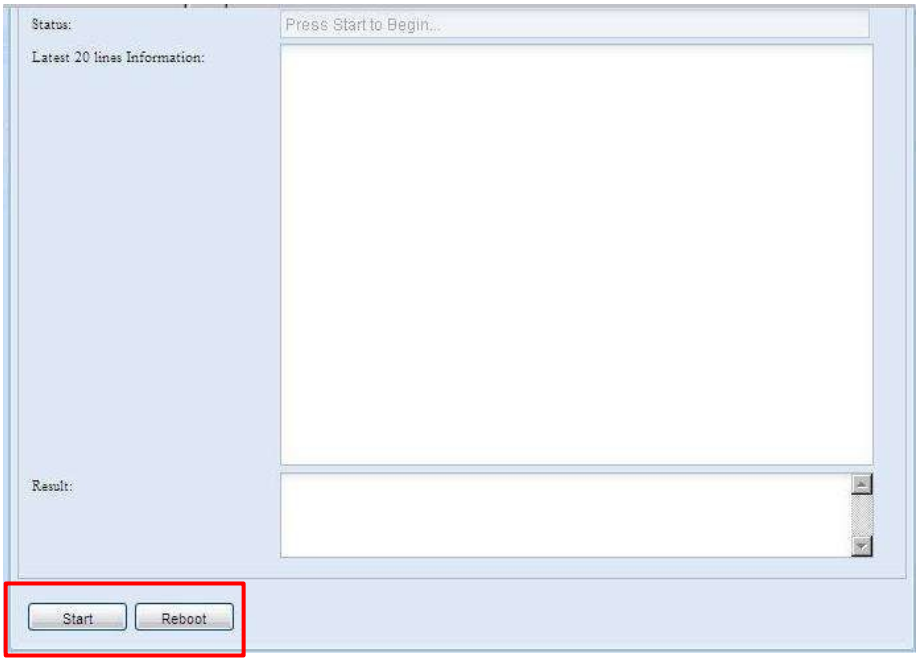


Figure 52: Buttons



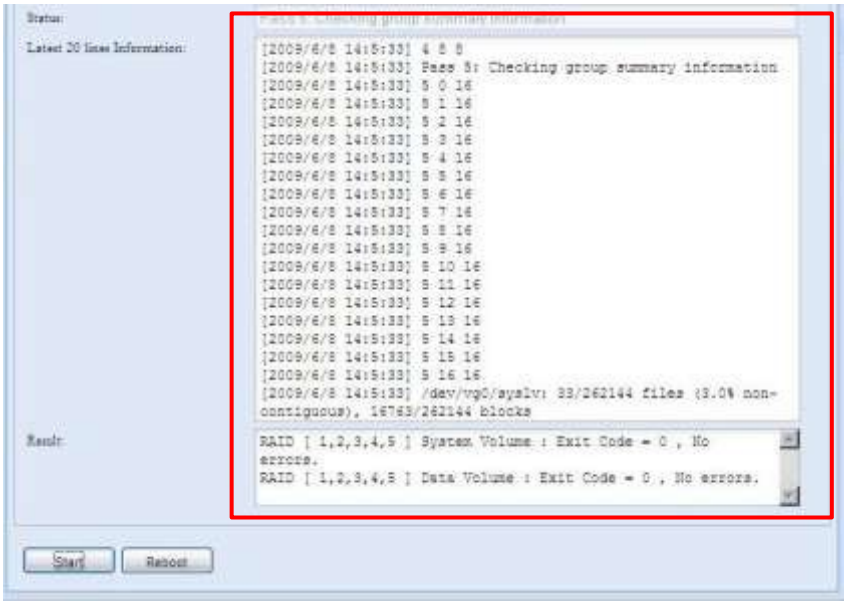
Once you click **Next**, you will see the following screen:

Figure 53: Status screen



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.

Figure 54: Status screen example

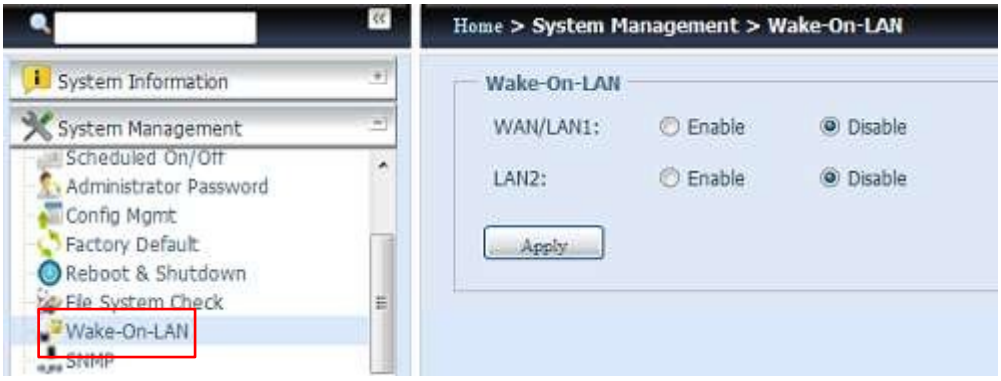


The system must be rebooted before the CS3160 can function normally after file system check completes.

4.4.10. Wake-Up on LAN (WOL)

The CS3160 has the ability to be awoken from sleep mode via WAN/LAN1 or LAN2 port.

Figure 55: Wake-up on LAN



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

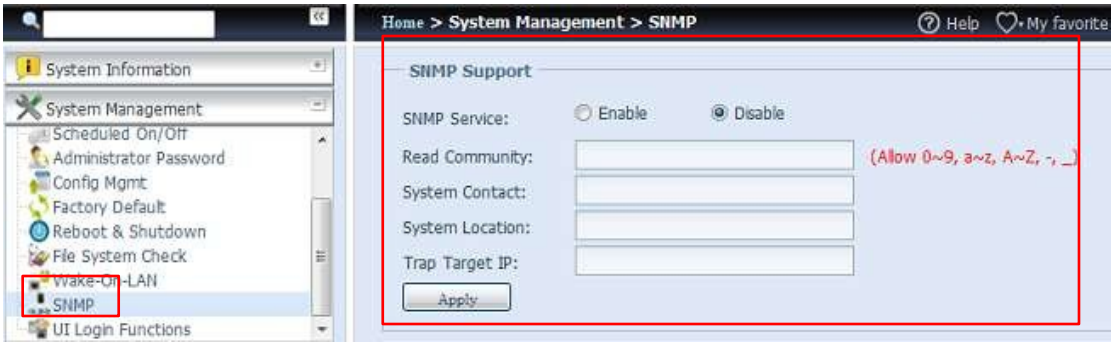
Table 19: Wake-up on LAN

Item	Description
WAN/LAN1	Enable or Disable WOL service from WAN/LAN1
LAN2	Enable or Disable WOL service from LAN2
Apply	Click Apply to save changes.

4.4.11. SNMP Support

From the menu, 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.

Figure 56: SNMP support

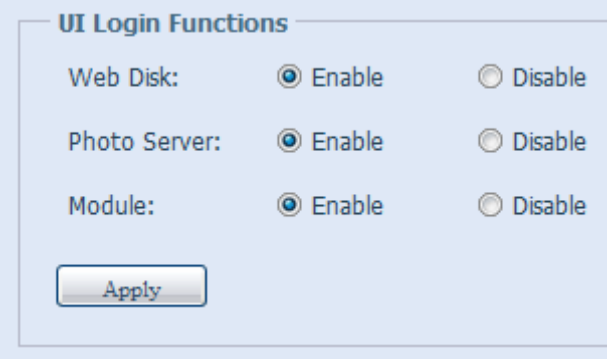


From the menu, choose the SNMP item, and the SNMP Support screen appears. From here, you can Enable or Disable.

4.4.12. UI Login Function

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

Figure 57: UI login function



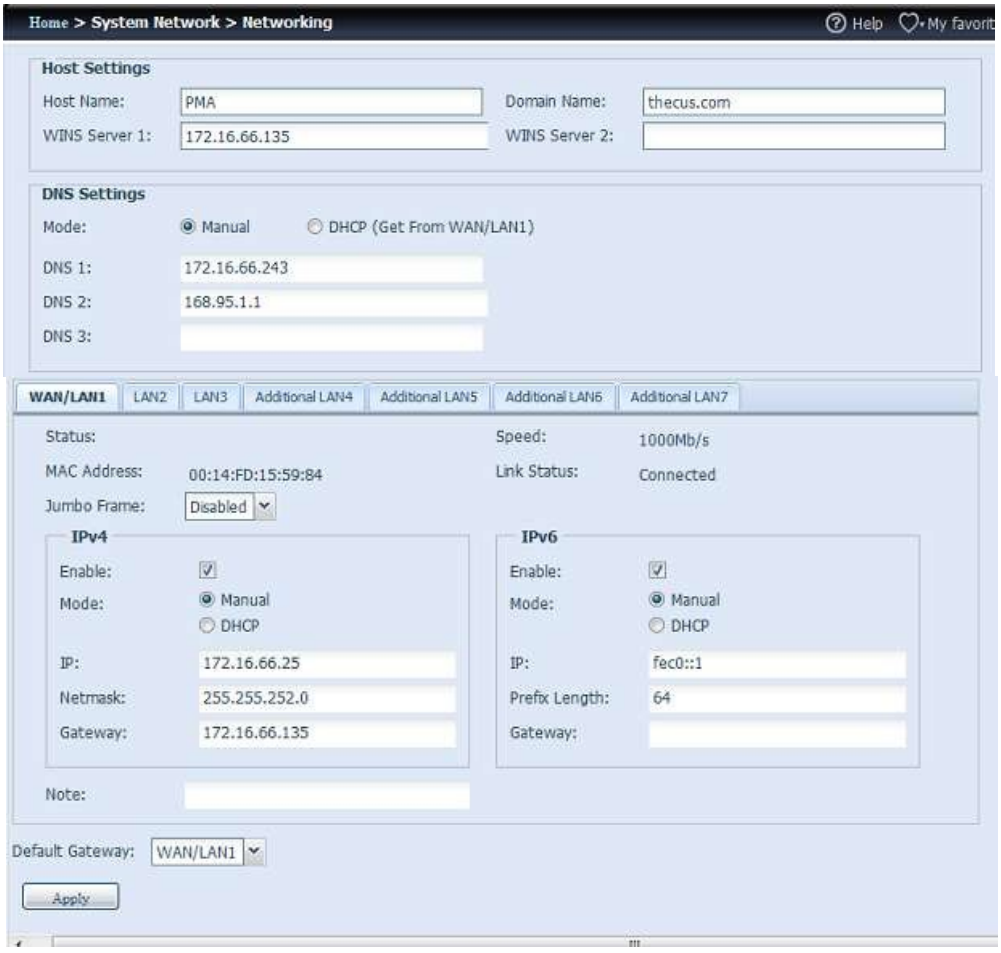
4.5. System Network

Use the System Network menu to make network configuration settings to an on board network port or additional NIC as well as DHCP and link aggregation.

4.5.1. Networking

From the System Network menu, 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:

Figure 58: Networking



The available system network ports are coming from embedded system ports and additional system ports added through the reserved PCI-e slot with associated compatible list. Therefore, the screen shown above is an example of a Kontron CS3160 with 3 on board GbE NIC and an additional Intel PRO/1000 PT quad port NIC, for a total of 7 NIC ports.

Table 20: Network configuration (global parameters)

Item	Description
Host name	Host name that identifies the CS3160 on the network.
Domain name	Specifies the domain name of the CS3160.
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.

Table 21: Network configuration (NIC port)

Item	Description
Link speed	Display associated NIC port link speed.
Link status	Display associated NIC port link status.
MAC address	MAC address of the network interface.

Item	Description
Jumbo Frame Support	Enable or disable Jumbo Frame Support of associate interface on your CS3160.
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 CS3160.

Only use Jumbo Frame settings when operating in a Gigabit environment where all other clients have Jumbo Frame Setting enabled.

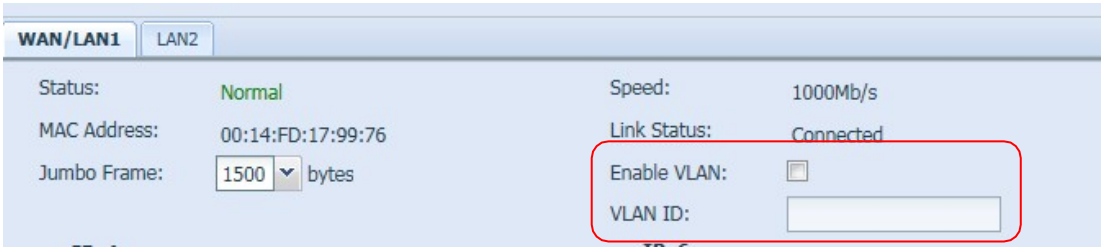
Proper DNS setting is vital to networks services, such as SMTP and NTP.

Most faster Ethernet (10/100) Switches/Routers do not support Jumbo Frame and will not be able to connect to your CS3160 NAS after Jumbo Frame is turned on.

4.5.2. VLAN

Each NIC is capable of VLAN support. To enable VLAN, simply click the checkbox and input the VLAN ID (VLAN ID can be any digital number). The system withthe same VLAN ID will become a Virtual LAN group to allow more specific communication among members.

Figure 59: VLAN



4.5.3. DHCP/RADVD

From the System Network menu, choose DHCP/RADVD, and the DHCP/RADVD Configuration screen appears. This screen displays available NIC status. If each NIC has been set-up to a static IP, then each NIC can be configured to act as DHCP/RADVD server.

Figure 60: DHCP/RADVD

4.5.3.1. DHCP/RADVD Server Configuration

A DHCP/RADVD server can be configured to assign IP addresses (IPv4) orPrefix (IPv6) to devices connected to the associated NIC port.

Table 22: DHCP configuration

Item	Description
DHCP/RADVD Service	Enable or disable the DHCP/RADVD service to automatically assign IP address to PCs connected to associate NIC interface.
Start IP (IPv4)	Specifies the lower IP address of the DHCP range.
End IP in (IPv4)	Specifies the highest IP address of the DHCP range.
Default Gateway (IPv4)	Specifies gateway for the DHCP server service.
DNS Server 1,2,3 (IPv4)	Displayed the DNS server IP address.
Prefix (IPv6)	Specifies prefix
Prefix Length (IPv6)	Specifies prefix length

The IP address of associated NIC should not be in the range of the Start IP address and End IP address (IPv4).

4.5.4. Linking Aggregation

The CS3160 supports link aggregation from either on board network port or additional NIC. Simply click on "+" as shown in the screen shot below.

Figure 61: Link aggregation screen 1

The associated screen shot will appear after the "+" is clicked.

Figure 62: Link aggregation screen 2

Select from available network port then move over to selected box.

Figure 63: Link aggregation screen 3

Click "Link" to confirm the selection. The newly created tab will appear for more settings required to complete the link aggregation configuration.

Figure 64: Link type

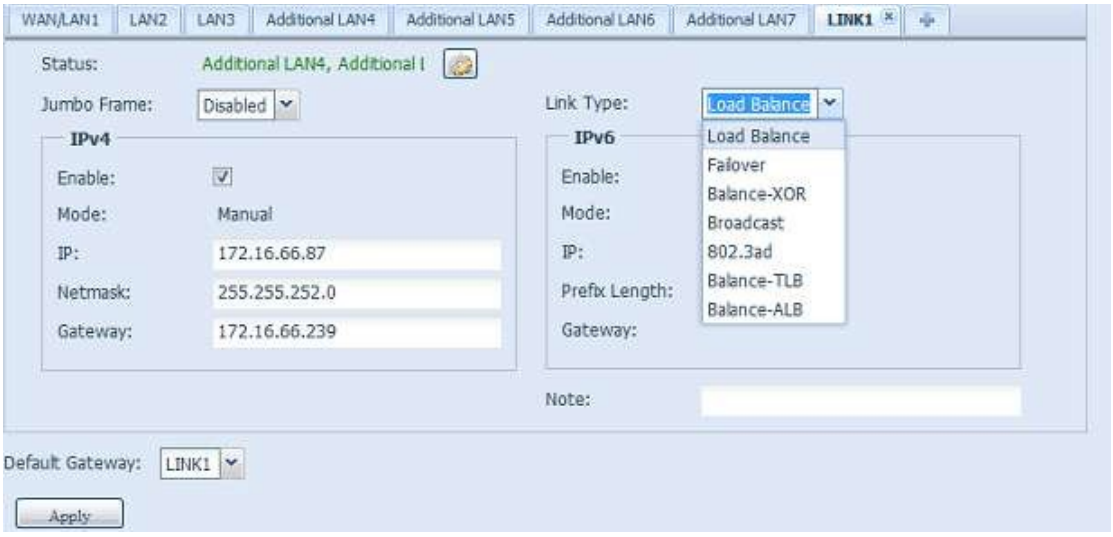
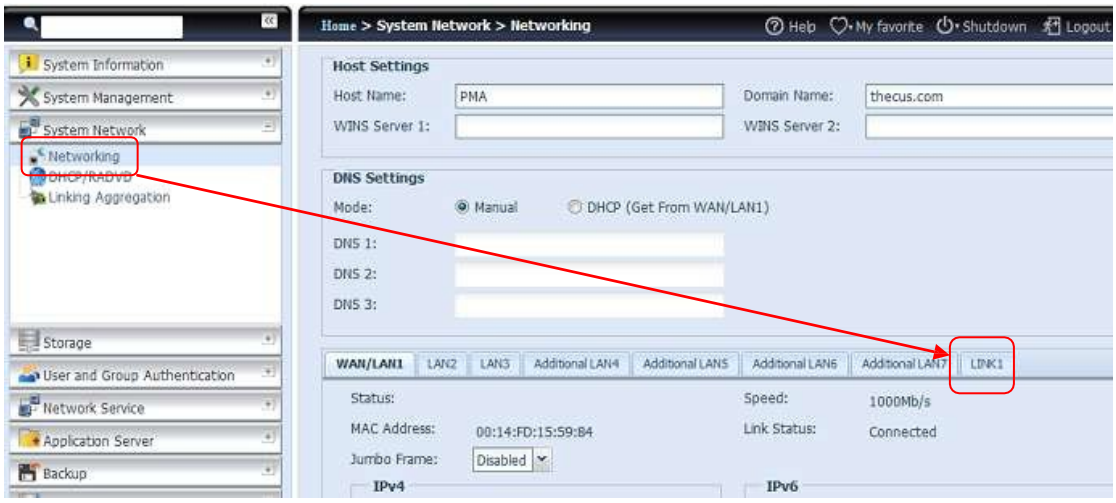


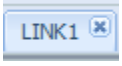
Table 23: Link1 configuration

Link1 Configuration	
Status	Specifies the network ports being used with the associated link aggregation. Click on  to modify the selected network ports.
Jumbo Frame Support	Enable or disable Jumbo Frame Support of the associated interface on your CS3160.
Link Type	Select from drop down list for desired mode.
IPv4/IPv6	Click to enable IPv4/IPv6 for TCP/IP. The default is IPv4 enabled.
Mode	It has to be a static IP with the link aggregation being used.
IP	IP address of link aggregation.
Netmask/Prefix Length	Input netmask for IPv4 and Prefix length for IPv6.
Gateway	Gateway for associated link aggregation
Default gateway	It can be chosen from the drop down list of default gateway being used for the CS3160.

Now under the networking, a "Link1" tab will appear from the network title bar.

Figure 65: Link 1 tab



To modify or delete LINK1, go to Link Aggregation setting page. Click on 

to modify the settings or click on 

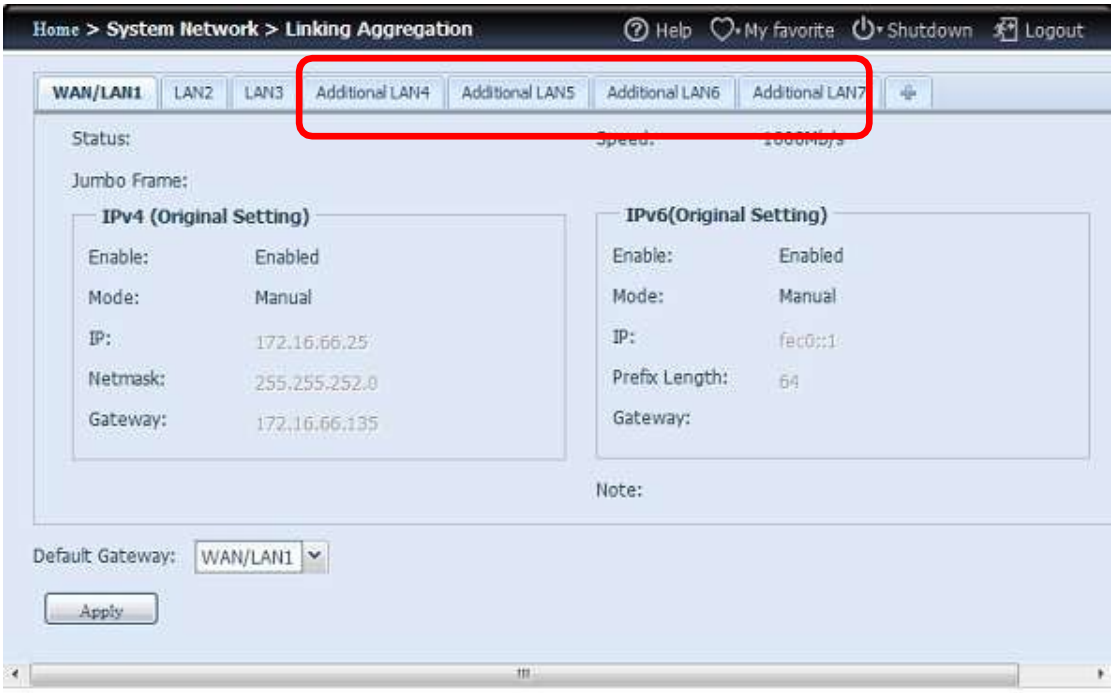
to delete this link aggregation. If any ports are still available, additional link aggregation links can be created by clicking  .

4.5.5. Additional LAN

Other than on-board LAN port, the CS3160 supports additional NIC to be added in its available PCI-e slot. For the details of additional NIC support list please visit www.kontron.com/.

Once the additional NIC is installed into the CS3160, the "Additional LANx" will appear under the "Networking" category. Click the associated NIC to setup the details. The screen shot below shows an example of an Intel PRO/1000 PT Quad port installed thru a PCI-e slot in the CS3160.

Figure 66: Additional LAN



4.6. Storage Management

The Storage menu displays the status of storage devices installed in the CS3160. It includes storage configuration options such as RAID and disk settings, folder configuration, iSCSI and ISO Mount.

4.6.1. Disk 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 CS3160 storage, which has 16 slots. Also it will list the disk info of JBOD devices if applicable.

Figure 67: Disk Information

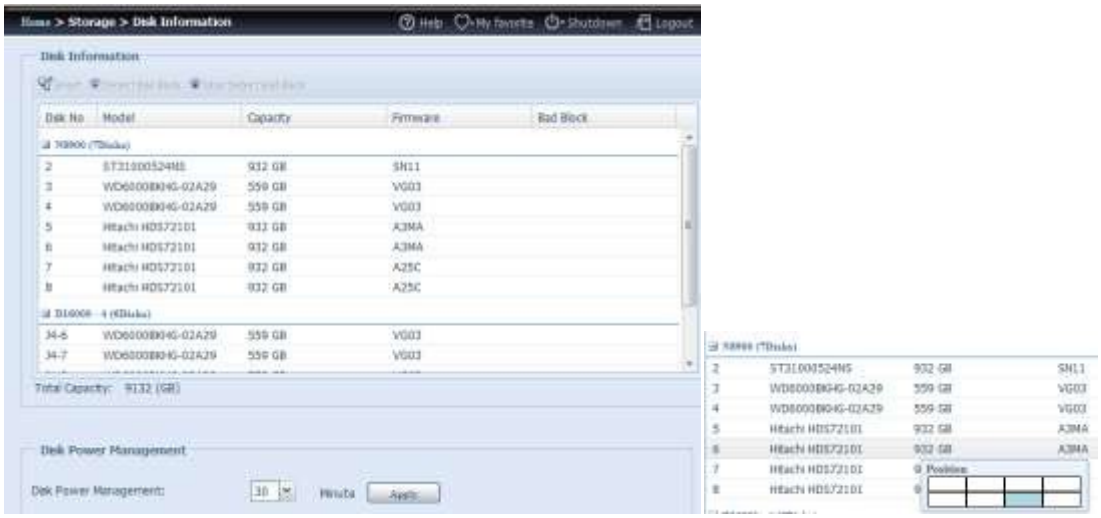


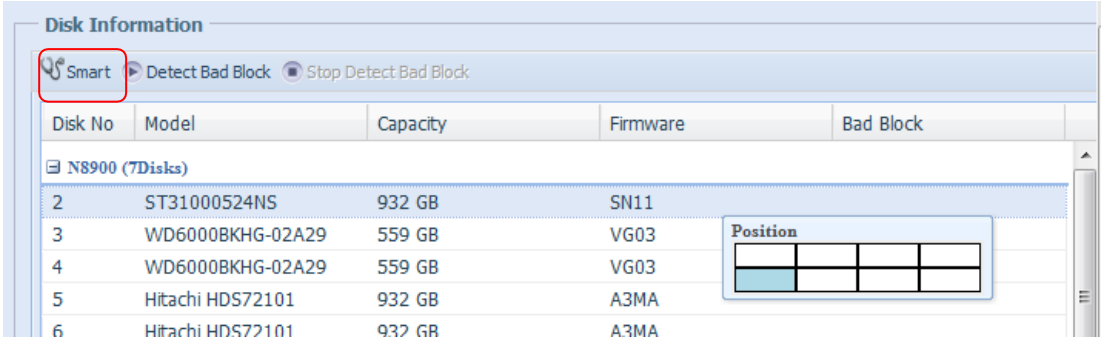
Table 24: Disk information

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.

4.6.1.1. SMART 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.

Figure 68: Smart selection



You may also perform a disk SMART test (doesn't apply to SAS HDD); 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.

Figure 69: Smart info

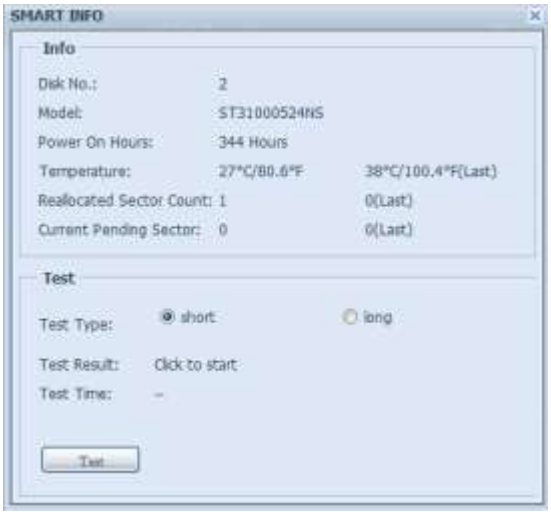


Table 25: SMART information

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.

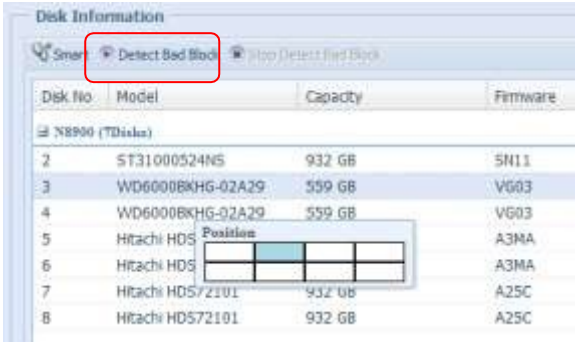
NOTICE

If the Reallocated Sector Count > 32 or the Current Pending Sector of a hard disk drive > 0 , the status of the disk will show "Warning". This warning is only used to alert the system administrator that there are bad sectors on the disk, and they should replace those disks as soon as possible.

4.6.1.2. Bad Block Scan

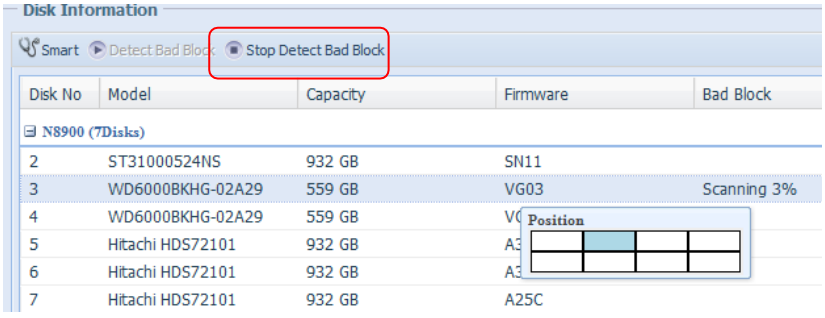
On the Disk Information screen, select a disk then click on "Detect Bad Block" to perform bad block scan of the associated disk. The result is only for reference and the system will not take any action from its results.

Figure 70: Detect bad block selection



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

Figure 71: Detect bad block termination



4.6.2. RAID Information

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

This screen lists the RAID volumes currently residing in the CS3160. From this screen, you can get information about the status of your RAID volumes, as well as the capacities allocated for data.

Figure 72: RAID management

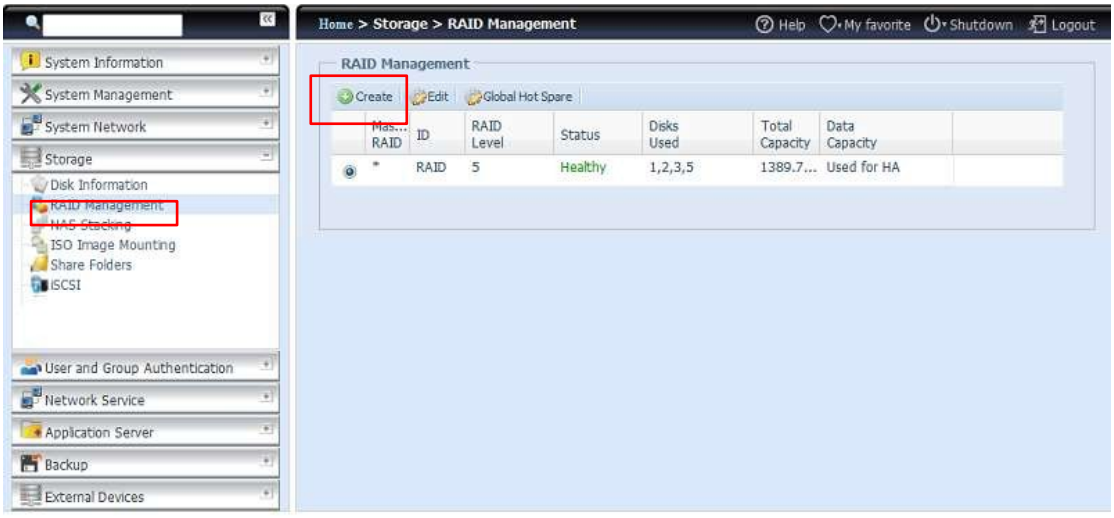


Table 26: RAID information

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.

4.6.2.1. 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.

Table 27: RAID configurations

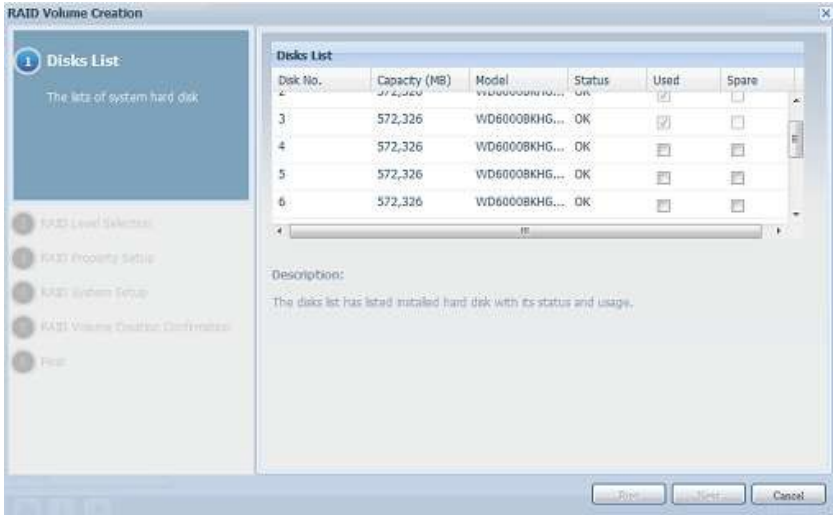
Item	Description
Disk No.	Number assigned to the installed hard disks.
Capacity (MB)	Capacity of the installed hard disks.
Model	Model number of the installed hard disks.
Status	Status of the installed hard disks.
Used	If this is checked, current hard disk is aalready part of a RAID volume.
Spare	If this is checked, current hard disk is designated as a spare for a RAID volume.

Item	Description
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:

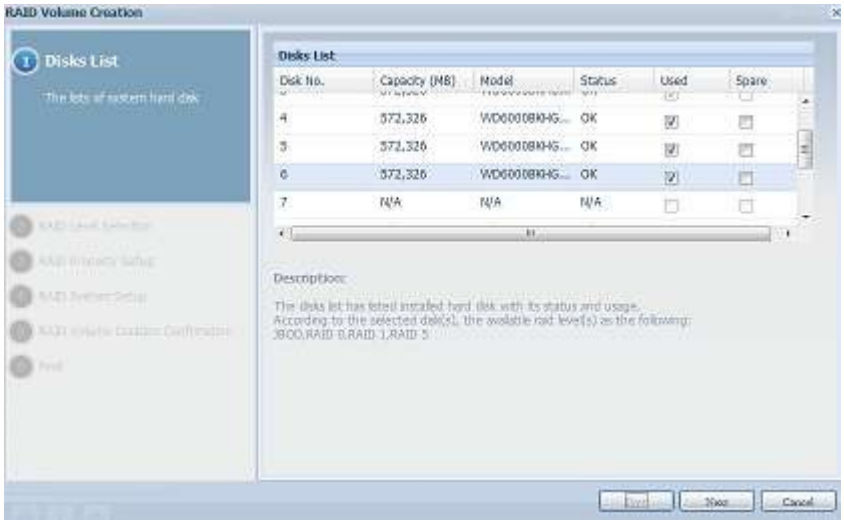
1. On the RAID Information screen, click **Create**.

Figure 73: RAID Information screen 1



2. On the RAID Configuration screen, set the RAID storage space as JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50 or RAID 60— see Appendix B: RAID Basics for a detailed description of each.

Figure 74: RAID Information screen 2



The CS3160 storage supports multiple RAID modes and is capable of creating up to five RAID volumes within a single NAS system.

3. Specify a RAID ID.

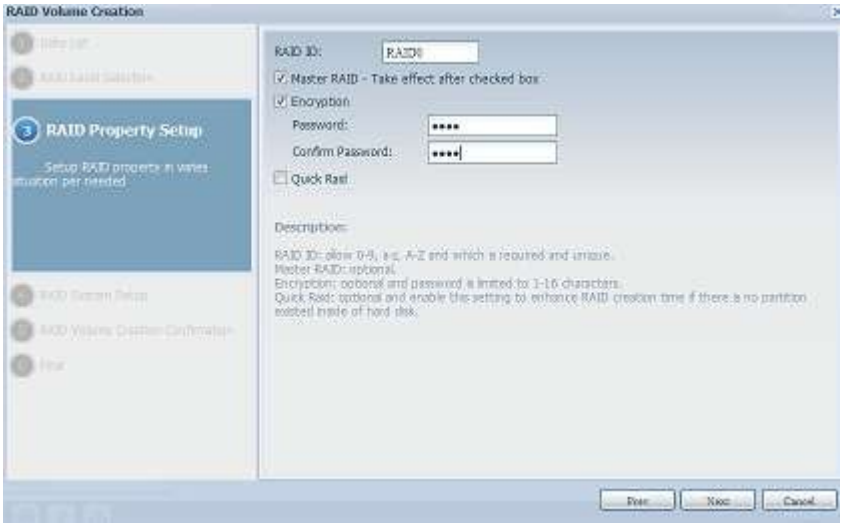
Figure 75: RAID ID

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.

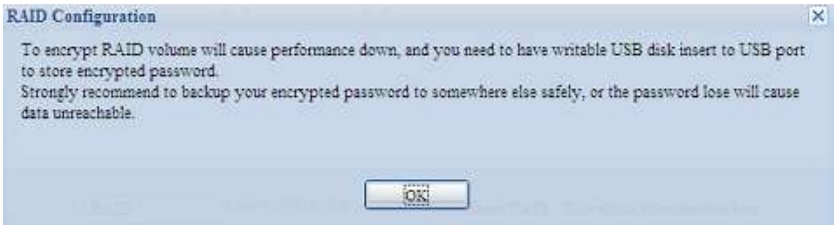
Selected whether the RAID volume will be encrypted or not. The RAID volume can protect data by using RAID Volume Encryption function to prevent the risk of data exposure. To activate this function, the Encryption option needs to be enabled while the RAID is created and followed by a password input for 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.

Figure 76: RAID configuration



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

Figure 77: Pop-up



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 creation date)_xxxxxx.key

NOTICE

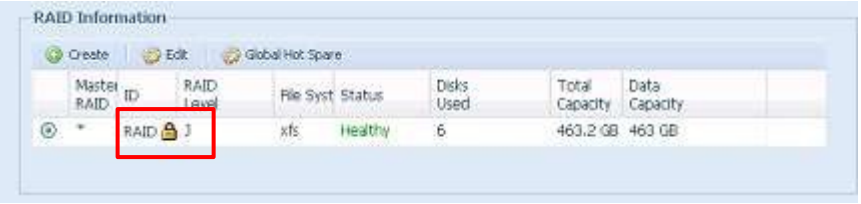
Please keep your USB disk in a safe place and also backup the encrypted key.

There is no way to rescue data back if the key is lost.

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

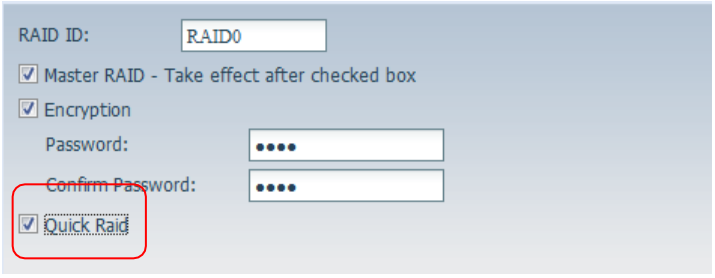
RAID volumes with encryption enabled will be displayed with a key lock symbol next to volume ID name.

Figure 78: Encrypted volume



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

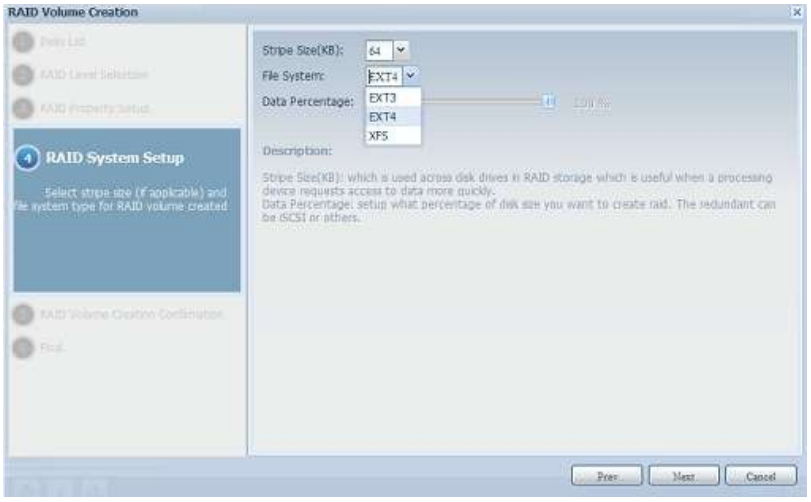
Figure 79: Quick RAID



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

6. Specify a stripe size — 64K is the default setting.
7. Selected the file system you would like to have for this RAID volume. The selection is available from ext3, XFS and ext4.

Figure 80: File system



Single volume size supported:

ext3 › 8TB

XFS › 48TB

ext4 › 36TB

8. Press **Submit** to build the RAID storage volume.

Figure 81: Creation confirmation

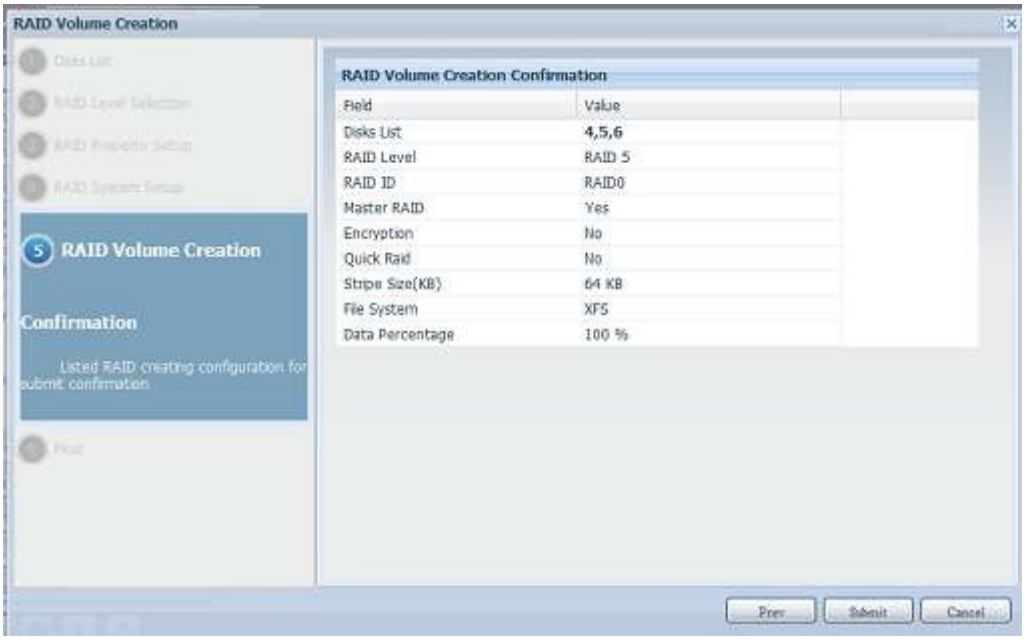
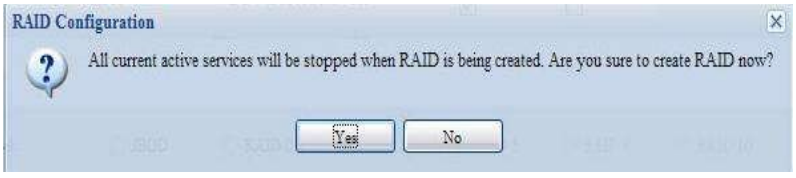


Figure 82: Pop-up



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

Figure 83: Start RAID volume building

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.

NOTICE

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

4.6.2.2. RAID Level

You can set the storage volume as JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID 50 or RAID 60.

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

Table 28: 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.

Level	Description
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.
RAID 50	RAID 50 combines the straight block-level striping of RAID 0 with the distributed parity of RAID 5. This is a RAID 0 array striped across RAID 5 elements. It requires at least 6 drives.
RAID 60	RAID 60 combines the straight block-level striping of RAID 0 with the distributed double parity of RAID 6. That is, a RAID 0 array striped across RAID 6 elements. It requires at least 8 disks.

NOTICE

If the administrator improperly removes a hard disk that should not be removed when RAID status is degraded, all data will be lost.

4.6.2.3. 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.

Figure 84: Edit RAID

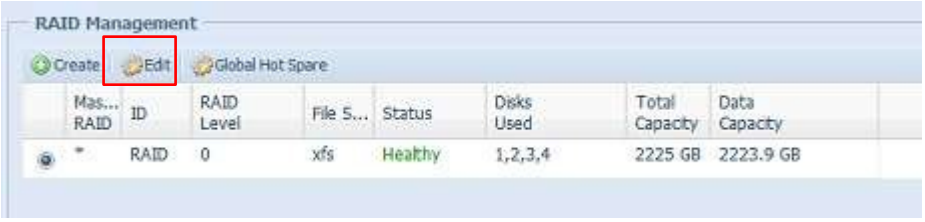
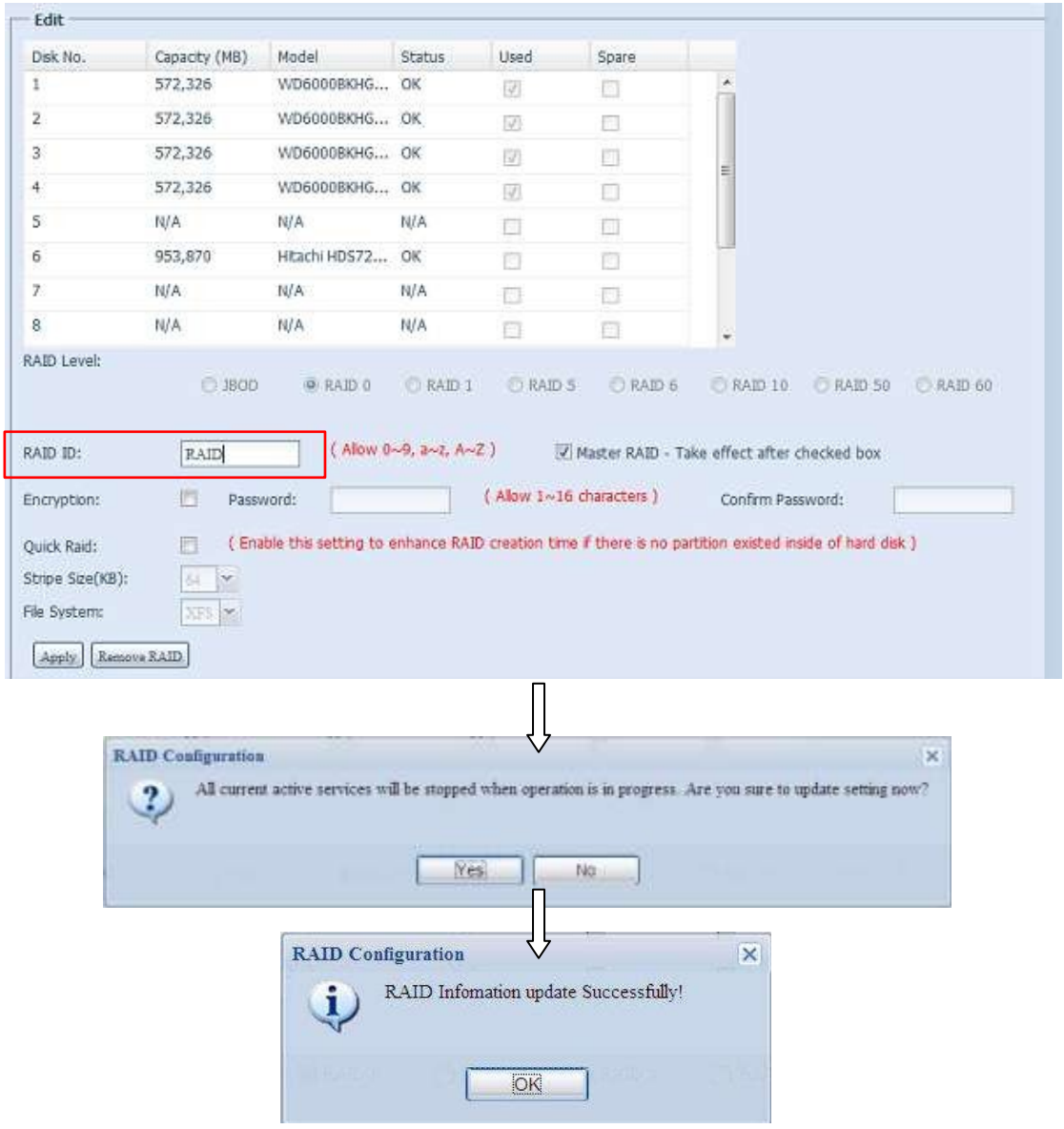


Figure 85: RAID ID



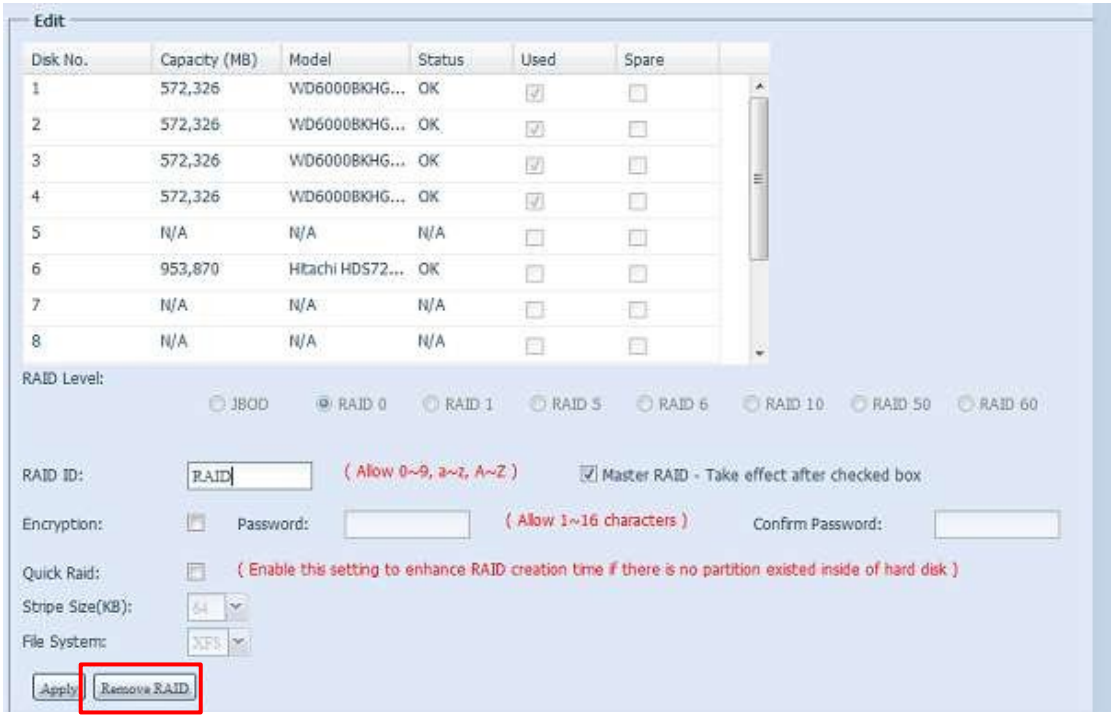
4.6.2.4. Remove RAID

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.

Figure 86: Remove RAID

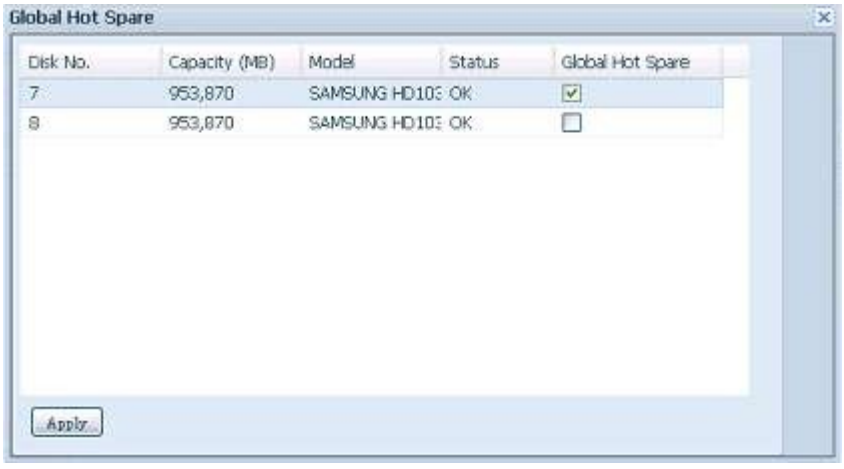


NOTICE Remove RAID destroys all data in the selected RAID volume. The data will be unrecoverable.

4.6.2.5. Global Hot Spare

Up to 5 RAID volumes can be created per system. The global hot spare support can eliminate the redundant disk usage in each RAID volume. Simply select an unused disk from the global hot spare disk list then apply to activate.

Figure 87: Global hot spare



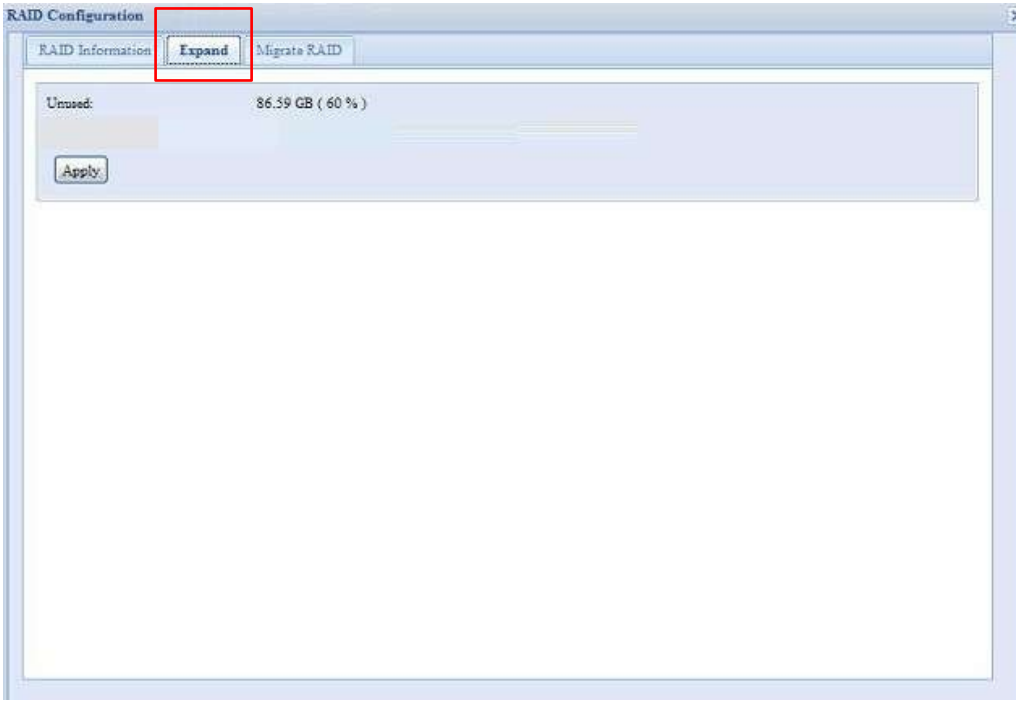
4.6.2.6. Expanding a RAID

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.

Figure 88: Expanding a RAID



4.6.2.7. Migrating a RAID

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, RAID 6, RAID50 or RAID 60 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.

Figure 89: Migrating a RAID

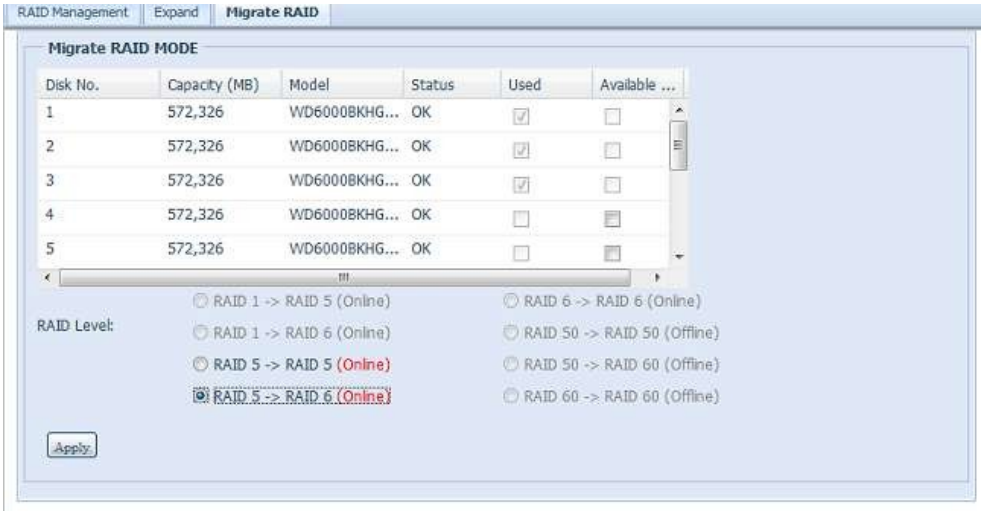
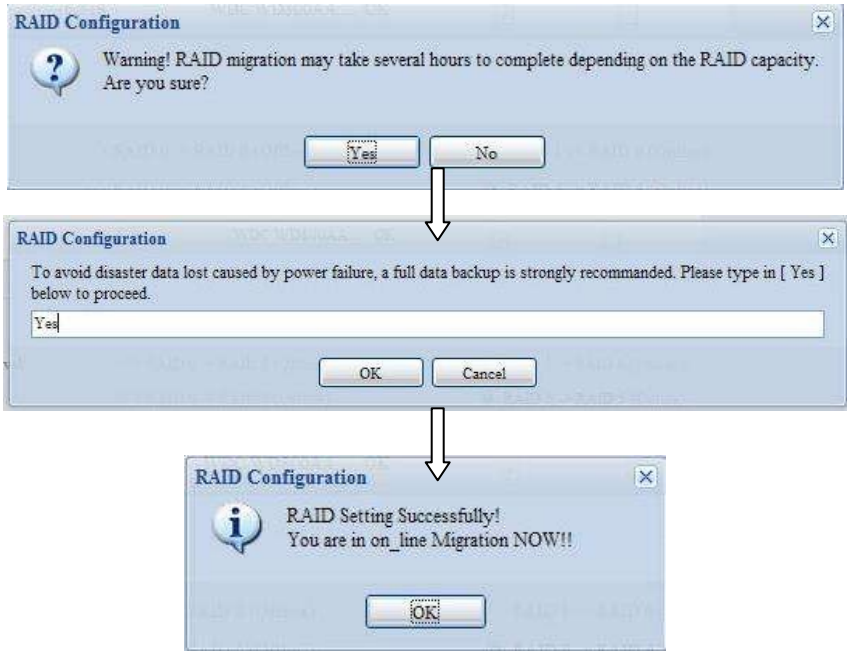


Figure 90: Migrating a RAID prompts



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 the CS3160 product's maximum possible combination.

Below is a table listing of possible RAID migration schemes:

Table 29: RAID migration schemes

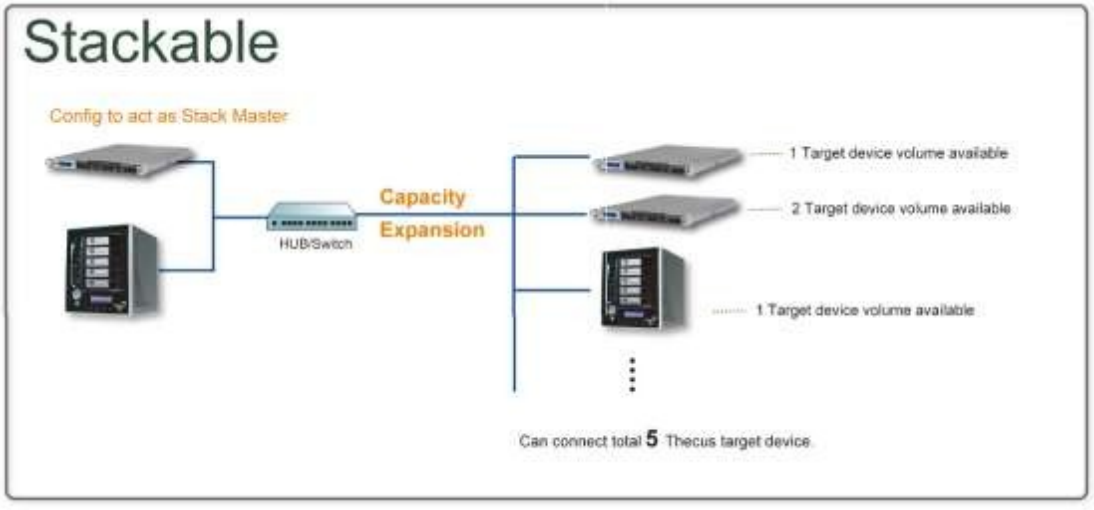
To From	RAID 0	RAID 5	RAID 6
RAID 1		[RAID 1] HDDx2 to [RAID 5] HDDx3 [RAID 1] HDDx2 to [RAID 5] HDDx4 [RAID 1] HDDx2 to [RAID 5] HDDx5 [RAID 1] HDDx2 to [RAID 5] HDDx6 [RAID 1] HDDx2 to [RAID 5] HDDx7 [RAID 1] HDDx2 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx3 to [RAID 5] HDDx4 [RAID 1] HDDx3 to [RAID 5] HDDx5 [RAID 1] HDDx3 to [RAID 5] HDDx6 [RAID 1] HDDx3 to [RAID 5] HDDx7 [RAID 1] HDDx3 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx4 to [RAID 5] HDDx5 [RAID 1] HDDx4 to [RAID 5] HDDx6 [RAID 1] HDDx4 to [RAID 5] HDDx7 [RAID 1] HDDx4 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx5 to [RAID 5] HDDx6 [RAID 1] HDDx5 to [RAID 5] HDDx7 [RAID 1] HDDx5 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx6 to [RAID 5] HDDx7 [RAID 1] HDDx6 to [RAID 5] HDDx8 ……..HDDx16 [RAID 1] HDDx7 to [RAID 5] HDDx8 ……..HDDx16	[RAID 1] HDDx2 to [RAID 6] HDDx4 [RAID 1] HDDx2 to [RAID 6] HDDx5 [RAID 1] HDDx2 to [RAID 6] HDDx6 [RAID 1] HDDx2 to [RAID 6] HDDx7 [RAID 1] HDDx2 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx3 to [RAID 6] HDDx4 [RAID 1] HDDx3 to [RAID 6] HDDx5 [RAID 1] HDDx3 to [RAID 6] HDDx6 [RAID 1] HDDx3 to [RAID 6] HDDx7 [RAID 1] HDDx3 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx4 to [RAID 6] HDDx5 [RAID 1] HDDx4 to [RAID 6] HDDx6 [RAID 1] HDDx4 to [RAID 6] HDDx7 [RAID 1] HDDx4 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx5 to [RAID 6] HDDx6 [RAID 1] HDDx5 to [RAID 6] HDDx7 [RAID 1] HDDx5 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx6 to [RAID 6] HDDx7 [RAID 1] HDDx6 to [RAID 6] HDDx8 ……..HDDx16 [RAID 1] HDDx7 to [RAID 6] HDDx8 ……..HDDx16
RAID 5	X	[RAID 5] HDDx3 to [RAID 5] HDDx4 [RAID 5] HDDx3 to [RAID 5] HDDx5 [RAID 5] HDDx3 to [RAID 5] HDDx6 [RAID 5] HDDx3 to [RAID 5] HDDx7 [RAID 5] HDDx3 to [RAID 5] HDDx8 ……..HDDx16 [RAID 5] HDDx4 to [RAID 5] HDDx5 [RAID 5] HDDx4 to [RAID 5] HDDx6 [RAID 5] HDDx4 to [RAID 5] HDDx7 [RAID 5] HDDx4 to [RAID 5] HDDx8 ……..HDDx16 [RAID 5] HDDx5 to [RAID 5] HDDx6 [RAID 5] HDDx5 to [RAID 5] HDDx7 [RAID 5] HDDx5 to [RAID 5] HDDx8 ……..HDDx16 [RAID 5] HDDx6 to [RAID 5] HDDx7 [RAID 5] HDDx6 to [RAID 5] HDDx8 ……..HDDx16	[RAID 5] HDDx3 to [RAID 6] HDDx5 [RAID 5] HDDx3 to [RAID 6] HDDx6 [RAID 5] HDDx3 to [RAID 6] HDDx7 [RAID 5] HDDx3 to [RAID 6] HDDx8 ……..HDDx16 [RAID 5] HDDx4 to [RAID 6] HDDx6 [RAID 5] HDDx4 to [RAID 6] HDDx7 [RAID 5] HDDx4 to [RAID 6] HDDx8 ……..HDDx16 [RAID 5] HDDx5 to [RAID 6] HDDx7 [RAID 5] HDDx5 to [RAID 6] HDDx8 ……..HDDx16 [RAID 5] HDDx6 to [RAID 6] HDDx8 ……..HDDx16

To From	RAID 0	RAID 5	RAID 6
		[RAID 6] HDDx7 to [RAID 5] HDDx8 ……..HDDx16	
RAID 6	X	X	[RAID 6] HDDx4 to [RAID 6] HDDx5 [RAID 6] HDDx4 to [RAID 6] HDDx6 [RAID 6] HDDx4 to [RAID 6] HDDx7 [RAID 6] HDDx4 to [RAID 6] HDDx8 ……..HDDx16 [RAID 6] HDDx5 to [RAID 6] HDDx6 [RAID 6] HDDx5 to [RAID 6] HDDx7 [RAID 6] HDDx5 to [RAID 6] HDDx8 ……..HDDx16 [RAID 6] HDDx6 to [RAID 6] HDDx7 [RAID 6] HDDx6 to [RAID 6] HDDx8 ……..HDDx16 [RAID 6] HDDx7 to [RAID 6] HDDx8 ……..HDDx16

4.6.3. NAS Stacking

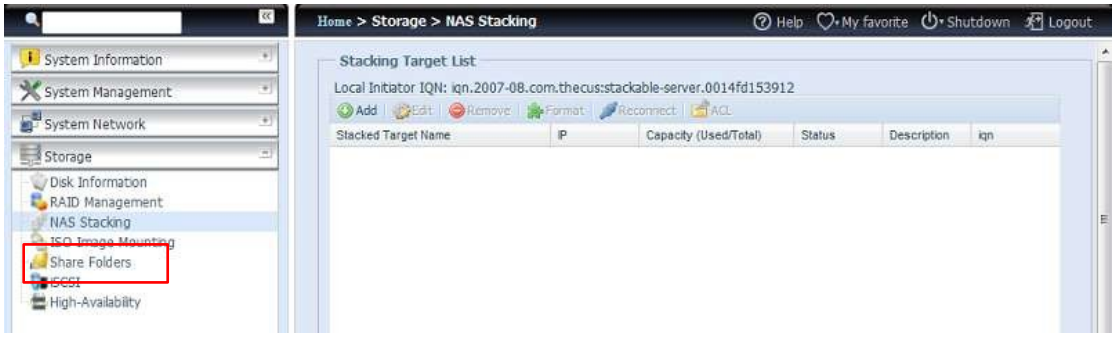
The CS3160's capacity can be expanded even further using the stackable function. With it, users can expand the capacity of their network storage systems up to 5 other stack target volumes which are located in different systems. These can be stacked through single network access like SMB or AFP acting as a share folder type.

Figure 91: NAS stacking



From the main menu, the stackable feature is located under “Storage”. Please refer the figure below for reference.

Figure 92: Main menu

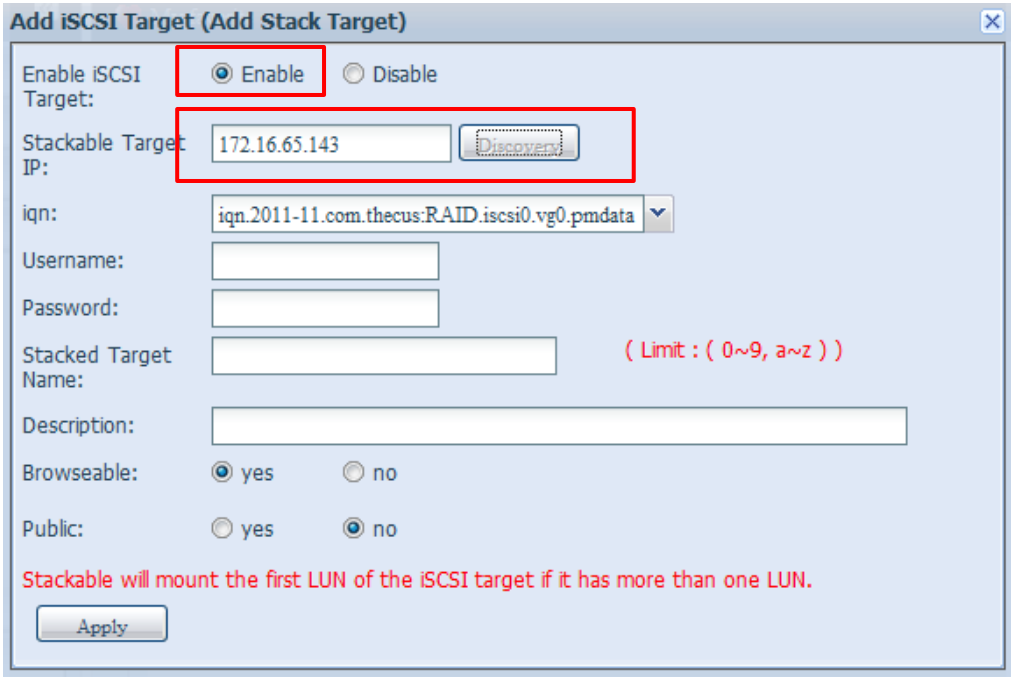


A. Add a Stack Target Volume

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.

Figure 93: Enabling stack target

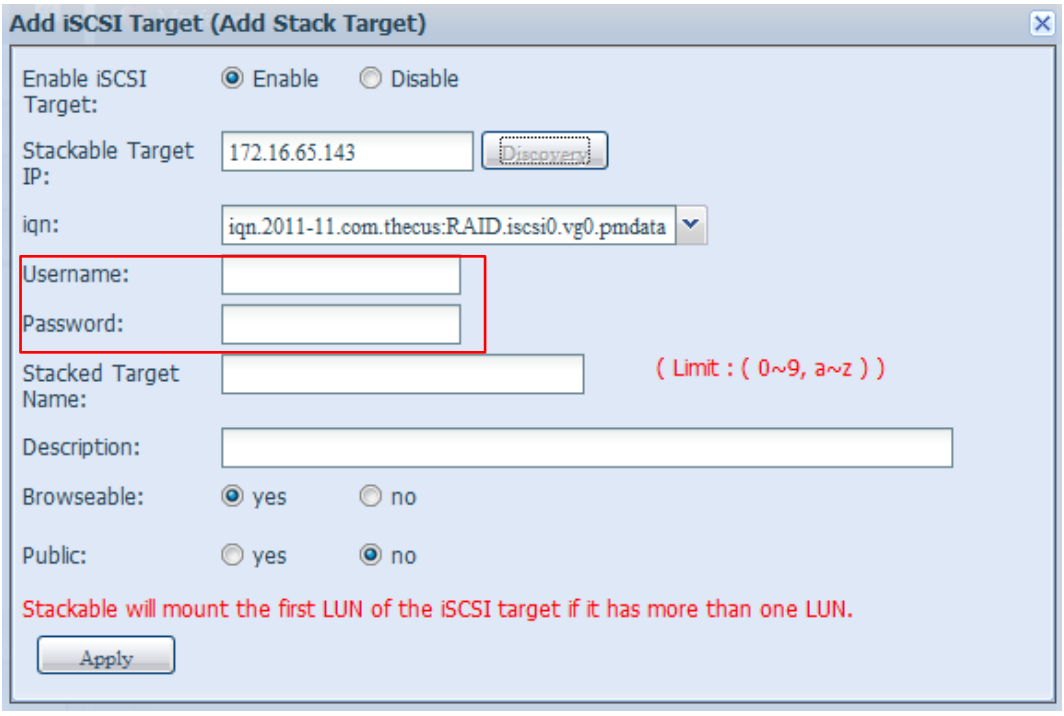


Next, input the target IP address of the stackable device and click the Discovery

button. The system will list available target volumes from the inputted IP address.

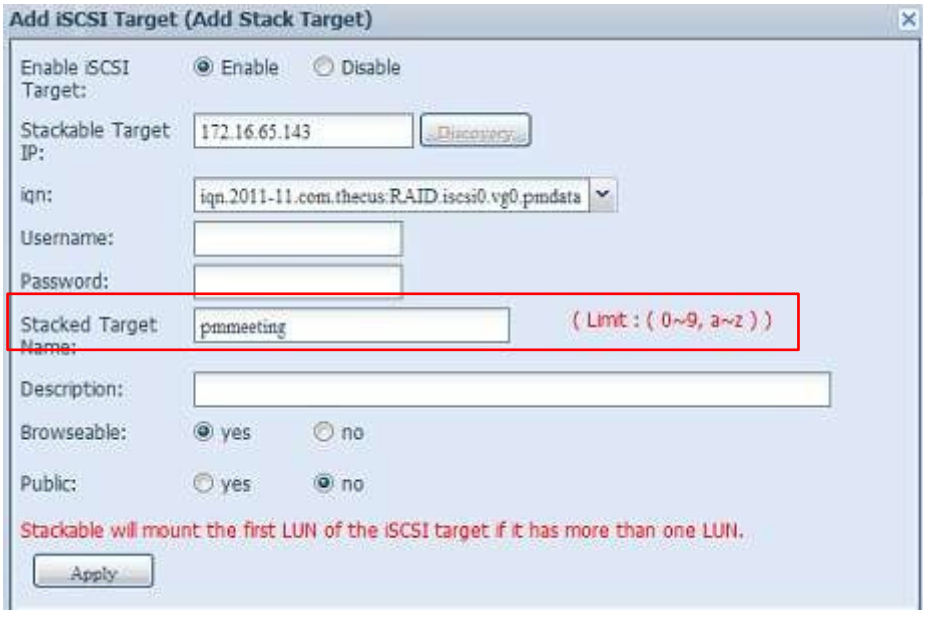
Once the volume IP has been set, you may need to input a valid user name and password to validate your access rights. If there is no user name and password needed to access target volume, then leave it blank.

Figure 94: User name and password



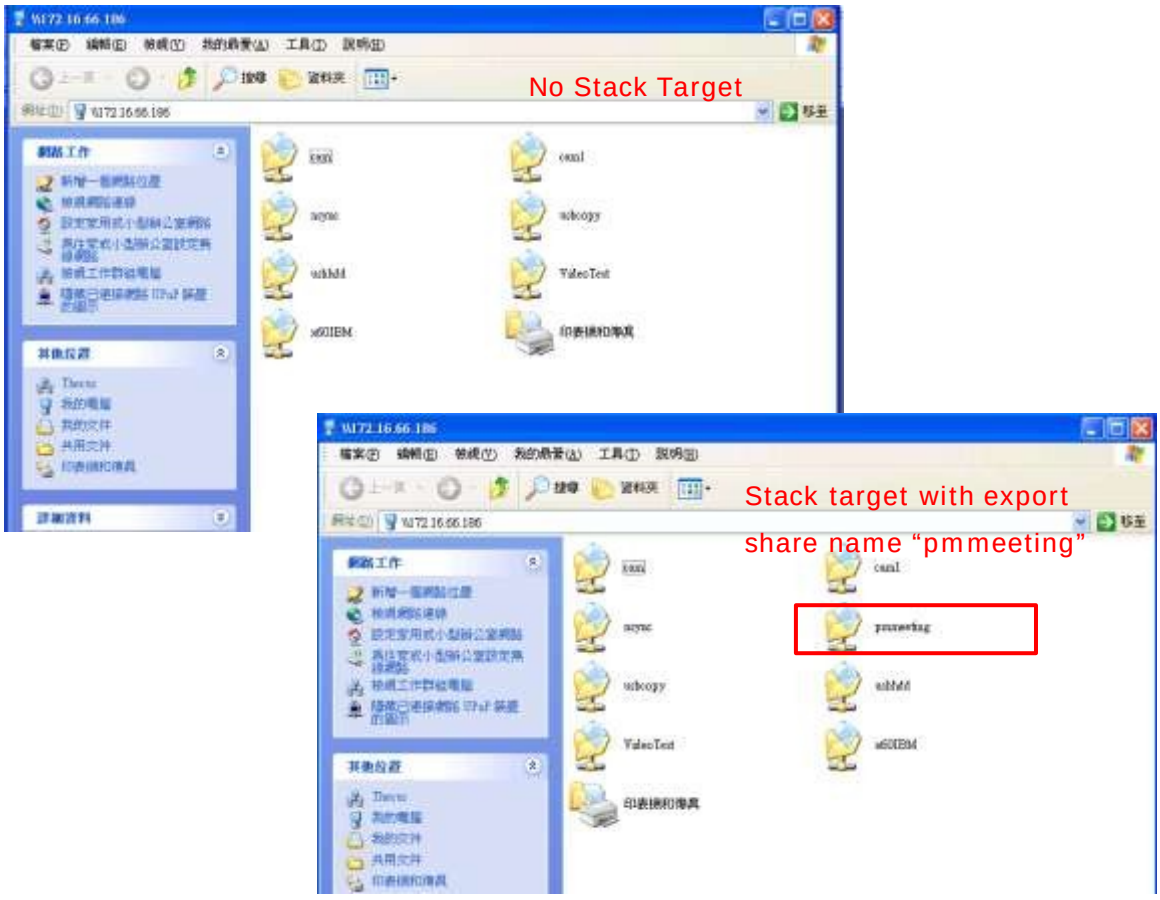
The Stacked Target name will become the network share name and will be displayed through network access such as SMB. You may refer to the figure below to see the result. Please note the naming limitation.

Figure 95: Stacked target name



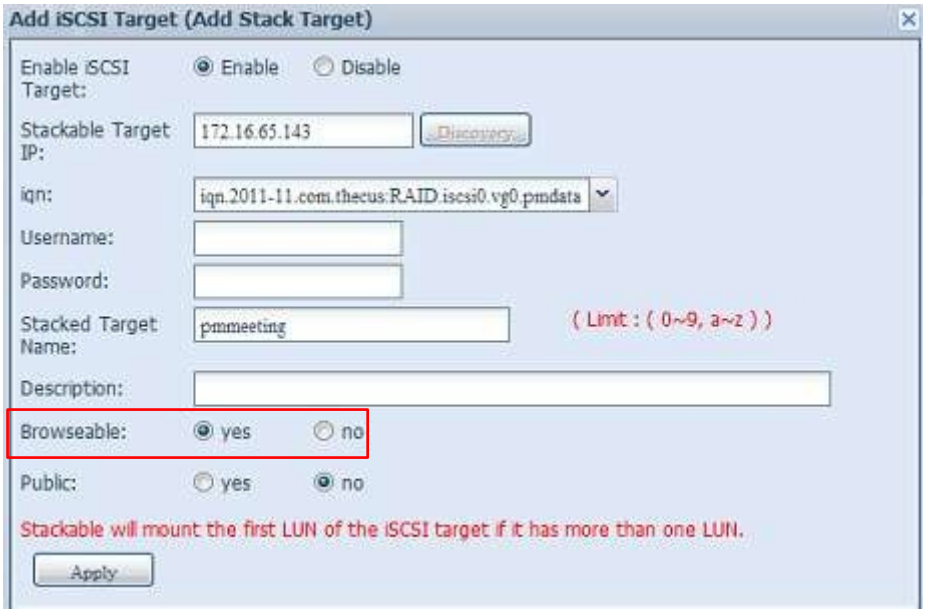
From the figure above, the Stacked Target name is “pmmeeting”. The figures below show the result before and after via Microsoft Network Access when settings have been completed.

Figure 96: Results



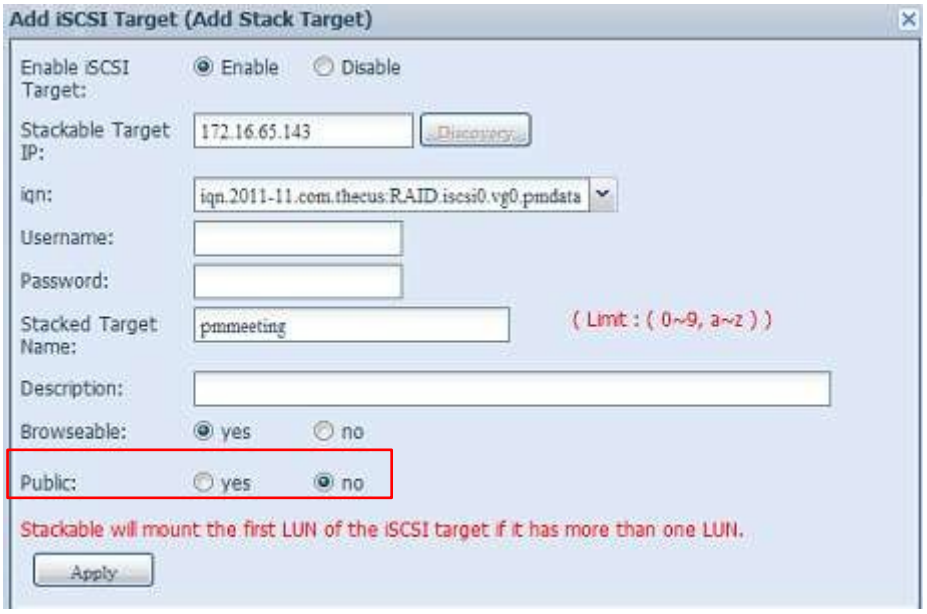
The Browseable setting is the same method used for setting a system share folder. It designates whether or not this folder will be visible through web disk. You may refer to the figure below for reference when Yes and No are selected.

Figure 97: Browseable setting



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.

Figure 98: Public setting

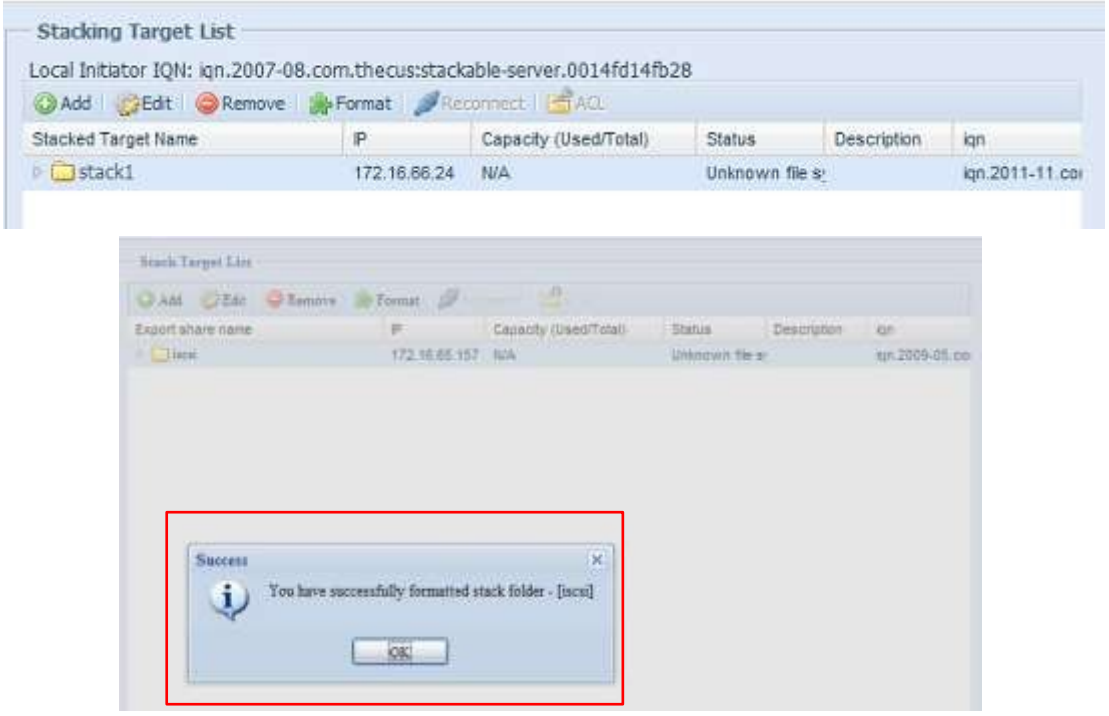


Click **Apply** to save your changes.

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.

Figure 99: Activate a stack target



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 CS3160 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:

Figure 100: Edit a stack target

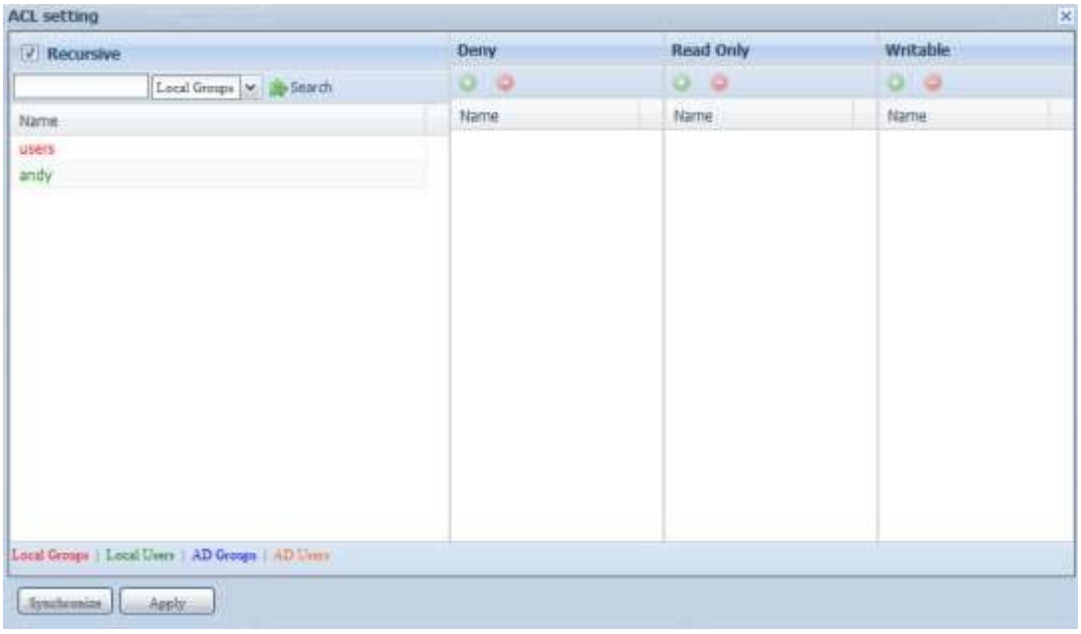
After your changes have been made, click Apply to confirm any modifications. Once changes are applied, the associated information will be updated on the Stack Target List window.

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.

Figure 101: Stack target ACL

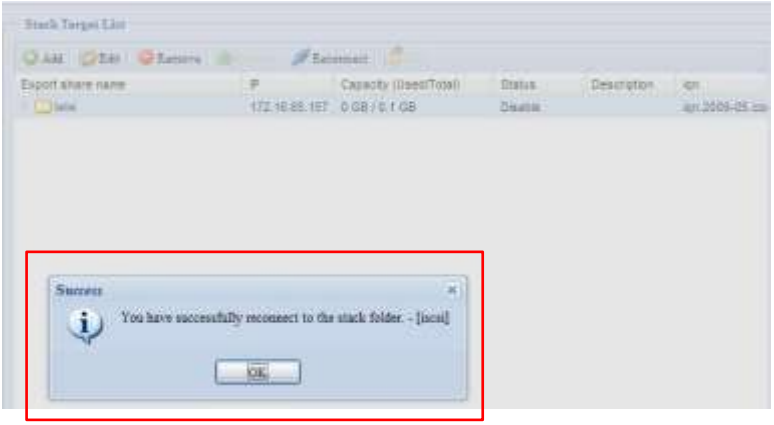


E. Reconnect a Stack Target

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.

Figure 102: Reconnect a stack target

Figure 103: Reconnect confirmation



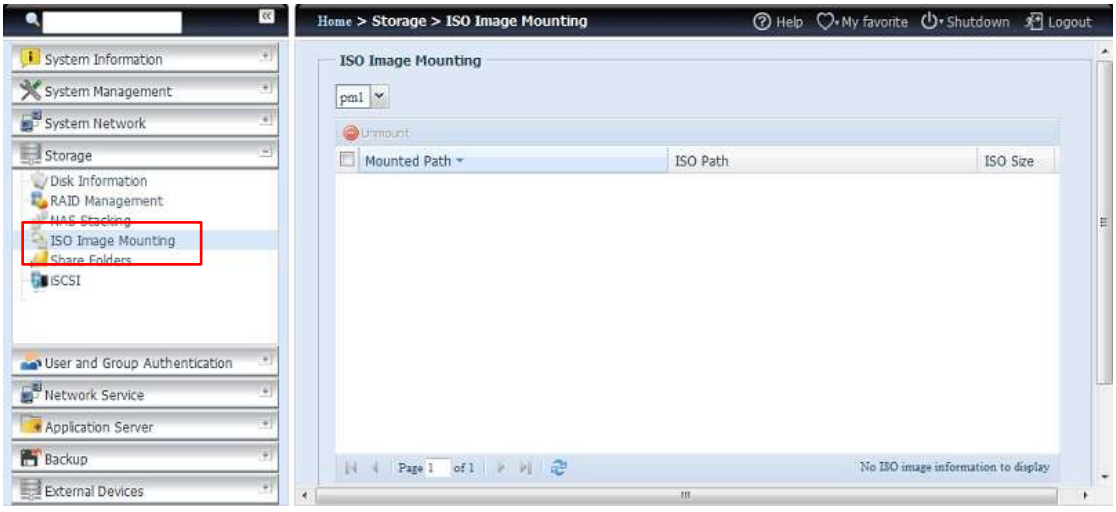
4.6.4. ISO Mount

The ISO Mount feature is a very useful tool from the Kontron 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 main menu, the ISO Mount 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.

Figure 104: ISO image mounting



A. Add an ISO file

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

Figure 105: ISO file selection

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

Figure 106: Mount table screen

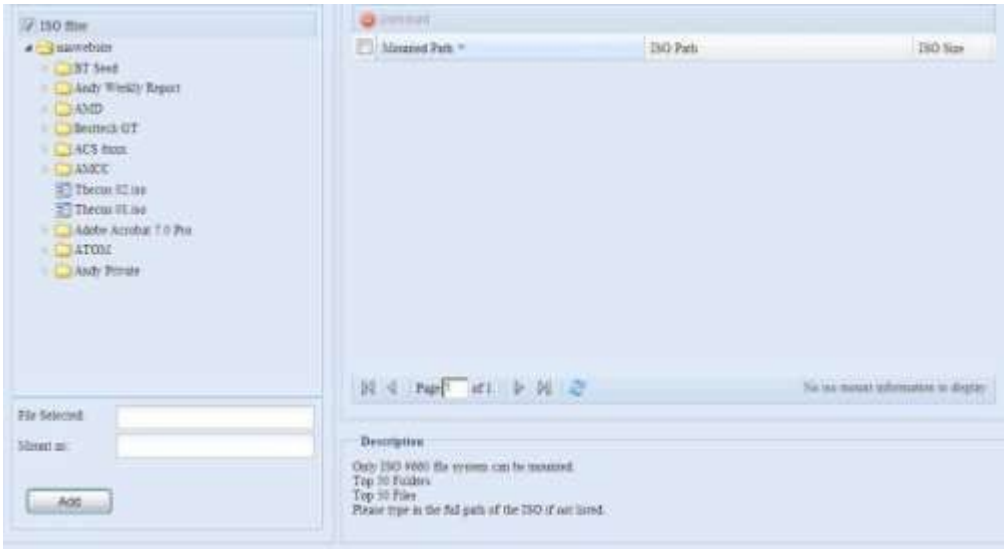
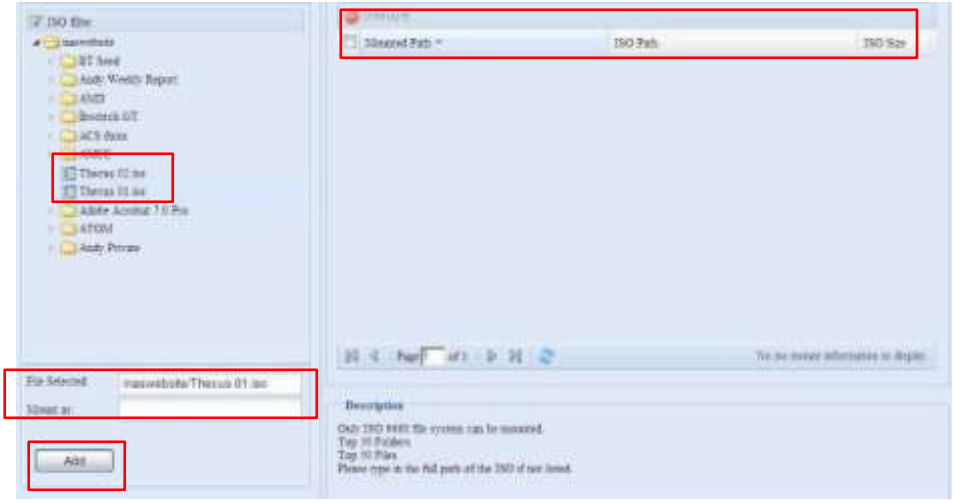


Figure 107: File selection



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.

Figure 108: Prompt 1

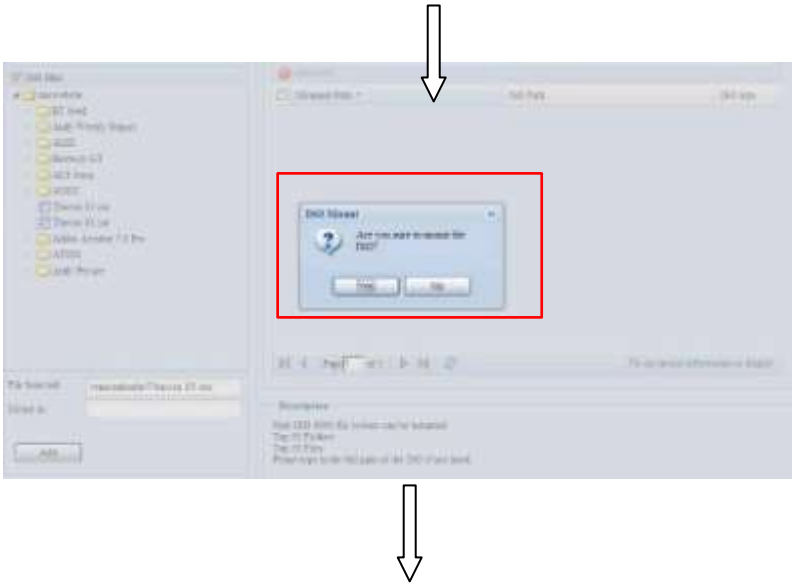
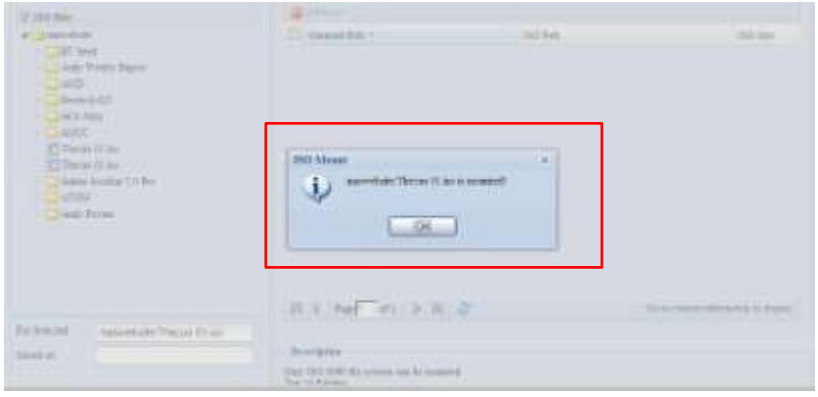
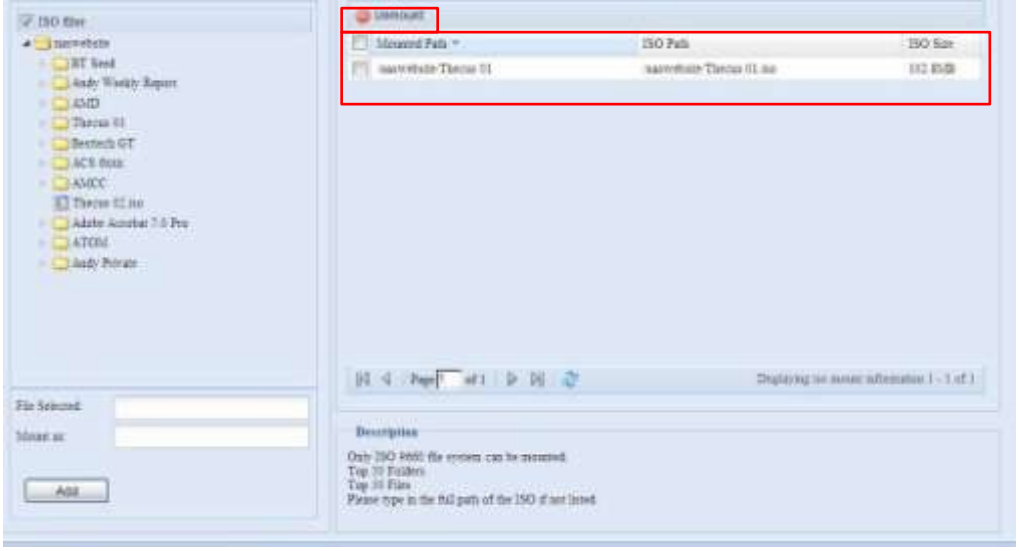


Figure 109: Prompt 2



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

Figure 110: Mounted ISO files

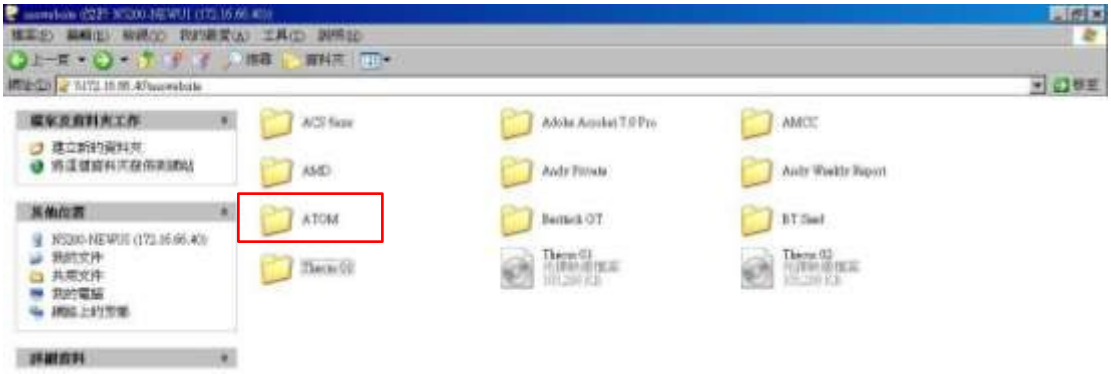


You can click “Unmount” to eliminate a mounted ISO file.

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".

Figure 111: Using ISO



4.6.5. Share Folder

From the Storage menu, choose Share Folders, and the Shared Folder screen appears. This screen allows you to create and configure folders on the CS3160 volume.

Figure 112: Share folders

4.6.5.1. 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.

Figure 113: Add folders

Figure 114: New folder information

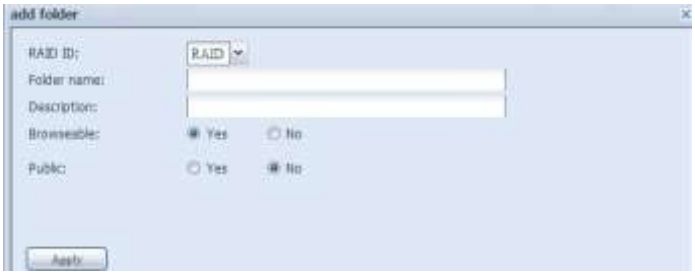


Table 30: Add folder

Item	Description
RAID ID	RAID volume where the new folder will reside.
Folder Name	Enter the name of the folder.
Description	Provide a description the folder.
Browseable	Enable or disable users from browsing the folder contents. If Yes is selected, then the share folder will be browseable.
Public	Admit or deny public access to this folder. If Yes is selected, then users do not need to have access permission to write to this folder. When accessing a public folder via FTP, the behavior is similar to anonymous FTP. Anonymous users can upload/download a file to the folder, but they cannot delete a file from the folder.
Apply	Press Apply to create the folder.

Folder names are limited to 60 characters. Systems running Windows 98 or earlier may not support file names longer than 15 characters.

4.6.5.2. 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.

Figure 115: Modify folders

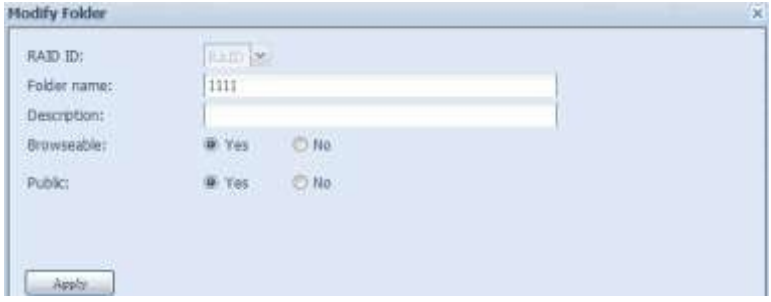


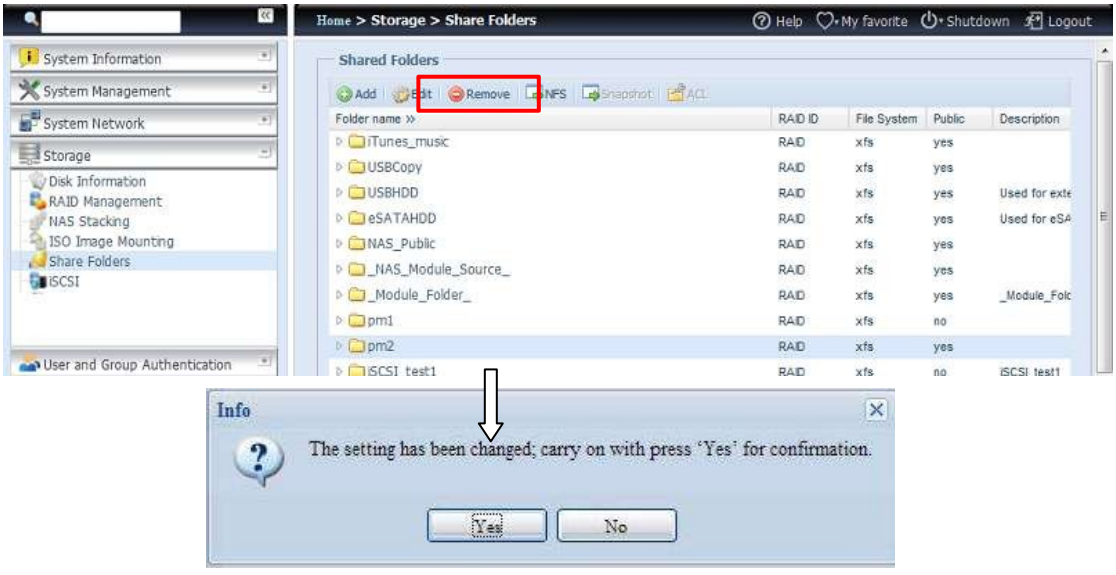
Table 31: Modify folders

Item	Description
RAID ID	RAID volume where the folder will reside.
Folder Name	Enter the name of the folder.
Description	Provide a description the folder.
Browseable	Enable or disable users from browsing the folder contents. This setting will only apply while access via SMB/CIFS and web disk.
Public	Admit or deny public access to this folder.

4.6.5.3. 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.

Figure 116: Remove folders



NOTICE

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

4.6.5.4. 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.

Figure 117: NSF screen

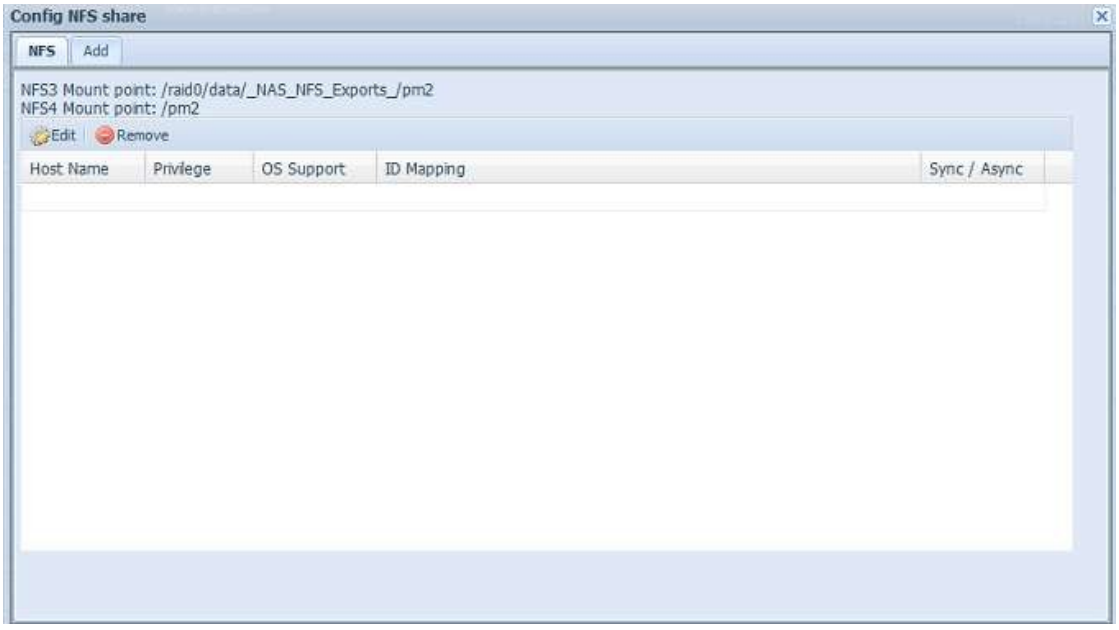


Figure 118: Add screen

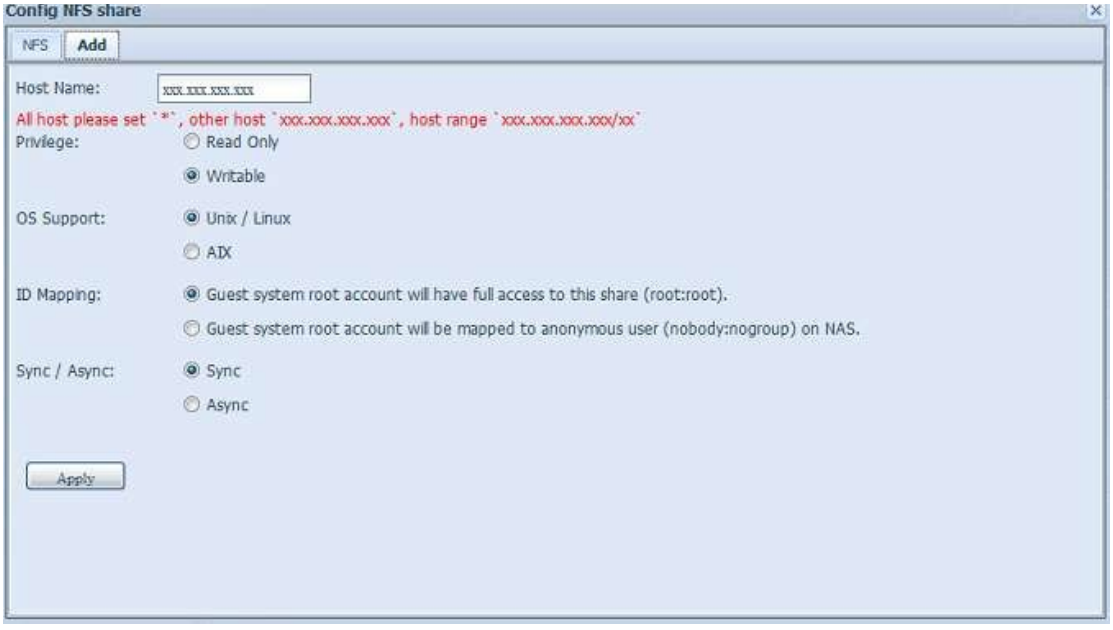


Table 32: NFS share

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.

4.6.5.5. 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.

Figure 119: ACL confirmation

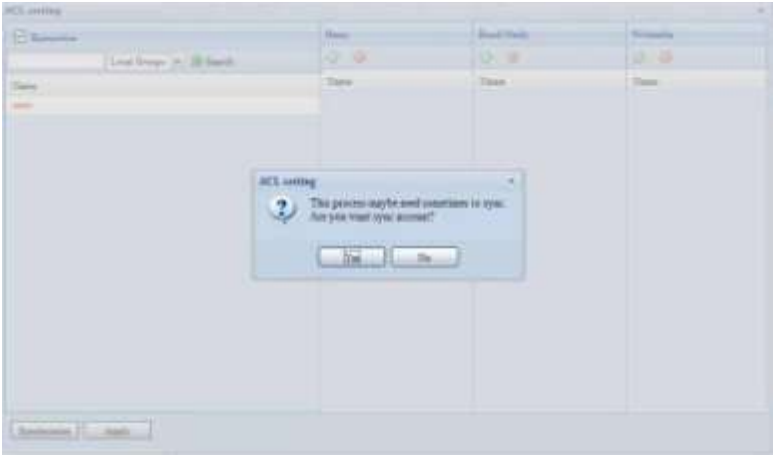


Figure 120: ACL settings

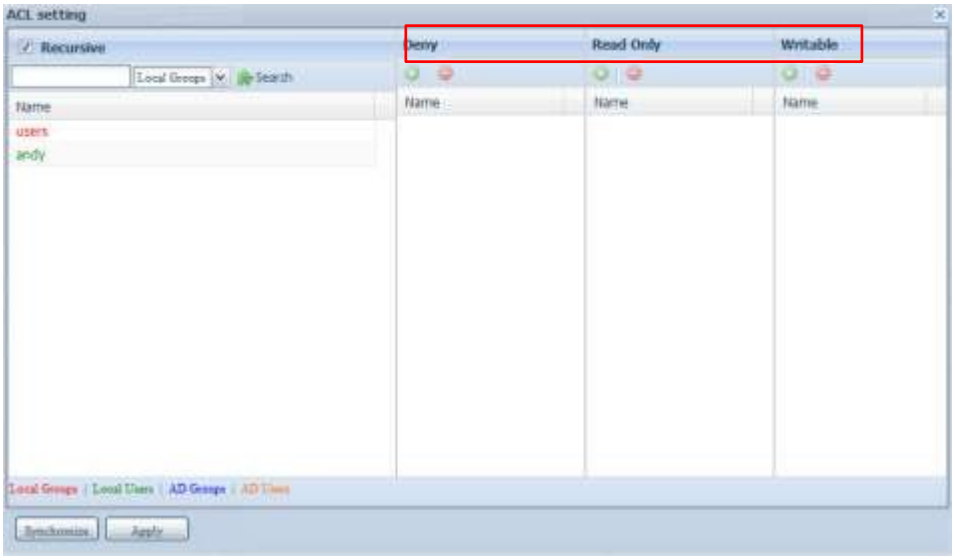


Table 33: ACL settings

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.

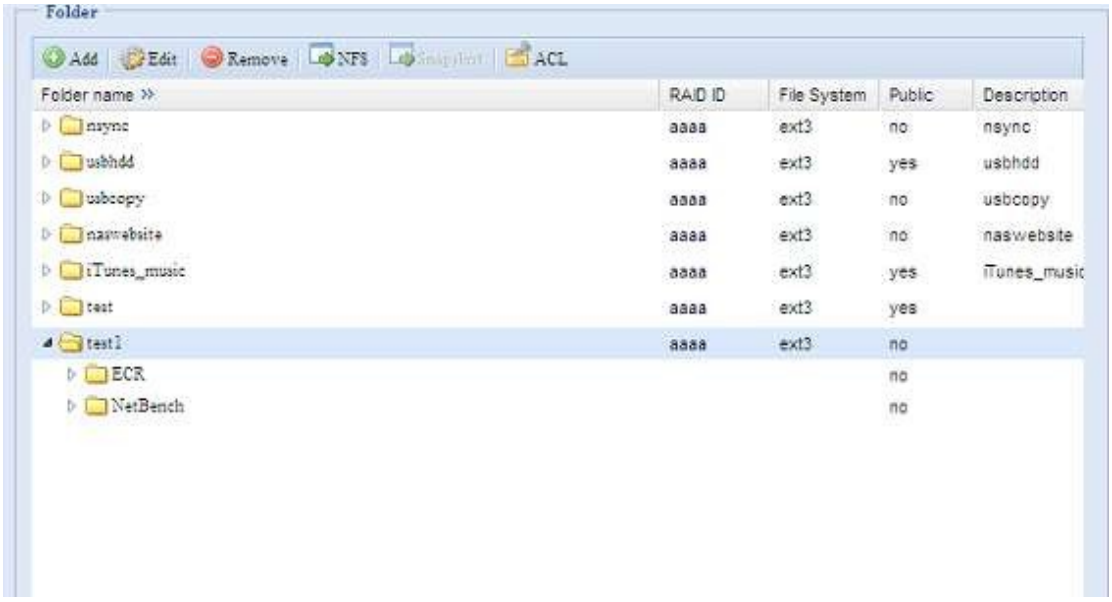
To configure folder access, follow the steps below:

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: Deny > Read Only > Writable

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.

Figure 121: Sub folders



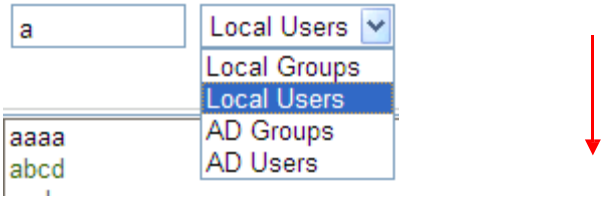
The ACL can only be set for share and sub-folders level, not for files.

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.

Figure 122: Search

Figure 123: Drop down menu

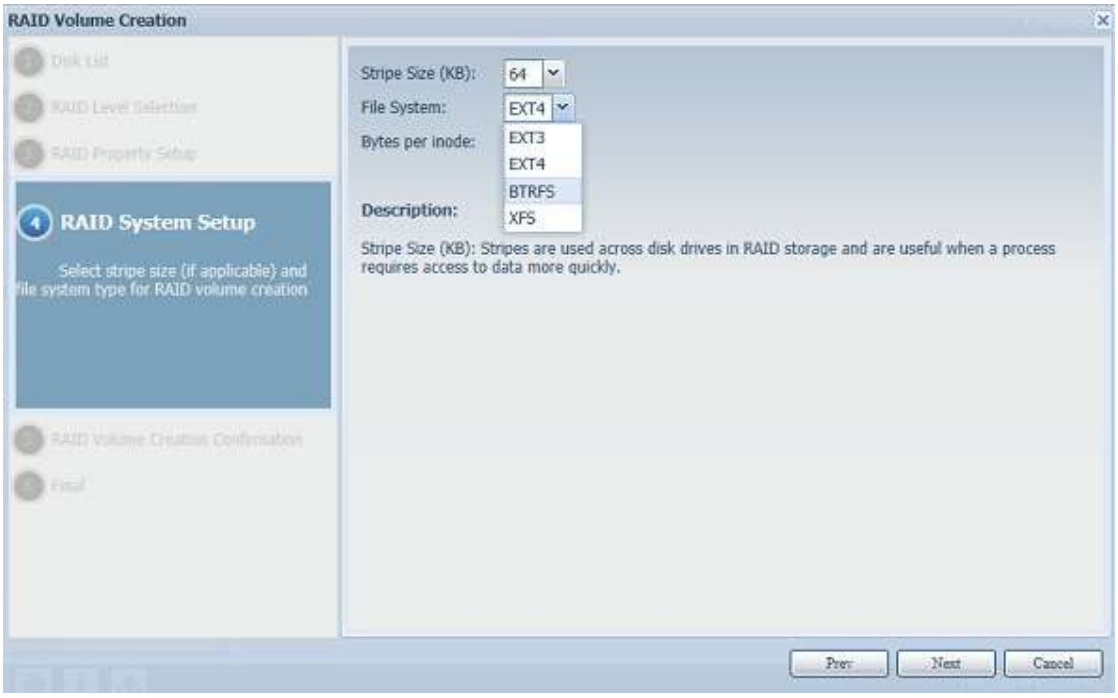


The system will list up to 1,000 users from the chosen category. To narrow your search, enter a search term in the blank provided.

4.6.6. Snapshot

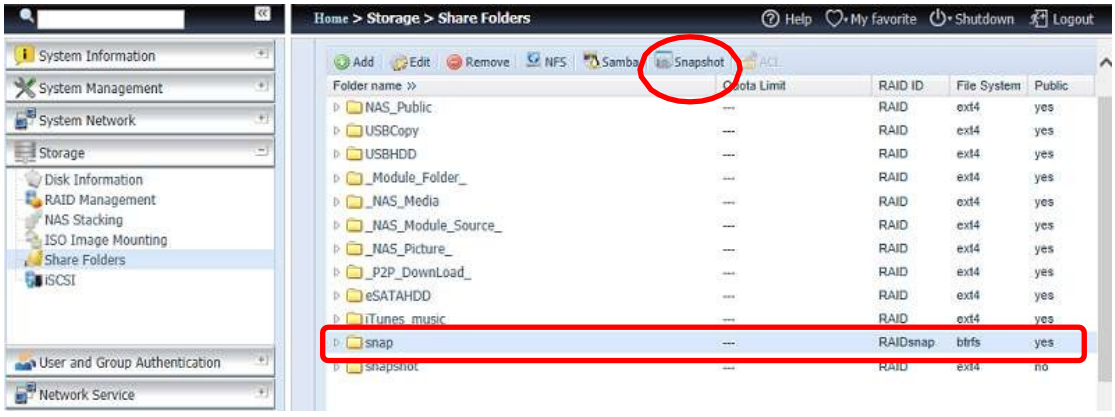
SMB and enterprise CS3160 systems are now capable of saving 16 Snapshot versions of files and folders. For Snapshot to function, a "BTRFS" file system is required.

Figure 124: BTRFS file system



Any folder using a "BTRFS" file system is capable of being included in the Snapshot function. In the "Share Folder" submenu, the Snapshot button is available in the tool bar.

Figure 125: Snapshot button



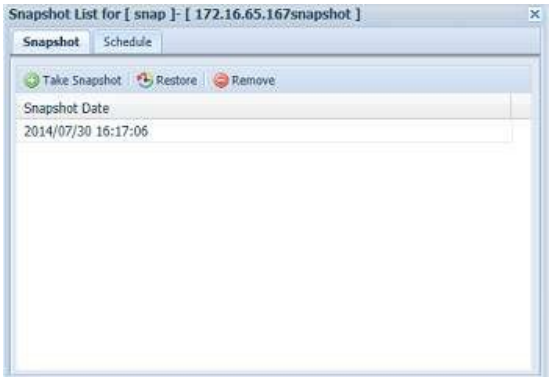
4.6.6.1. Taking a Snapshot

Click on the "Snapshot" button. The management screen will then appear as below for the associated folder.

Figure 126: Management screen

To manually take a Snapshot, simply click “Take Snapshot” and the Snapshot history will be listed. It can store up to 16 versions.

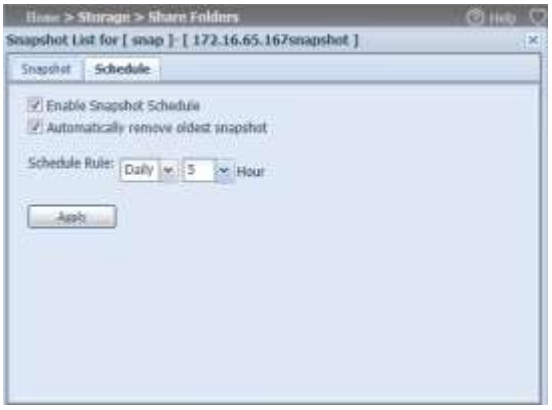
Figure 127: Manual snapshot



To locate where the Snapshot files or folders are stored, please browse to \\System_IP\Snapshot. Please note that you will need to have the relevant folder permissions enabled for your account.

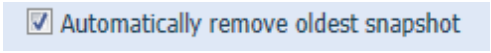
Besides manual Snapshots, this feature also allows for scheduled backups. Click on “Schedule” and the setup screen will appear. Check “Enable Snapshot Schedule” and select the desired Snapshot interval. Options include Daily, Weekly, or Monthly.

Figure 128: Scheduled snapshot



Since files and folders are limited to 16 Snapshots versions, the "Automatically remove oldest Snapshot" option allows for the removal of the oldest version automatically once the limit is reached.

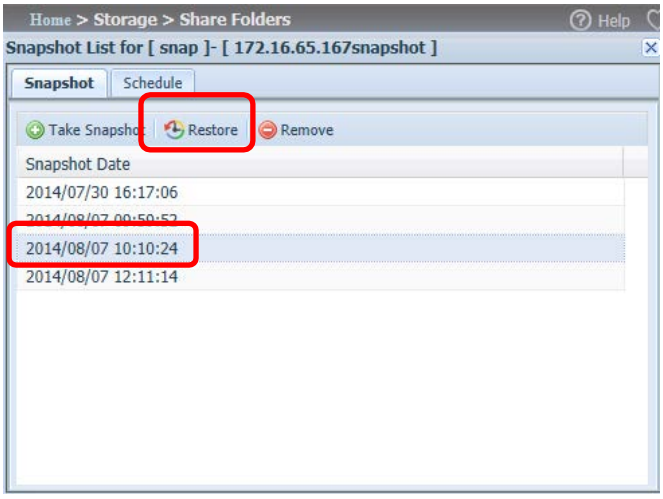
Figure 129: Automatically remove oldest snapshot



4.6.6.2. Snapshot Restore

To restore a Snapshot, simply select the desired version from list and click "Restore". Once the restore confirmation has been made, the selected Snapshot will overwrite the current associated file or folder.

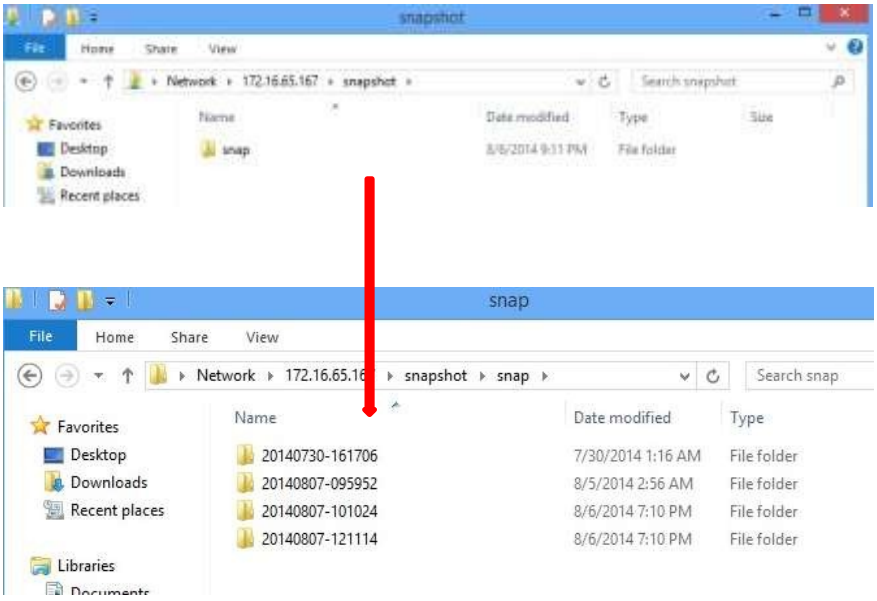
Figure 130: Snapshot selection



The other way to restore a recorded Snapshot version is manually by browsing to the "Snapshot" folder via SAMBA (\\System_IP\Snapshot). All Snapshot versions are stored here, and you can copy or paste to restore a version manually.

For example, the NAS system at 172.16.65.167 has a folder named "snap" with a Snapshot version backed up. If the user were to browse to \\172.16.65.167\Snapshot, the following details would be visible:

Figure 131: Example



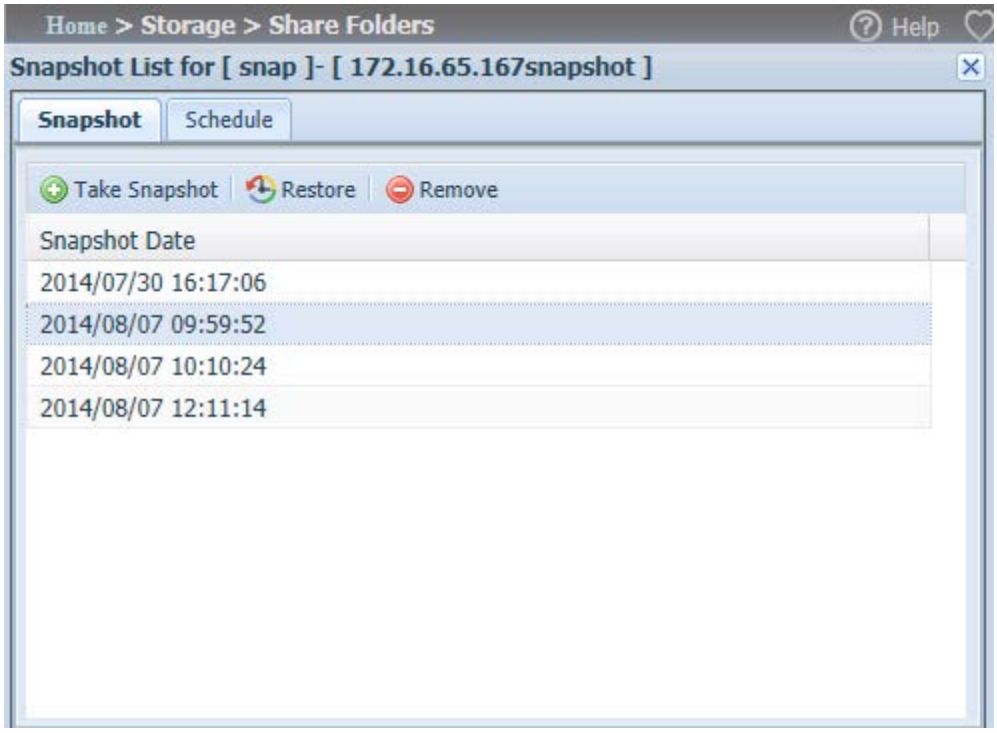
To access the Snapshot folder, a user requires the relevant authentication rights.

If the Snapshot folder is used for iSCSI purposes, it can only be restored from the WebUI (i.e. through the Snapshot feature) and cannot be done manually.

4.6.6.3. Snapshot Removal

To remove a Snapshot, simply select the desired version from list and click "Remove".

Figure 132: Snapshot removal



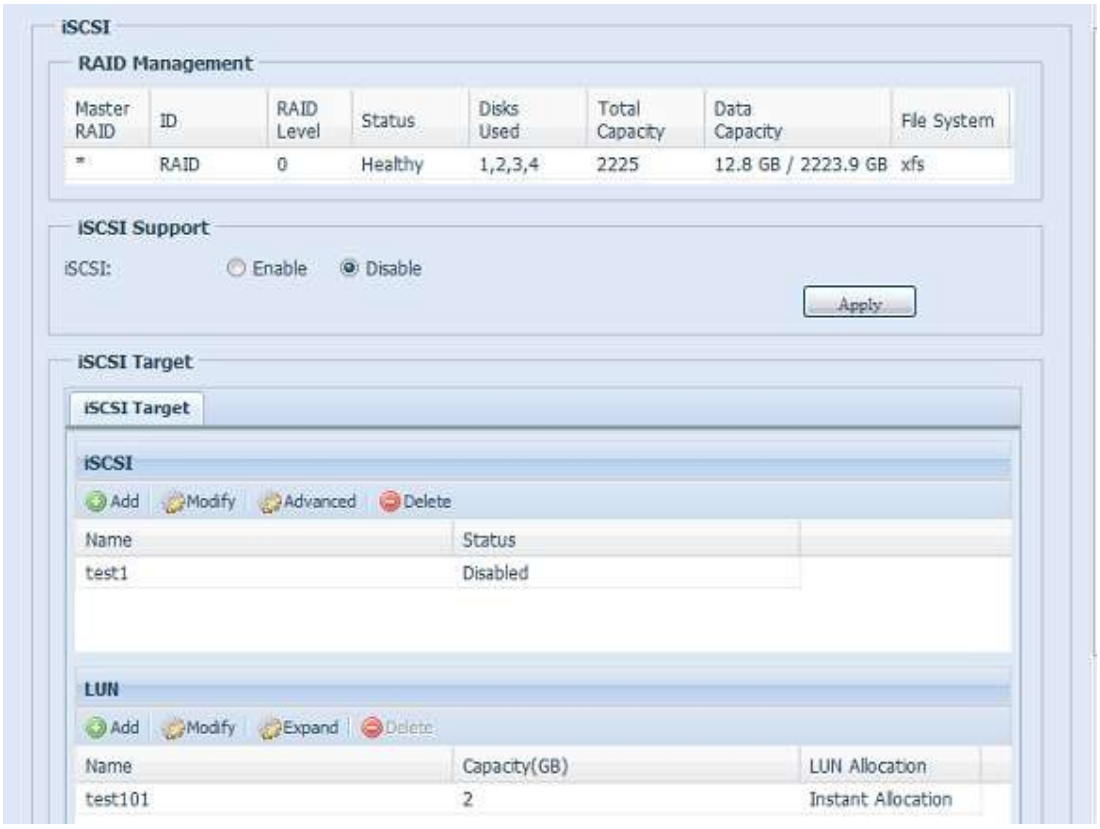
4.6.7. iSCSI

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

Table 34: Allowed iSCSI target number

Model	CS3160
Allowed iSCSI volume	50

Figure 133: iSCSI



4.6.7.1. iSCSI Target

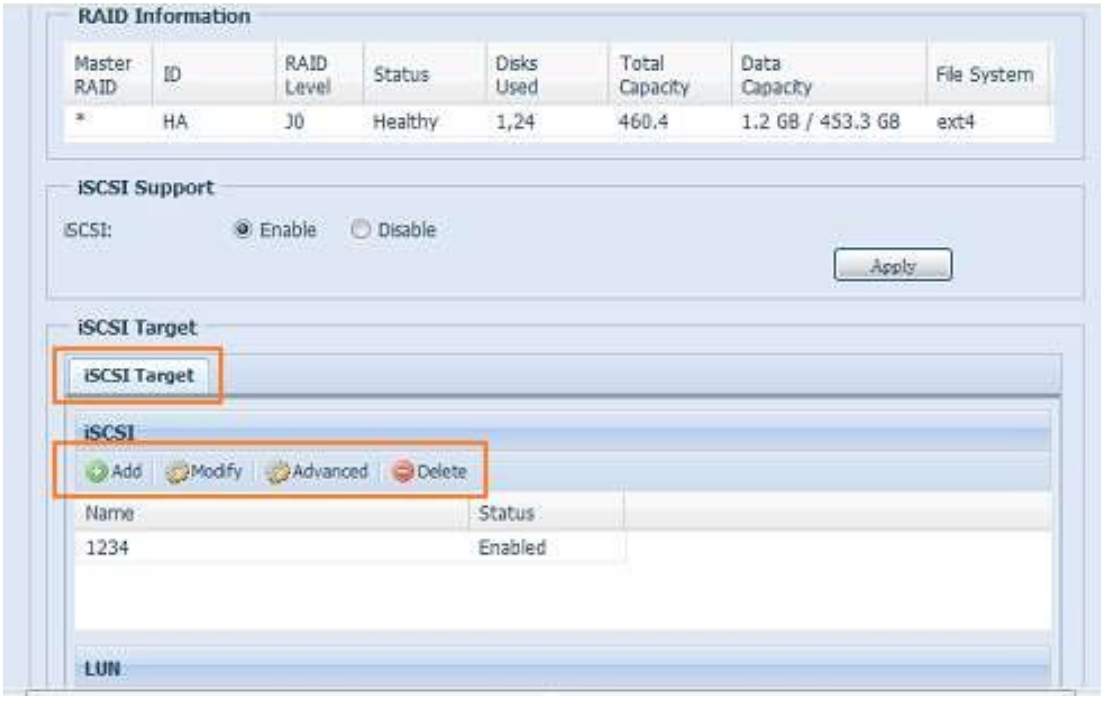
To add iSCSI target volume, click iSCSI with associated RAID volume from its drop down list and select the desired RAID volume.

Table 35: 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 CS3160 associated with the iSCSI setting.
Delete	Click this to delete the iSCSI Target.

4.6.7.2. Allocating Space for iSCSI Volume

Figure 134: iSCSI target



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.

Figure 135: Create iSCSI volume screen

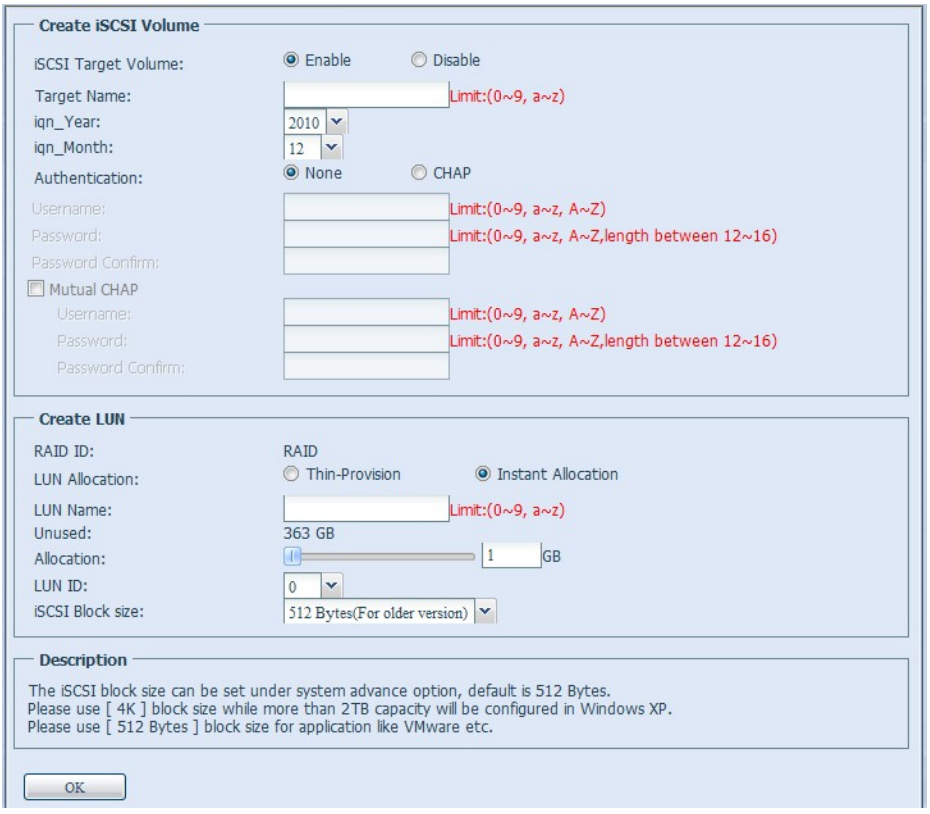


Table 36: Create iSCSI volume

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.

Item	Description
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”.

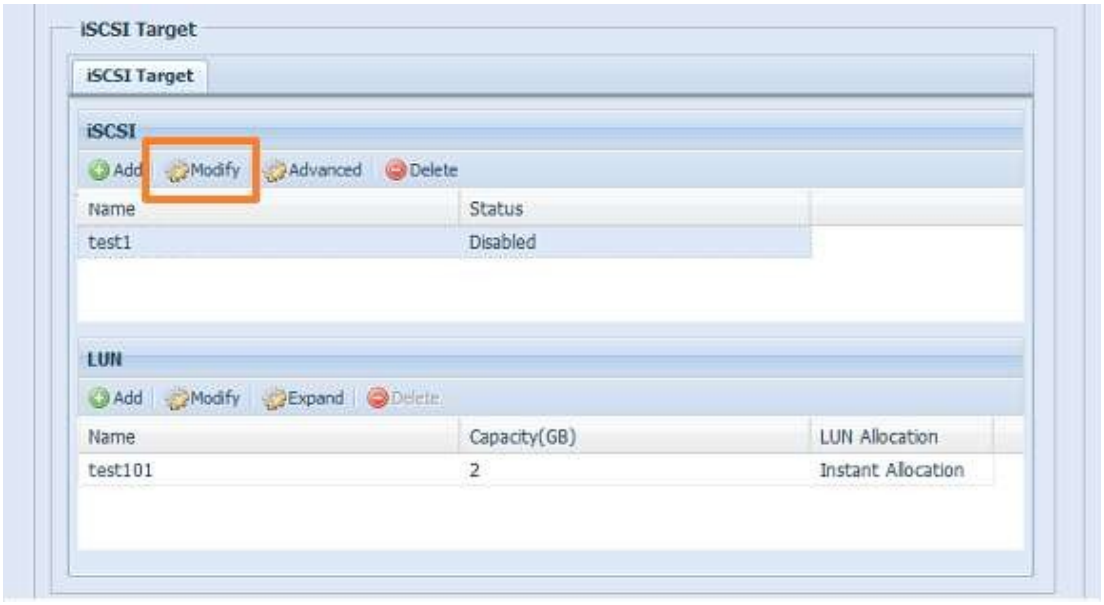
2. Enable the iSCSI Target Volume by selecting Enable.
3. Enter a Target Name. This will be used by the Stackable NAS function to identify this export share.
4. Choose the current year from the Year dropdown.
5. Choose the current month from the Month dropdown.
6. Choose to enable CHAP authentication 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.

4.6.7.3. Modify iSCSI Volume

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

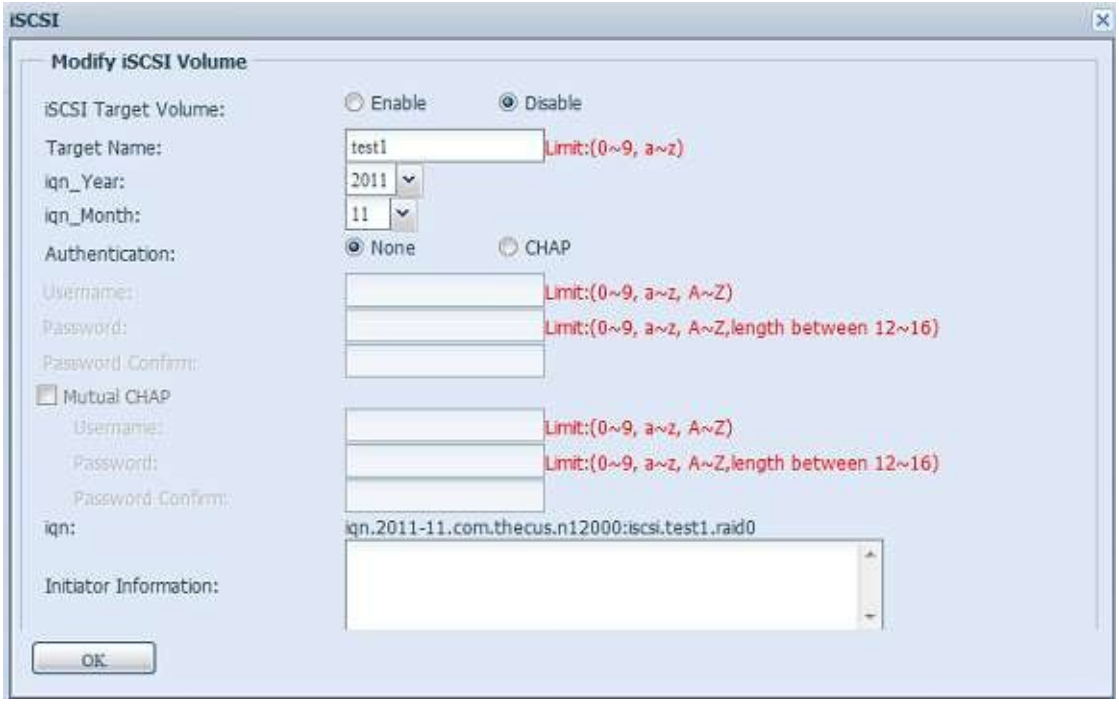
1. Under the iSCSI Target List, click Modify. The Modify iSCSI Volume screen appears.

Figure 136: Modify button



2. Modify your settings. Press ok to change.

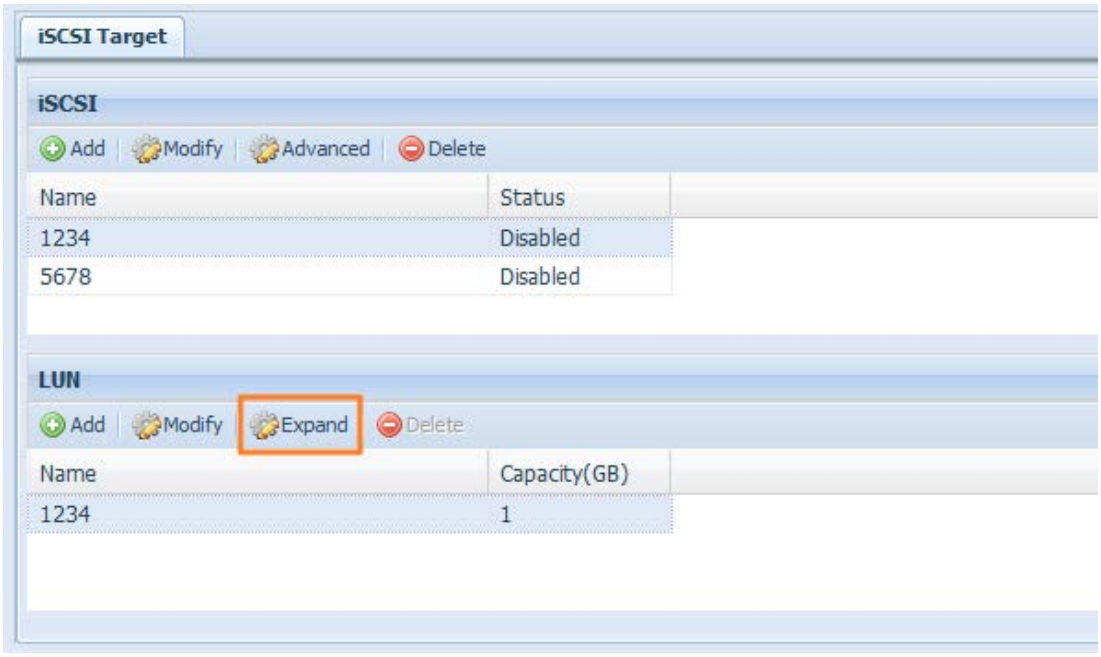
Figure 137: Modify iSCSI volume



4.6.7.4. Expand Volume

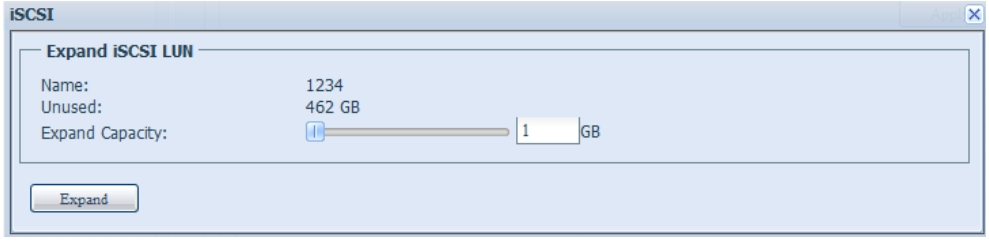
The iSCSI volume is now able to expand its capacity from unused space (Instant Allocation mode only). From the volume list, simply select the iSCSI volume you like to expand and click the Expand button:

Figure 138: Expand button



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.

Figure 139: Dialog box



4.6.7.5. 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.

Figure 140: Delete button

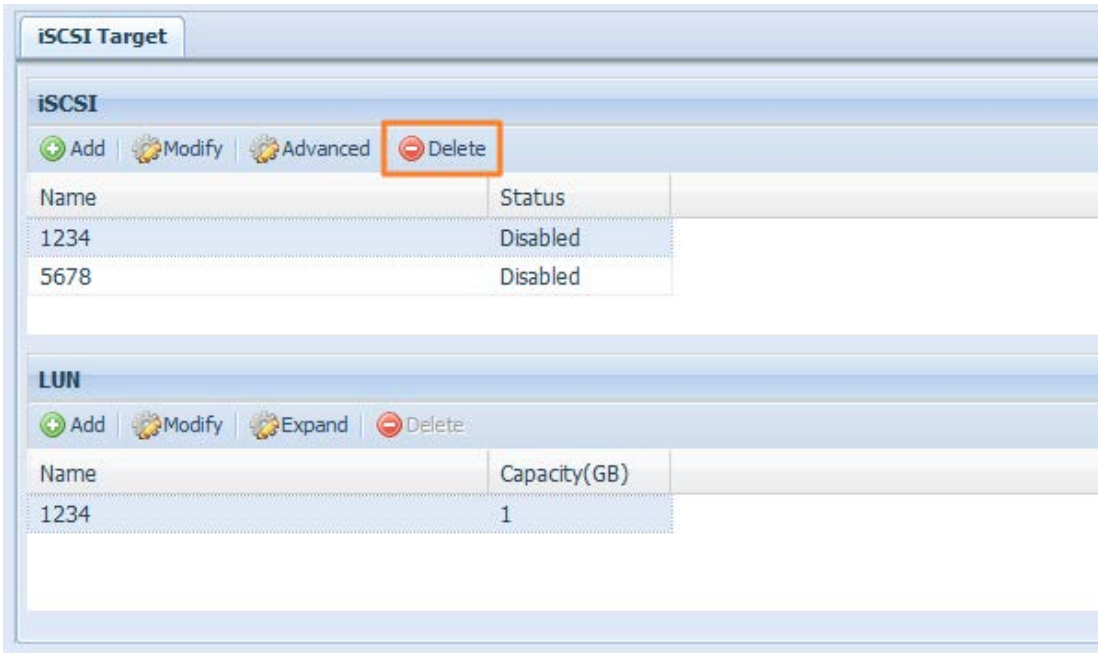
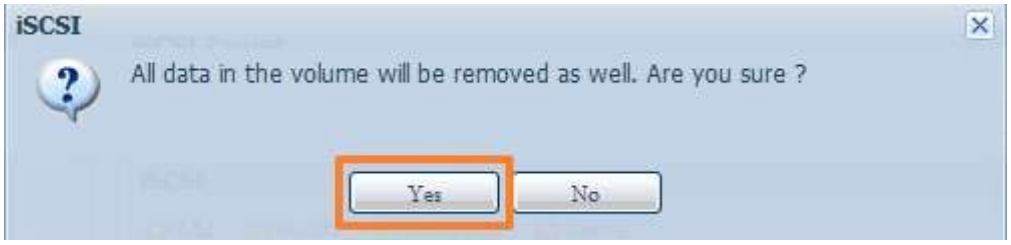


Figure 141: Confirmation prompt



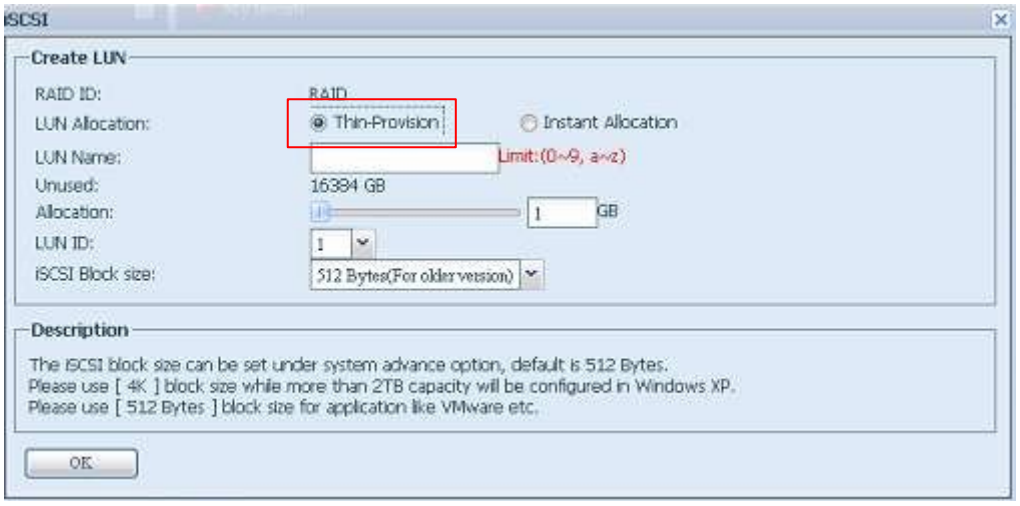
2. Press YES. All data in the volume will be removed.

4.6.8. 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.

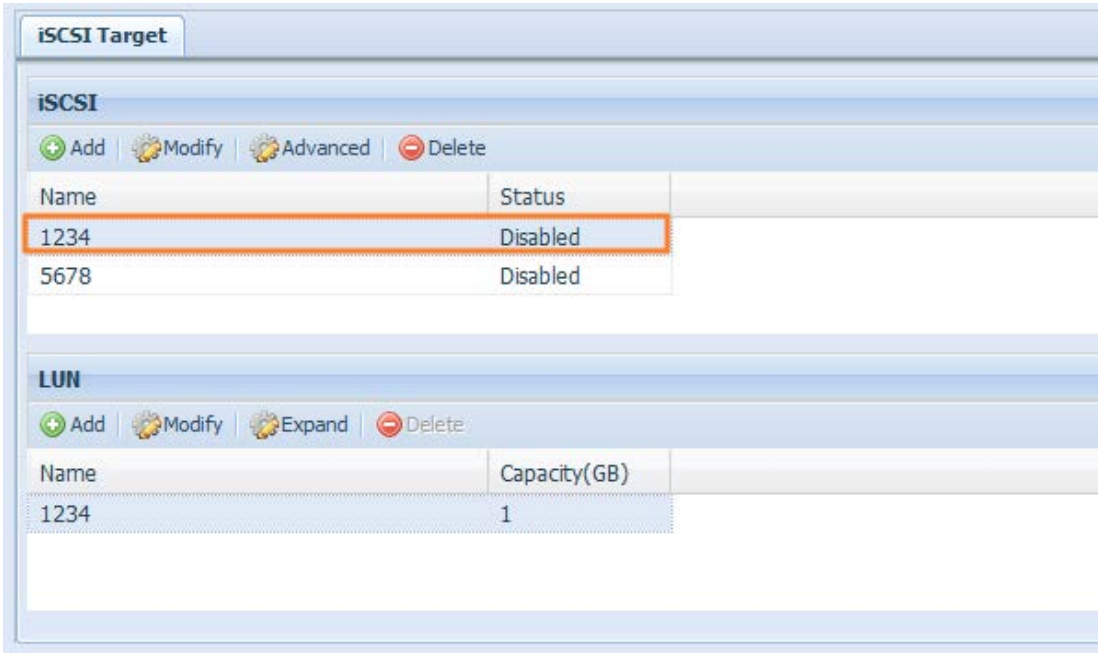
Figure 142: Thin-provision



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.

Figure 143: iSCSI thin-provisioning volume

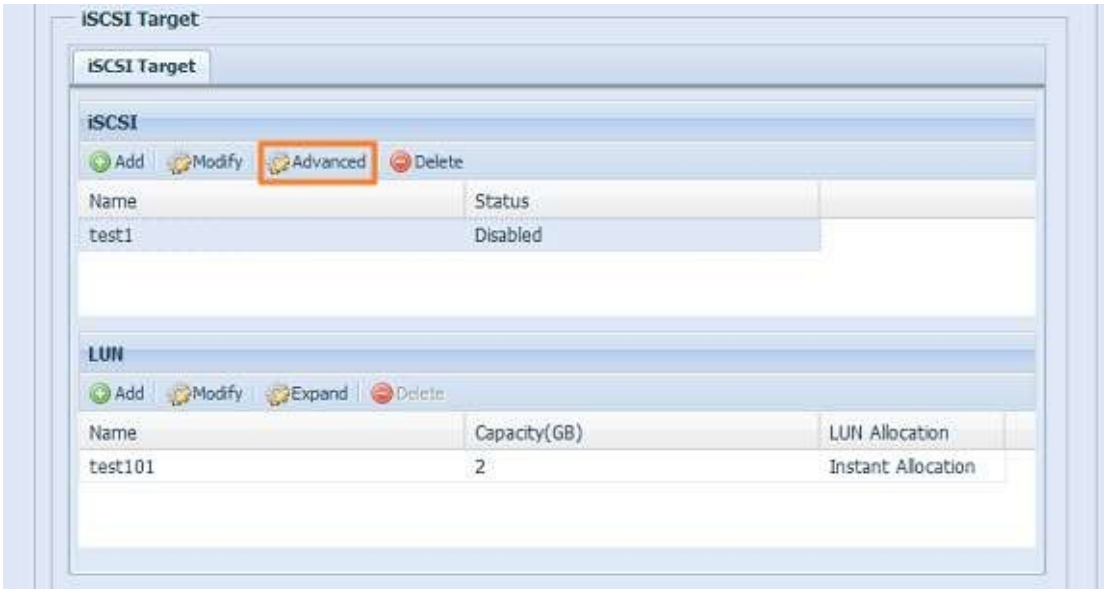


If creating an iSCSI target volume under "Instant Allocation", physical memory is assign to the target, being limited by the available memory. For the iSCSI target volume created under "thin-provisioning", virtual memory is assigned to the volume, which can go up to 16384GB (16TB).

4.6.9. Advanced Option

There are 3 available options for the user to operate the CS3160 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.

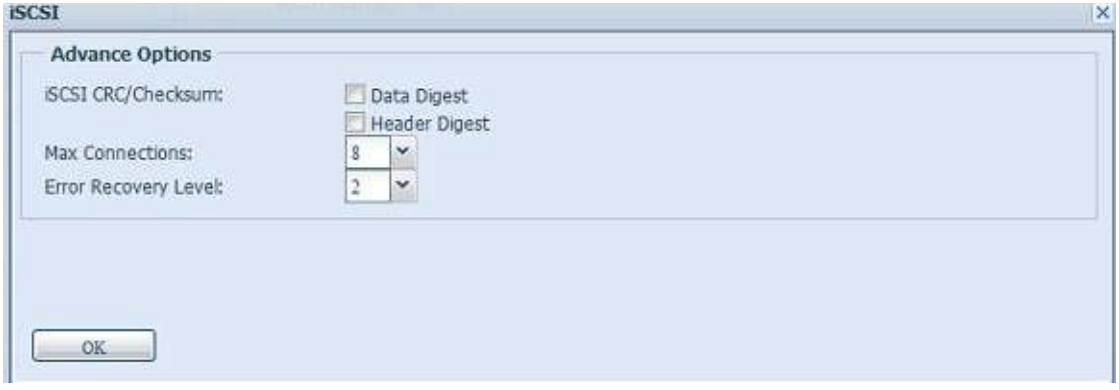
Figure 144: Advanced options



iSCSI CRC/Checksum

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

Figure 145: Advance options



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).

4.6.10. Disk Clone and Wipe

Disks installed on this device are able to utilize the Disk Clone and Wipe function

Figure 146: Disk clone and wipe

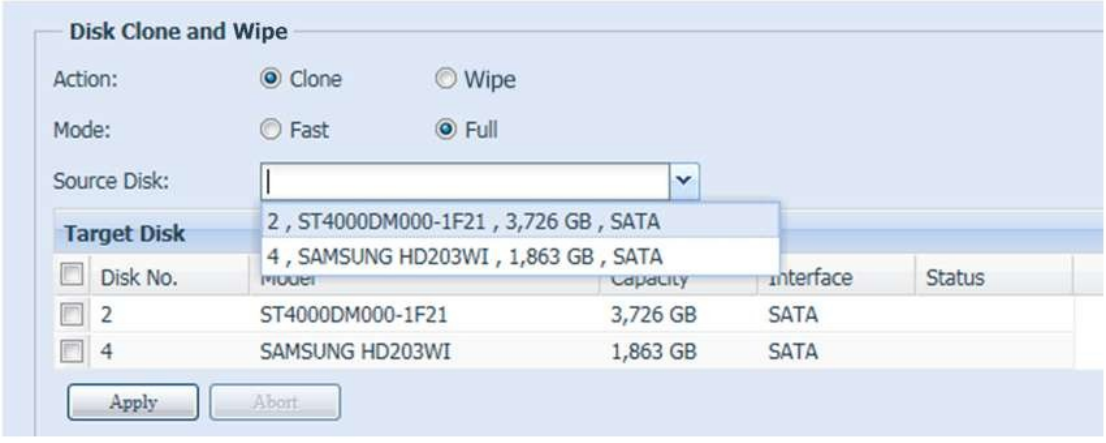
4.6.10.1. Disk Clone

Unused Disks that have been installed on this storage device can utilize the disk clone function. If disks have already been configured in a RAID volume or as a spare disk, they cannot perform disk clone.

To start disk clone, select the source disk from the drop down menu and target a disk from the dialog box as seen below. Carry on to press "Apply," then the task will start. It may take a few hours depending on the size of the disk.

Please be sure the source disk is equal to or smaller than the target disk.

Figure 147: Disk clone



4.6.10.2. Disk Wipe

Disk Wipe is able to erase data from selected disks. Again, disks that have already been configured in a RAID volume or as a spare disk cannot perform this function.

Figure 148: Disk wipe

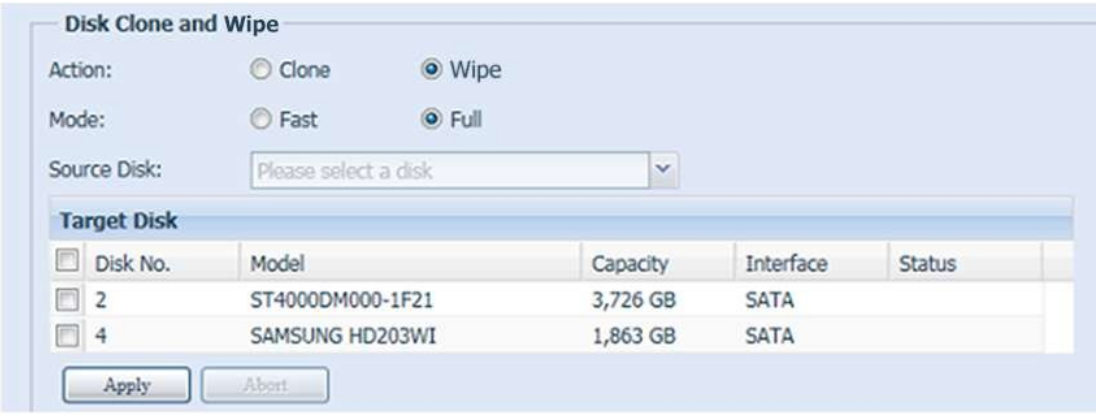


Table 37: General component description

Item	Description
Action	Click to choose to perform Disk Clone or Disk Wipe
Mode	2 options can be chosen: Fast: suitable for single disk to many tasks but less information to be displayed Full: suitable for single to single disk operation and will have a complete log recorded during operation
Source Disk	Listed available disks can used as the source disk while performing disk clone
Target Disk	Listed available disks can be used for disk clone or disk wipe
Apply	To save your settings

4.6.11. High-Availability

HA keeps your data active on two separate systems, Kontron Supports Active/Passive HA — provides a fully redundant instance of each node, which is only brought online when its associated primary node fails.

4.6.11.1. HA setup procedure

HA needs two identical Kontron systems (same models and same hard disk slot installed) which are capable for high availability features. One needs to be setup as “Primary” and the second unit as “Secondary”, both units’ needs to have the RAID volume build up prior installation.

NOTICE

Please be notified that if the system has been used as a standalone station before and contained more than one RAID volume with data inside, once it is used for HA, all of data will be destroyed.

Let’s see an example with two Kontron Units.

1st unit: Host name: PMA (172.16.66.25) with JBOD RAID volume. This unit will be setup as the Primary server.

Figure 149: Networking, unit 1

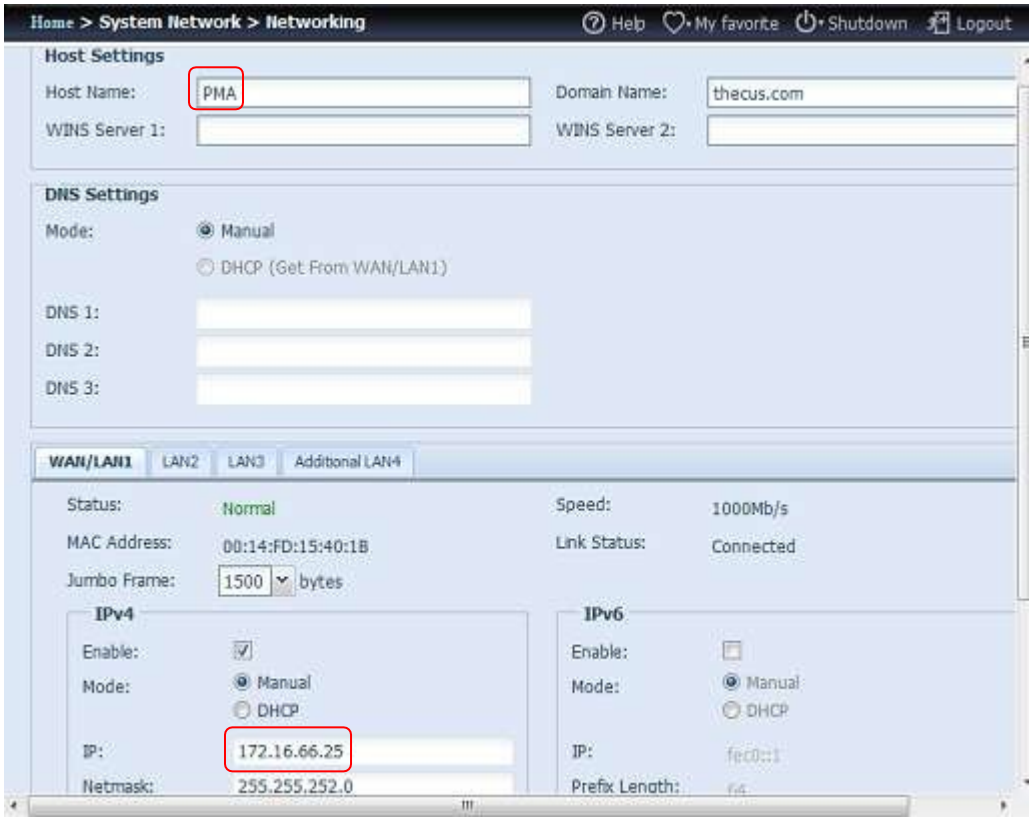
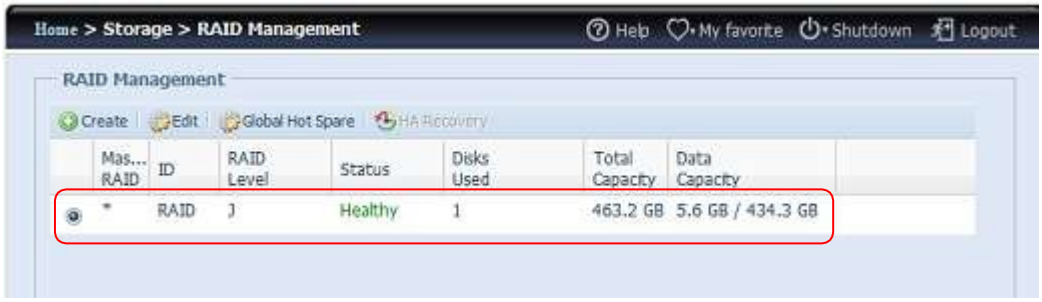


Figure 150: RAID management, unit 1



2nd unit: Host name: PMS (172.16.66.24) with JBOD RAID volume. This unit will be setup as the Secondary server.

Figure 151: Networking, unit 2

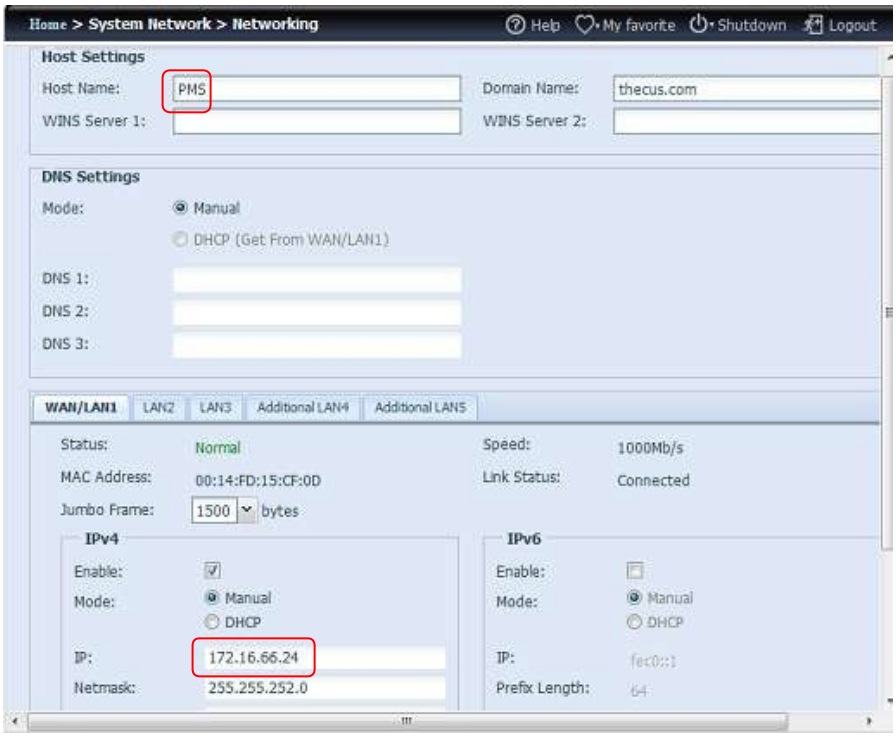
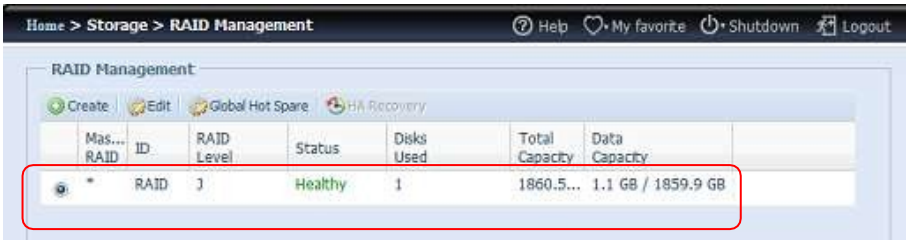


Figure 152: RAID management, unit 2



The HDD capacity of HA Secondary server must be equal or greater than the Primary server or a warning message will appear.

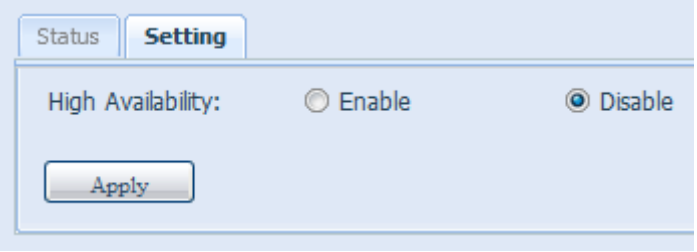
Setting up the Primary Unit for HA

Let's use the Primary unit from our example PMA (172.16.66.25):

I. Login in to web UI of system 172.16.66.25. Then go to "High Availability" HA configuration page under the Storage category.

II. Click on "Enable" radio button, then the setting page will appear.

Figure 153: Setting page



III. Choose the server role of the system, for this example, we will have this unit as 'Primary Server". So "Primary Server" is checked.

Figure 154: Primary server

IV. Choose the "Auto Failback" option, the default is disabled. For more details about auto failback, please refer to the description below.

Figure 155: Auto failback

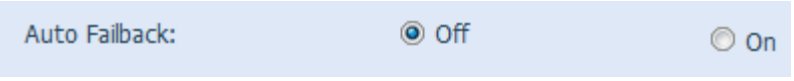
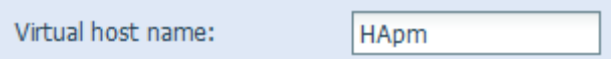


Table 38: Auto failback

Auto Fail Back:	In legacy Heartbeat clusters, the auto failback option would determine whether a resource would automatically fail back to its "Active" node, or remain on whatever node is serving it until that node fails, or an administrator intervenes. The possible values for auto failback were: ▶ on - enable automatic failbacks ▶ off - disable automatic failback When auto failback is off (default): After the original active server is damaged and then returned to a healthy state, the original standby server will remain active and the original active server will go into standby mode. The servers will exchange roles. When auto failback is on: After the original active server is damaged and then returned to a healthy state, the original standby server will go back into standby mode and the original active server will become active again. The servers return to their original roles. With or without auto failback, synchronization will begin immediately without a break in service when the damaged server returns. The roles described above are assumed immediately and do not need to wait for synchronization. The virtual IP will always be mapped to the current active server.

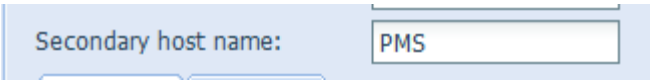
V. Fill in the "Virtual Server" hostname information for further access need. For this example, we will use "HApm" for the virtual server hostname.

Figure 156: Virtual host name



VI. Fill in the "Secondary Server" hostname information. For this example, we will use "PMS" for the secondary server hostname. Please make sure the associated Secondary server with the "PMS" host name has been setup.

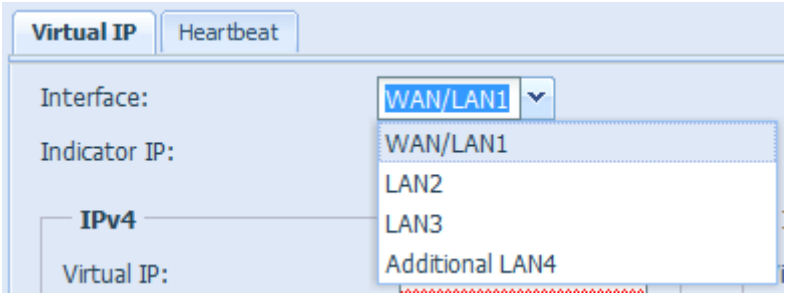
Figure 157: Secondary host name 1



VII. Fill in the "Virtual IP" information:

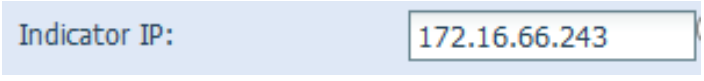
1. Please select the network interface from the drop down list of physical connective available. It can be either on board LAN ports or additional add-in NIC, even 10G.

Figure 158: Secondary host name 2



2. Input "Indicate" IP address. This "indicate IP" is used for the system to ping out then check whether the system is still alive. So please input an IP address that is going to response properly.

Figure 159: Secondary host name 3



3. Filled in IP information for the "Virtual IP" and "Secondary Server IP" in either IPv4 or IPv6. For our example we chose the "WAN/LAN1" for the connection interface and virtual IP 172.16.66.87. The secondary server IP address is 172.16.66.24 has mentioned earlier.

Figure 160: Secondary host name 4

VIII. Choose the network interface for heartbeat in between the systems. It can be selected from the drop down list, if there is additional LAN card that has been installed, such as 10G card, it can be used for the heartbeat role. After inserting the IP addresses for direct link needed in between the primary and secondary servers, default value will appear. Normally, no modifications will be required.

The example here we will use the "Additional LAN4" which is a 10G NIC to be used for the heartbeat link between the primary and secondary servers.

Figure 161: Interface

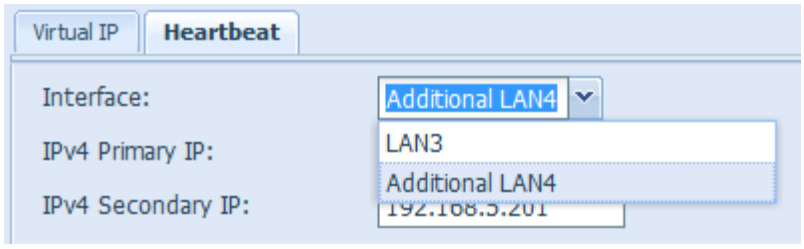
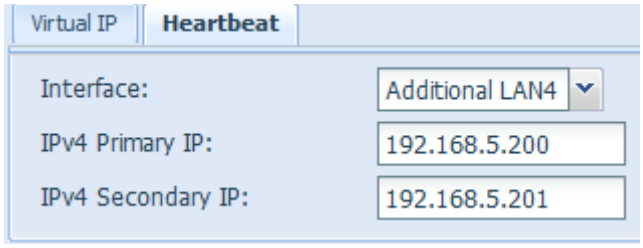


Figure 162: Default value



IX. Advance options can be setup by pressing the associated button.

Figure 163: Advance options button

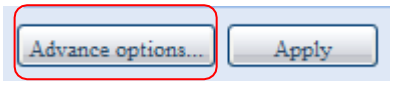


Figure 164: Advance options

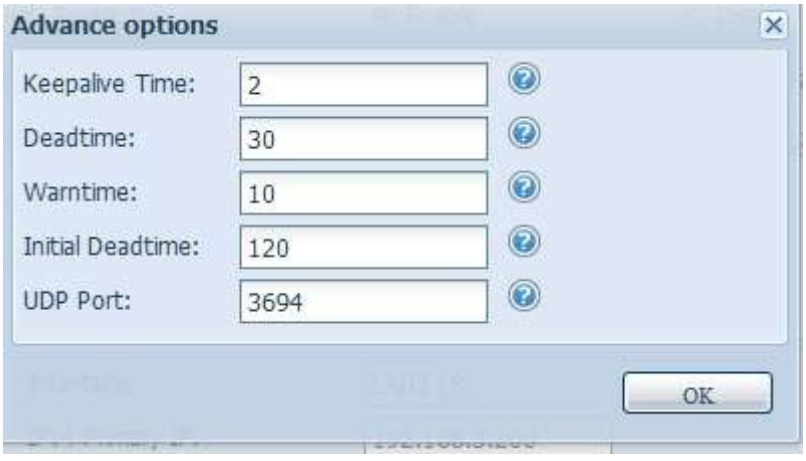


Table 39: Heart beats configuration

Item	Description
Keep alive time	The keep alive directive sets the interval between heartbeat packets. It is specified according to the Heartbeat time syntax.
Dead time	The dead ping directive is used to specify how quickly Heartbeat should decide that a ping node in a cluster is dead. Setting this value too low will cause the system to falsely declare the ping node dead. Setting it too high will delay detection of communication failure. This feature has been replaced by the more flexible ping resource agent in Pacemaker, and should no longer be used.
Warning time	The warn time directive is used to specify how quickly Heartbeat should issue a "late heartbeat" warning.

Item	Description
Initial dead time	The initial dead parameter is used to set the time that it takes to declare a cluster node dead when Heartbeat is first started. This parameter generally needs to be set to a higher value, because experience suggests that it sometimes takes operating systems many seconds for their communication systems before they operate correctly.
UDP port	The udp port directive specifies which port Heartbeat will use for its UDP intra-cluster communication. The default value for this parameter is UDP 694 port.

X. Click "Apply", the Primary server will prompt the message below and wait for the "Standby" server settings to be completed.

Figure 165: Message prompt

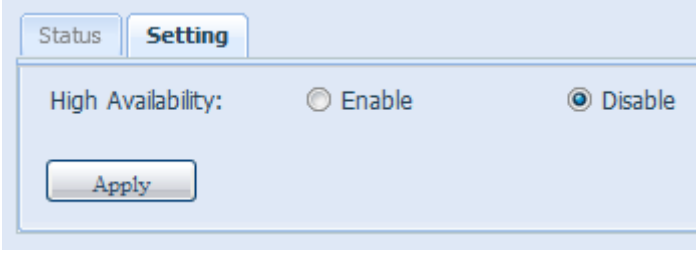
Setting up the Secondary Unit for HA

The secondary unit for our example is PMS (172.16.66.24):

XI. Login in to the web UI of the system 172.16.66.24 then go to "High Availability" HA configuration page under the Storage category.

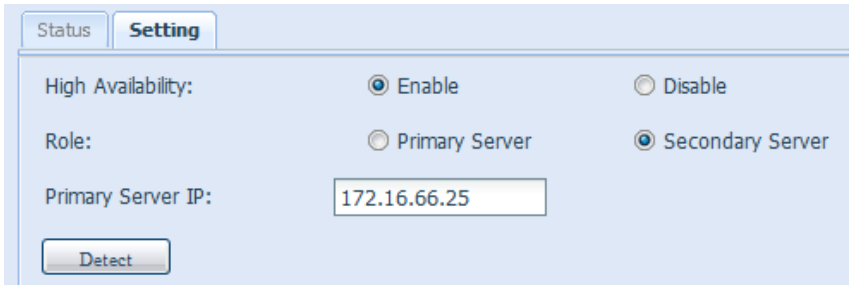
XII. Click on the "Enable" radio button, the setting page will appear.

Figure 166: Enable radio button



XIII. Choose the server role of the system, for this example, we will have this unit set as the "Secondary Server". So "Secondary Server" is checked. After, please fill in the associated "Primary Server" IP address.

Figure 167: Role radio button



XIV. Click "Detect" and the Secondary unit will start to check for the Primary server status. If the Primary server has replied properly, then the message will appear as below.

Figure 168: Message

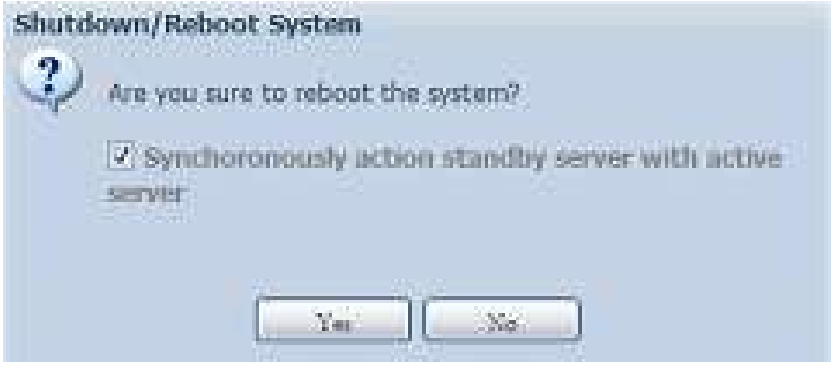
Please check the Primary Server unit. You will see an interactive message saying to reboot both "Primary" and 'Secondary" server together to complete the High Availability settings.

The last state of the Primary server is: waiting for the Secondary server as shown in the screen shot below:

Figure 169: System standing by

After the Secondary server has communicated with Primary Server successfully, then the state will changed to:

Figure 170: System shutdown/reboot



Click "Yes" to reboot both Primary and Secondary server.

If the communication has failed then you will see an error message as below.

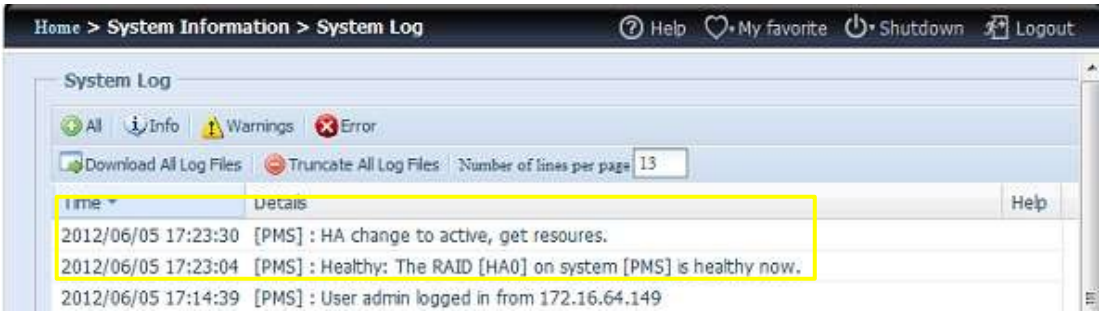
Figure 171: Error message

Conditions in which the secondary server will take over to play the role as Active:

1. Primary server RAID is damaged
2. Loss of the primary server's data port connection
3. Primary server goes down for any other reason

When the primary server encounters the above-mentioned situations, the secondary server (PMS) will immediately take over to play the role as active. The secondary server's system log will show "HA changed to active, getting resources", and "Healthy: The RAID [HA] on system [PMS] is healthy now."

Figure 172: System log



At this time, the virtual IP address will be mapped to the PMS system because it is in an active state.

4.6.11.2. HA Ready

After both Primary and Secondary systems has rebooted, the HA link status and the HA RAID volume can be seen from the HA status page.

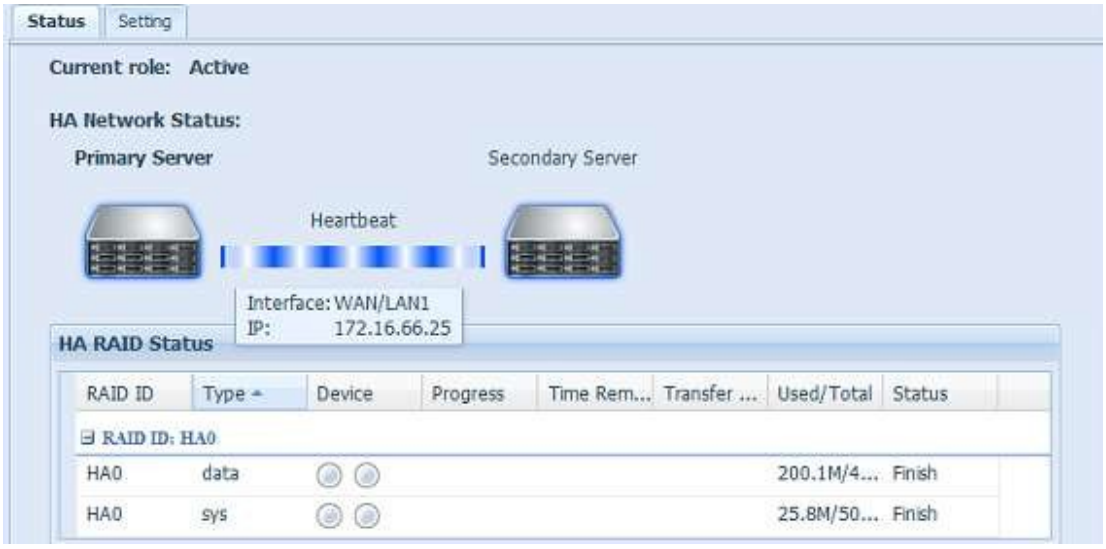
Please note, it will take 1~2 minutes to complete the primary and secondary servers' role played. If both servers are displayed as standby, please wait for the systems to synchronize with each other.

Figure 173: Status

From the HA Primary server "PMA (172.16.66.25)" it will denote the role of "Active" and for the "PMS (172.16.66.24)", it will show the role as Standby.

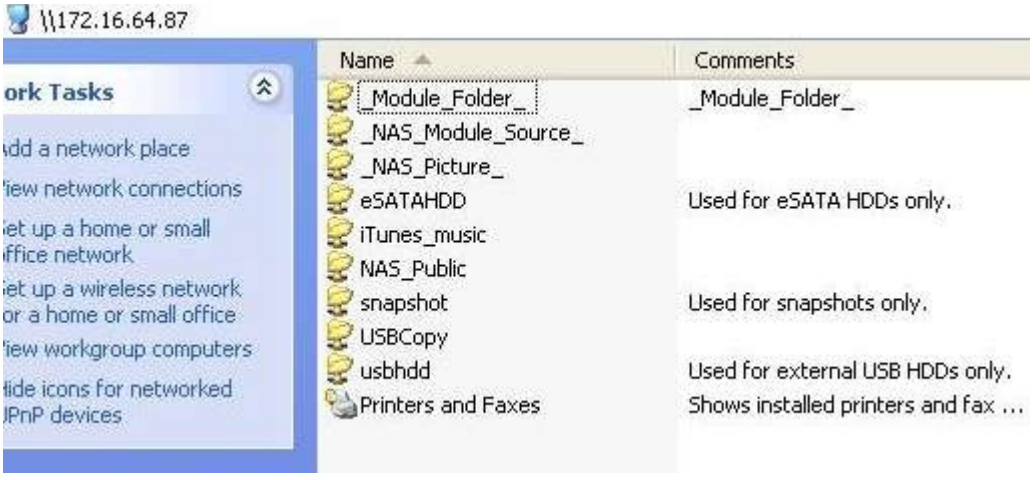
The HA RAID volume status can be found as shown in the screen shot below.

Figure 174: HA RAID volume status



The user can access this newly create HA system by its virtual IP. Using widows, the user can simply input 172.16.64.87 or HApm in the navigation bar then the available share files will be listed as below:

Figure 175: HA system



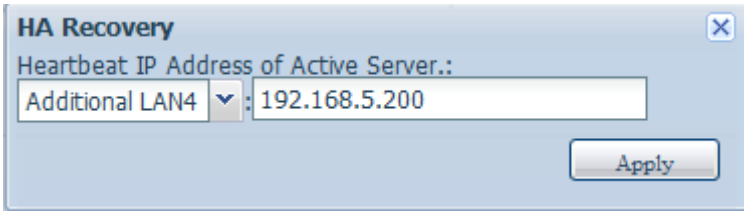
4.6.11.3. HA Recovery

If one of the HA member is down and need to be recovered, simply go to the RAID management page and the "HA Recovery" icon will be available.

Click on the "HA Recovery" icon, then the system will prompt a box to inquire about the Active server heartbeat link IP address. After inputting the IP address and pressing Apply, the unit will be recovered fully.

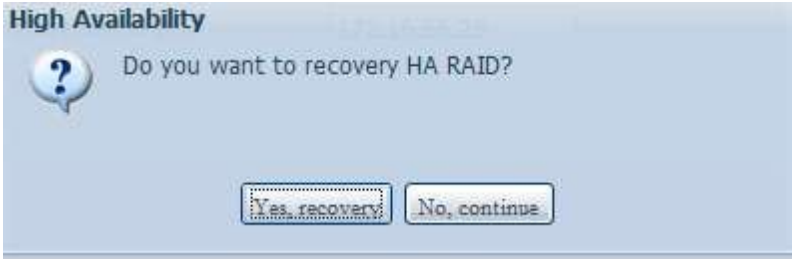
Figure 176: HA recovery icon

Figure 177: HA recovery



Another circumstance where HA recovery might be needed is when the HA button has been enable but the system detected a previously existing HA configuration. Then the screen will prompt the message box as shown below:

Figure 178: Message prompt



If the other HA member is running smoothly, please choose “Recovery HA” to complete HA recovery. Or select “No, continue” to let both HA members has they are.

NOTICE

If there are transfers in progress when the Primary server encounters problems and the Secondary server becomes active, the session will be stopped. Please contact your network administrator to determine whether or not your transfers were completed.

NOTICE

When the original primary server rejoins the HA environment, it will be updated with the newer data from the secondary server to synchronize for HA. Please be aware that the data on the original primary server will be replaced by the data from the secondary server.

4.7. User and Group Authentication

The CS3160 has built-in user database that allows administrators to manage user access using different group policies. From the User and Group Authentication menu, you can create, modify, and delete users, and assign them to groups that you designate.

4.7.1. ADS/NT Support

If you have a Windows Active Directory Server (ADS) or Windows NT server to handle the domain security in your network, you can simply enable the ADS/NT support feature; the CS3160 will connect with the ADS/NT server and get all the information of the domain users and groups automatically. From the Accounts menu, choose Authentication item and the ADS/NT Support screen appears. You can change any of these items and press Apply to confirm your settings.

Figure 179: ADS/NT support screen

A description of each item follows:

Table 40: 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 the CS3160 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 CS3160 for associated filed input:

Figure 180: System properties

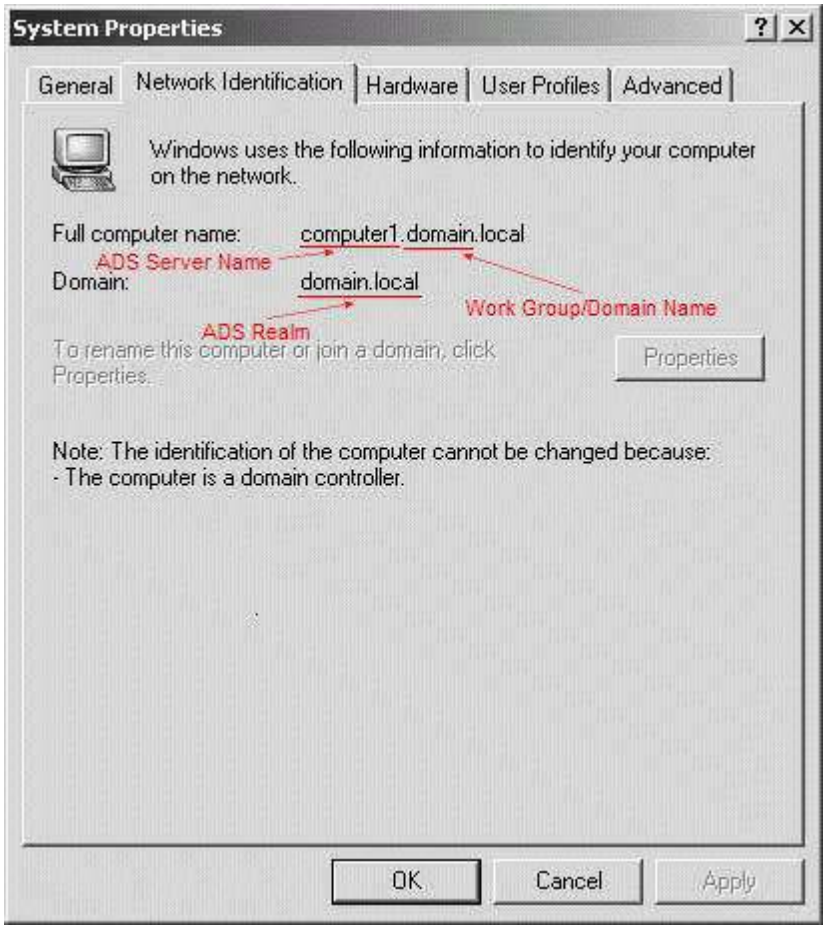


Table 41: AD domain example

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 the CS3160 and ADS should be identical.
- The system time difference between the CS3160 and ADS should be less than five minutes.
- The Administrator Password field is for the password of ADS (Active Directory Server) not the CS3160.

4.7.2. Local User Configuration

From the Accounts menu, choose the User item, and the Local User Configuration screen appears. This screen allows you to Add, Edit, and Remove local users.

Figure 181: Local user configuration screen

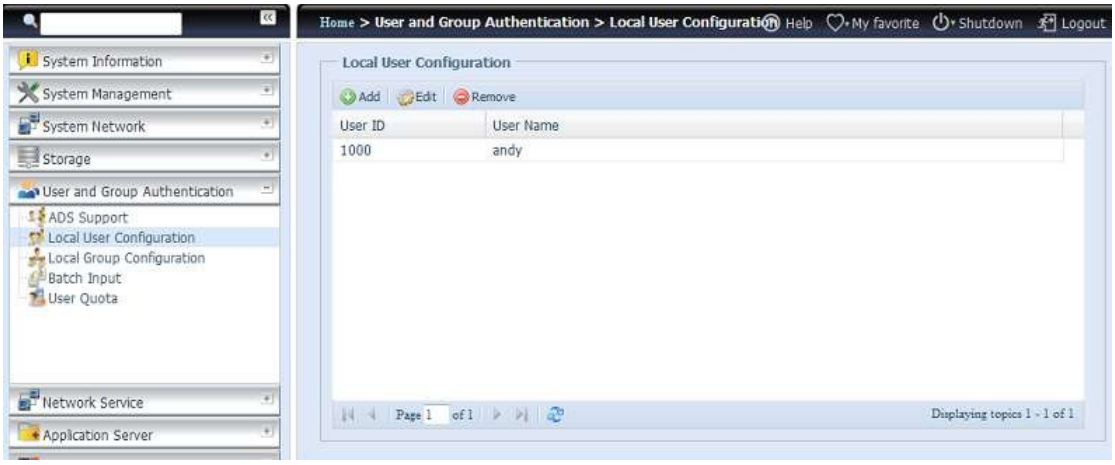


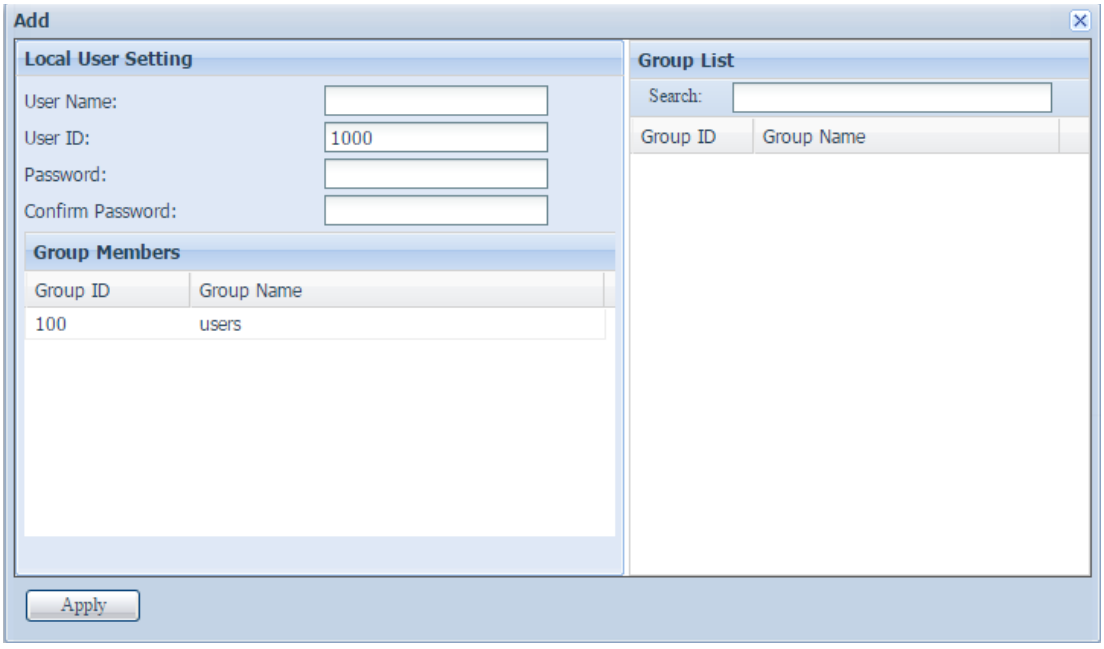
Table 42: Local user configuration

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.

4.7.2.1. 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. Drag and drop to have this user join or leave a group.
6. Press the Apply button and the user is created.

Figure 182: Add users

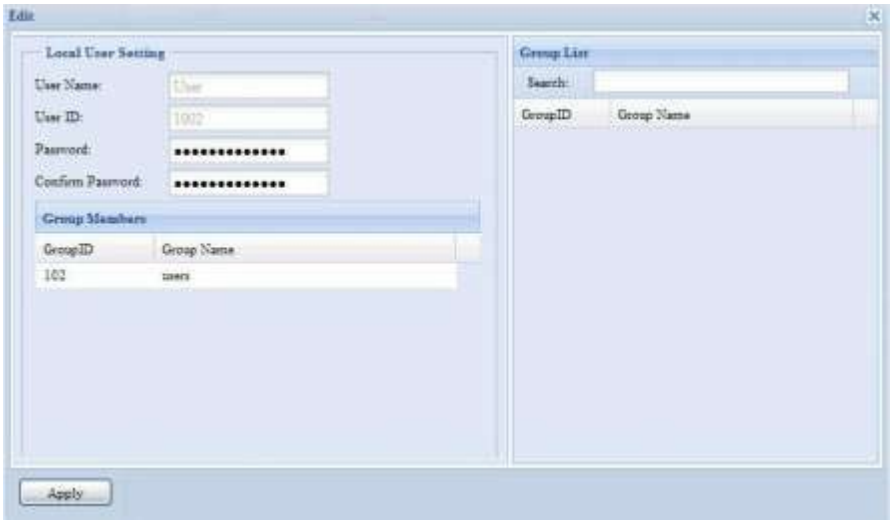


All users are automatically assigned to the 'users' group.

4.7.2.2. 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 drag and drop list items to have this user join or leave a group. Click the Apply button to save your changes.

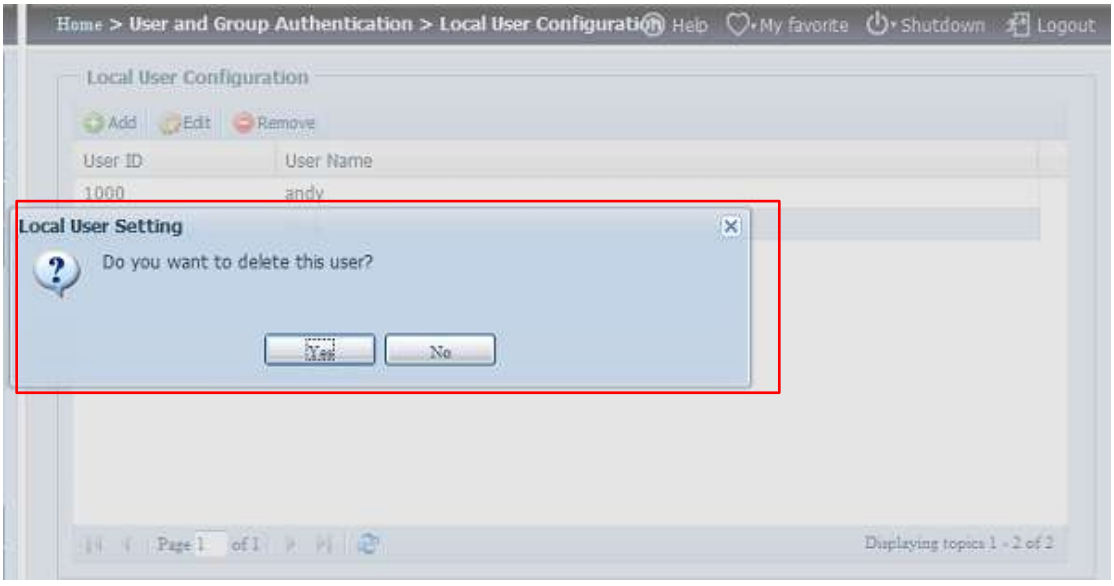
Figure 183: Edit users



4.7.2.3. 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.

Figure 184: Remove users



4.7.3. Local Group Configuration

From the Accounts menu, choose the Group item, and the Local Group Configuration screen appears. This screen allows you to Add, Edit, and Remove local groups.

Figure 185: Local group configuration

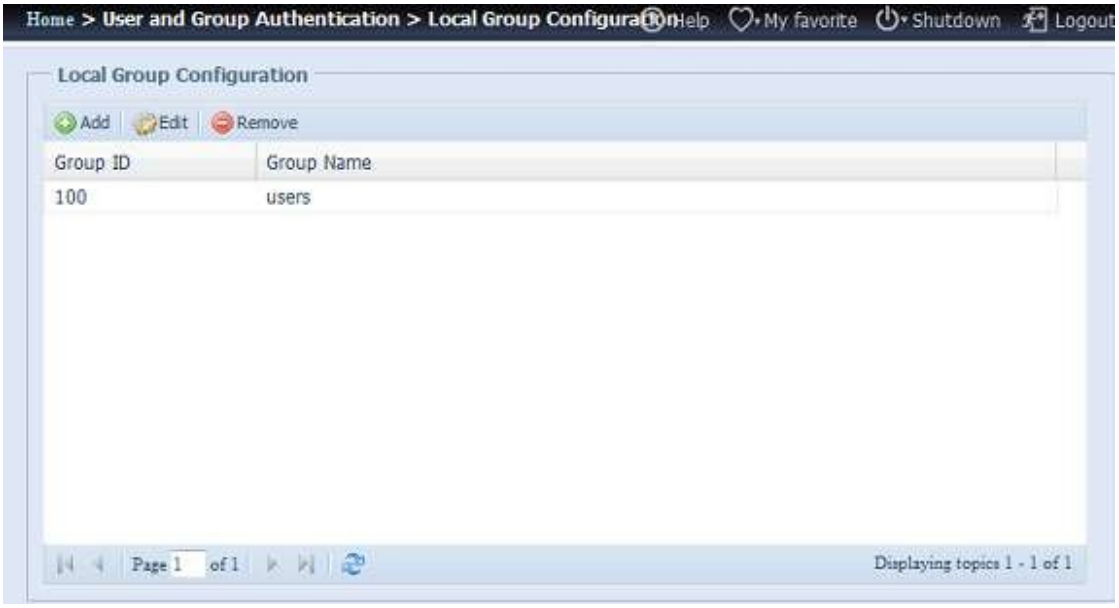


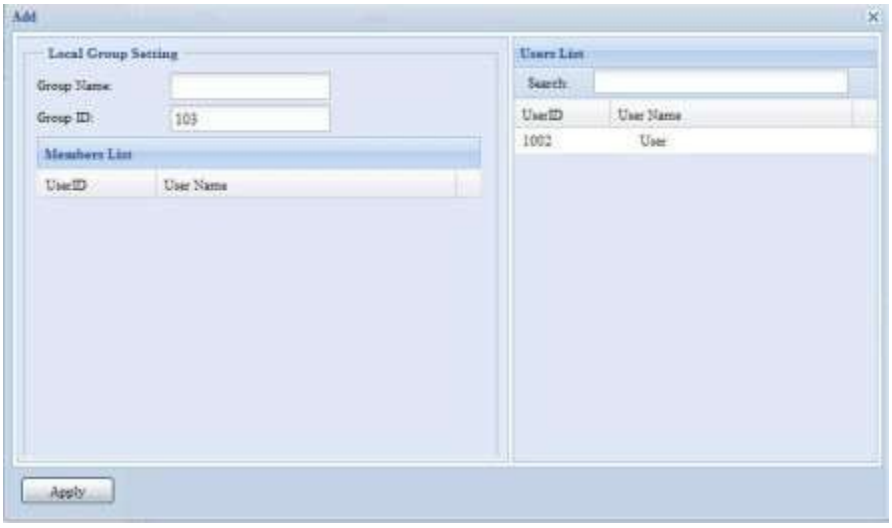
Table 43: Local group configuration

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.

4.7.3.1. 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.

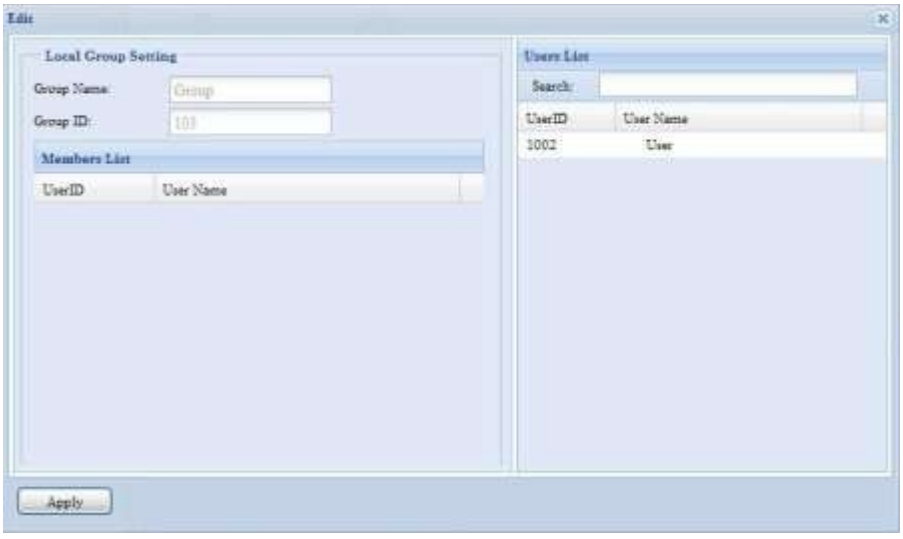
Figure 186: Add groups



4.7.3.2. 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, drag and drop the user from the Users List to move the user into the Members List.
4. To remove a user from a group, drag and drop the user from Members List.
5. Click the Apply button to save your changes.

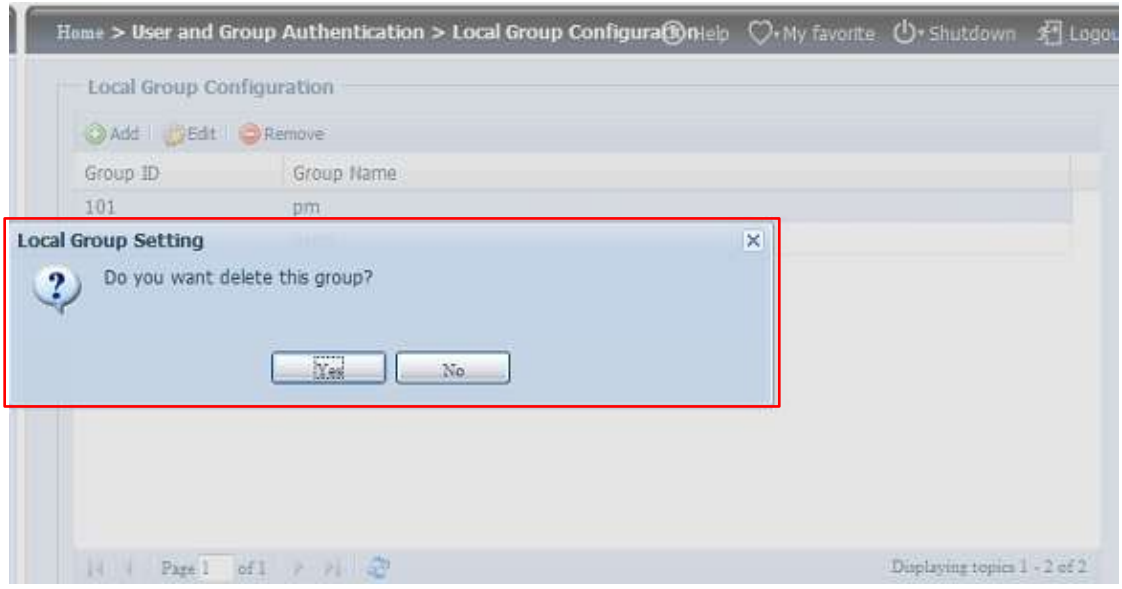
Figure 187: Edit groups



4.7.3.3. 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.

Figure 188: Remove groups



4.7.4. Batch Users and Groups Creation

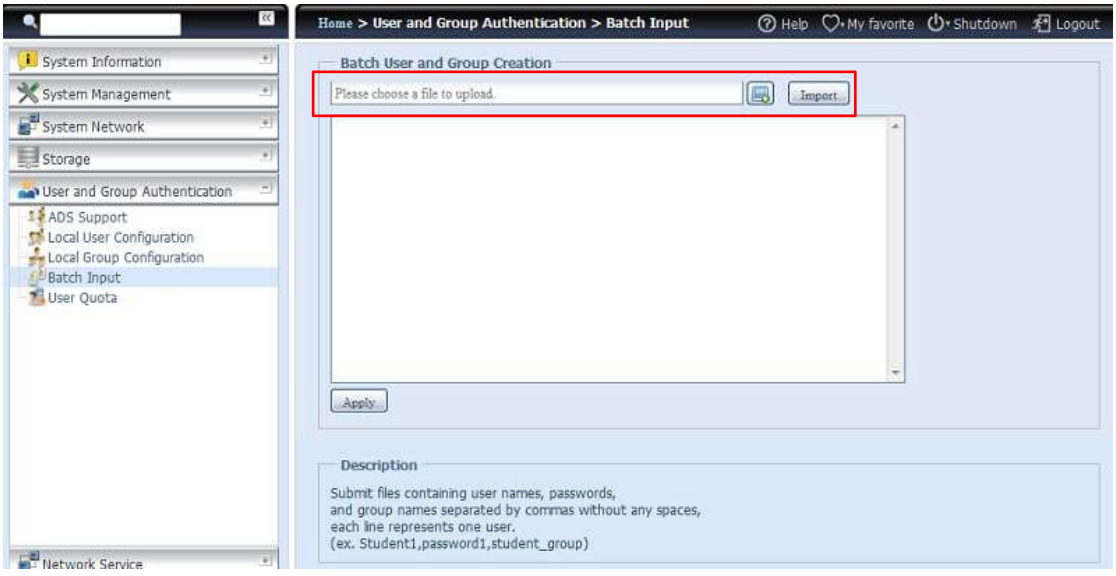
The CS3160 can also add users and groups in batch mode. This enables you to conveniently add numerous users and groups automatically by importing a simple comma-separated plain text (*.txt) file.

From the Accounts menu, click Batch Input and the Batch User and Group Cration dialogue will appear. To import your list of users and groups, follow these steps:

Click the Browse icon to locate your comma-separated text file. The information in the text file should follow this format: [USERNAME], [PASSWORD], [GROUP]

1. Click Open.
2. Click Import to begin the user list import.

Figure 189: Batch user and group creation



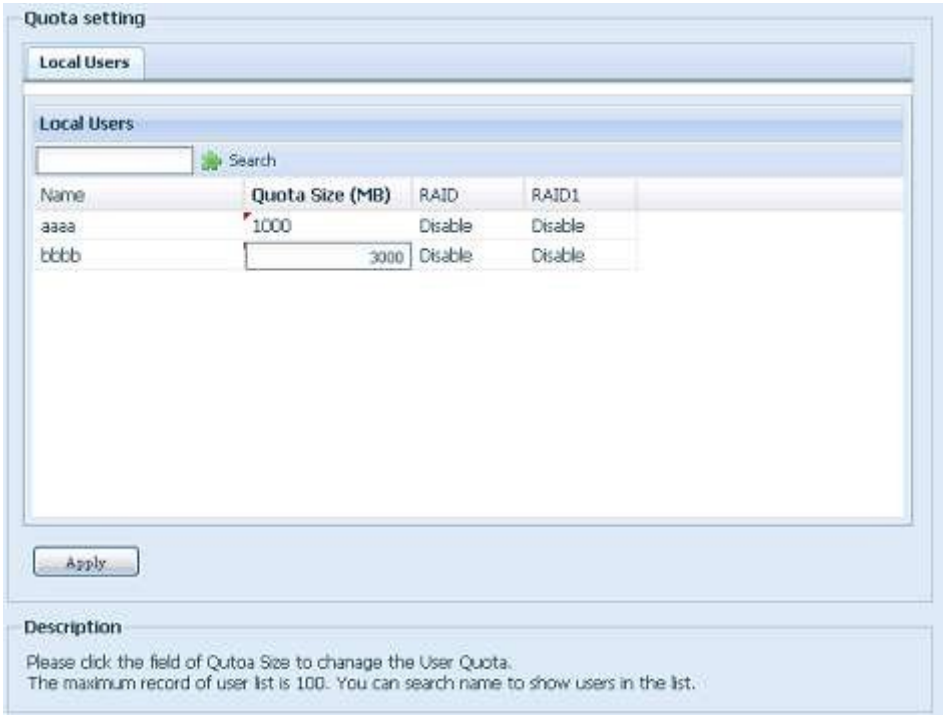
4.7.5. User Quota

The CS3160 supports local or AD users with storage quota limitations in each RAID volume of the system. To enable this function, simply click “Enable”, then apply.

Figure 190: Quota support

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.

Figure 191: Quota setting

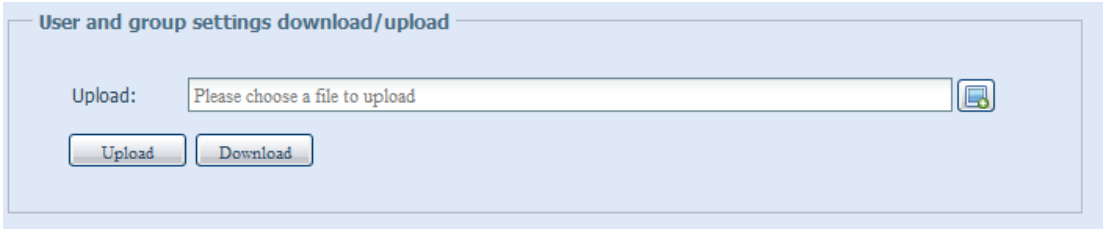


4.7.6. User and Group Backup

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.

Figure 192: User and group backup



4.7.7. LDAP Support

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

Figure 193: LDAP support

A description of each item follows:

Table 44: LDAP support

Item	Description
LDAP Support	Enable or Disable LDAP service.
LDAP Server IP	Input LDAP server IP address.
Base DN	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.
Apply	Click Apply to save your changes.
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.

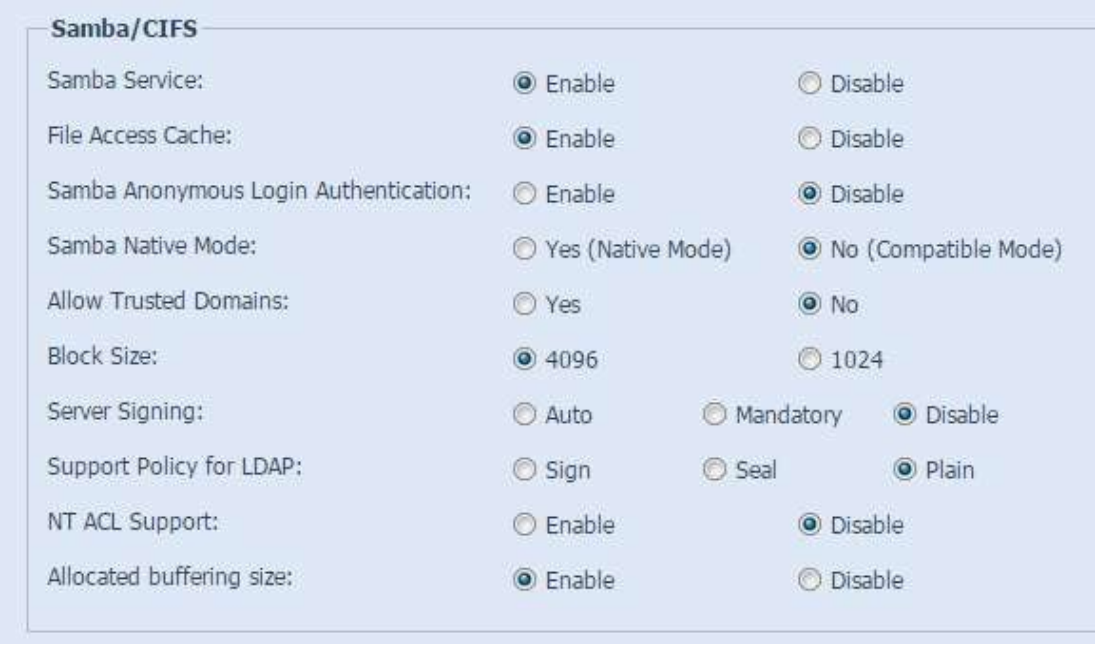
4.8. Network Service

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

4.8.1. Samba / CIFS

There are options allow Admin to Enable/Disable to operate the CS3160 associated with Samba / CIFS protocol. With the option changed, it will need to reboot system to activate.

Figure 194: Samba / CIFS



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.

NOTICE

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

File Access Cache

File Access Cache is default Enable. This option will help to increase the performance while single client access share folder in writing under SMB/CIFS protocol.

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 Native mode

The CS3160 is supported Samba mode options. In the ADS environment with “Native” mode selected then the CS3160 is capable to become local master position.

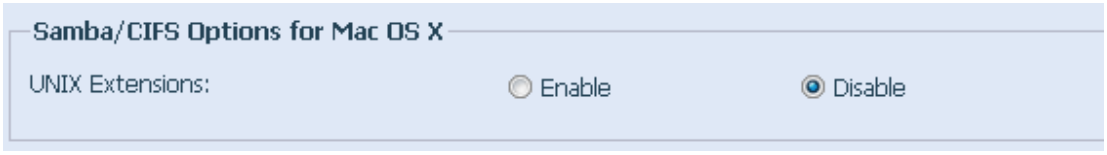
Optimize Block Size

This function controls the behavior of Samba when reporting available disk space. This function was added to allow advanced administrators to increase block size to increase write performance without re-compiling the code.

Server Signing

This is setting while Samba server has been used in US of FDCC. If the system has used only in Windows environment choose "Mandatory" otherwise "Auto".

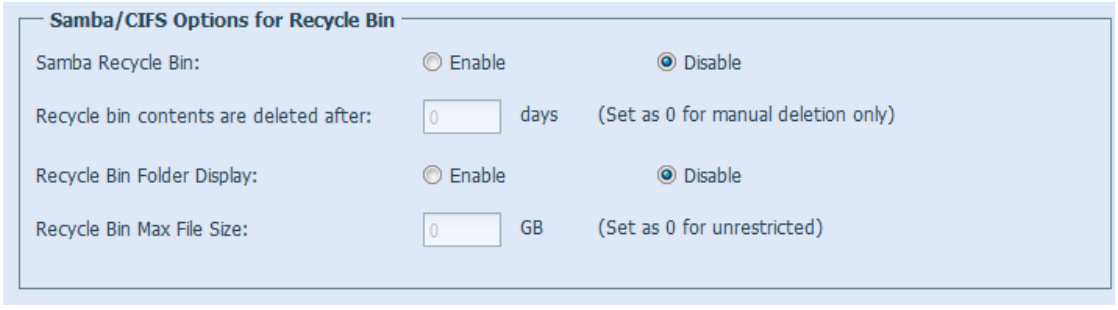
Figure 195: UNIX extension



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.

Figure 196: Samba recycle bin

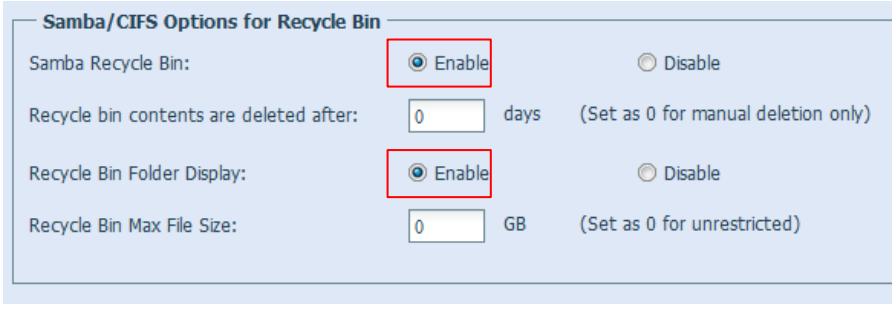


Samba Recycle Bin

The CS3160 is supported recycle bin via SMB/CIFS protocol.

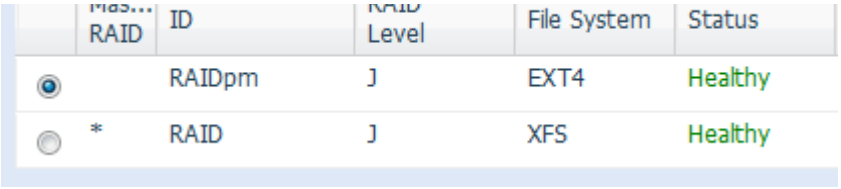
Simply enable the "Recycle Bin" function and "Recycle Folder Display" then all of deleted files/folders will reside in the "_NAS_Recycle_(Associated RDID Volume)" share folder.

Figure 197: Recycle bin options



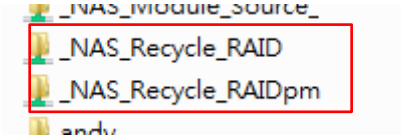
For example, the system has created 2 RAID volumes with ID "RAIDpm" and 'RAID". Then it will have 2 recycle bin folder appear as "_NAS_Recycle_RAID" and "_NAS_Recycle_RAIDpm".

Figure 198: Example



	RAID	ID	Level	File System	Status
◉		RAIDpm	J	EXT4	Healthy
○	*	RAID	J	XFS	Healthy

Figure 199: Example folders



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.

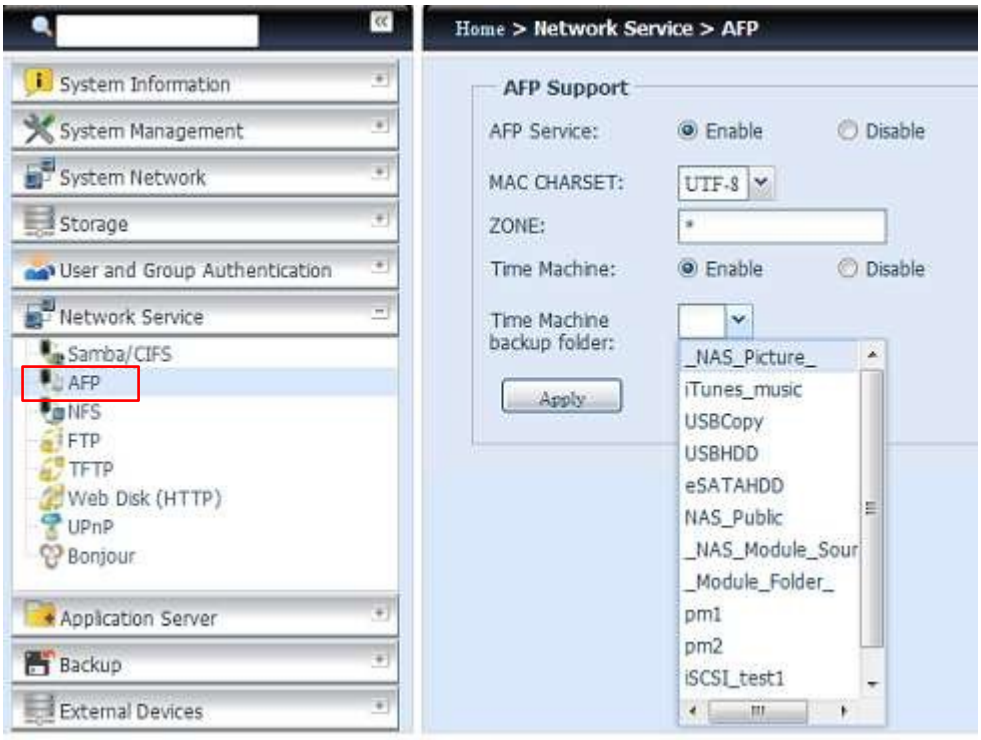
The deleted files/folders which have resided in recycle bin will keep its permission. On the other hand, only the admin and owner can view/read/write these folders/files.

If deleted single file size is large than 2GB then it won't reside in the recycle bin but erase permanently.

4.8.2. AFP (Apple Network Setup)

From the Network Service menu, 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.

Figure 200: Apple network configuration



A description of each item follows:

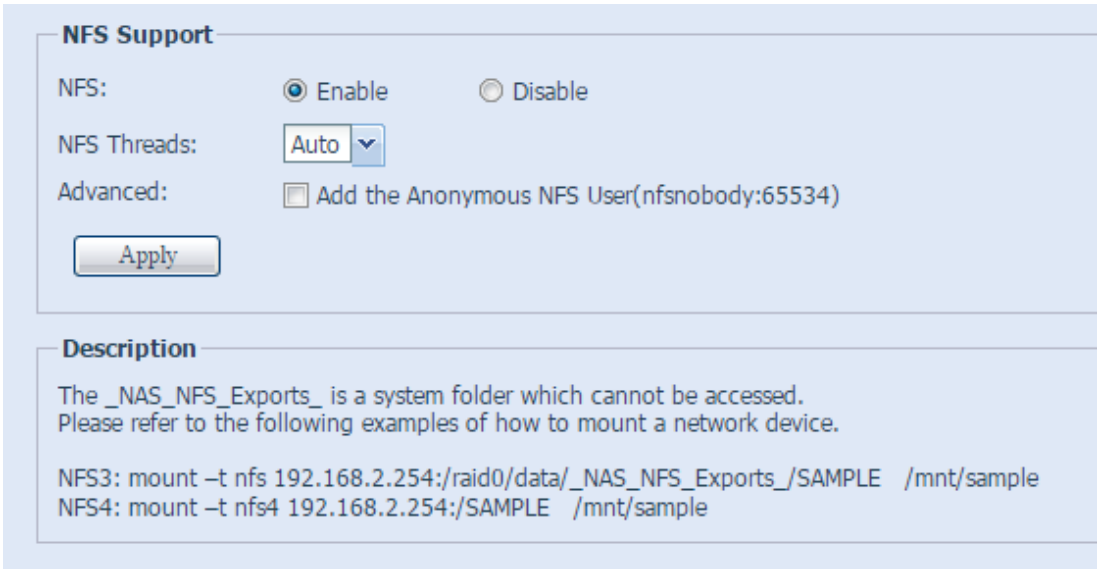
Table 45: Apple network configuration

Item	Description
AFP Server	Enable or disable Apple File Service to use the CS3160 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 CS3160. 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 CS3160 as MAC time machine backup.
Time Machine backup folder	Select from the drop down list to designate the folder for time machine backup destination.

4.8.3. NFS Setup

From the Network Service menu, choose the NFS item, and the NFS Support screen appears. The CS3160 can act as an NFS server, enabling users to download and upload files with their favorite NFS clients. Press Apply to confirm your settings.

Figure 201: NFS setup



A description of each item follows:

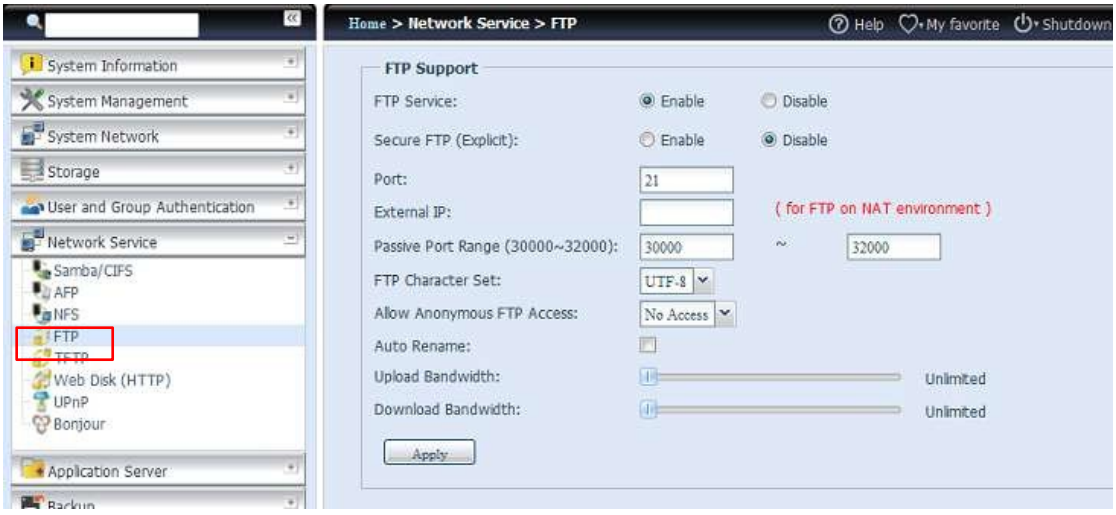
Table 46: NFS server setting

Item	Description
NFS	Enable or Disable NFS support.
NFS Threads	Choose the number of NFS threads.
Advanced	Checked to add the Anonymous NFS User.
Apply	Click Apply to save your changes.

4.8.4. FTP

The CS3160 can act as an FTP server, enabling users to download and upload files with their favorite FTP programs. From the Network Service menu, choose the FTP item, and the FTP screen appears. You can change any of these items and press Apply to confirm your settings.

Figure 202: FTP



A description of each item follows:

Table 47: FTP

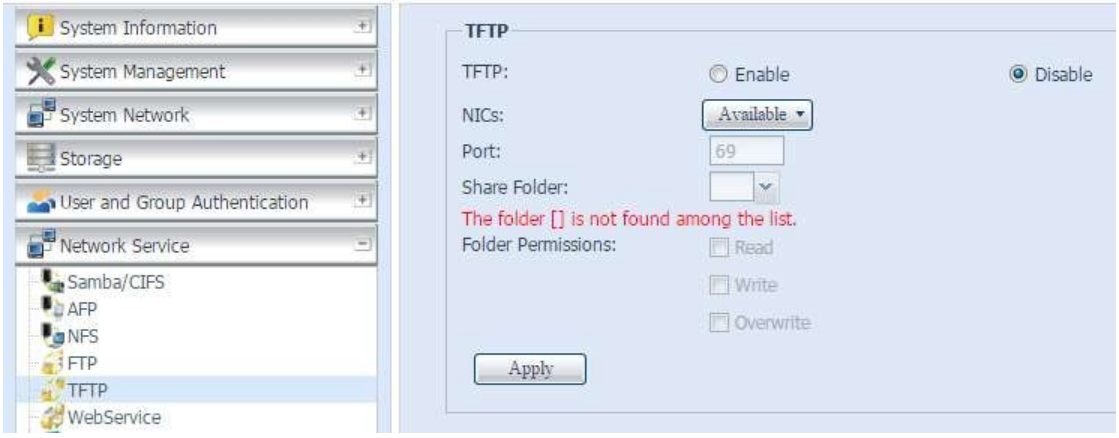
Item	Description
FTP	Enables FTP Service on the CS3160.
Security FTP	Enable or disable Security FTP, be sure the client FTP software has also security FTP setting enabled.
Port	Specifies the port number of an incoming connection on a non-standard port.
External IP	Input the public IP address of the router when the Kontron 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 CS3160, 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).

4.8.5. TFTP

The CS3160 can act as a TFTP server, enabling users to download and upload files with their favorite TFTP programs. From the Network Service menu, choose the TFTP item, and the TFTP screen appears. You can change any of these items and press Apply to confirm your settings.

Figure 203: TFTP



A description of each item follows:

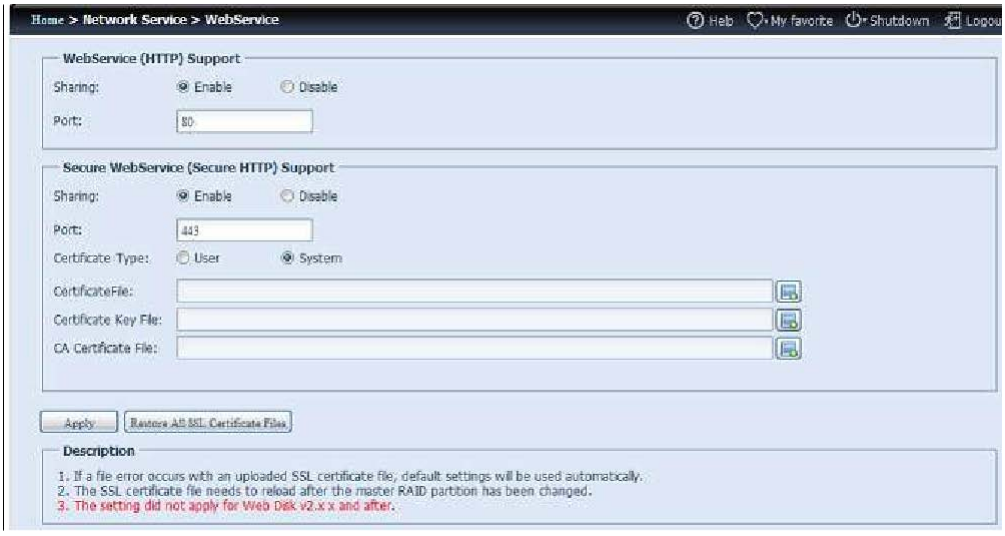
Table 48: TFTP

Item	Description
TFTP	Enables TFTP Service on the CS3160.
NICs	Choose NICs 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

4.8.6. WebService

From the Network Service menu, 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.

Figure 204: WebService



A description of each item follows:

Table 49: WebService

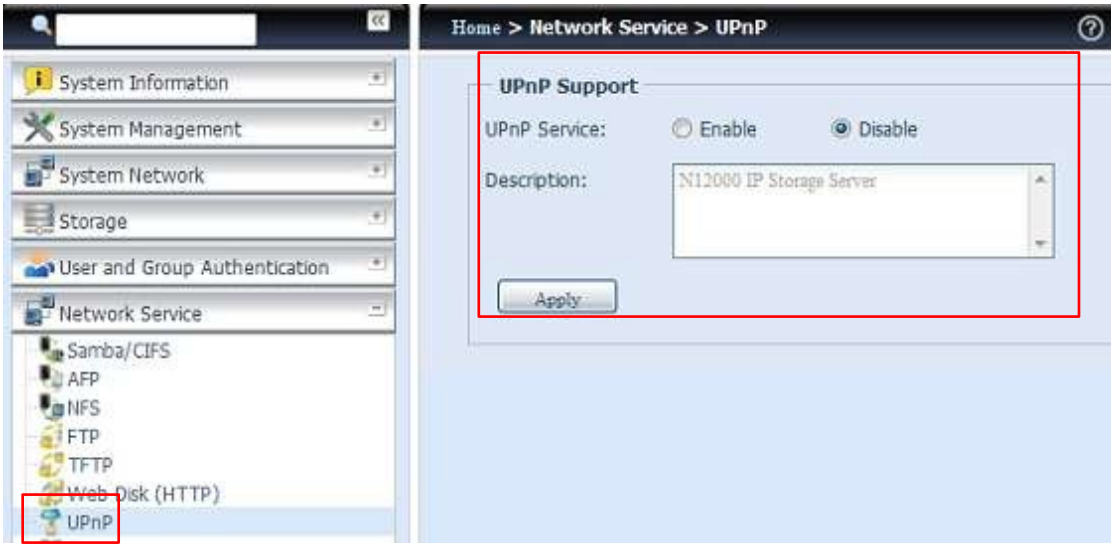
Item	Description
WebService (HTTP) Support	Enable or disable WebDisk support. Enter the port number if this option is enabled. The port number is default 80.
Secure WebService (Secure HTTP) Support	Enable or disable secure WebDisk support. Enter the port if this option is enabled.
Certificate File	Upload 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.

4.8.7. UPnP

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 the CS3160.

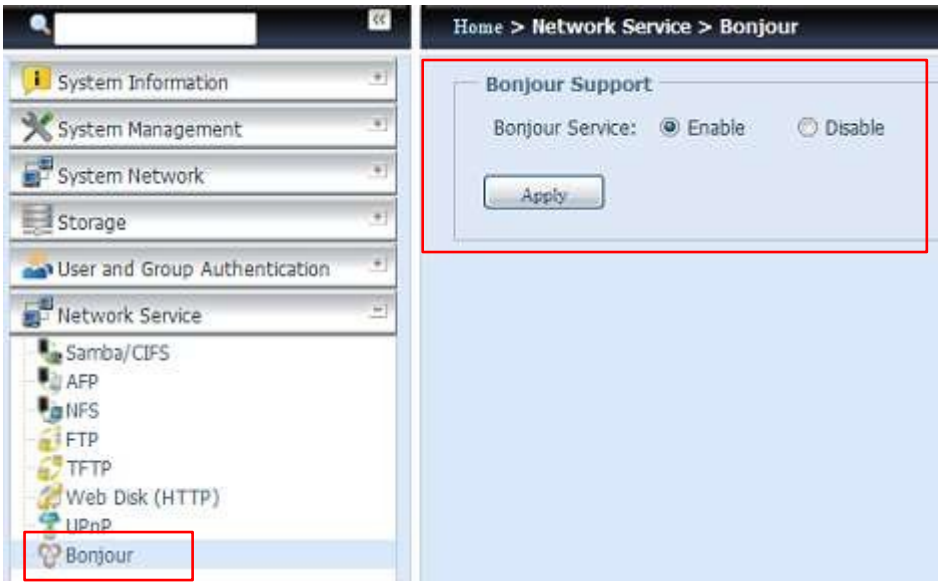
Figure 205: UPnP



4.8.8. 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.

Figure 206: Bonjour setting



4.8.9. 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:

Table 50: 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.

Figure 207: SSH

4.8.10. 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.

A description for each item as following:

Table 51: 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.

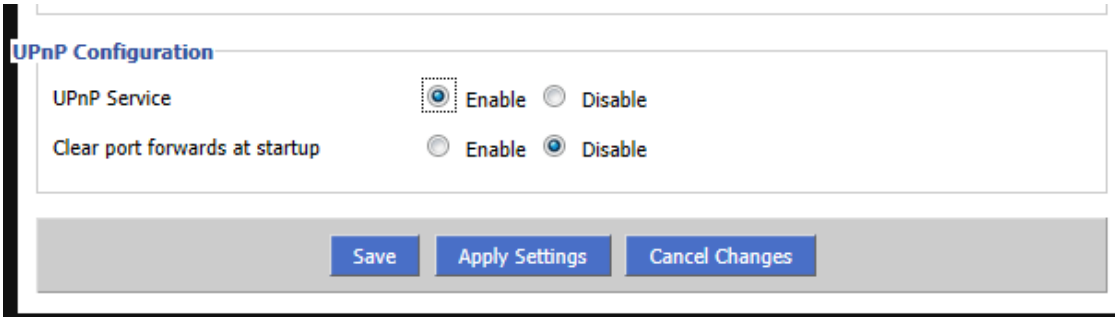
Figure 208: DDNS

4.8.11. 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.

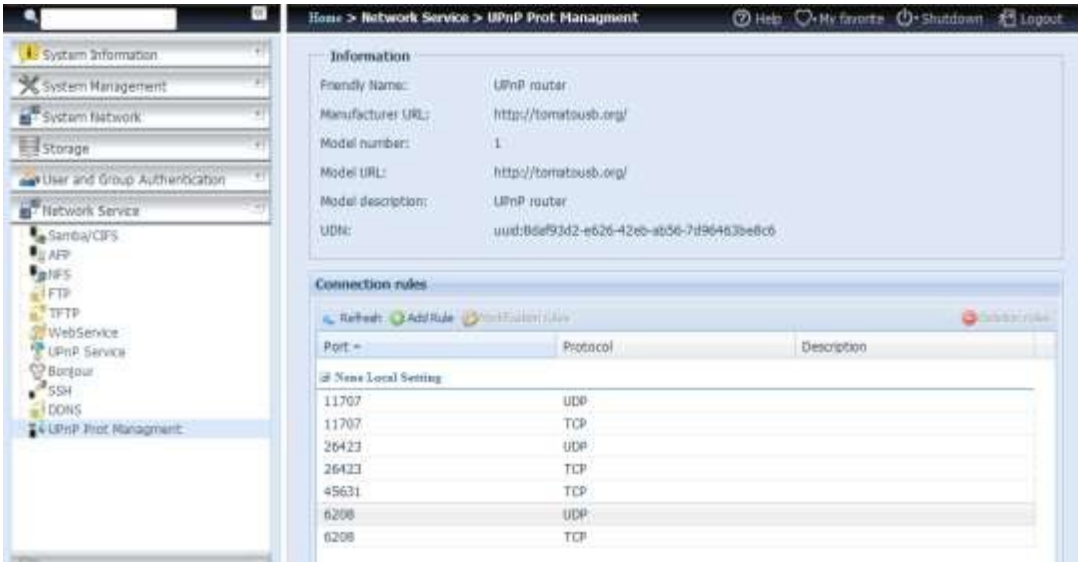
To set up this UPnP port forwarding feature, please be sure that the router has “UPnP Service” Enabled. The following is an example from one of the router manufacture with UPnP Configuration page.

Figure 209: UPnP configuration page



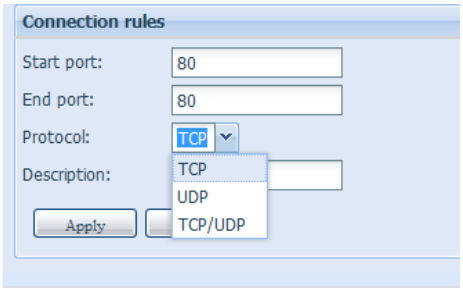
After the router has enabled "UPnP Service" then you will have information come from associated router to UPnP port management as shown in the screen shot below.

Figure 210: UPnP port management



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

Figure 211: Connection rules



A description for each item as following:

Table 52: 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”.

4.8.12. 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.

Figure 212: WebDAV support

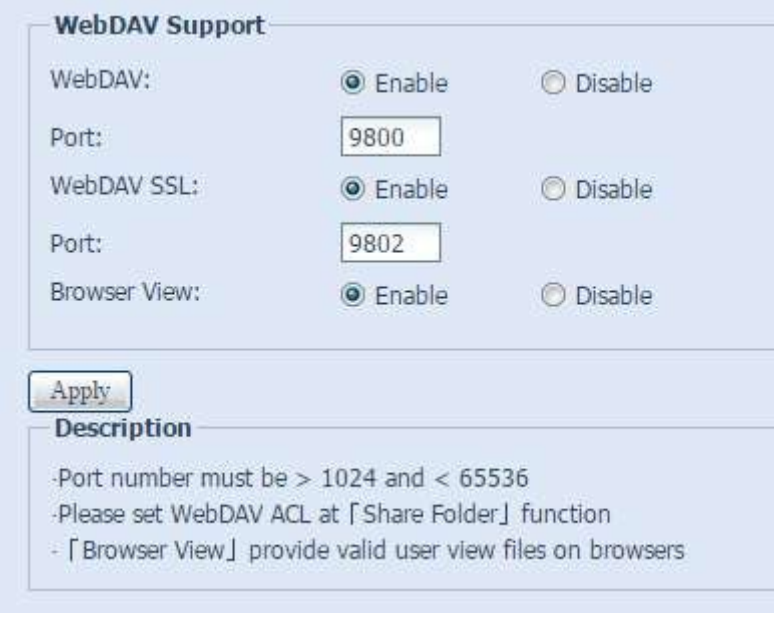


Table 53: WebDAV configuration

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

Item	Description
Browser View	Press the Enable button and viewing the share folder list through the browser will be allowed
Apply	Click "Apply" to confirm the changes.

4.8.13. 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.

Figure 213: Auto thumbnail

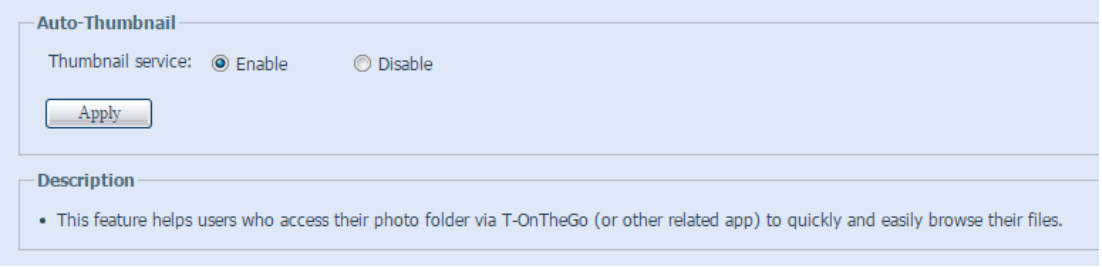


Table 54: Auto thumbnail configuration

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

4.8.14. Thecus ID

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.

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.

Figure 214: DDNS settings

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.

Figure 215: Create Thecus ID

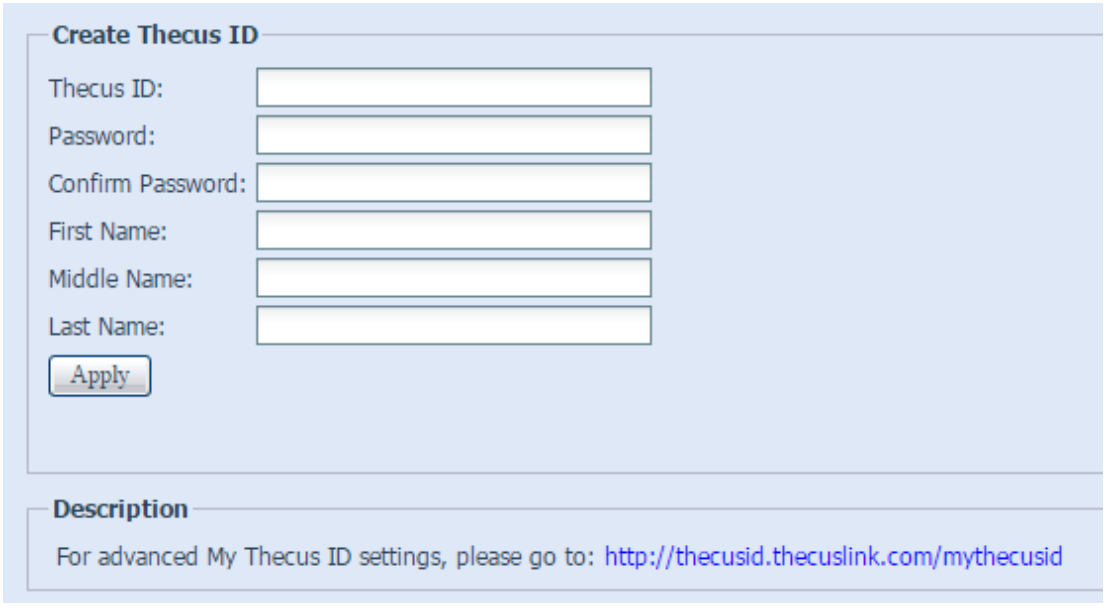


Table 55: Register Thecus ID

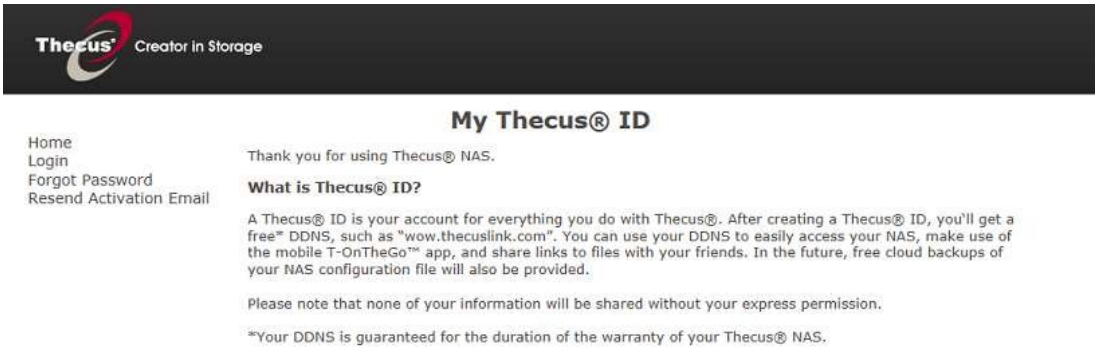
Item	Description
Thecus ID	Input a valid email address. It will require confirmation to activate your Thecus ID.
Password	Input the password for your Thecus ID
Confirm Password	Re-input the password for your Thecus ID.
First Name	Input your First name

Item	Description
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

Figure 216: Thecus webpage



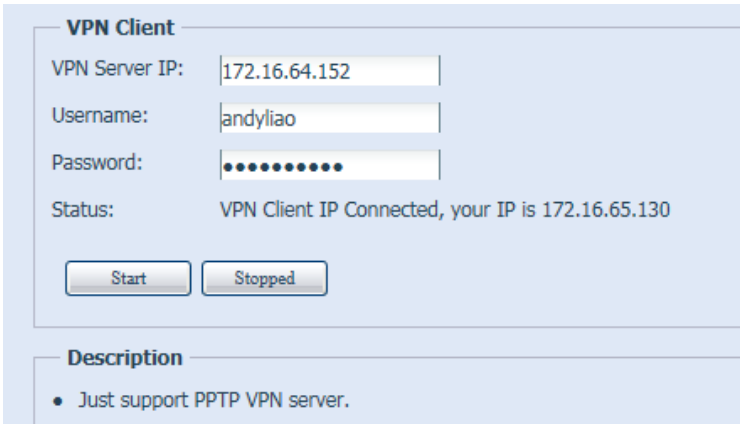
4.8.15. VPN Client

To have this storage device join a Virtual Private Network, simply provide a VPN server IP address and a valid login user name and password. Once the input information has been confirmed, the connection will be made. This storage device will be capable of playing a role as a local device to communicate with other systems.

Figure 217: VPN client

Once a connection has been successfully made, the granted IP address willbe displayed in your status.

Figure 218: VPN client status



Please notice that the connection to the VPN server only supports PPTP.

4.8.16. VPN Server

This storage device provides VPN server service and this allows remote access to this device via a secure connection. Settings can be found in the "Application Server" tab as seen below

Figure 219: VPN server

To setup your VPN server you must first choose the NIC interface from the drop down menu and complete the rest of the necessary information.

Below is a description of each item:

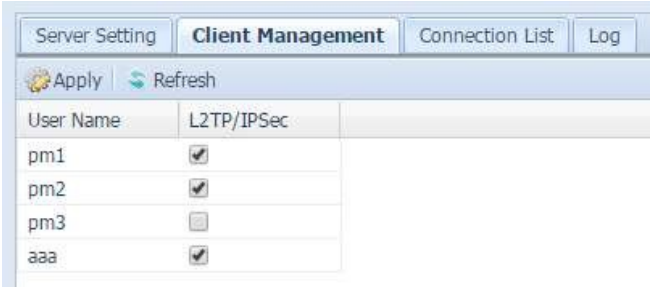
Table 56: VPN server

Item	Description
Network Interface	Select the NIC interface to use for VPN server
Enable L2TP/IPSec VPN Server	Check to enable L2TP/IPSec VPN server service
VPN Client IP Pool	Input the IP range for client IP.
VPN Server remote IP	Input the IP for the VPN server for VPN client connection

Item	Description
Authentication	Input domain name with DDNS registry.
IKE Authentication	Internet Key Exchange for authentication while connection is made.
Pre-shared key	Input the key for connection authentication in between VPN client and server.
Confirm Pre-shared Key	Confirm the key
Apply	Click "Apply" to confirm the changes.

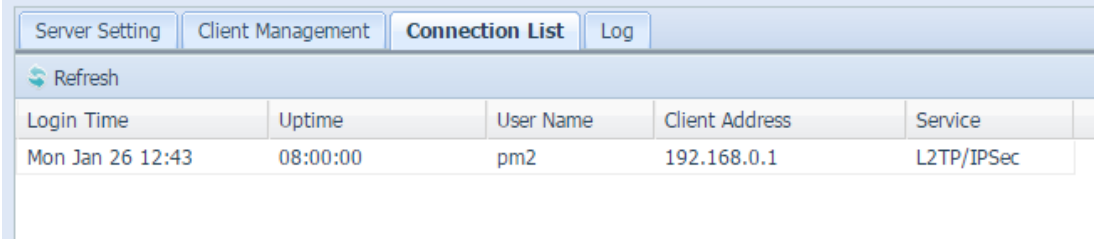
For the VPN client access control, simply click on "Client Management" tab. It will list all the users on this system and default "Allowed" for VPN connection. Un-tick the check box and confirm with the "Apply" button if users are prohibited from connecting with this VPN server.

Figure 220: Client management



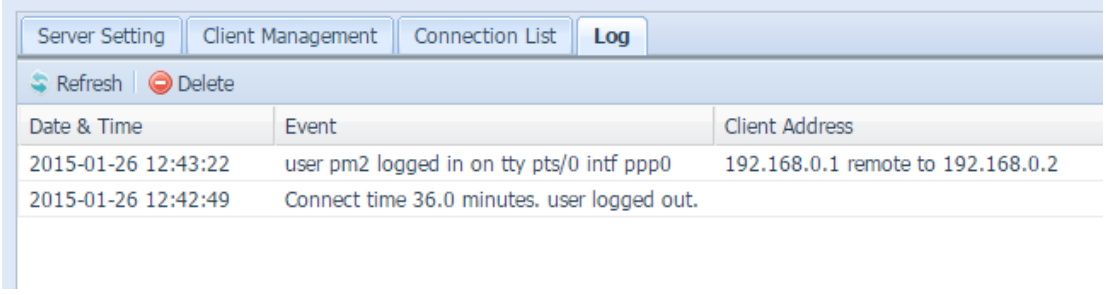
To get the on-line connection list, click on the "Connection List" tab. It will display connected users with associated connection information.

Figure 221: Connection list



To retrieve the VPN service connection history information, click on "Log" tab. It will display the complete access log of the VPN service.

Figure 222: Log



The VPN server only supports L2TP/IPSec connection.

4.9. Application Server

The CS3160 supports build-in application such as iTunes server. The CS3160 provides activation of the iTunes Server on the device. You will be able to play music files on this device with your iTunes client software directly. The following section shows you how.

4.9.1. iTunes® Server

With the built-in iTunes server capability, the CS3160 enables digital music to be shared and played anywhere on the network!

From the Network Service menu, choose the iTunes Server item, and 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.

Figure 223: iTunes server

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

Table 57: iTunes server configuration

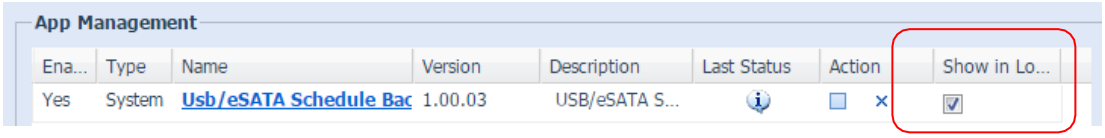
Item	Description
iTunes Service	Enable or disable the iTunes Service.
iTunes Server Name	Name used to identify the CS3160 to iTunes clients.
Password	Enter a password to control access to your iTunes music.
Rescan Interval	Rescan interval in seconds.
MP3 Tag Encode	Specify tag encoding for MP3 files stored in the CS3160. All ID3 tags will be sent out in UTF-8 format.

Once the iTunes service is enabled, the CS3160 will make all music located in the Music folder available for iTunes-equipped computers on the network.

4.9.2. App Installation

From the login page, other than admin, web disk and Piczza (Photo server) the app icon is a newly added feature for this FW release. After an app has been installed, a new option will be available to “Show in Login”.

Figure 224: App management



If this option is enabled then, when login to the system, the module icon will be available for all valid users to login through.

Figure 225: Module icon

4.9.3. Auto App Installation

Choose the Auto App Installation item and the Auto App Installation screen appears. The default for this apps list is located online. So if the CS3160 is capable to connect to Internet, then it will automatically link to the Thecus official website and list the available apps. Please refer the screen shot below.

Figure 226: Auto module installation

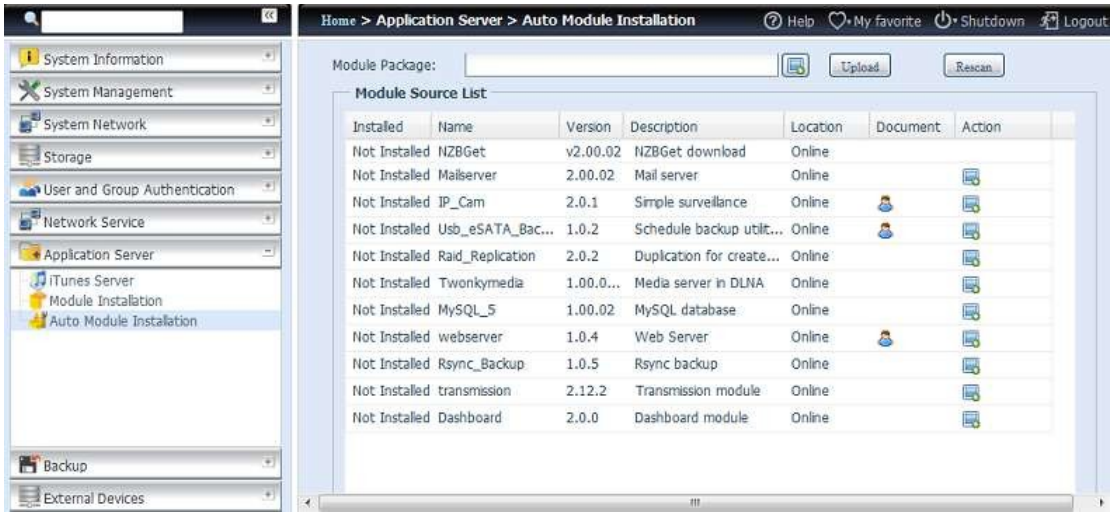


Table 58: Auto module source list

Item	Description
Installed	Status of module
Name	Module name

Item	Description
Version	The version of the released module
Description	The description of the module
Location	The module is either located on-line or disk
Document	The available documentation of the module
Action	To install or delete module. p.s. If the module list from on-line, then no delete option will be available
Rescan	Click to rescan from both on-line and disk

Figure 227: Module source list

After clicking on "Action" to install a module, the module will become available under the list of Module Installation. Please go to Module installation and click "Enable" to activate the module.

4.10. Backup

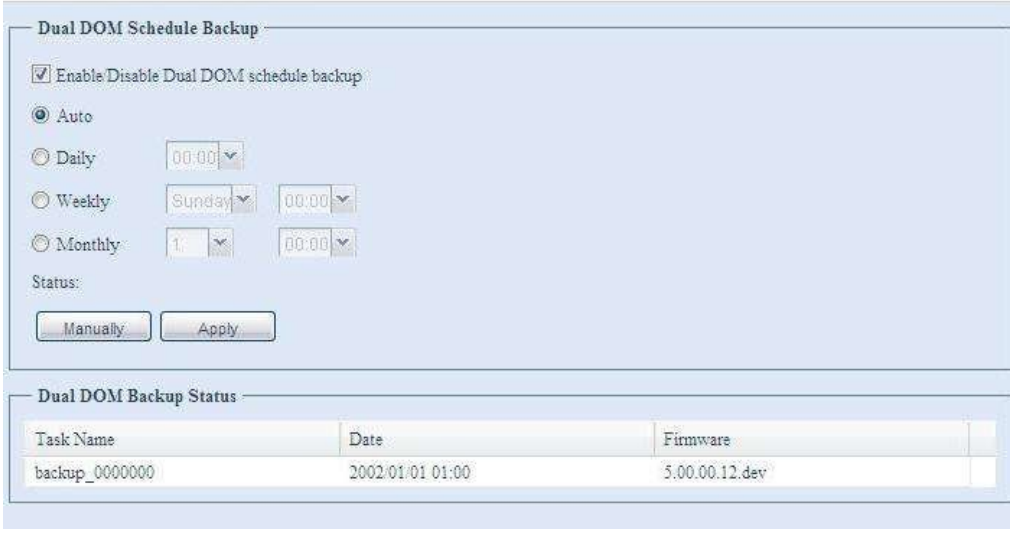
There are a number of ways to back up data with the CS3160.

4.10.1. Dual DOM

The unique Dual DOM feature can now perform "Auto Repair". The CS3160 NAS will backup up to five versions of the system configuration either by the default timing of 1:00am every day automatically or as scheduled by the user.

This unique "Auto Repair" will be triggered if the primary DOM has a booting issue. In this instance, the 2nd DOM will take over the boot function. Then, the system will automatically load the most recent system configuration backup image to repair the primary DOM.

Figure 228: Dual DOM schedule backup



4.10.2. Rsync Target Server

Figure 229: Rsync target server icon

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

Figure 230: Rsync target server

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.

4.10.3. 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.

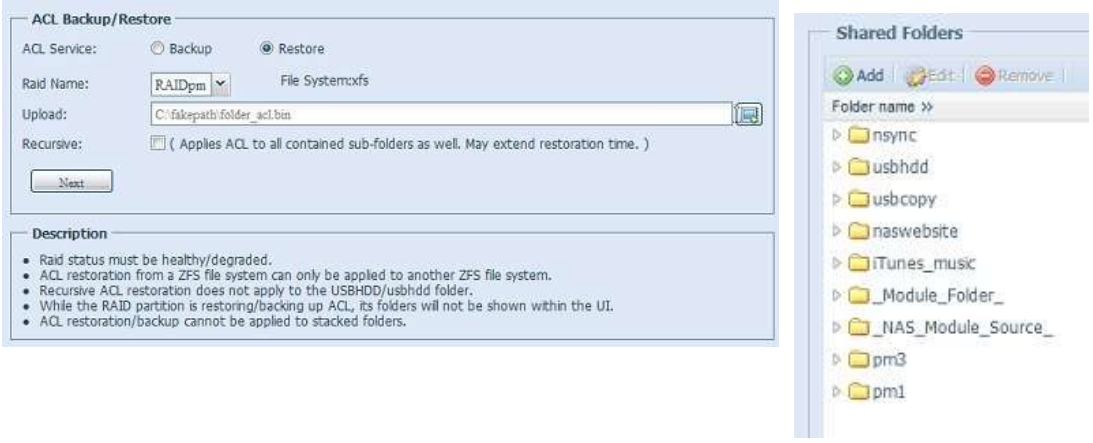
Let's look at the example bellow to see how it works.

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.

Figure 231: ACL backup and restore

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.

Figure 232: Example



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.

Figure 233: Matched folders

The ACL backup will only back to share folder level; it does not apply to its sub-layer.

The ACL backup/restore can be used among ext3/ext4/XFS file system. ZFS can only be used with other RAID volume with ZFS file system created.

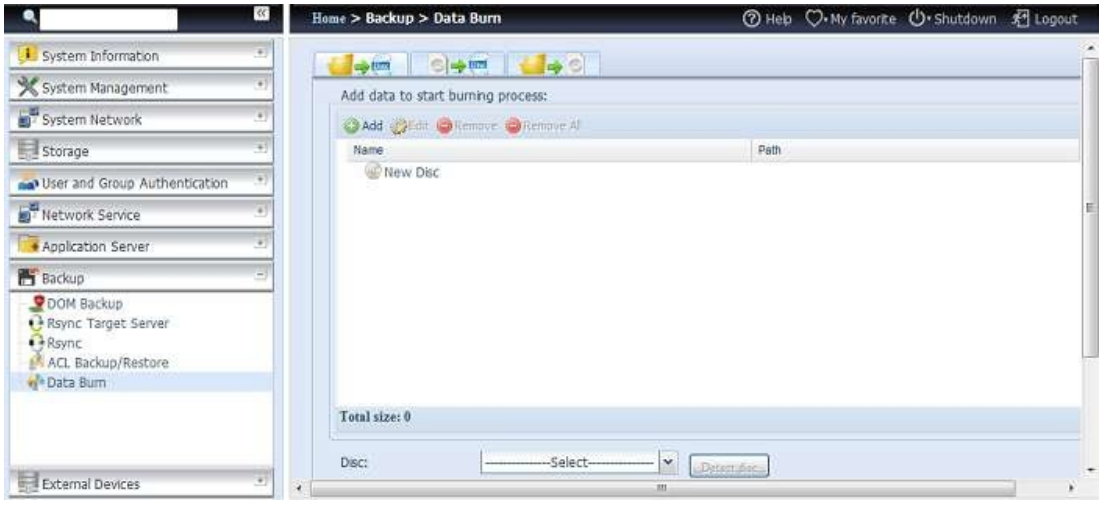
If recursive has been checked during the ACL restoration, it will apply to all of its sub-folders with the same permission.

4.10.4. 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.

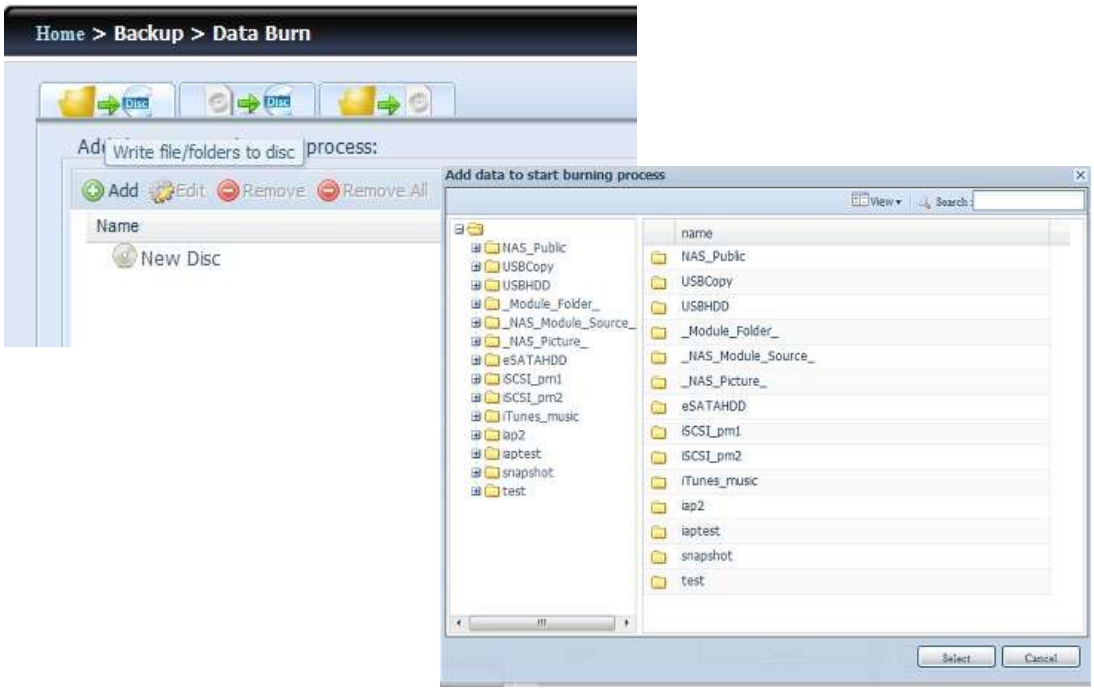
The 3 different modes are “Write Files/folders to disc”, “Write image to disk” and “Write files/folders to image”.

Figure 234: Data burn



1. Write Files/folders to disc

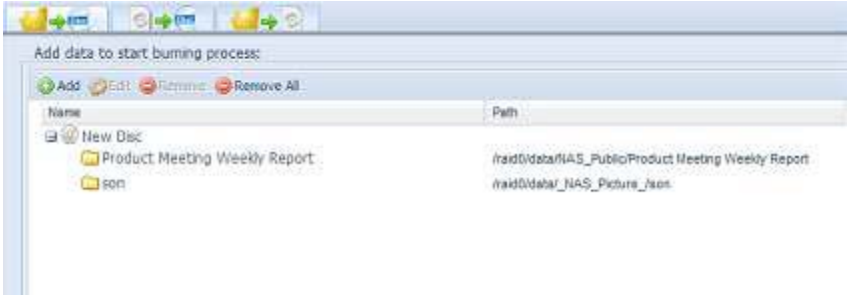
Figure 235: Write files/folders to disc



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.

Figure 236: File selection



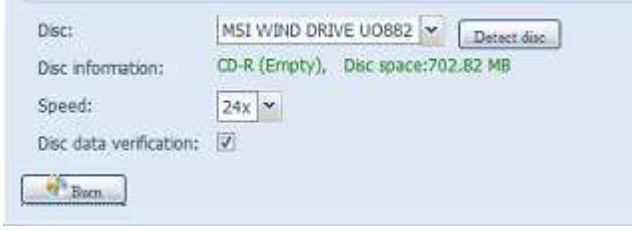
c. Select from the installed USB or SATA(for N6850/N8850/N10850) burning devices. Please click the “detect disc” button to check the status once the disc is inserted.

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

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

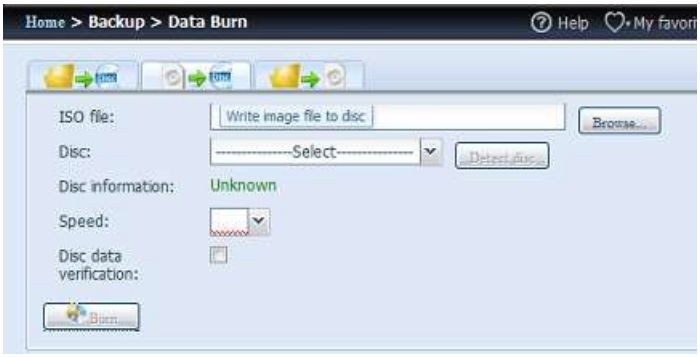
f. Click “Burn” to start disc burning.

Figure 237: Burn options



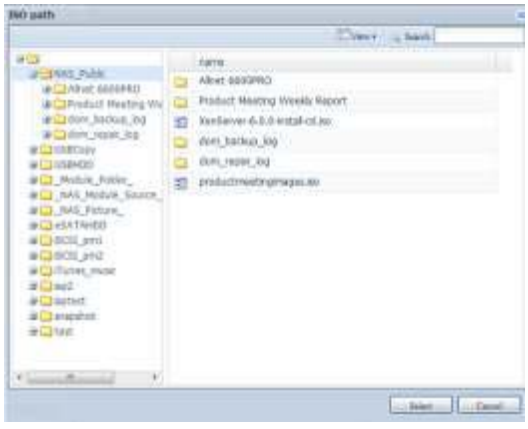
2. Write image file to disc

Figure 238: Write image file to disc



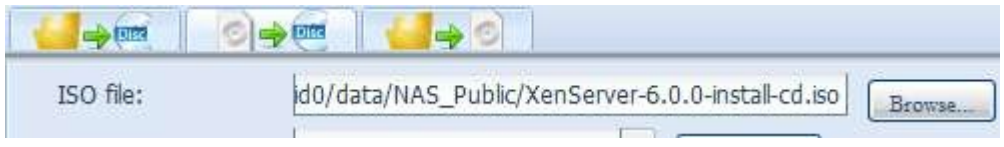
a. Click “Browser” and the NAS share list will appear to locate the desired image file to burn.

Figure 239: NAS share list



b. Select the ISO file.

Figure 240: ISO file selection



c. Select from the installed USB or SATA (for the CS3160) 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.

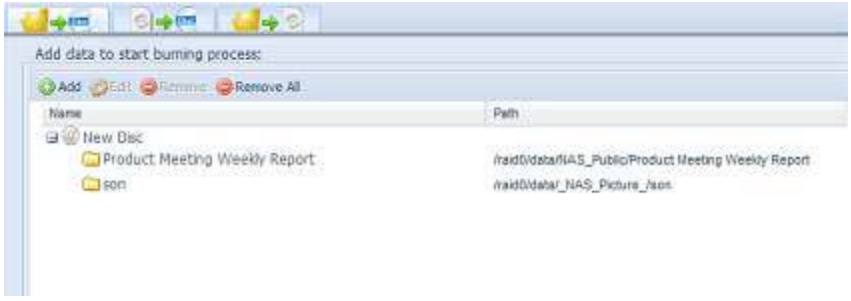
3. Create image file from files/folders

Figure 241: Create image file from files/folders

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.

Figure 242: Files/folders selection



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.

NOTICE

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.

4.10.5. Data Guard (Remote Backup)

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 menu of the UI

-From the Data Guard function list, choose Add

Figure 243: Remote data backup

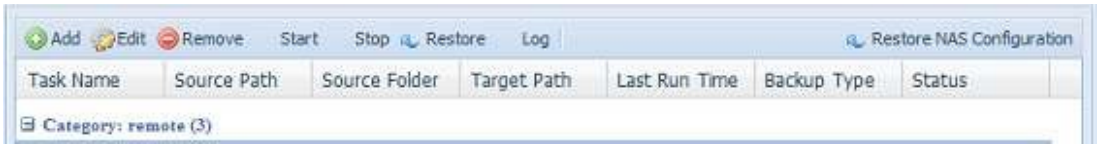


Table 59: Remote data backup

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":

Figure 244: Data backup wizard

Then 3 different selections appear and can be chosen from:

Figure 245: Data backup options

Table 60: Data backup options

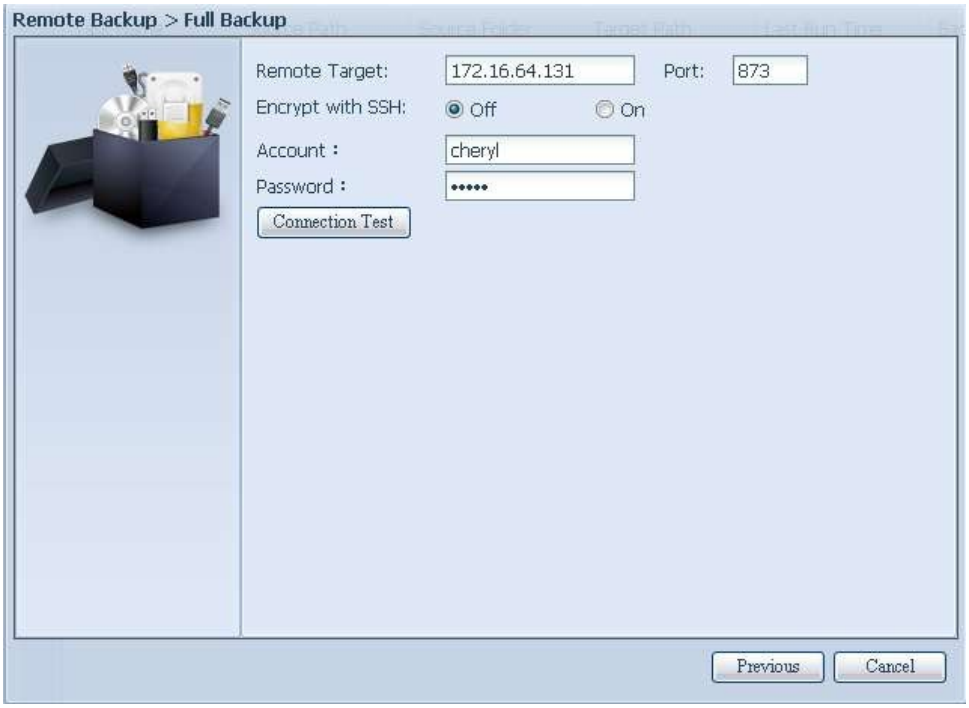
Item	Description
Full Backup	The "Full backup" will have all shares from source backup to destination. It could also create shares automatically from destination if it is not existent. This only applies if the target server is the same model as the source.
Custom Backup	The "Custom backup" allows user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

4.10.5.1. 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.

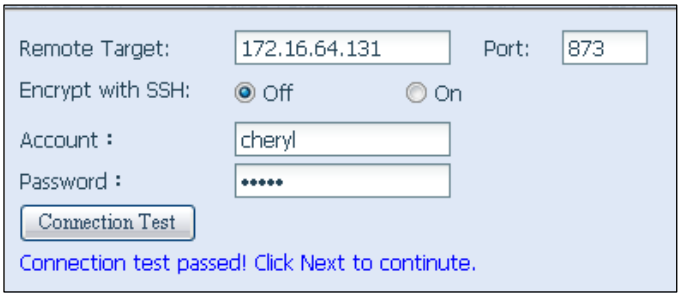
Carry on with inputting valid remote target server account name and password.

Figure 246: Full backup settings



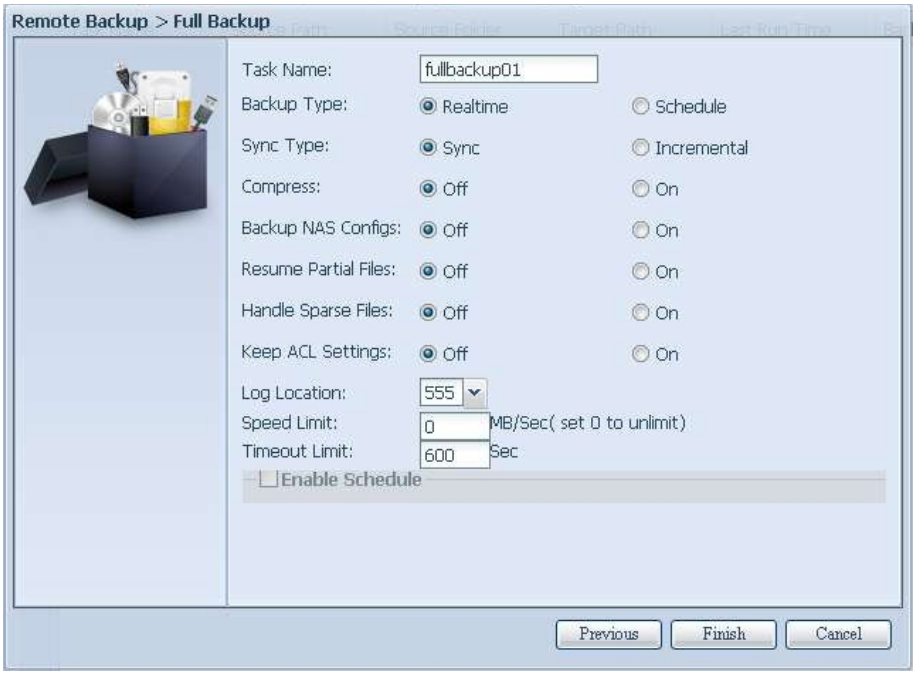
After the settings are complete, please click on "Connection Test". The source unit will try to connect with the associated target system. If a connection can be built up successfully then "Connection passed" will be prompted, otherwise "Failed" will appear.

Figure 247: Connection test result



Click "Next" and more setting will appear.

Figure 248: Additionnal settings



-Fill out all the necessary details and choose your parameters

Table 61: 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.
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.

Item	Description
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.

Figure 249: Task list

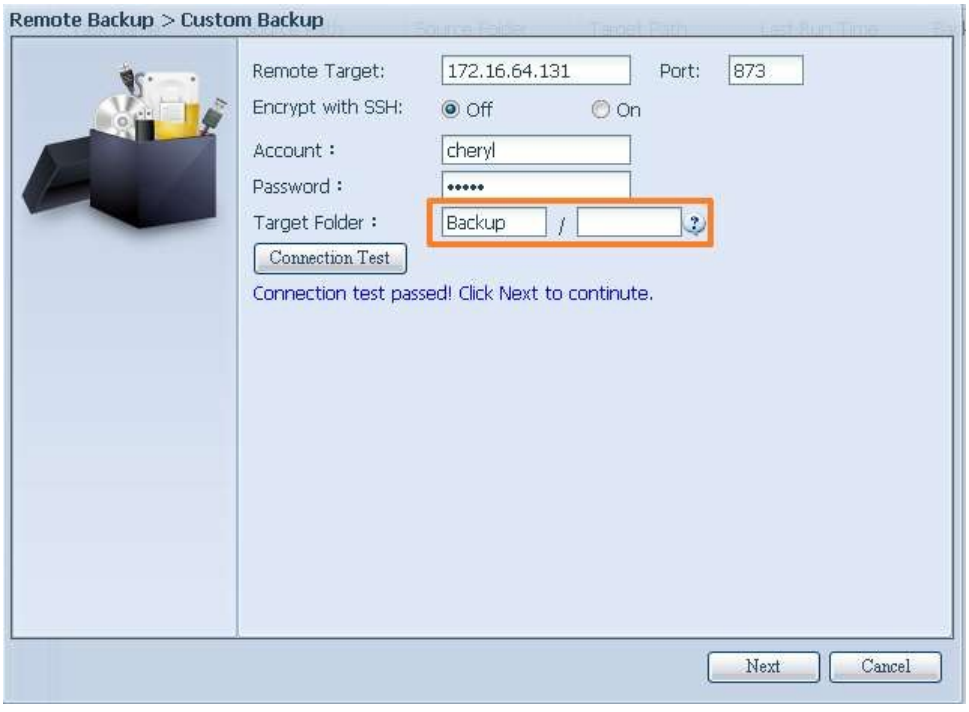
From the task list, you can now see the newly added task "fullback01". The backup is setup as "real time". From the status field, "Processing" can be read as the back-up is performed on the fly.

4.10.5.2. 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.

Figure 250: Taget server name

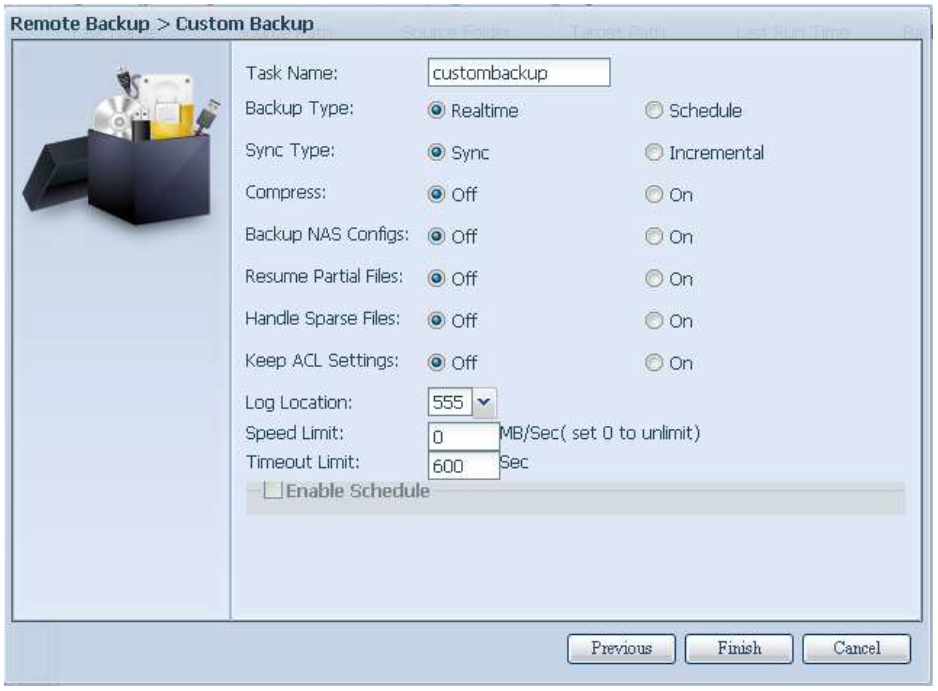


2. Select the source share folder(s) which are desired to be backed up to the target server. You can also click on "Select All" from top right corner check box.

Figure 251: Source selection

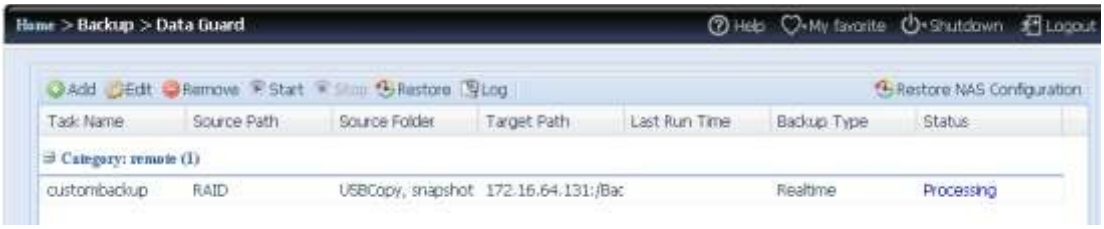
3. Click "Next" and more setting appears. These are the as the settings for "Full backup"

Figure 252: Additionnal settings



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

Figure 253: Task list



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

4.10.5.3. iSCSI Backup

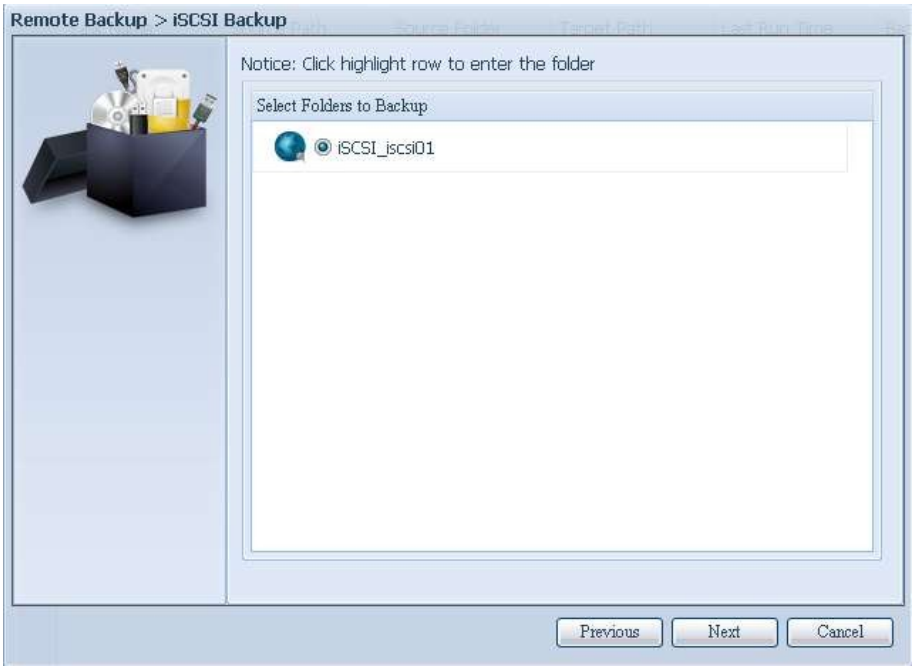
If the source unit contains iSCSI volume, it can be backed up to the target unit as a single file. The procedure is the same as for the previous "Full backup" and "Custom backup", select "iSCSI backup" from data guard wizard.

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.

Figure 254: Target server name

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

Figure 255: iSCSI target volume selection



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.

Figure 256: Additionnal settings

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

Figure 257: Task list

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.

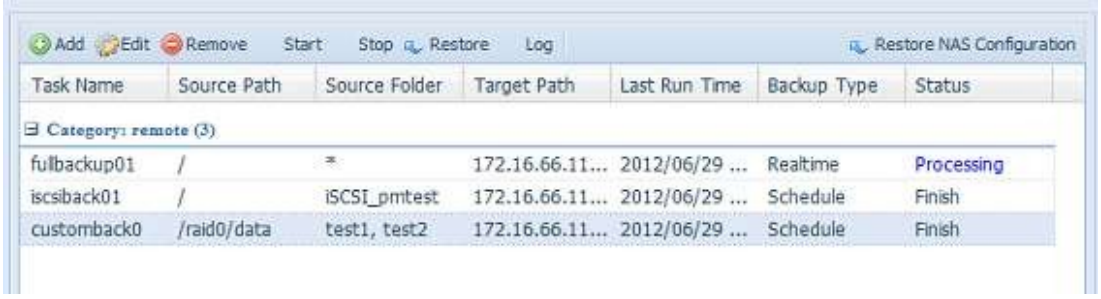
The iSCSI backup can see the result as below. The task "iSCSI_pmtest" has backup to target 172.16.66.131 and share folder NAS_Public with file "iSCSI_pmtest".

Figure 258: Result

4.10.5.4. 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.

Figure 259: Restore



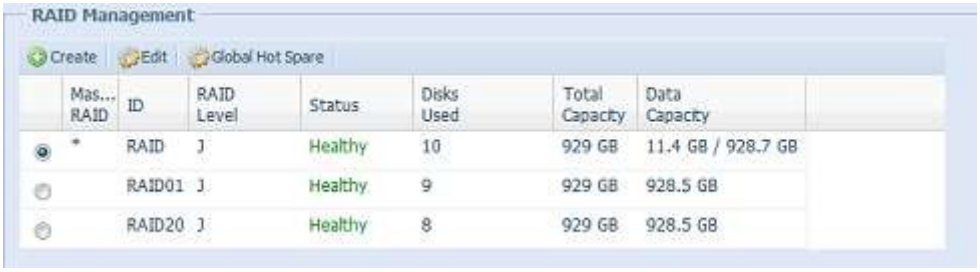
To restore task with backup type set as "Real time", first you need to stop the task then you can proceed with the restore operation.

4.10.5.5. 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.

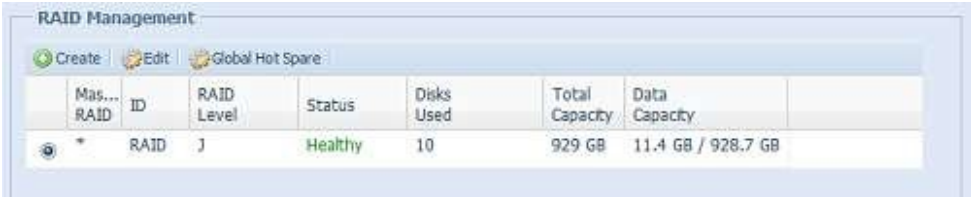
The original source system has 3 RAID volume, "RAID", 'RAID10" and "RAID20", and has backed up the system configurations to the target server.

Figure 260: Original source



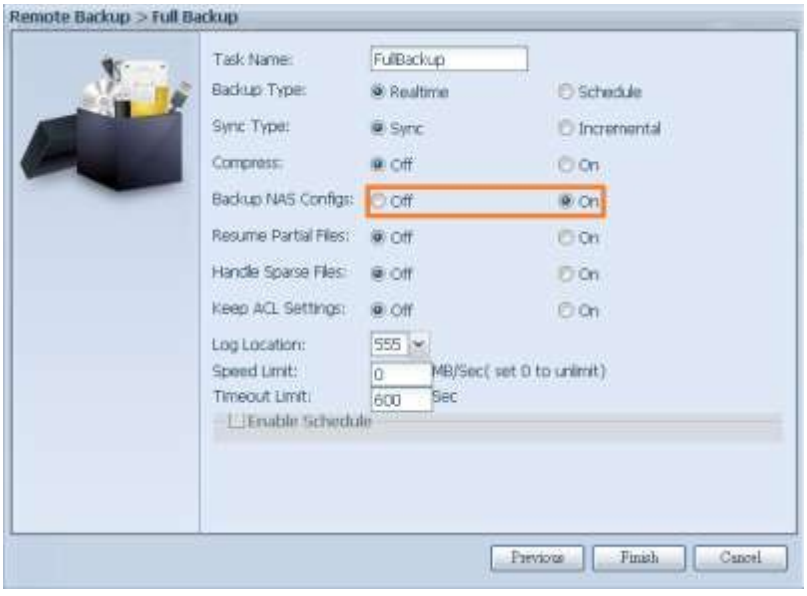
The brand new source unit only has a 1 RAID volume 'RAID".

Figure 261: New source



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.

   Figure 262: Options



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.

Figure 263: Restore NAS configuration button

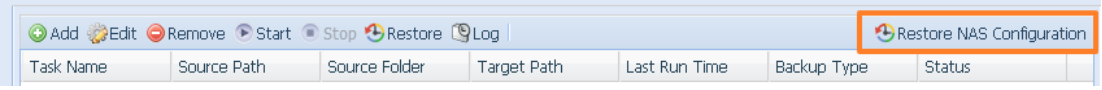
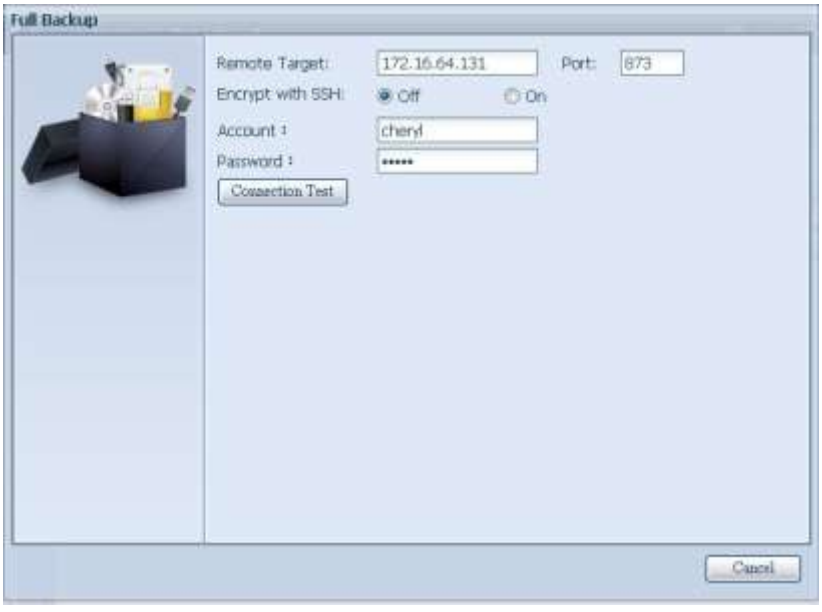
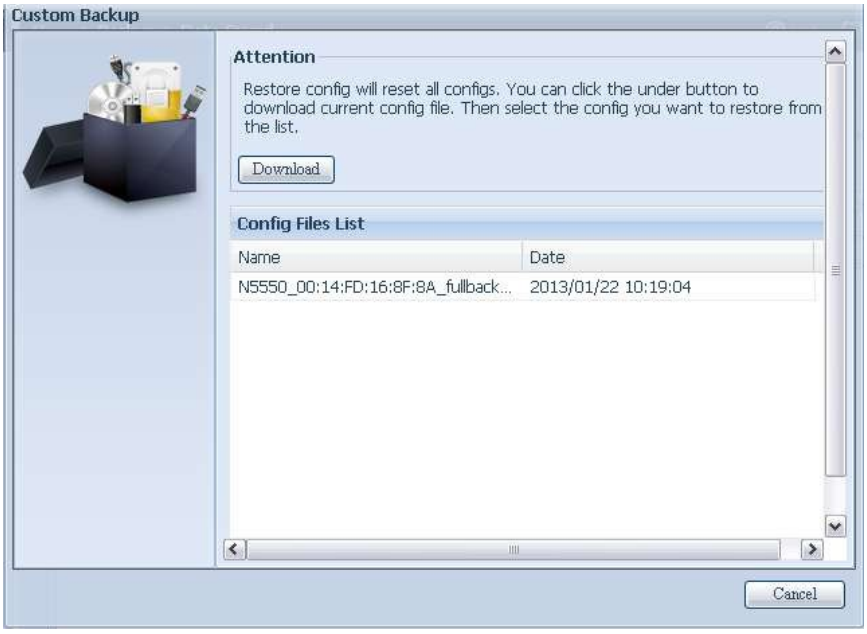


Figure 264: Connection test



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.

Figure 265: Config files list



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.

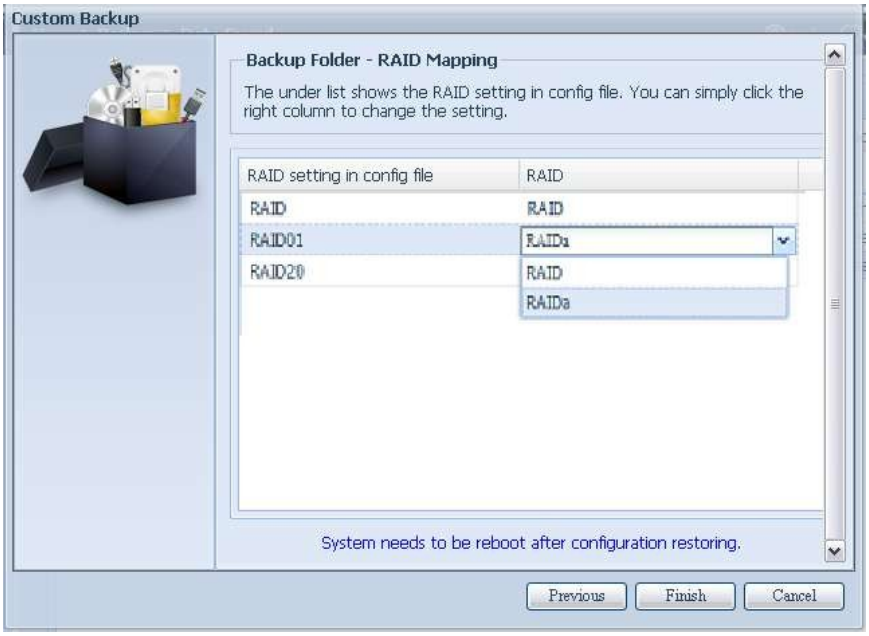
Figure 266: Configuration backup details

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.

Figure 267: RAID selection



4.10.6. Data Guard (Local Backup)

The CS3160 Cloud Storage product provides complete backup solution between other Kontron NAS systems as well as between folders of local systems. For remote data guard backup, please refer to 4.10.6 Data Guard (Local Backup).

Figure 268: Local data backup

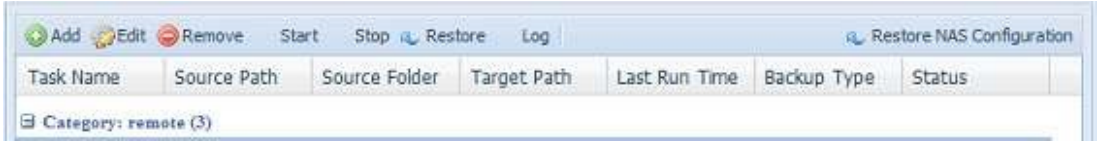


Table 62: Local data backup

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.

Item	Description
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":

Figure 269: Data backup wizard

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

Figure 270: Local backup options

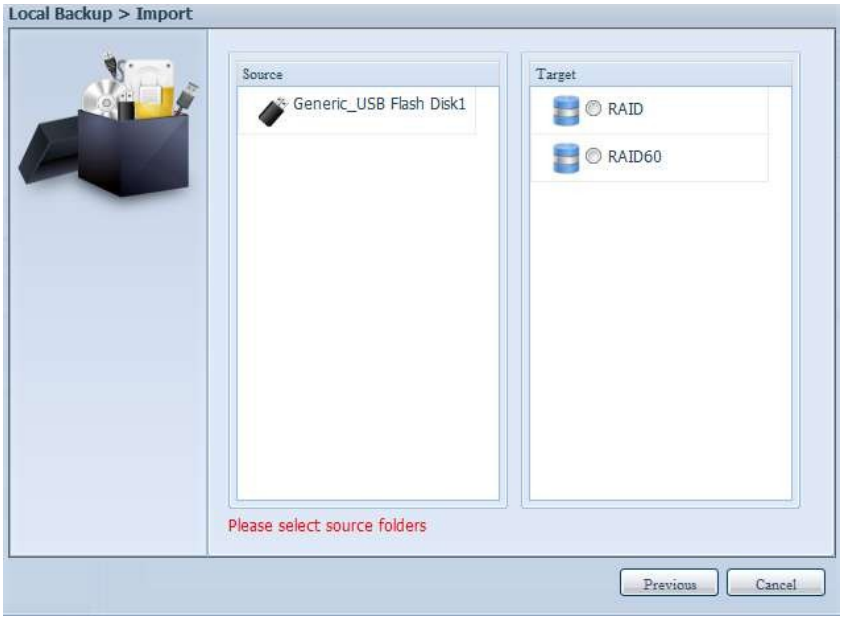
Table 63: Local data backup

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.

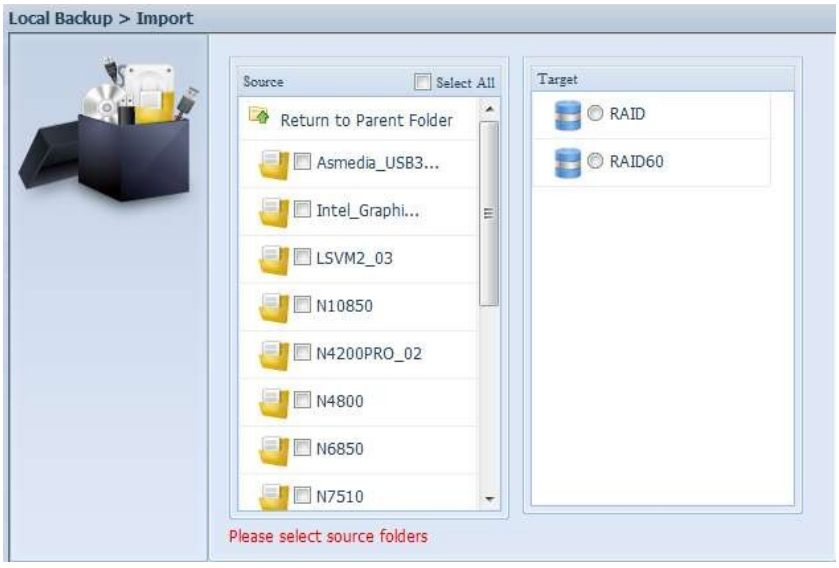
   If there is an external device installed on system such as USB disk, then it will be listed in the Source pane.

   Figure 271: Import screen



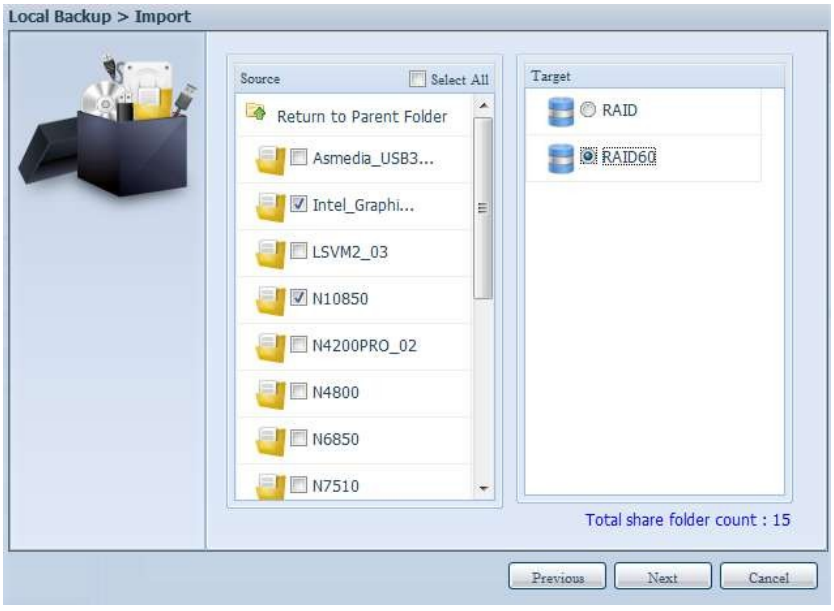
   Click on the associated external device and the contain folders will be listed. Select the folders that are going to be imported to the NAS and select the available RAID volume which is listed in Target pane.

Figure 272: Folder selection



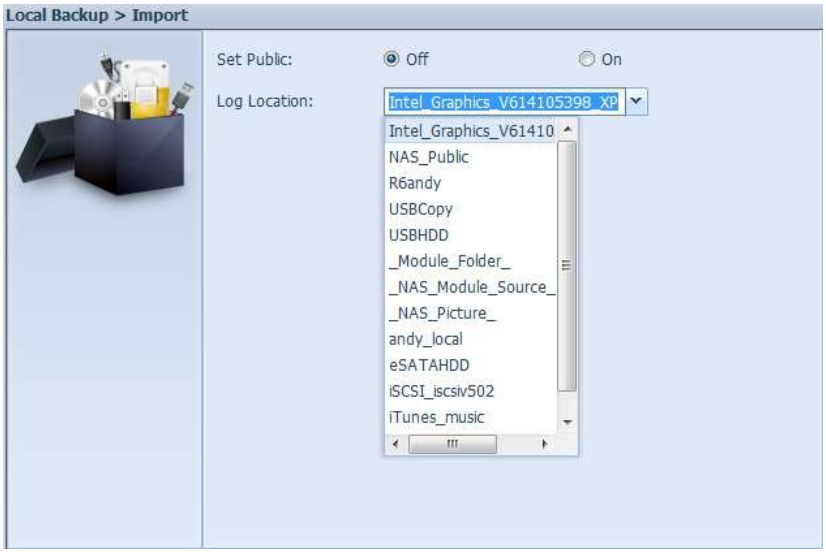
In here, we have selected the “Intel Graphi…” and “CS3160” folders from the external device and imported them to the NAS under the RAID60 volume.

Figure 273: Selected folders



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.

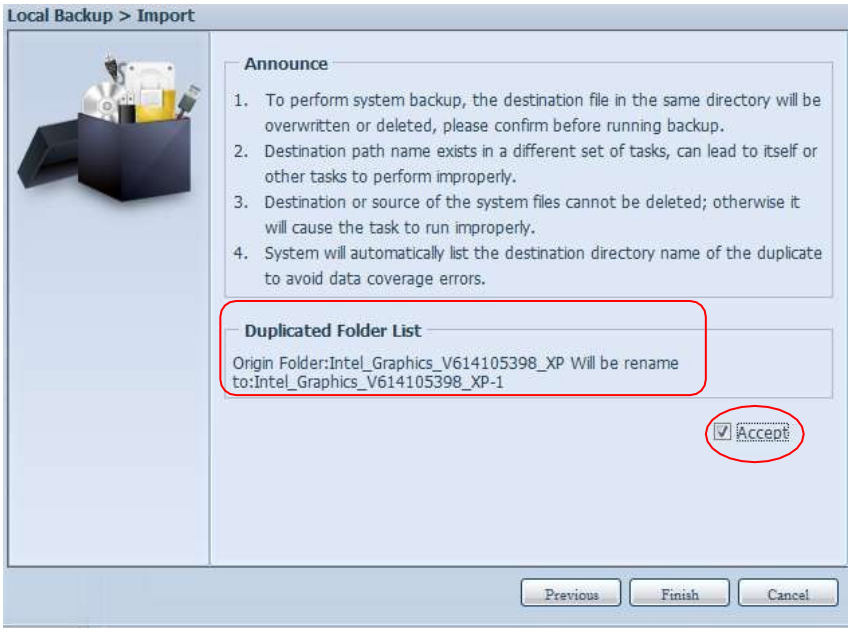
Figure 274: Path selection



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".

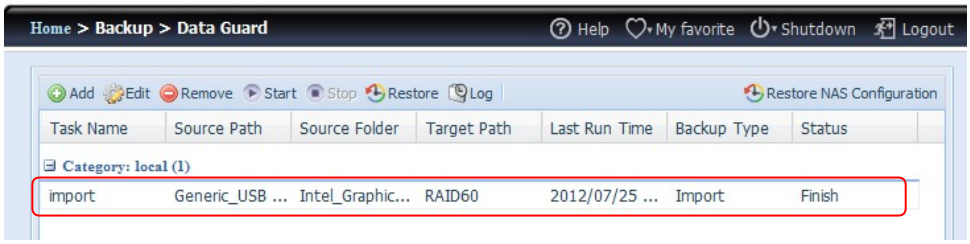
For example, if the NAS RAID volume "RAID60" already has a folder named "Intel_Graphics_V614105398_XP", the import folder will then be rename to: "Intel_Graphics_V614105398_XP-1".

Figure 275: Existing share name



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

Figure 276: Created task



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

Figure 277: Created folders

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.

Figure 278: Copy options

Folder to Folder

Figure 279: Folder to folder

Folder to external device

Figure 280: Folder to external device

External device to Folder

Figure 281: External device to folder

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.

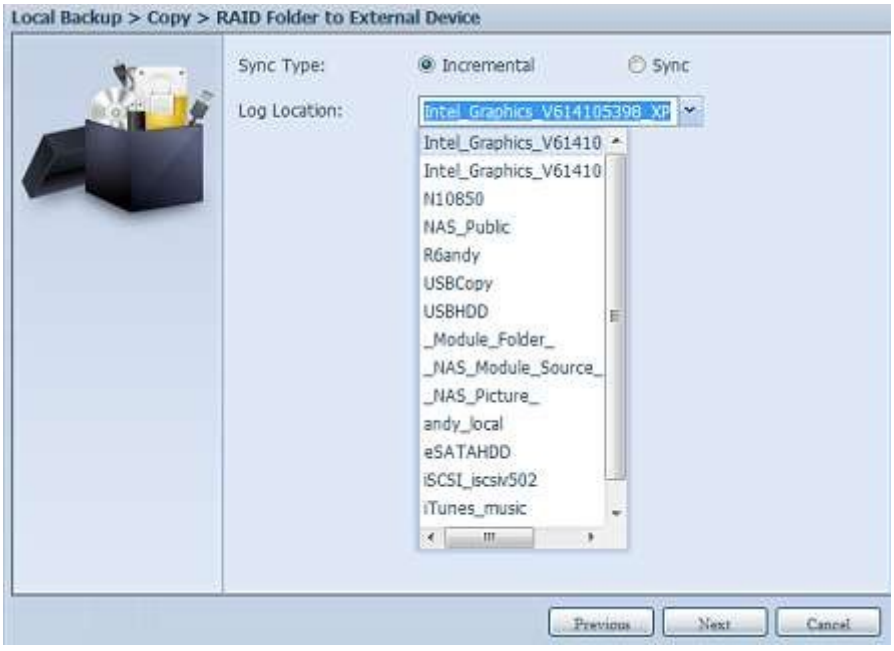
Figure 282: Folder to external device screen

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

Figure 283: Folder and target selection

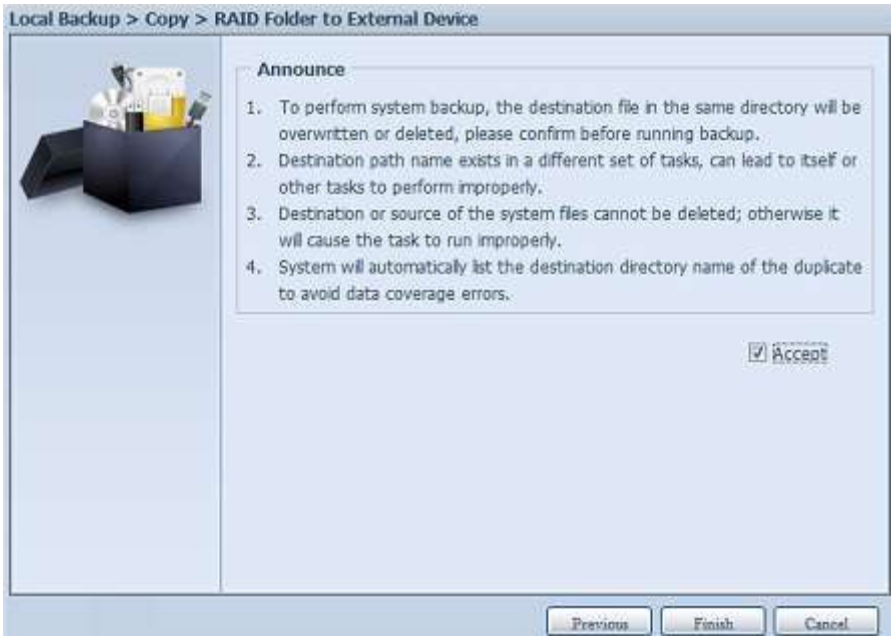
Choosing the sync type, "Incremental" or 'Sync", and select the log path from the drop menu list.

Figure 284: Sync type



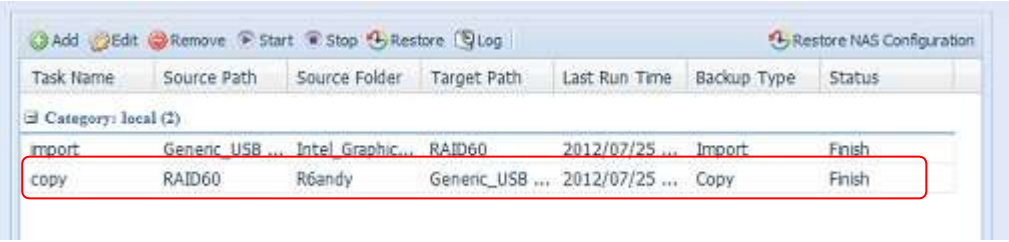
Read the notes and check the “Accept” box for confirmation.

Figure 285: Notes



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

Figure 286: Created task



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 sourcepane the folder "NAS_Public", then select its destination in the target panefolder "R6andy".

   Figure 287: Folder to folder screen

Next, fill in the task name and related settings.

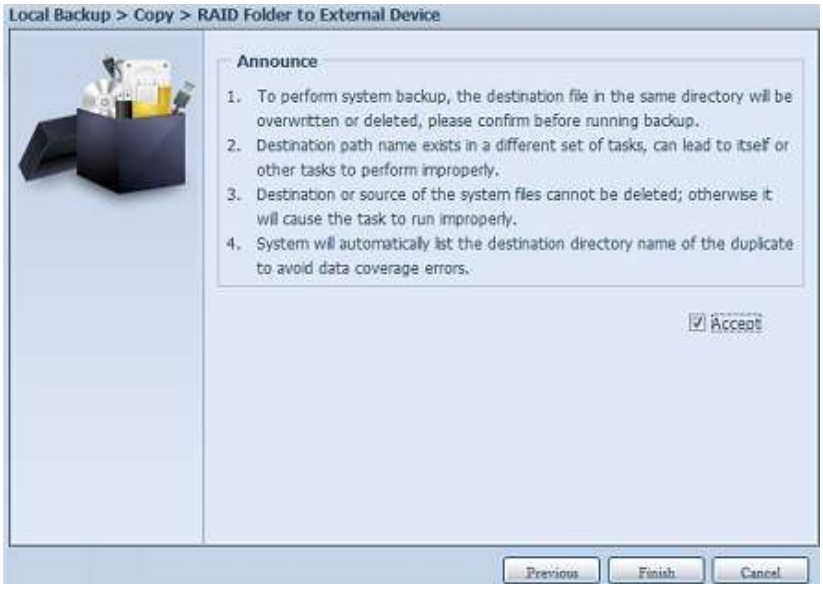
Figure 288: Task name and settings

Table 64: 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.

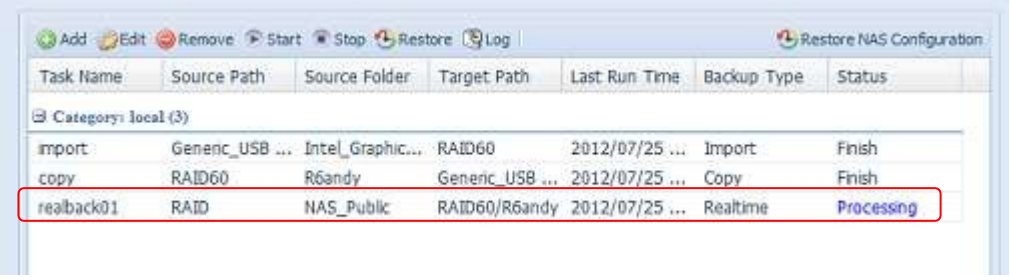
Read the notes and check the "Accept" box for confirmation.

Figure 289: Notes



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.

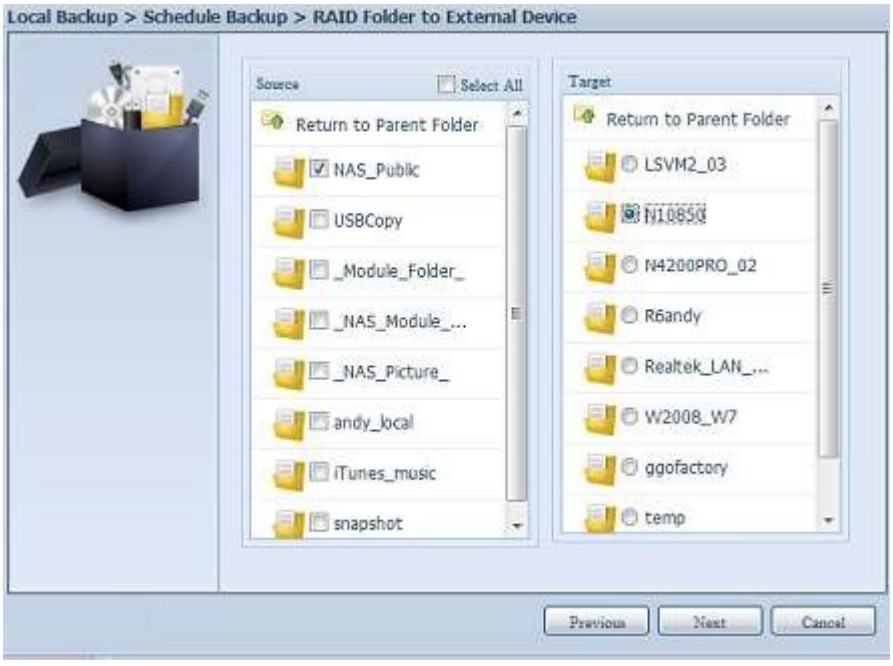
Figure 290: Created task



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".

Figure 291: Folder to external device example

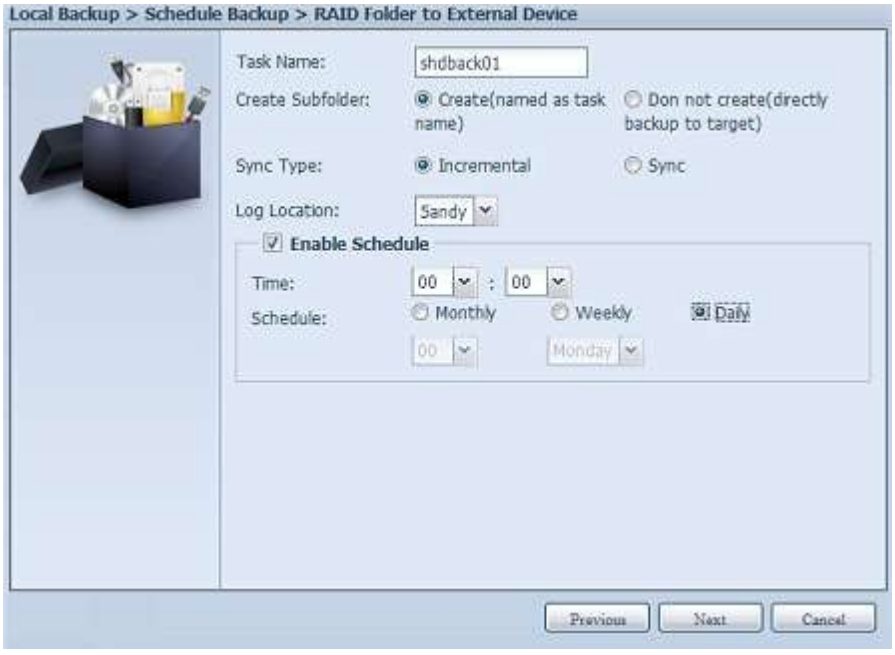


Next, fill in the task name and related settings.

Table 65: Schedule backup

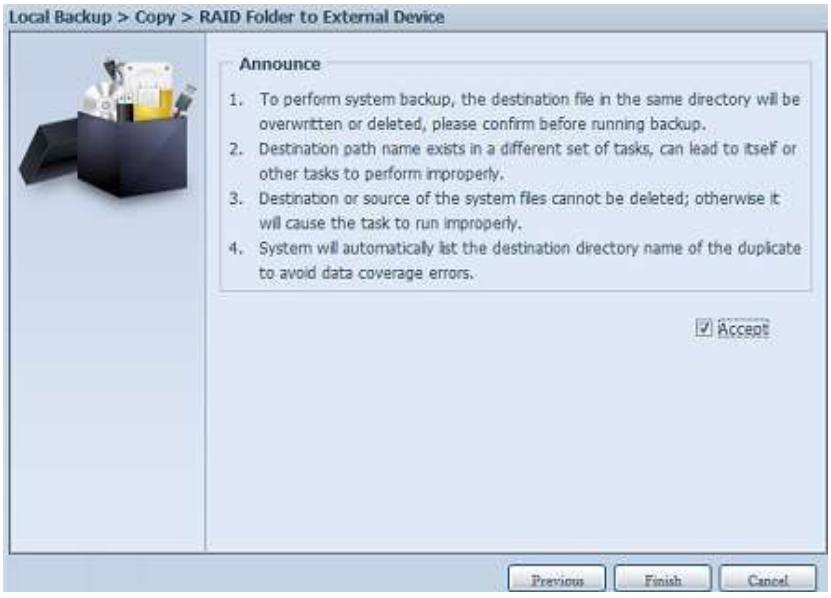
Item	Description
Task Name	Input the task name, length limited to 4~12 characters.
Create Sub-folder	If you choose to create a sub-folder, then it will use the task name as folder name then copy the source under it. Or it will copy the source to the same level as the destination.
Sync Type	Select “Incremental” 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.

Figure 292: Task name and settings



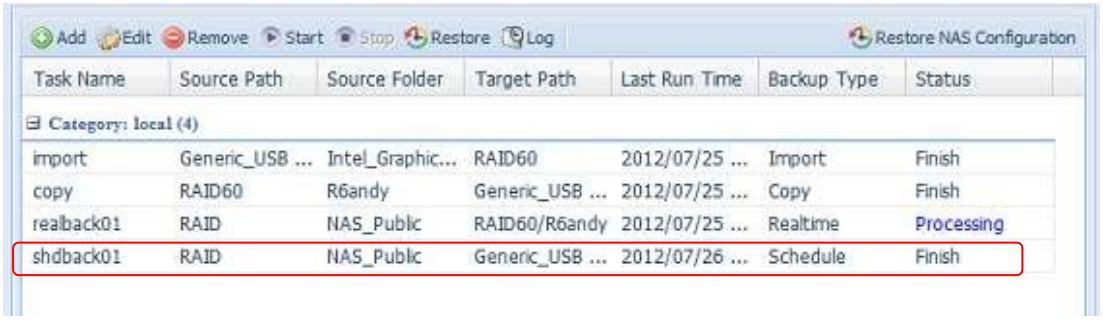
Read the notes and check the "Accept" box for confirmation.

Figure 293: Notes



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

Figure 294: Created task



5. iSCSI Backup: click on "iSCSI Backup" and screen appear as below.

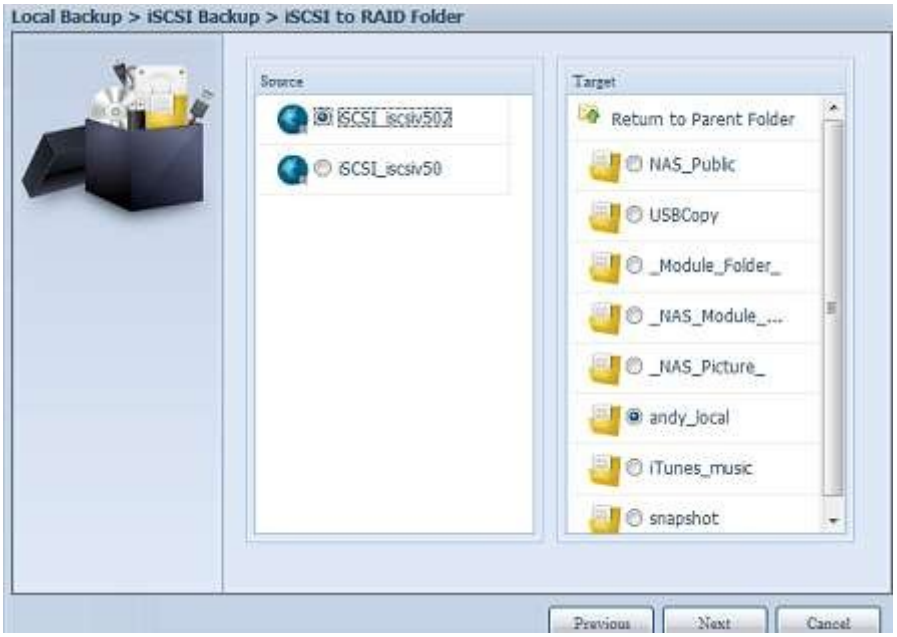
   It can be backup to two different storage pool, iSCSI to folder, iSCSI to external device.

   Figure 295: iSCSI backup screen

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

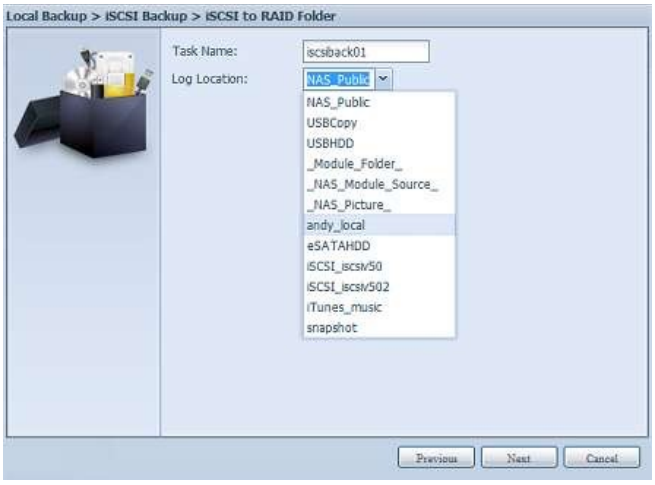
   The source pane listed "iSCSI_iscsiv502" and "iSCSI_iscsiv50" where are iscsi volume has existed in this system with name "iSCSI_+iscsi target volume name".

   Figure 296: iSCSI to folder example



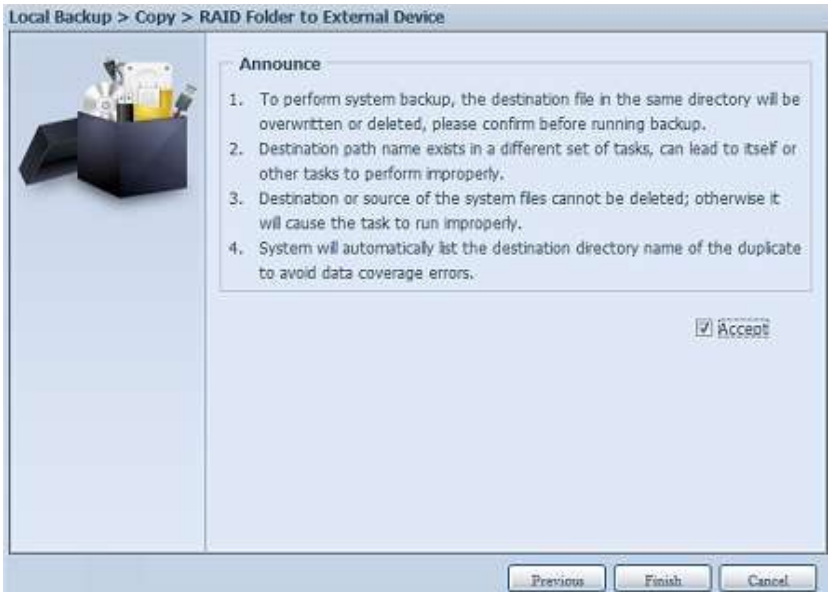
Next, provide the task name and where the task log will store.

Figure 297: Task details



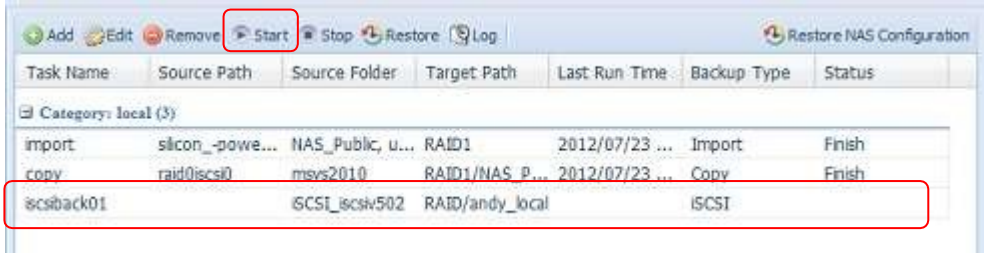
Reading the note and check on "Accept" for confirmation.

Figure 298: Note



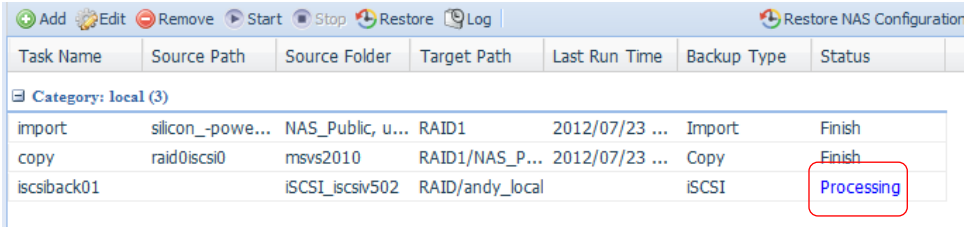
Now, from the data guard task list will have created task listed. To start the iSCSI volume backup, select the task and click "Start" from task bar.

Figure 299: Created task



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

Figure 300: Processing task

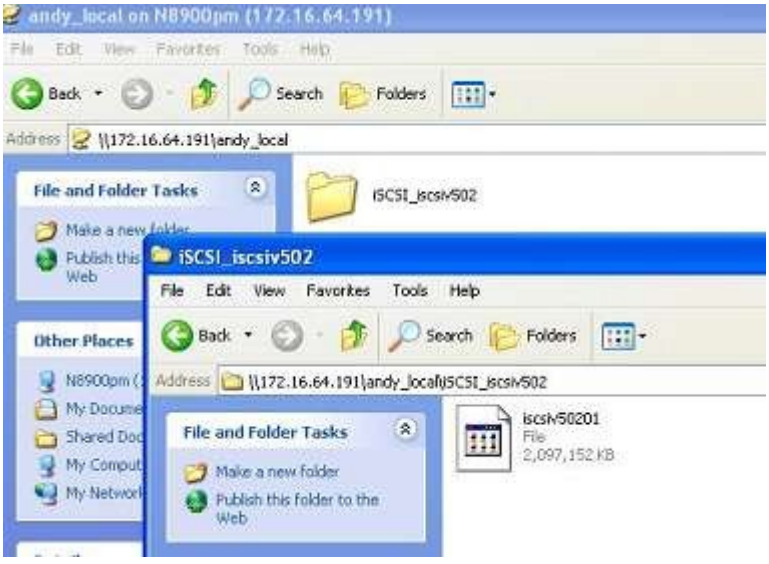


States change to "Finish" after task complete.

Figure 301: Task finished

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.

Figure 302: RAID volume folder



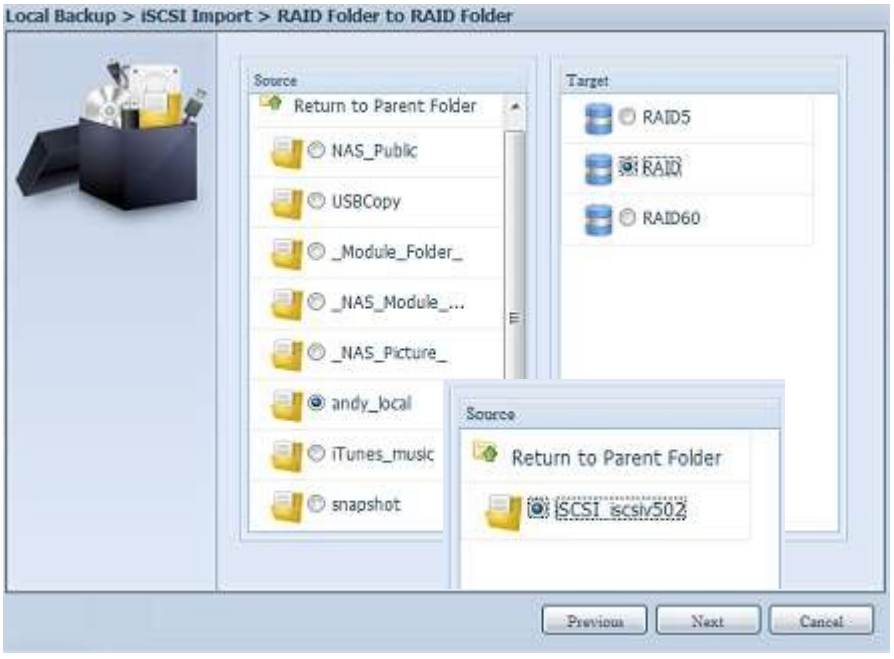
6. iSCSI Import: click on "iSCSI Import" and screen appear as below.

   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 backupto.

Figure 303: Import options

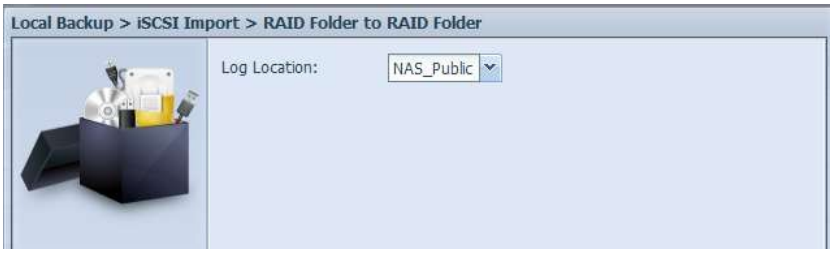
Let's take example to import "RAID folder to iSCSI" which is the iSCSI volume we have backup earlier to RAID volume folder andy_local than import to volume RAID.

Figure 304: RAID folder to iSCSI example



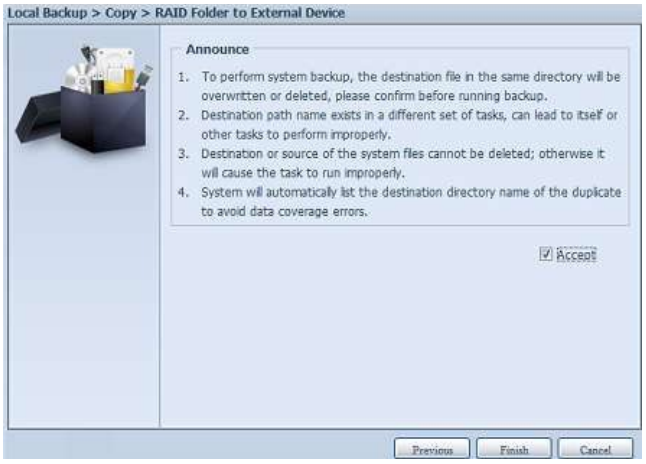
Next, provide where the task log will store.

Figure 305: Log location



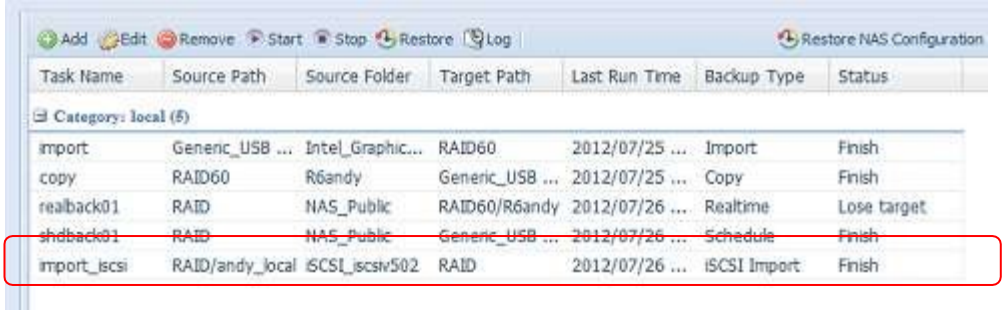
Reading the note and check on "Accept" for confirmation.

Figure 306: Note



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

Figure 307: Created task



4.10.7. USB Copy

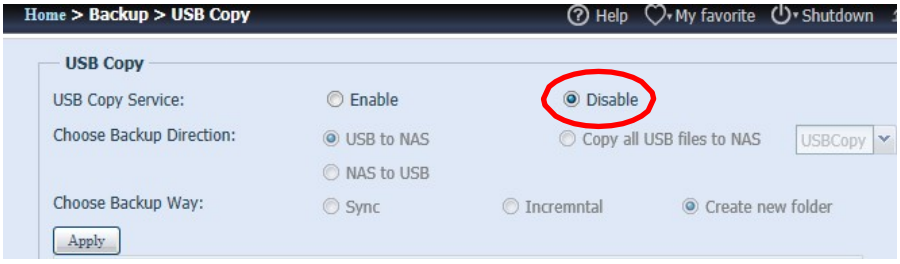
The USB Copy function using the USB copy button or front panel LCM/OLED of system used to only offer one-way transfers (i.e. only from the USB drive to the designated NAS folder). Now numerous options are available, such as: Disabled, bi-directional, and scheduled.

Figure 308: USB copy

4.10.7.1. Disable USB Copy

Simply select "Disable" for the USB Copy Service option and the USB Copy button or LCM/OLED USB Copy item will become inactive.

Figure 309: Disable USB copy



4.10.7.2. Using USB Copy

Enable the USB Copy service and select one of the 3 options available: "USB to NAS", "NAS to USB", and "Copy all USB files to NAS".

If select "USB to NAS" or "NAS to NAS", you will also need to set up the type of backup desired.

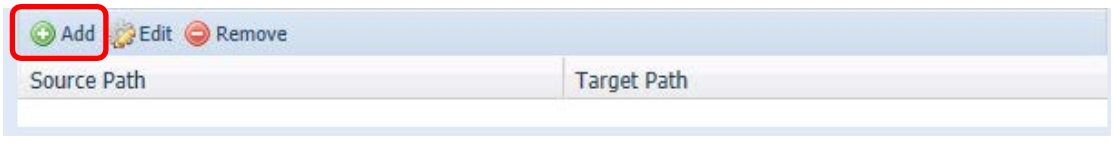
Table 66: USB copy service transfer options

Item	Description
Sync	Makes your source match your target completely; deleting and adding files on your target as they are deleted and added on your source.
Incremental	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.
Create New	Create new folder on target based on the task's "Date+Time".
Apply	Press Apply to confirm the settings.

Now, add the task for the USB Copy service you have selected (for "USB to NAS" or "NAS to USB").

Click on "Add" and select "Source Path" and "Target Path" from the drop-down list.

Figure 310: Adding task

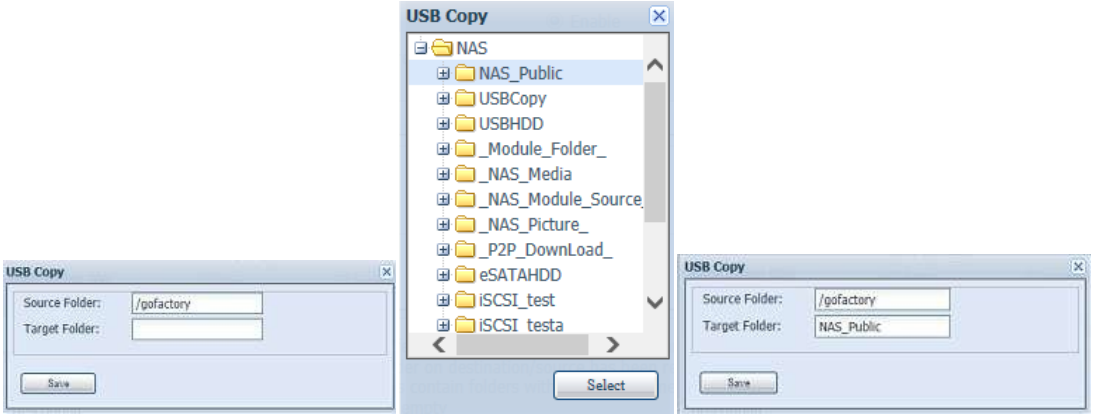


Add Source:

Figure 311: Adding source

Add Target:

Figure 312: Adding taget



Save the completed task:

Figure 313: Saved task

To "Edit" or "Remove" a USB Copy task, select the task item and click on the associated function:

Figure 314: Editing task

If you select "Copy all USB files to NAS", then please choose the target path from the drop-down list. All files and folders on the USB device will be copied over to the NAS.

Figure 315: Choosing target path

If "Sync" mode has been selected, the target-side redundant folders/files will be deleted after a comparison has been conducted of the source.

Once the USB Copy service has completed, the USB device will un-mount from system. To start another task, please re-insert the USB device.

4.10.8. Volume Expansion Management

Please refer to the CS3160 - Volume Expansion User Guide document. This document can be found on our website: www.kontron.com.

4.10.9. Thecus Backup Utility

The Thecus Backup Utility is on your Installation CD. When you click on the CD, the Backup Utility will be installed under Program Groups > Thecus > Thecus Backup Utility. If it is not installed, you can copy the file (Thecus Backup Utility.exe) to a convenient location on your hard disk and double click to execute it.

Figure 316: Thecus backup utility

If you can not find Thecus Backup Utility on your CD, please download it from the Kontron website (www.kontron.com).

When you execute this utility for the first time, it will ask you to create a DB file. Click Yes.

1. Click Add to create a Backup task. The Add New Task dialog box will appear.

Table 67: Add new task

Item	Description
Task	Specifies a name for the current task.
Source	Click to specify the source folder/file location.
Incremental	Click to specify whether the backup will be incremental. If unchecked, the backup will be a full backup.
Destination	Click to specify the destination folder/file location.
Excluded extensions	Files with these file name extensions will be skipped and not backed up to the destination.
Comments	If you wish, enter a comment here for your records.

2. To schedule the task to run at regular intervals, click on the Schedule icon for that task. You can schedule the task to run Monthly or Weekly.
3. To check the log for that task, click on the Log icon for that task.

Thecus Backup Utility also supports MAC OS X. Just copy the Thecus Backup Utility.dmg to your MAC OS X machine and double click to execute it.

4.10.10. Windows XP Data Backup

If you use Windows XP Professional, you can also use the Windows Backup Utility (Ntbackup.exe) to back up your files.

If you use Windows XP Home Edition, follow these steps to install the utility:

1. Insert the Windows XP CD into a drive and double-click the CD icon in My Computer.
2. When the Welcome to Microsoft Windows XP screen appears, click Perform Additional Tasks.
3. Click Browse this CD.
4. In Windows Explorer, navigate to ValueAdd > Msft > Ntbackup.
5. Double-click Ntbackup.msi to install the backup utility.

Once installed, you can use the Windows Backup Utility by following the steps below:

1. Click Start, and point to All Programs > Accessories > System Tools > Backup to start the wizard.
2. Click Next to skip past the opening page. Choose Backup files and settings from the second page, and then click Next.
3. Select which option you want to back up.
4. Click Next and in the Backup Type, Destination, and Name page, specify a backup location using the Browse button.
5. Find and select the drive that specifies your CS3160 as your backup destination and click Next.
6. Click Next to display the wizard's final page and click Finish to start backing up.

4.10.11. Apple OS X Backup Utilities

Mac OS X does not include any backup software. However, there are a numberof backup solutions available for the Mac OS X, including: iBackup, Psyncx, iMSafe, Rsyncx, Folder Synchronizer X, Tri-BACKUP, Impression, Intego Personal Backup, SilverKeeper, and Apple's dotMac Backup utility to name just a few. To findeven more freeware and shareware backup utilities to choose from, go to VersionTracker or MacUpdate and search on "backup".

4.11. External Devices

The CS3160 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, the CS3160 support via USB, Series and Network interface. The following section shows you how.

4.11.1. 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.

Figure 317: Printers

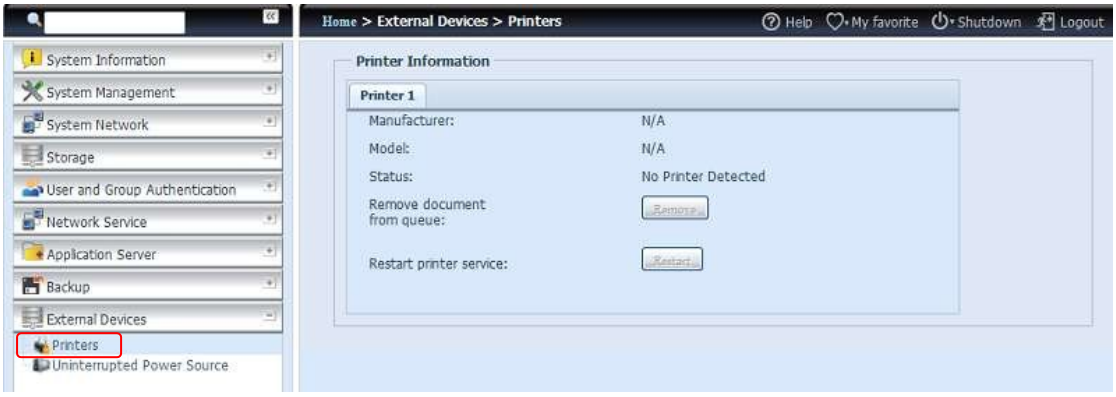


Table 68: Printer information

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 the CS3160 to act as a printer server. That way, all PCs connected to the network can utilize the same printer.

4.11.1.1. 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://CS3160 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.

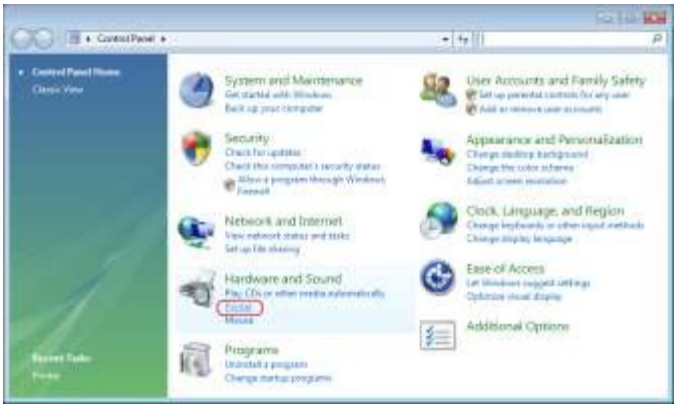
Note that if a multi-function (all-in-one) printer is attached to the CS3160, usually only the printing and fax functions will work. Other features, such as scanning, will probably not function.

4.11.1.2. Windows Vista

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

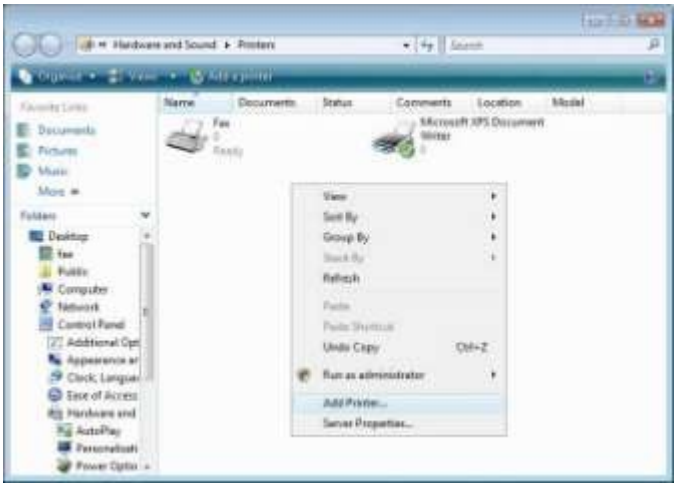
1. Open Printer Folder from the Control Panel.

Figure 318: Control panel



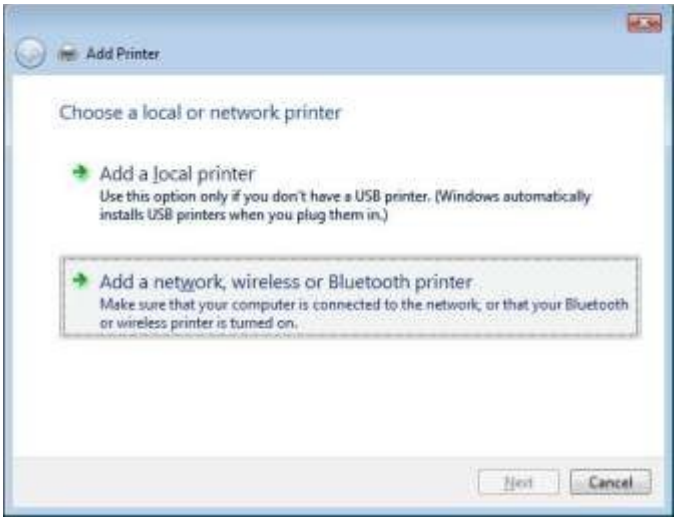
2. Click the right mouse button in anywhere on the Printers folder and then select Add Printer.

Figure 319: Add printer



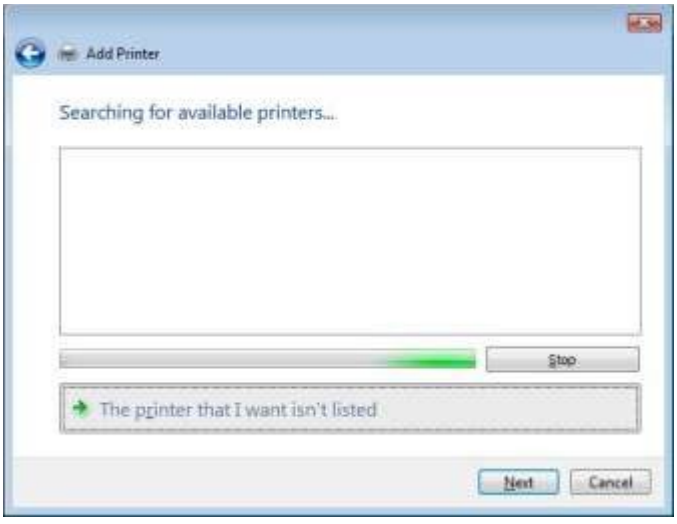
3. Select Add a network, wireless or Bluetooth printer.

Figure 320: Add network



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

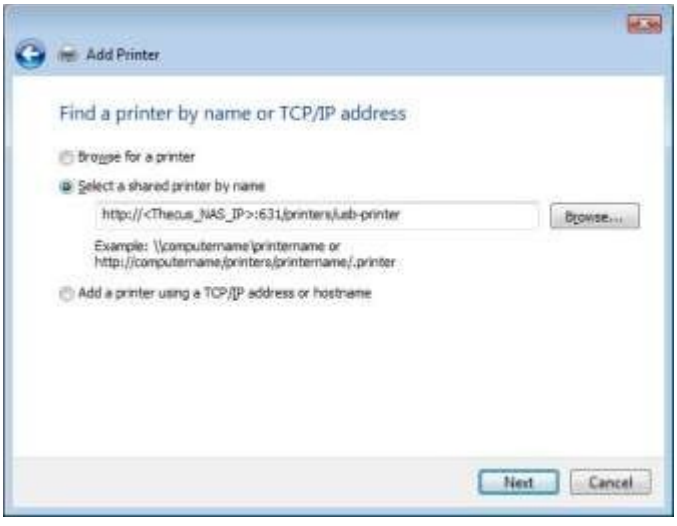
Figure 321: Printer search



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.

Figure 322: Select a shared printer by name



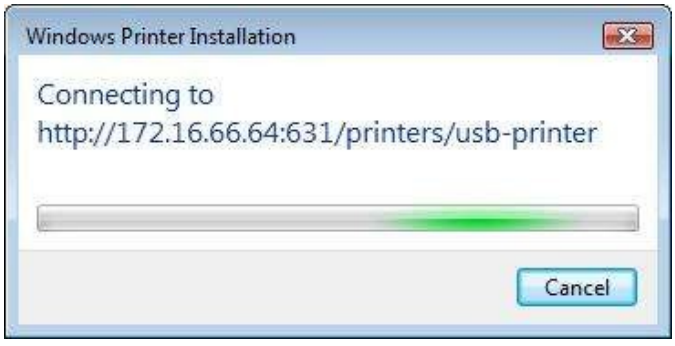
Type http://<CS3160_NAS>:631/printers/usb-printer in the box, where <CS3160_NAS_IP> is the IP address of the CS3160. Click Next.

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

Figure 323: Printer selection or installation

7. Windows will attempt to connect to the printer.

Figure 324: Printer connection

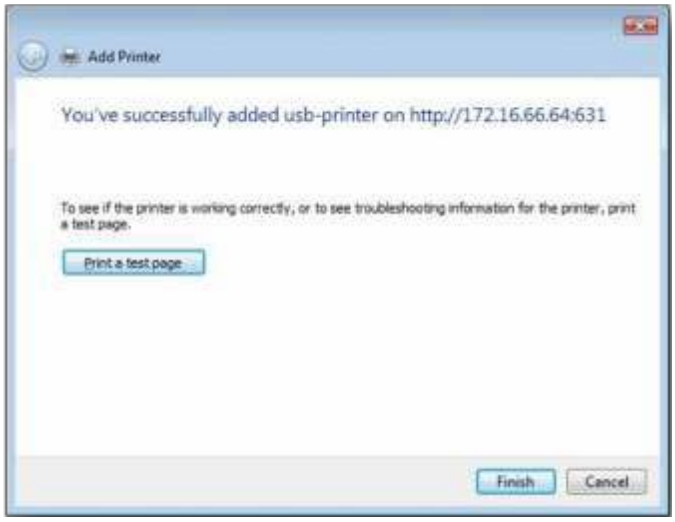


8. You can choose to set this printer as the default printer by checking the Set as the default printer box. Click Next to continue.

Figure 325: Set as the default printer

9. Done! Click Finish.

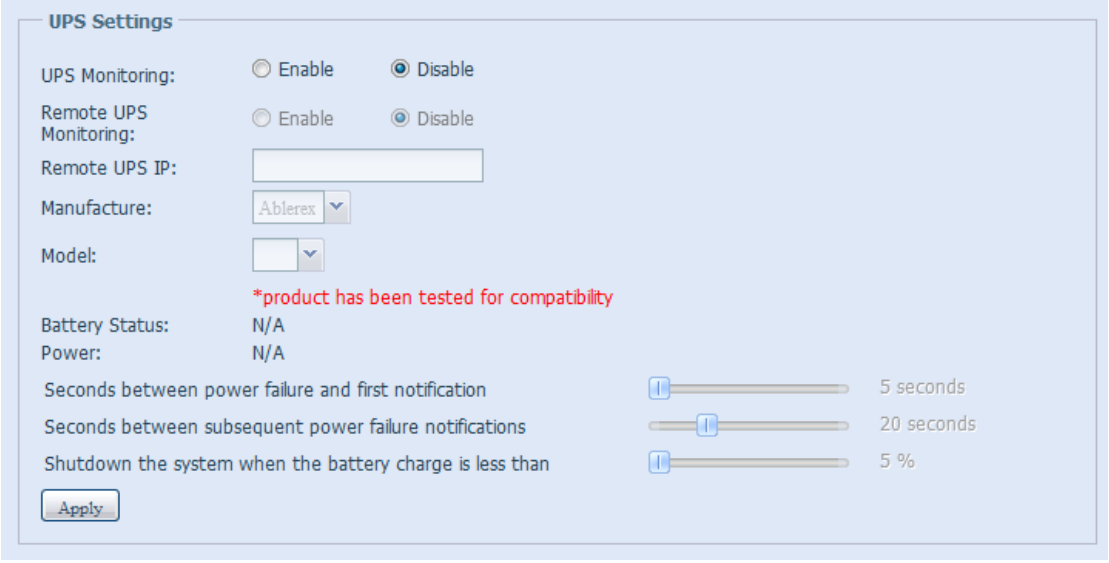
Figure 326: Finish



4.11.2. 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.

Figure 327: Uninterrupted power source



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

Table 69: UPS setting

Item	Description
UPS Monitoring	Enable or disable UPS monitoring.
Remote UPS Monitoring	Enable or disable Remote UPS monitoring.

Item	Description
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.

5/ Tips and Tricks

5.1. USB and eSATA Storage Expansion

The CS3160 supports external USB hard disks through its USB ports. Once a USB hard disk is successfully mounted, the entire volume will be linked automatically to the default USB HDD folder. The CS3160 supports USB external storage devices. All file names on the USB disk volume are case sensitive.

The CS3160 also supports eSATA hard disks with its eSATA port.

Before attaching an eSATA or USB disk drive to the CS3160, you have to partition and format it on a desktop computer or a notebook first. The attached device will be located at \\192.168.1.100\usbhdd\sd(x)1 where 192.168.1.100 means the IP address of the CS3160 and sd(x)1stands for the first partition on the eSATA or USB disk drive.

5.2. Remote Administration

You can set up your CS3160 for remote administration. With remote administration, you can access your CS3160 over the Internet, even if your CS3160 is behind a router. This is especially useful if you are traveling and suddenly need a file from your CS3160.

Setting up remote administration is a three-part process, and will require the following equipment:

- CS3160 device
- Cable / DSL Router with Dynamic DNS support
- Home PC
- Internet Connection

Router setup will differ slightly depending on router used. For this example, we will use the Asus WL500g because it has support for Dynamic DNS.

Contact your router hardware vendor for setup help.

5.2.1. Part I - Setup a DynDNS Account

1. Go to www.dyndns.org from your home PC.
2. Click on the Sign Up Now link.
3. Check the Check boxes, select a user name (i.e.: N12000), enter your email address (i.e.: xxx@example.com), check Enable Wildcard, and create a password (i.e.: xxxx).
4. Wait for an email from www.dyndns.org.
5. Open the email and click on the link to activate your account

5.2.2. Part II - Enable DDNS on the Router

1. Go to the router setup screen and select IP Config > Miscellaneous DDNS Setting from your Home PC.
2. Click on Yes for Enable the DDNS Client?
3. Select www.dyndns.org.
4. Go to router setup screen, and enter the following information:

a. User Name or E-mail Address: xxx@example.com

b. Password or DDNS Key: xxxx

c. Host Name: www.N12000.dyndns.org

d. Enable wildcard? Select Yes

e. Update Manually: Click Update

5.2.3. Part III - Setting up Virtual Servers (HTTPS)

1. Navigate to NAT Setting > Virtual Server.
2. For Enable Virtual Server?, select Yes
3. Setup the HTTPS Server
    a. Well-Known Applications: Select User Defined
    b. Local IP: Enter 192.168.1.100
    c. Port Range: 443 (the default HTTPS port setting on the CS3160)
    d. Protocol: select TCP
    e. Click Add.
    f. Click Apply.
4. Test the HTTPS connection from another computer on the Internet
    a. From a remote computer, open your browser and enter www.n12000.dyndns.org
    b. You should see the login page of the CS3160.

5.3. Firewall Software Configuration

If you are using a software firewall (i.e. Norton Internet Security) and are having trouble connecting to the CS3160, you can try the following steps:

1. Double click the NIS icon on system tray, and then configure the Personal Firewall.
2. On the Programs page, find the SetupWizard.exe and change its permission to "Permit All". If it's not in the program list, use the Add or Program Scan buttons to find it.
3. On the Networking page, manually add the CS3160 IP address (i.e. 192.168.1.100) to the Trusted list.

5.4. Replacing Damaged Hard Drives

If you are using RAID 1, RAID 5, RAID 6, RAID 50 or RAID 60 you can easily replace a damaged hard drive in the CS3160 while keeping your data secure with the system's automatic data recovery.

5.4.1. Hard Drive Damage

When a hard drive is damaged and data in the RAID volume is corrupted, the system OLED will display a warning message and the system will beep.

5.4.2. Replacing a Hard Drive

To replace a hard disk drive in the CS3160:

1. Remove the tray with the damaged hard disk.
2. Unscrew the damaged hard disk and remove it from the tray.
3. Slide a new hard disk into the tray and fasten the screws.
4. Insert the hard disk tray back into the CS3160 until it snaps into place. You can also lock it with a key if desired.
5. The LED will blink green when the HDD is accessed.

5.4.2.1. RAID Auto-Rebuild

When using RAID 1, 5, 6, 10, 50 or 60 on the CS3160, you can use the auto-rebuild function when an error is detected.

1. When a hard disk fails the system beeps and/or an email notification is sent to the specified receivers.
2. Check the OLED to see which disk has failed.
3. Follow the steps mentioned above to replace the failed hard disk.
4. The system automatically recognizes the new hard disk and starts the auto-rebuild sequence to resume its status before the hard disk crash.

6/ Troubleshooting

6.1. Forgot My Network IP Address

If you forget your network IP address and have no physical access to the system, you can find out the IP address by either looking directly onto the CS3160 OLED panel, or by using the setup wizard to retrieve the IP of your CS3160.

1. Start the Setup Wizard, and it will automatically detect all CS3160 products on your network.
2. You should be able to find the IP address of the CS3160 which you have forgotten in the Device Discovery screen.

6.2. Can't Map a Network Drive in Windows XP

You may have problems mapping a network drive under the following conditions:

1. The network folder is currently mapped using a different user name and password. To connect using a different user name and password, first disconnect any existing mappings to this network share.
2. The mapped network drive could not be created because the following error has occurred: Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.

To check out existing network connections, type net use under the DOS prompt.

6.3. Restoring Factory Defaults

From the System menu, choose the Factory Default item and the Reset to Factory Default screen appears. Press Apply to reset the CS3160 factory default settings.

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.

6.4. Problems with Time and Date Settings

The administrator is able to select an NTP Server to keep the CS3160 time synchronized. However, if the CS3160 cannot access the Internet, you may encounter a problem when setting the Time and Time Zone. If this happens:

1. Login to the Web Administration Interface.
2. Navigate to System Management>Time.
3. Under NTP Server, select No.
4. Set the Date, Time, and Time Zone.
5. Click Apply.

In addition, if the CS3160 is able to access the Internet and you want to keep the NTP Server clock.isc.org by default, please make sure the DNS Server is correctly entered, thereby allowing the NTP Server name to correctly resolve. (See System Network > WAN/LAN1 > DNS Server)

6.5. Dual DOM Supports for Dual Protection

The most advance and useful feature on the CS3160 (depend on models) is the implemented Dual DOM. Under normal circumstances, there is no need to have this feature involved. But some unpredictable problems like power

cut or human error can occur by accident, especially during system booting stage; the Dual Dom will become the best feature to prevent system down time.

Practically while it happened, system will try to recover the DOM 1 from DOM 2 first. If it is unachievable then the system can boot from DOM 2. And all of these procedures can be operated through the OLED.

The DOM1 in Dual DOM is by default the master DOM and FW updates will

only apply to DOM1. DOM2 is 'Read only".

If anything happened and the DOM1 is recovered from DOM2, the FW version will be the one of the DOM2. Therefore, it may need to be upgraded to the version of DOM1.

If DOM1 can not be recovered from DOM2, the system will boot up from DOM2. The original configuration of DOM1 may need to be setup again with DOM2 operations.

Appendix A: Customer Support

If your CS3160 is not working properly, we encourage you to check out Chapter 6/, located in this manual. You can also try to ensure that you are using the latest firmware version for your CS3160. Kontron is committed to providing free firmware upgrades to our customers. Our newest firmware is available on our Download Center:

www.kontron.com

If you are still experiencing problems with your CS3160, or require a Return Merchandise Authorization (RMA), feel free to contact technical support via our Technical Support Website:

www.kontron.com

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

www.kontron.com

For Sales Information you can e-mail us at: www.kontron.com

Thank you for choosing Kontron!

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 CS3160 supports standard RAID levels 0, 1, 5, 6, 10, 50, 60 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.

RAID 50

A RAID 50 combines the straight block-level striping of RAID 0 with the distributed parity of RAID 5. This is a RAID 0 array striped across RAID 5 elements. It requires at least 6 drives.

RAID 60

A RAID 60 combines the straight block-level striping of RAID 0 with the distributed double parity of RAID 6. That is, a RAID 0 array striped across RAID 6 elements. It requires at least 8 disks.

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, the CS3160 disk usage percentage is listed below:

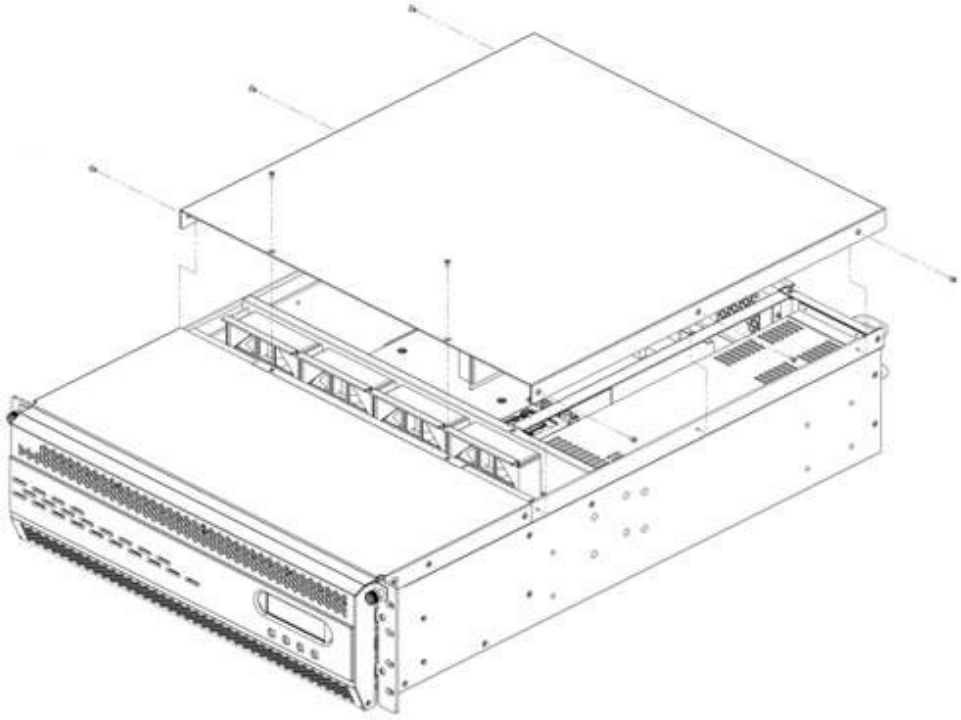
Table 70: Disk usage

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%
RAID 50	(n-1)/n x 100%
RAID 60	(n-2)/n x 100%
JBOD	100%

n：HDD number

Appendix C: How to Open the Top cover

Figure 328: CS3160



Appendix D: 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 the CS3160 integrate itself with the existing ADS in an office environment. This means the CS3160 is able to recognize your office users and passwords on the ADS server. Other major benefits ADS support provides include:

1. Easy integration of the CS3160 into the existing office IT infrastructure

   The CS3160 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 the CS3160.

2. Centralized user/password database

   The CS3160 does not maintain its own copy of the user/password database. This avoids data inconsistency between the CS3160 and other servers. For example, without ADS support, an administrator might need to remove a specific user privilege on the CS3160 and each individual server. With ADS support, the change on an ADS server is known to all of its ADS members.

Appendix E: 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, 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

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

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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 derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

12. 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.

13. 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

About Kontron

Kontron, a global leader in embedded computing technology and trusted advisor in IoT, works closely with its customers, allowing them to focus on their core competencies by offering a complete and integrated portfolio of hardware, software and services designed to help them make the most of their applications.

With a significant percentage of employees in research and development, Kontron creates many of the standards that drive the world's embedded computing platforms; bringing to life numerous technologies and applications that touch millions of lives. The result is an accelerated time-to-market, reduced total-cost-of-ownership, product longevity and the best possible overall application with leading-edge, highest reliability embedded technology

Kontron is a listed company. Its shares are traded in the Prime Standard segment of the Frankfurt Stock Exchange and on other exchanges under the symbol "KBC". For more information, please visit: http://www.kontron.com/

CORPORATE OFFICES

EUROPE, MIDDLE EAST & AFRICA

Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com

NORTH AMERICA

14118 Stowe Drive
Poway, CA 92064-7147
USA
Tel.: + 1 888 294 4558
Fax: + 1 858 677 0898
info@us.kontron.com

ASIA PACIFIC

1~2F, 10 Building, No. 8 Liangshuihe 2nd Street,
Economical & Technological Development Zone,
Beijing, 100176, P.R. China
Tel.: + 86 10 63751188
Fax: + 86 10 83682438
info@kontron.cn