D-Link®

Version 1.0 | 1/14/2011

User Manual

ShareCenter® 2-Bay Network Storage

DNS-320

Table of Contents

Product Overview 1
Introduction 1
Package Contents 2
System Requirements 2
Features 3
Hardware Overview 4
Front Panel 4
Rear Panel (Connections) 5

Getting Started 6
ShareCenter Software CD 6

Installation 7

Setup Wizard 7
Install the Hard Drives 8
Power and Device Selection 10
Admin password 11
Network Setup 12
Dynamic DNS 13
DDNS Account and System Time 14
E-mail Settings and Volume Information 15
RAID Configuration and Drive Mapping 16
Configuration Summary and Drive Formatting 17
Format Complete 18
D-Link Storage Utility 20

Configuration 22
Web UI Login 22
Web UI General Layout 23
Management 24
Setup Wizard (Web UI) 25
Disk Management 29
Hard Drive Configuration 29
Hard Drive Configuration Wizard 30
S.M.A.R.T Test 34
Scan Disk 36
Account Management 37
Users / Groups 37
Adding New Users Wizard 38
Adding New Groups Wizard 42
Quotas 46
Network Shares 47
Adding New Network Shares Wizard 48
Adding New ISO Mount Shares Wizard 54
Admin Password 58
Network Management 59
LAN Setup 59
Dynamic DNS 61
Application Management 62
FTP Server 62
UPnP AV Server 63

iTunes Server 64
AFP Service 65
NFS Service 66
System Management 67
Language 67
Time and Date 68
Device 69
System Settings 70
Power Management 72
Notifications 74
Logs 78
Firmware Upgrade 79
Status 80
System Info 80
Hard Drive Info 81
Applications 82
FTP/HTTP Downloads 82
Remote Backups 84
Local Backups 89
Local Backups - Time Machine 90
P2P Downloads - Settings 91
P2P Downloads - Downloads 92
Web File Server 93
AjaXplorer 94
My Favorites 95
Re-arranging the My Favorites View 95
Add an Icon to My Favorites 96
Remove an Icon from My Favorites 97

Knowledge Base 98
What is RAID? 98
Mapping a Drive 99
Mapping the Recycle Bin 102
USB Print Server 103
Yahoo! Widget Installation 106
Yahoo! Widget Display 107
USB Copy Function 108

Contacting Technical Support 109

Warranty 110

Registration 115

Product Overview

Introduction

The D-Link ShareCenter® DNS-320 2-Bay Network Storage, when used with internal SATA drives, enables you to share documents, files, and digital media such as music, photos, and video with everyone on the home or office network. Remotely accessing files through the Internet is also possible with the built-in FTP server and Web File server. Whether you are allowing access locally or over the Internet, keep data safe by only giving rights to specific users or groups. When configuring the ShareCenter®, you can create users and groups and assign them to folders with either read or read/write permissions. This is ideal for an office environment with employee-specific sensitive data or for the home where you can ensure your children will only have access to age appropriate material. The ShareCenter® will be available to any computer (PC, MAC, or Linux-based) on your network, without the need to install any software on the computer.

Back up your music, photo, and video collections to the ShareCenter® for safekeeping. Then, enjoy the benefits of the built-in DLNA Certified™ media server as you stream digital content to compatible media players (such as the D-Link's Boxee Box). This feature is highly convenient as it allows you to turn off a computer that would normally be needed for the same function.

The availability of four different hard drive modes (Standard, JBOD, RAID 0, RAID 1) allows you to choose the configuration best suited to your needs. Standard mode creates two separately accessible hard drives. JBOD combines both drives in linear fashion for maximum space efficiency. RAID 0 combines both drives in a 'striped' configuration, which provides the highest performance when using a Gigabit Ethernet connection. RAID 1 causes the drives to mirror each other, providing maximum protection. If one drive fails while configured as RAID 1, the unaffected drive continues to function as a single drive until the failed drive is replaced. The new drive will then be re-mirrored, allowing the ShareCenter® to return to its full protection.

1 Hard Drive(s) not included.

2 D-Link cannot guarantee full compatibility or proper playback with all codecs. Playback capability depends on the codec support of the UPnP™ AV media player.

Package Contents

- D-Link ShareCenter® DNS-320
- CD-ROM with Manual and Software
- Quick Installation Guide
- Power Adapter
- Power Cord
- CAT5 Ethernet Cable

Note: Using a power supply with a different voltage than the one included with the ShareCenter will cause damage and void the warranty for this product.

If any of the above items are missing, please contact your reseller.

System Requirements

For best results, the following minimum requirements are recommended on any system used to configure and use the ShareCenter:

- Computer with: 1GHz processor / 512 MB RAM / 200 MB available space / CD-ROM drive
- Internet Explorer version 7, Mozilla Firefox 3 or Apple Safari 4 and above
- Windows® XP (with Service Pack 2 or higher), Vista® or Windows® 7
- 3.5" SATA Hard Drive(s)

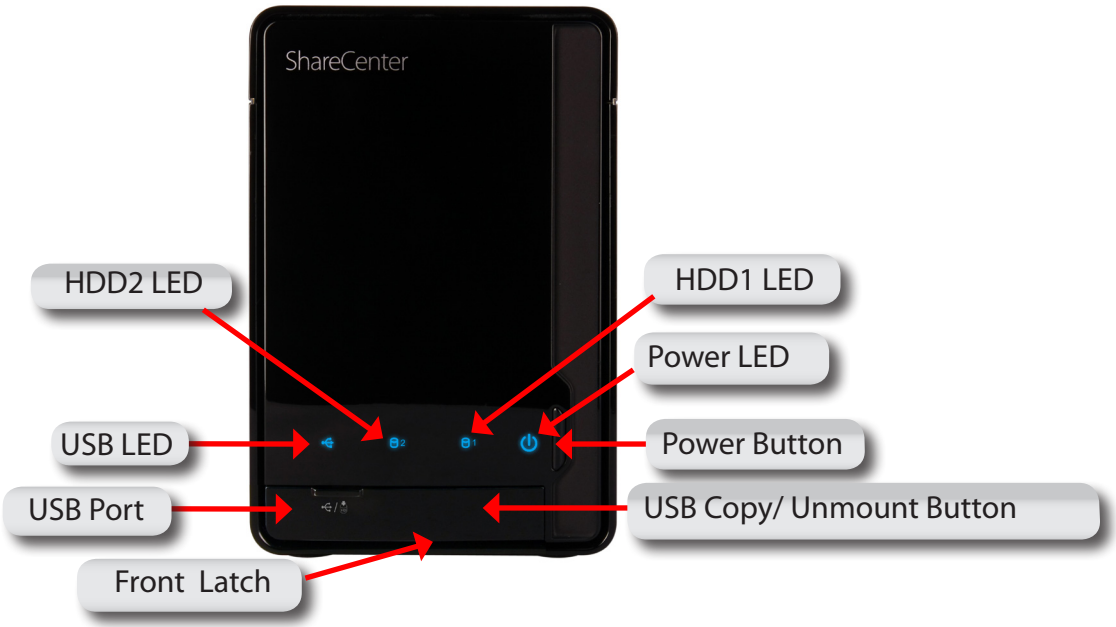
Features

The DNS-320 is an easy to install data storage platform used for remote access through a local network or from the Internet. This ShareCenter® supports up to 2 SATA hard drives and includes the product features listed below:

- Two Hard Drive Bays for 3.5" SATA Hard Drives
- Gigabit Ethernet Connectivity
- Simplified Hard Drive Installation Process
- USB port support External Storage Device, Printer Server, UPS Monitoring
- Four Hard Drive Configurations: Standard, JBOD (Linear), RAID 0, and RAID 1
- Supports RAID Migration: Standard to RAID1
- HDD S.M.A.R.T test
- Supports NFS/AFP.
- Supports DDNS
- Supports UPnP, Bonjour
- Supports PnP-X / LLTD
- Built-in FTP Server for File Access Over the Internet
- FTP Server supports FTP over SSL/TLS and FXP
- Supports Uni-code for both Samba and FTP Server
- Scheduled Downloads from Web or FTP Sites
- Supports P2P Downloading
- Supports Local Backup
- Full or Incremental Backups
- Supports Apple Time Machine
- Supports USB Copy Function
- Supports FAT16/32, NTFS (Read only) for USB external Storage
- Users and Groups Can Be Assigned to Folders with Read or Read/Write Permissions
- Quotas For Users and Groups
- Supports ISO mount Shares
- Power Management for Conserving Energy and Extending Hard Drive Life
- Supports Auto Power Recovery
- Supports Scheduled power off
- UPnP AV Server for Streaming Music, Photos, and Video to Compatible Media
- Designed for easy installation and allows remote access to important data via LAN or WAN.
- iTunes Software will be able to automatically find and play music directly from the DNS-320
- D-Link Storage Utility
- Configurable by Web Browser
- Supports HTTPS Management Function
- Network Recycle Bin
- Supports Yahoo! Widget
- Supports System Logging/FTP Logging
- Automatic E-Mail and SMS Notifications
- Supports Remote File Access

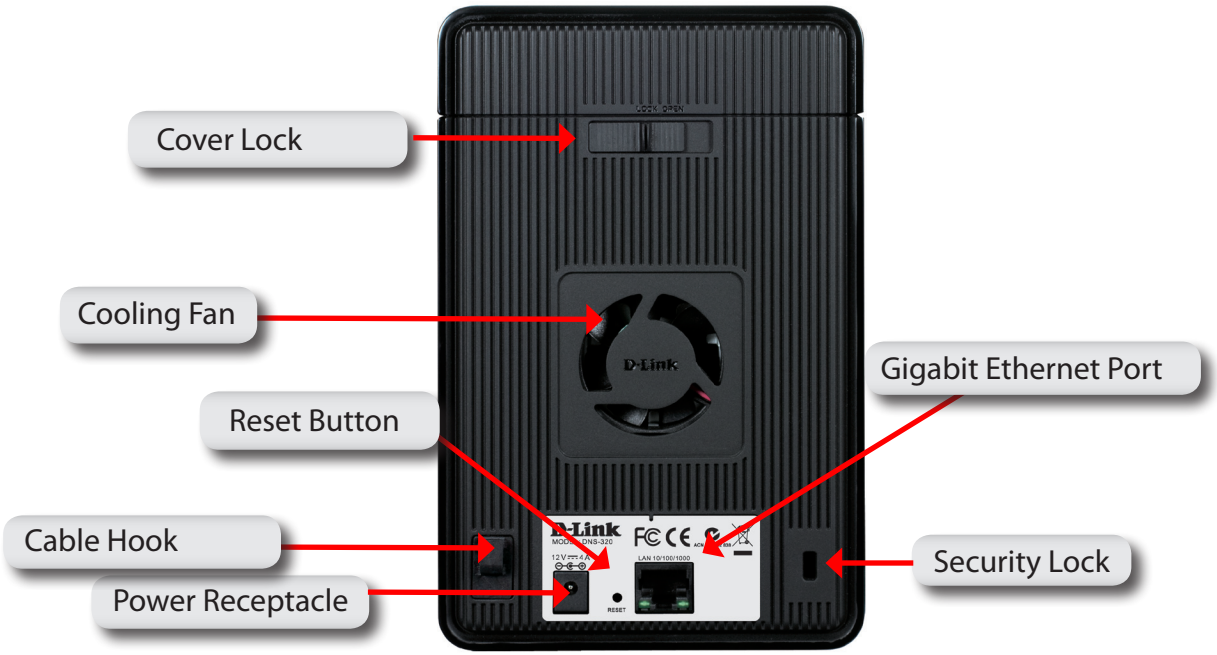
Hardware Overview

Front Panel



COMPONENT	DESCRIPTION
HDD1/HDD2 LED	These lights will be solid BLUE when drives are connected but inactive The lights will blink when the drives are being accessed, formatted or synchronized. They will illuminate AMBER if a drive has failed.
USB LED	This light will illuminate when a USB device is inserted into the USB Port. When there's traffic this light will blink.
USB Port	This is the USB Port. Devices like a USB Print Server, UPS or USB drive can be inserted here.
Front Latch	This latch can open and close by simply pressing it.
Power LED	This light will illuminate when this ShareCenter® is powered on.
Power Button	Press once to power on the device. To power down, press and hold the button until it begins to blink.
USB Copy / Unmount Button	Press 1~3 seconds to copy data from a USB drive to your ShareCenter®F. Press and hold 5 seconds to unmount a USB drive.

Rear Panel (Connections)

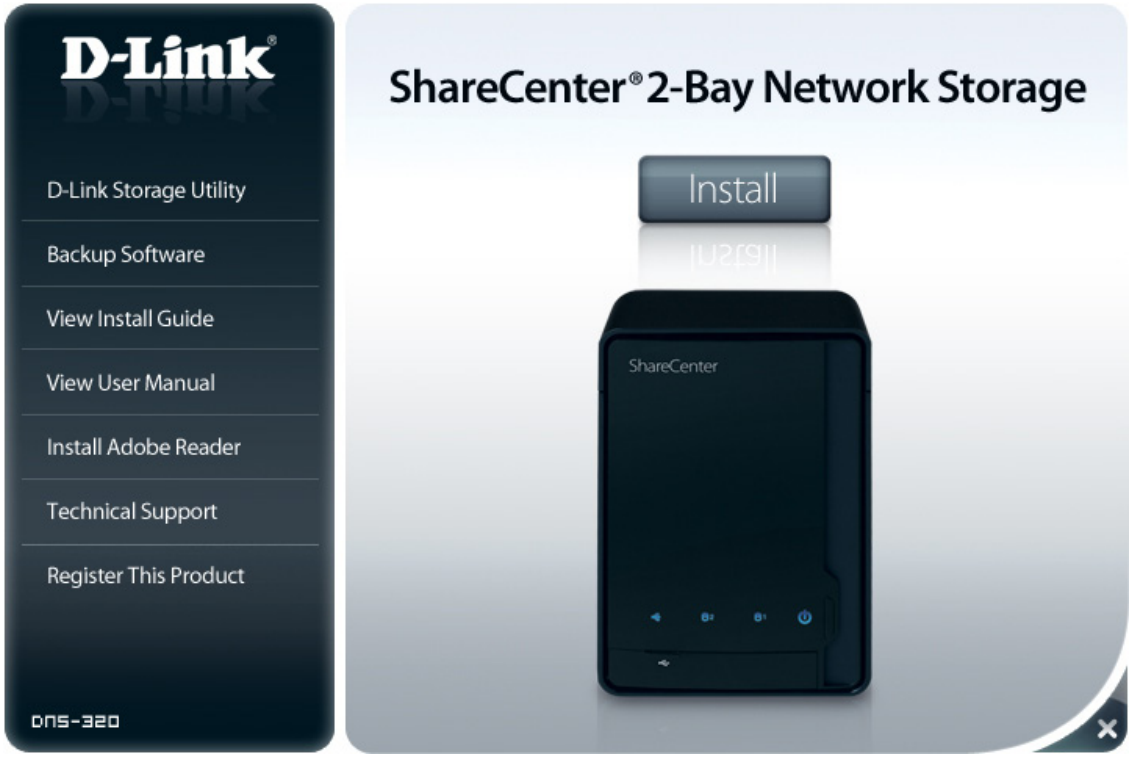


COMPONENT	DESCRIPTION
Cover Lock	This lock is used to remove the cover when unlocked. Locking it will restrict the removal of the top cover.
Cooling Fan	The cooling fan is used to cool the hard drives and features speed control. When the unit is first powered on the fans rotate at a low speed and rotate at a high speed when the temperature rises above 49 °C.
Reset Button	Press this button for more than 5 seconds to reset the unit to factory defaults.
Power Receptacle	Connect the supplied power cord to the receptacle.
Gigabit Ethernet Port	Use the Gigabit Ethernet Port to connect the device to the local network. The port is equipped with both a LAN LINK (R) and Traffic LED (L) to indicate connectivity and traffic respectively to the local LAN
Security Lock	This lock can be used to tie the ShareCenter® to the desk to prevent theft. Cables are sold separately.

Getting Started
ShareCenter Software CD

To get started with the ShareCenter® Setup Wizard, insert the supplied CD into your CD-ROM drive:

Click the **Install** button to start the ShareCenter® Setup Wizard.



Installation
Setup Wizard

The Setup wizard will walk you through the configuration of your ShareCenter® device.

Note: *The computer used to access the* ShareCenter® *web-based configuration manager must be on the same subnet as the ShareCenter. If your network is using a DHCP server, the* ShareCenter® *will automatically be in the same subnet.*

Install the Hard Drives

This step shows you how to open your ShareCenter so that you can install one or two hard drives. Click **Next** to continue.

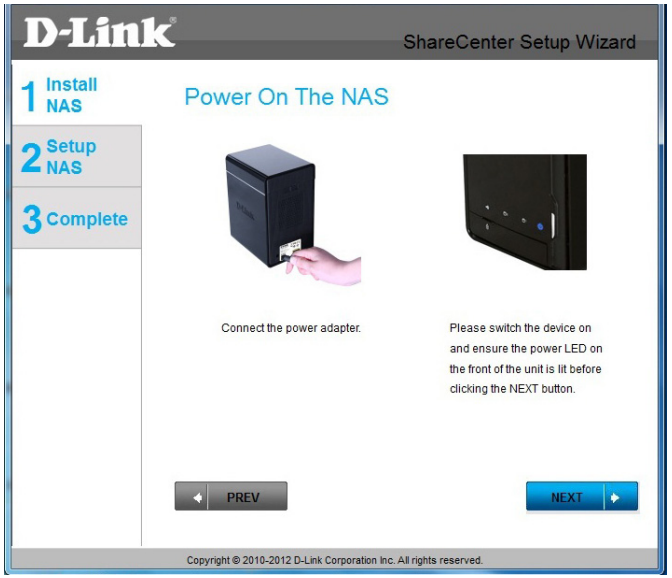
Slide either one or two hard drives into the open hard drive bays of your device. Click **Next** to continue.

Once the hard drives are installed, you can attach the top cover. Click **Next** to continue.

A standard CAT5E Ethernet cable with a RJ-45 connector is needed to connect your ShareCenter® to your network. Click **Next** to continue.

Power and Device Selection

Connect the power adapter to the power receptor on the back of the device. Press the power button located under the faceplate LEDs to turn on the device. Click **Next** to continue.



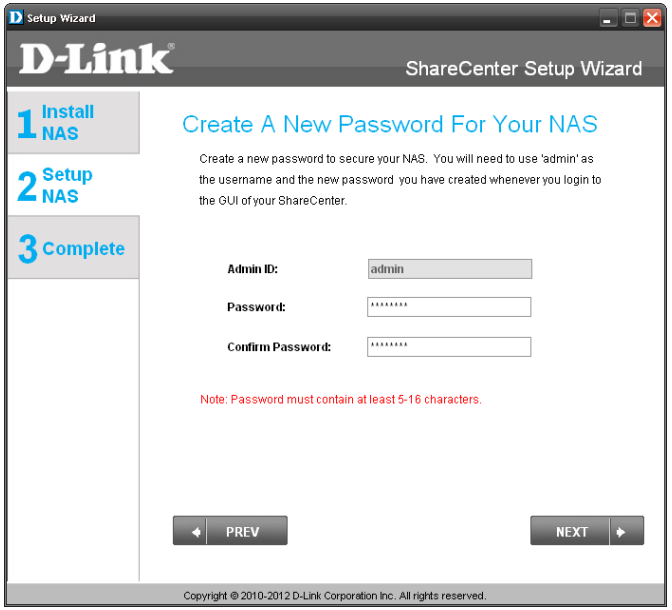
With the power on check that the Power LED is solid. If it is solid, answer **Yes** to the confirmation window otherwise select **No** and wait for the power connection to the ShareCenter. If the connection is good then check that the hard drives are installed correctly and have no other issues. Click **Next** to continue.

Note: When you select your device from the list, it will cause the LEDs to blink to confirm the device selection.

Admin password

This window requests the Admin (administrator) password. If this is the first installation of this device then the password will be blank. Click **Next** to continue.

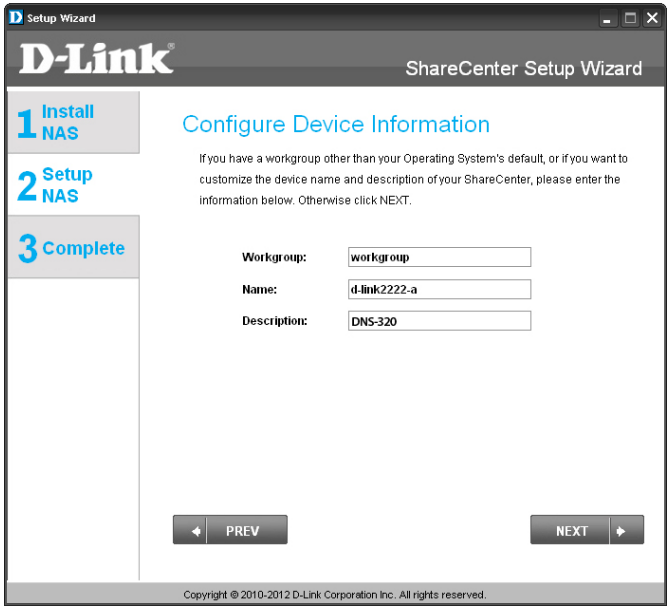
In this step you can create a new password for the Admin username. It is recommended you set a password however you may also leave the fields blank. Click **Next** to continue.



Network Setup

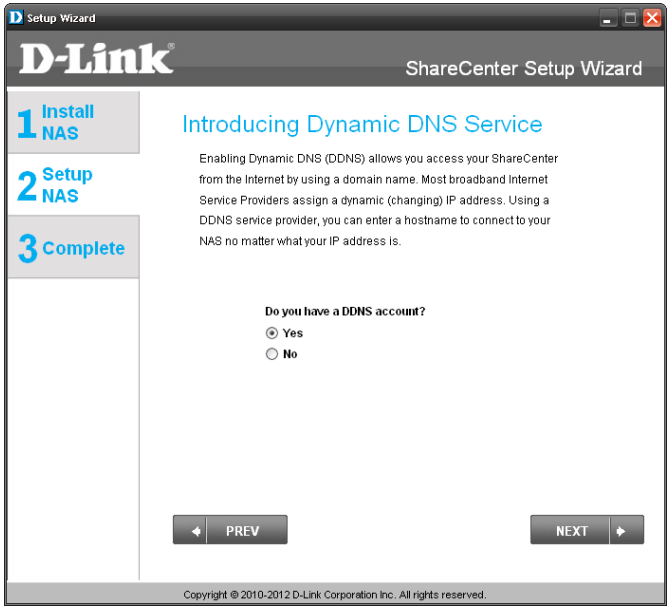
You may use either Static IP or DHCP to configure the IP network settings of the ShareCenter®. If you select Static IP then input the IP network settings. Click **Next** to continue.

If you want your ShareCenter® to be part of a Windows Workgroup network, enter the parameters requested or leave the default settings that appear initially in the window. The name will be used whenever you map one of the ShareCenter® volumes as a Network Drive. Click **Next** to continue.

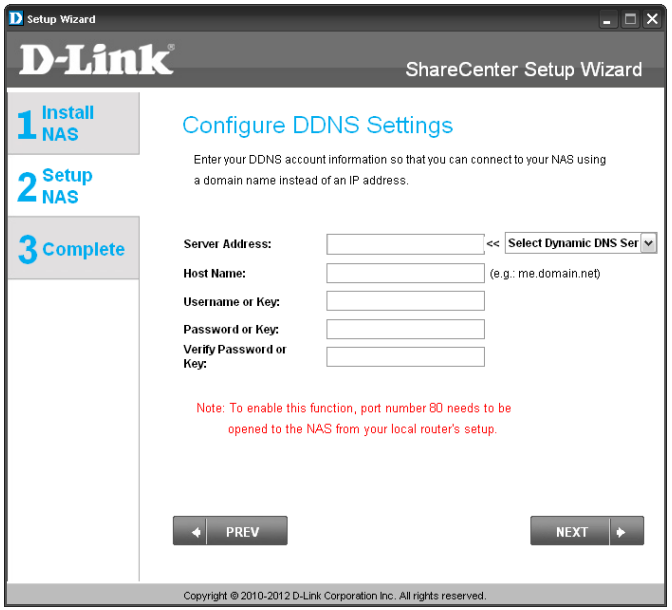


Dynamic DNS

Click on the **Yes** radio button if you already have a DDNS account to use for the ShareCenter® DDNS settings. If you do not have a DDNS account or do not want to use one, click on the **No** Radio button. Click **Next** to continue.



If you clicked **Yes**, enter the DDNS parameters requested in this window so that your ShareCenter® can be accessed by a URL over the Internet. Click **Next** to continue.

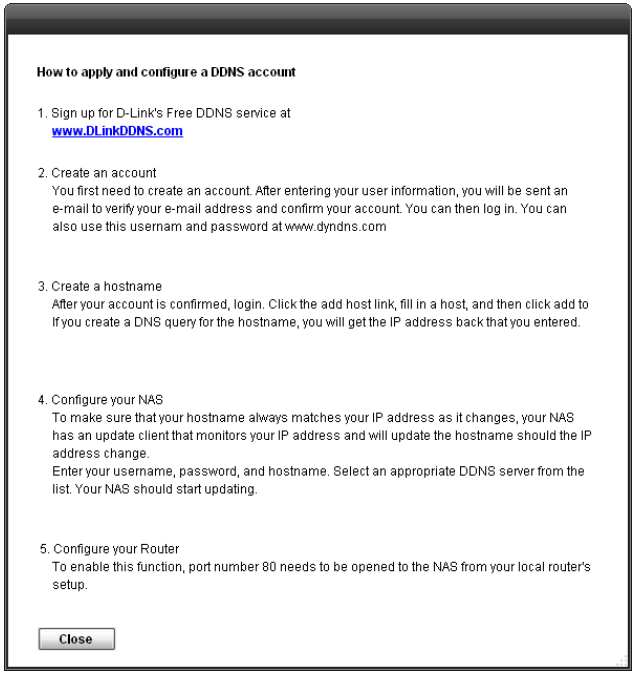


DDNS Account and System Time

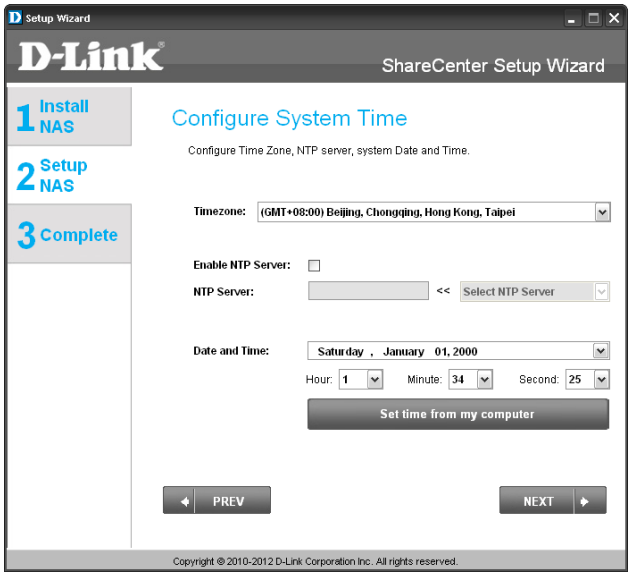
If you want a DDNS account to use with your ShareCenter®, D-Link provides a free DDNS account by clicking on the web link shown. You will need to do the following:

- Create an account with a username and password.
- Create a hostname that the DDNS service will use to track your device no matter what the Local Network WAN settings are (i.e. public IP address).
- Configure your device with the hostname and DDNS service provider details.
- Configure your router to forward port 80.

Follow the steps listed here in order to create a DDNS account and configure your LAN equipment and ShareCenter® to work with the new settings.



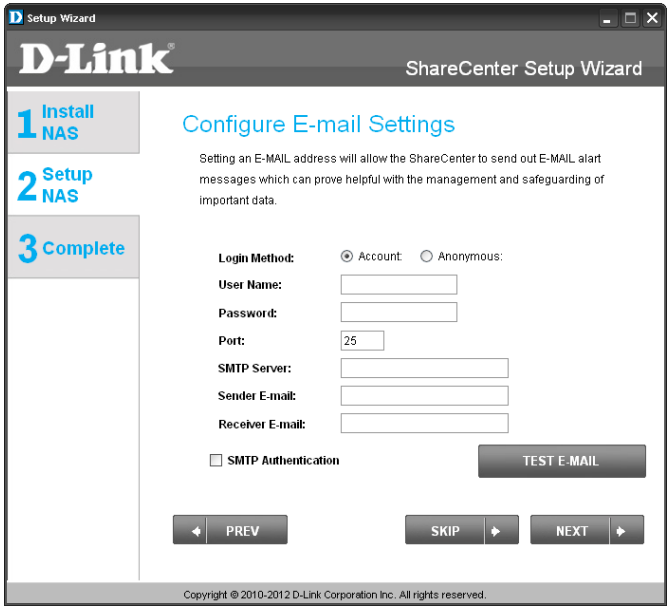
Configure the time, date and time zone settings here. Select the time zone from the drop-down menu. You can set the time and date manually, from a NTP server or from the computer's settings.



E-mail Settings and Volume Information

You can configure messages to be sent alerting you to certain operational conditions and drive status conditions to your e-mail account. These alerts can prove helpful with the management and safeguarding of important data.

Enter your e-mail information and settings and then click **Next** to continue. If you do not want to configure your e-mail settings, click **Skip** to continue.



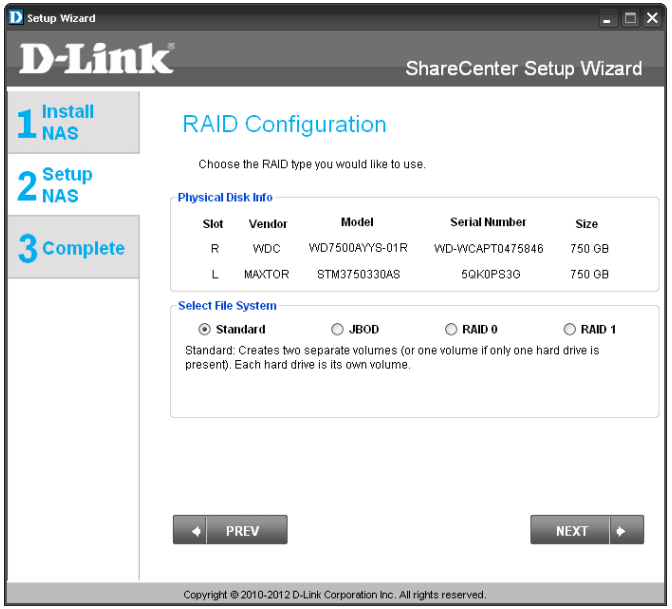
This step is informational and shows any currently configured Volumes previously setup on the ShareCenter®. Click **Next** to continue.

RAID Configuration and Drive Mapping

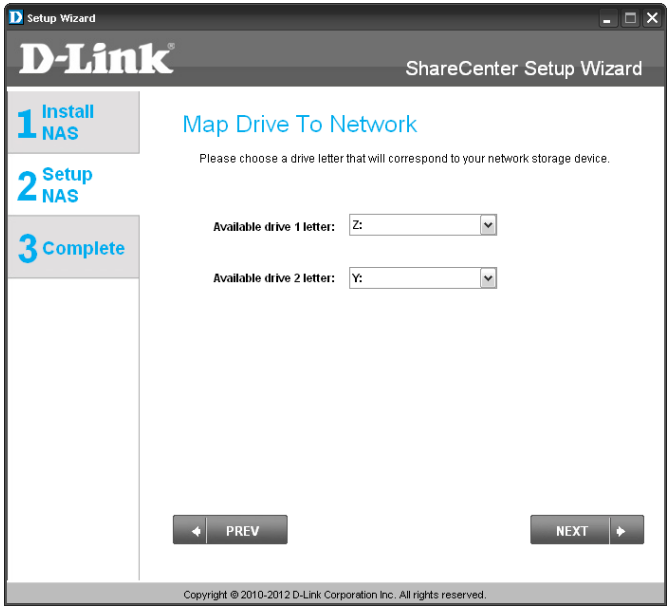
Select one of the Volume File Systems type. Clicking on each file system type radio button will give a description below.

For more information concerning the different RAID Disk Formats please refer to "What is RAID?" on page 98

Click **Next** to continue.

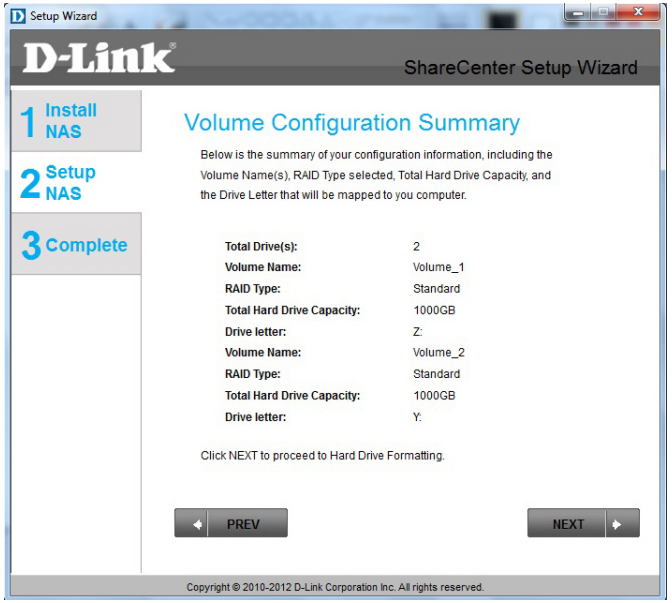


This step allows you to map the volume(s) created as network drive(s) on your computer. Click **Next** to continue.

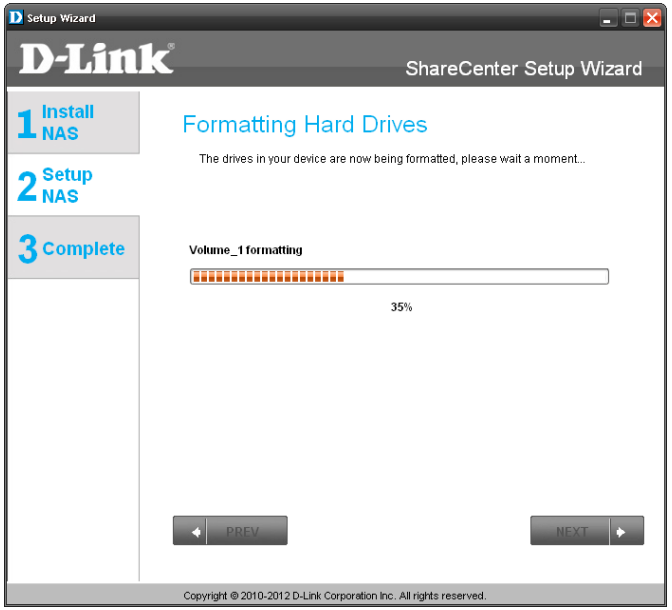


Configuration Summary and Drive Formatting

Review your volume configuration summary details here before clicking next and starting the drive format. If necessary use the **PREV** button to go back and reconfigure the RAID configuration of the volume(s). When you click **NEXT** a warning message will appear to confirm you want to format the drives as all the data on the drives will be deleted. Click on the **No** button if you are unsure.



During the hard drive formatting the wizard displays percentage complete bars.



Format Complete

The wizard will show this window if the hard drive format(s) are successful. Click **Next** to continue.

The final window of the installation wizard shows successful completion. Your device is now installed and ready for use. Your drives are network mapped from using the wizard so you will be able to access them under you *My Computer* icon.

D-Link Storage Utility

When first powered on, during the initial boot sequence, the device will wait to be assigned an IP address via DHCP. If it does not receive a DHCP assigned IP address the Auto-IP process will assign a 169.254.xxx.xxx address to the device If you want to change the IP address before logging in or are unable to connect to the ShareCenter® IP address, you can use the Storage Utility provided on the product CD to locate the device on your network and make any needed changes.

Network Storage Device: The D-Link Storage Utility displays any ShareCenter devices it detects on the network.

Refresh: Click to refresh the device list.

Configuration: Click **Configuration** to access the Web-based configuration of the ShareCenter.

LAN: Configure the LAN Settings for the ShareCenter here.

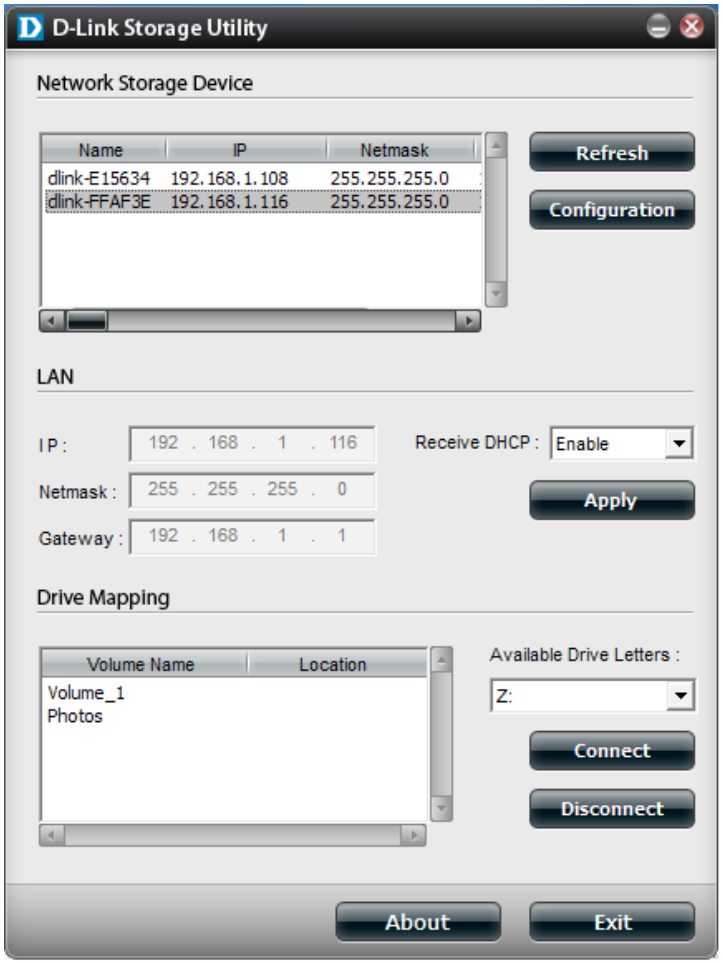
Apply: Click **Apply** to save and activate the changes to the LAN Settings.

Drive Mapping: Volumes available for mapping are displayed here.

Available Drive Letters: Select an available drive letter. Click **Connect** to map the selected volume. Click **Disconnect** to disconnect the selected mapped volume.

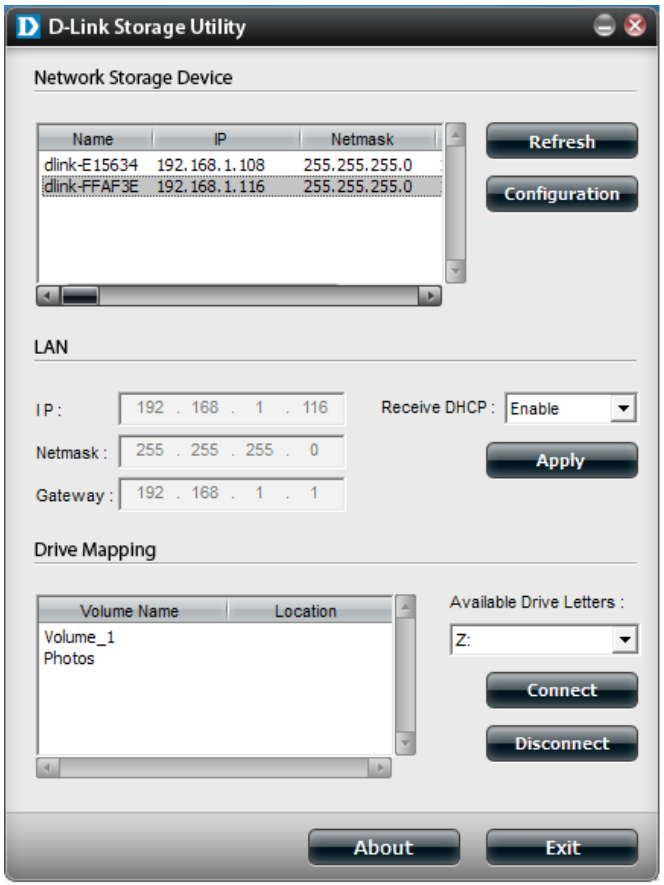
About: Click **About** to view the software version of the Easy Search Utility.

Exit: Click **Exit** to close the utility.



Select the device from the list and click the **Configuration** button. This will launch the computer's default web browser and direct it to the IP address listed for the device. Make sure the browser is not configured to use a proxy server.

Note: *The computer used to access the ShareCenter web-based configuration manager must be on the same subnet as the ShareCenter. If your network is using a DHCP server and the computer receives IP settings from the DHCP server, the ShareCenter will automatically be in the same subnet.*

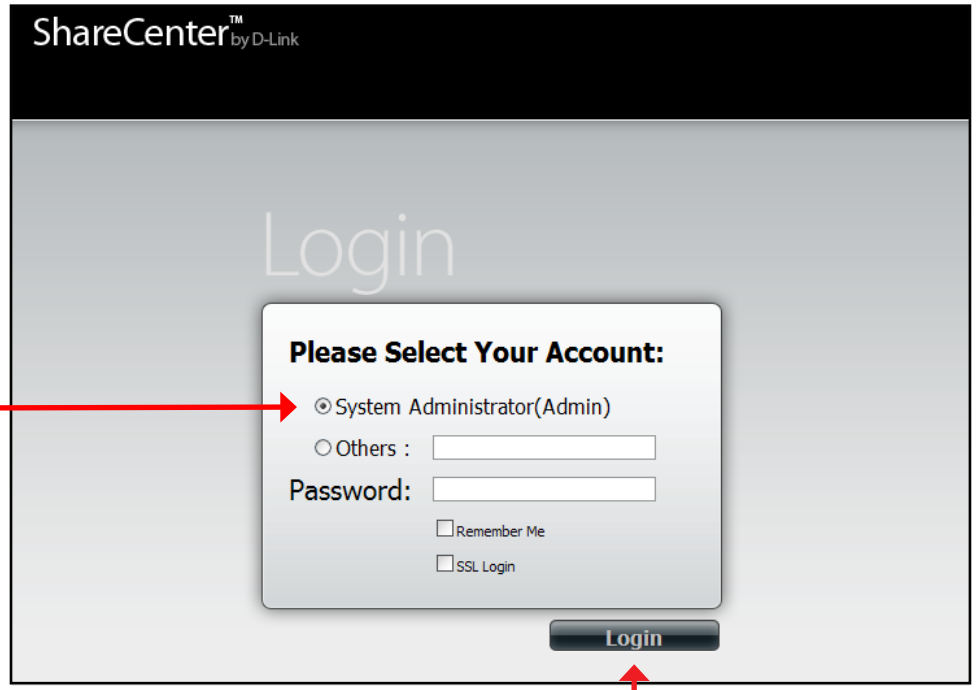


Configuration

Web UI Login

The Login screen will appear:

Select **System Administrator** and enter the password you created during the Setup Wizard.



Click **Login**

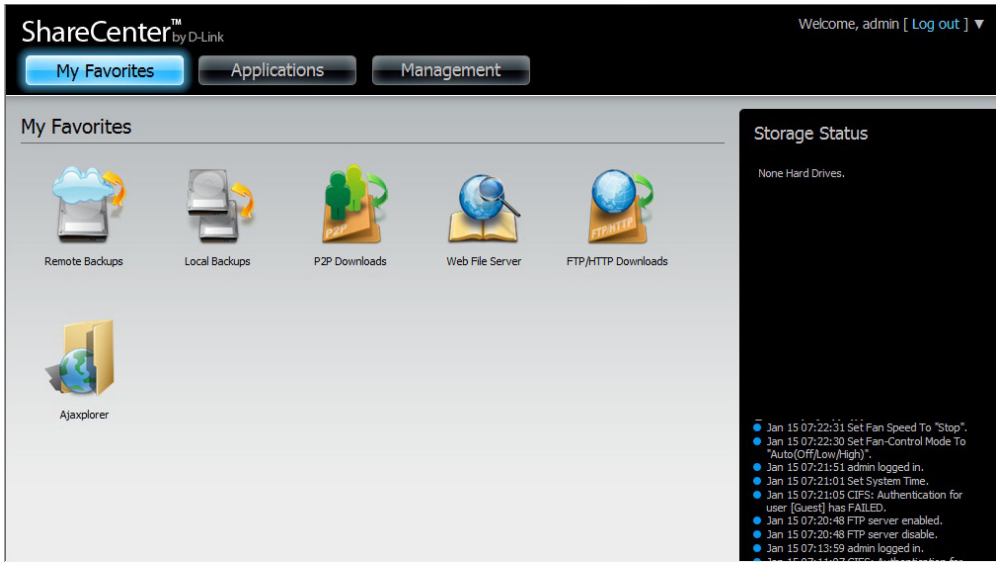
Note: *The computer, used to access the web-based configuration, manager must be on the same subnet as the ShareCenter. If your network is using a DHCP server and the computer receives IP settings from DHCP, the ShareCenter will automatically be in the same subnet.*

Web UI General Layout

If a hard disk volume has not been created, then the ShareCenter Web UI defaults to the Management tab. Once a volume is created, then the web UI defaults to the My Favorites tab. The configuration icons are located in the tabs at the top of the page. The icons available for configuration under each of the tabs include:

My Favorites - a user-configurable area where:

- Users can add customized access to preferable functions into My Favorites in order to give quick access to these functions.



Applications - Configuration for:

- **FTP/HTTP** and **P2P** Downloads.
- **Remote** and **Local** Backups.
- The **Web File Server.**
- Other applications which may be added to the page.

Management - Contains the:

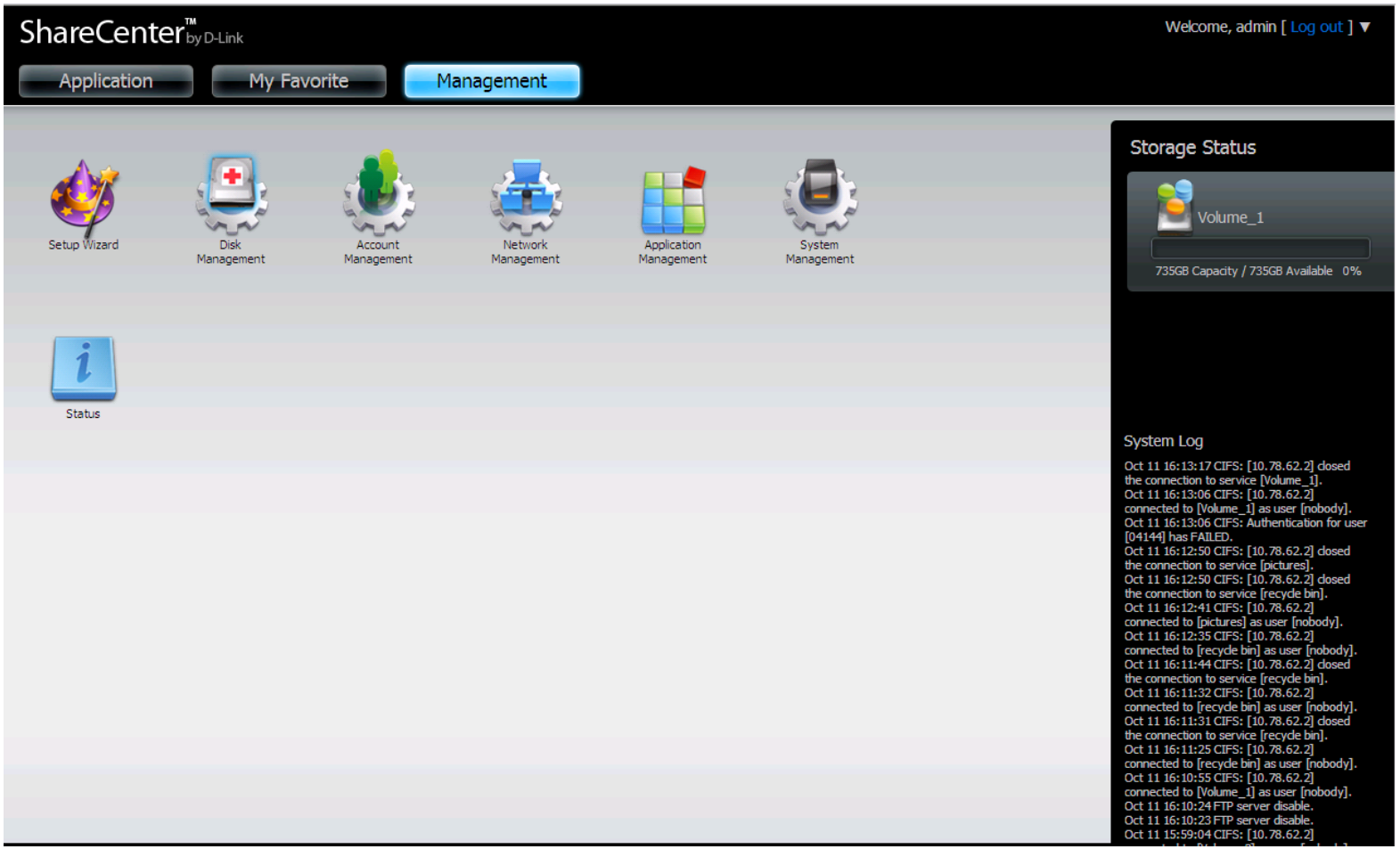
- **Setup Wizard** - Step-through settings for accounts, time and date, and connectivity.
- **Disk Management -** Configures the Volume Setup and perform Disk Diagnostics.
- **Account Management -** Configures the Admin Password, Users, Groups, Quotas and Network Share Folders.
- **Network Management -** Configures the LAN settings and Dynamic DNS.
- **Application Management** - Configures File Sharing protocols and Add-On management.
- **System Management -** Configures the Time and Date, Device, System Settings, Power Management, Email Alerts, Logs, and Firmware settings.

These icons and their configuration sub-menus will be discussed in detail in the following pages of this manual.

Note: After logging in to the ShareCenter for the first time it is recommended to add a password to the admin account.

Management

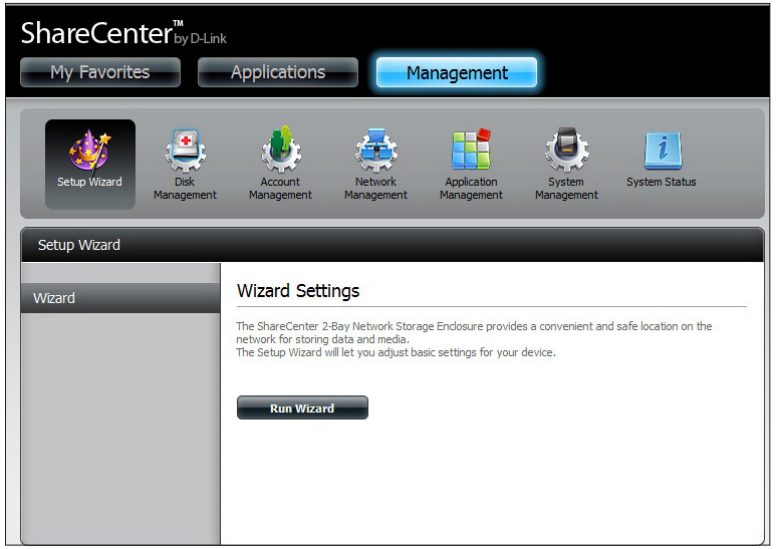
This tab contains the Setup Wizard, Disk Management, Account Management, Network Management, Application Management, System Management and Status Icons. Click each of the icons to see the submenus.



Setup Wizard (Web UI)

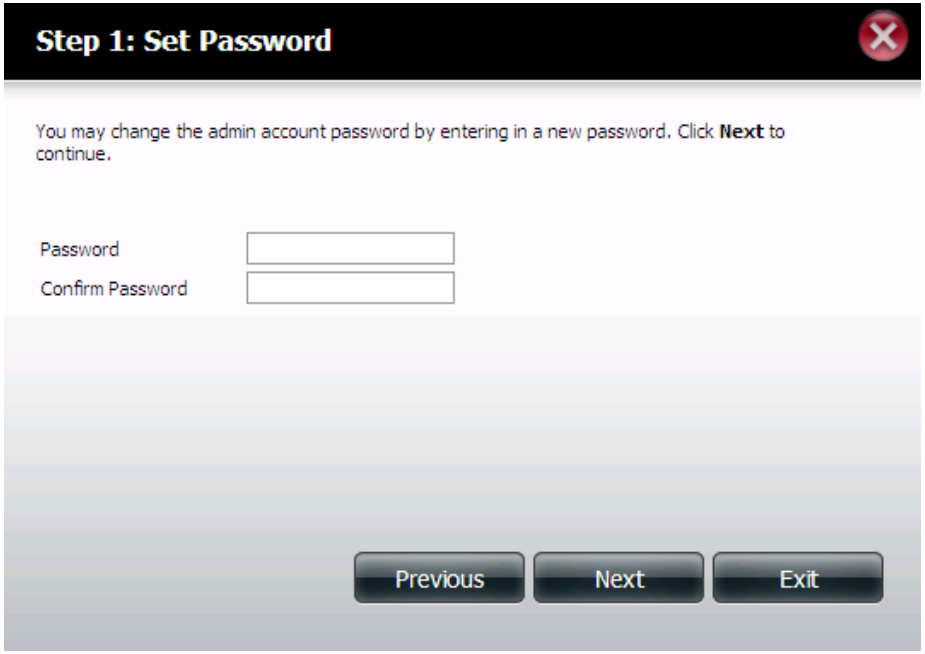
The ShareCenter® has a System Wizard that allows you to quickly configure some of the basic device settings. Click the **System Wizard** icon to start the Setup Wizard.

Click the **Run Wizard** button to start the setup wizard.

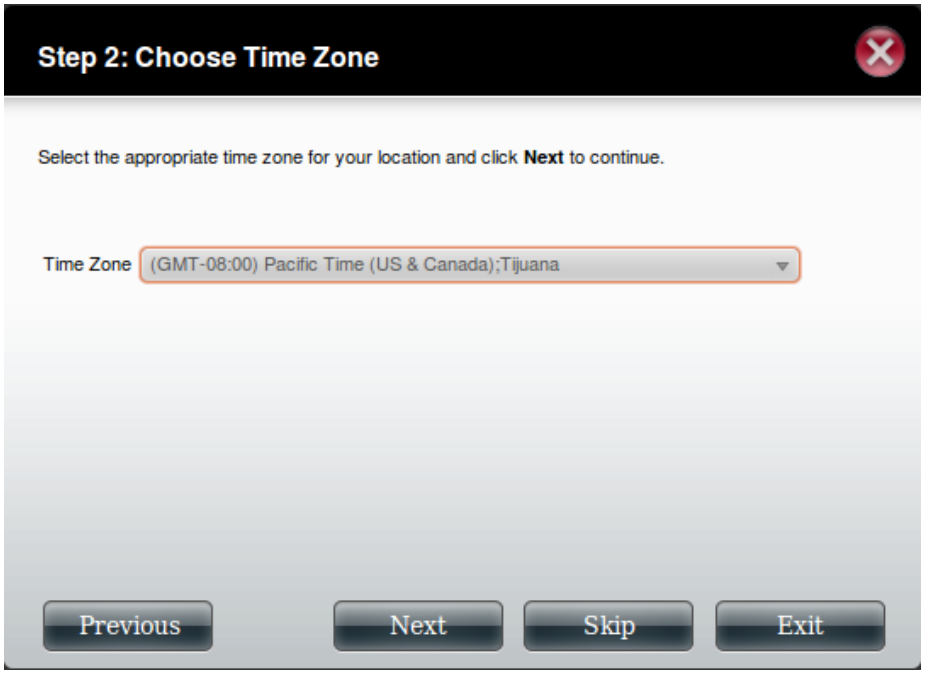


Click **Next** to continue.

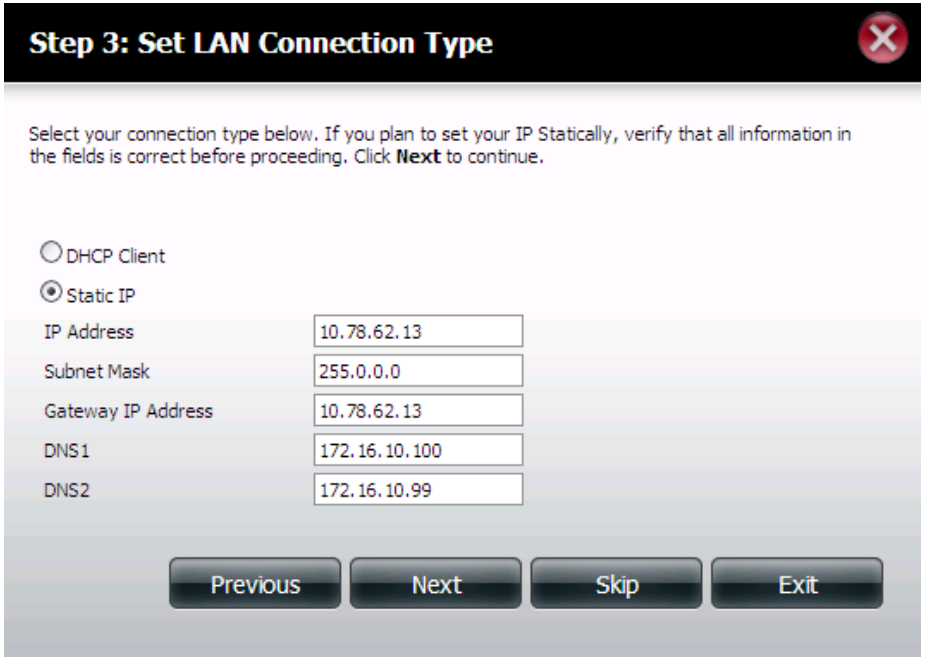
It is recommended you set an admin password here. Enter the new password and re-enter it for confirmation. Click **Next** to continue.



Set the appropriate Time Zone for your location. Click **Next** to continue.

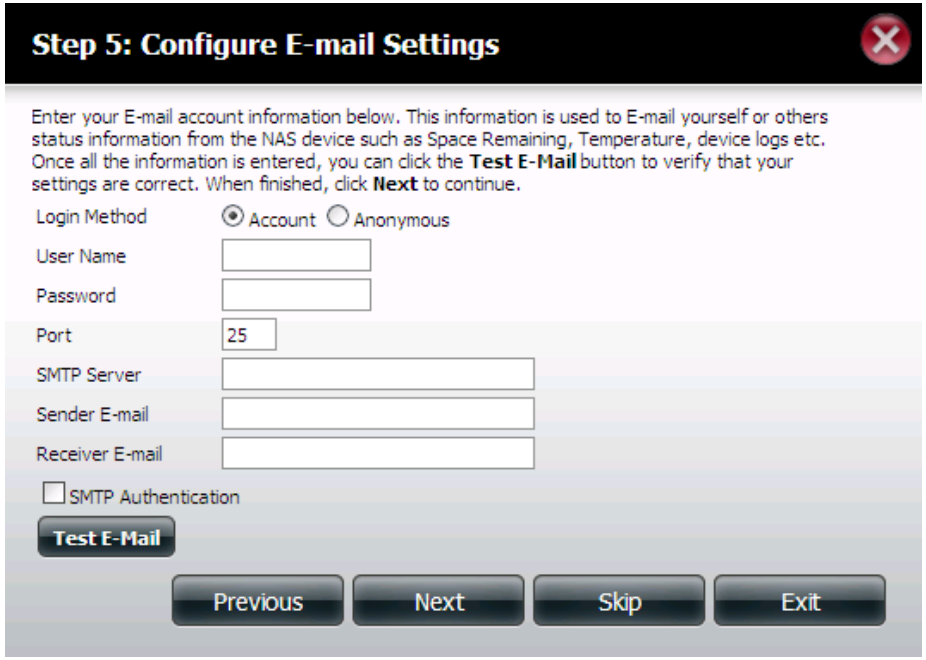


Edit or change the LAN settings. Selecting **DHCP Client** will cause the device to obtain an IP address from the local DHCP server such as a router. Selecting **Static IP** requires you to assign the IP information manually. Click **Next** to continue.



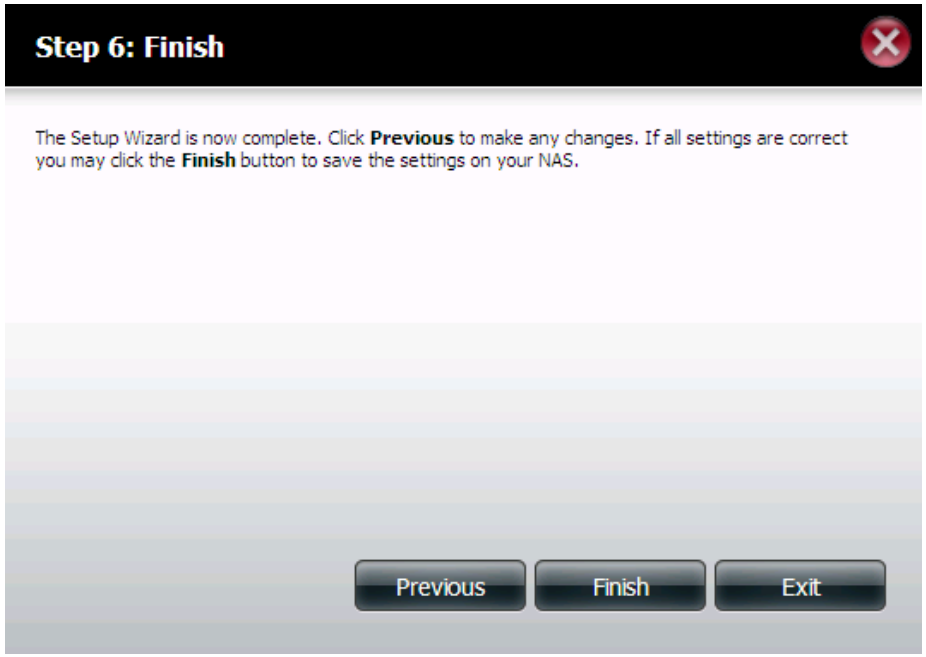
Enter your workgroup, name and description, or leave the default values and click **Next** to continue.

Select **Account** and enter your e-mail parameters in the boxes to send event alerts from the device. Click **Next** to continue.



Click **Finish** to save your settings and complete the wizard.

You may click the **Previous** button to go back and edit your settings or click **Exit** to end the wizard without saving the settings.



Disk Management

Hard Drive Configuration

To setup the Hard Drive RAID configuration of your ShareCenter®, click on the Management tab and then the Disk Management icon. Select the Hard Drive Configuration menu item on the left of the window. This menu will allow you set the RAID type and format your hard drives.

Hard Drive: Configuration Your ShareCenter® hard drive can be configured and formatted in various configurations here.

Current Raid Type: If the drives are already formatted the configuration will be displayed here.

Set RAID type and Re-Format: Click on this button to launch a wizard to allow you to select the RAID configuration and format the drives. Refer to the section titled "What is RAID?" on page 98 for more information about RAID.

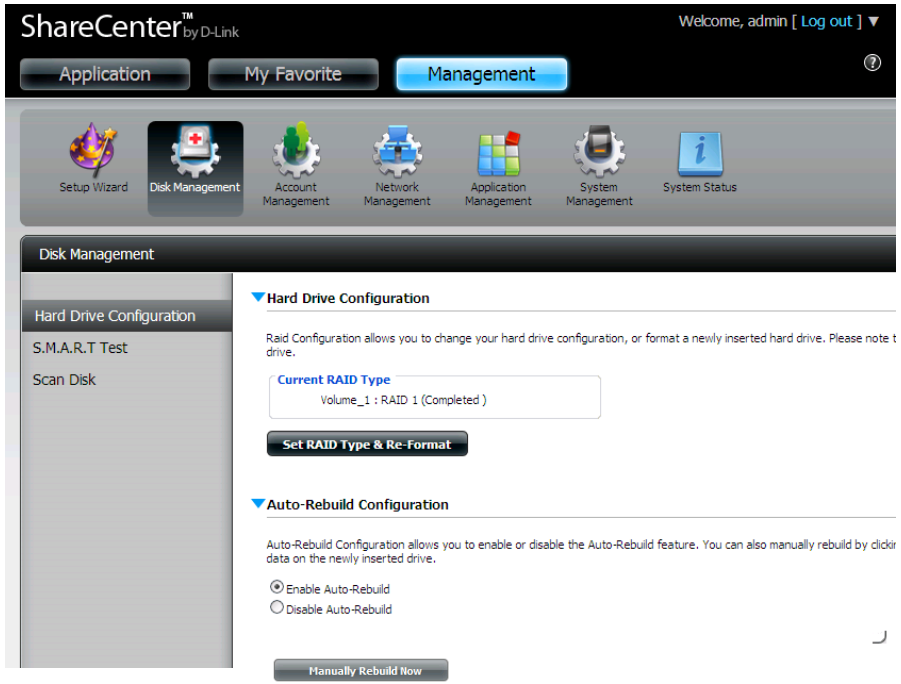
Auto-Rebuild Configuration: If you selected RAID 1 as the configuration option then set the Auto-Rebuild function here using the radio buttons.

Enable Auto-Rebuild: Enabling Auto-Rebuild will rebuild a failed RAID 1 drive when a new drive has replaced the degraded one.

Disable Auto-Rebuild: If you do not want to automatically rebuild drives after a failure when using the RAID 1 functionality then you can check this option.

Note: You can still rebuild a drive using the RAID 1 functionality however you must initiate the rebuild manually.

Manual Rebuild Now: If you have disabled Auto-Rebuild then you can use the Manual Rebuild option by clicking this button.

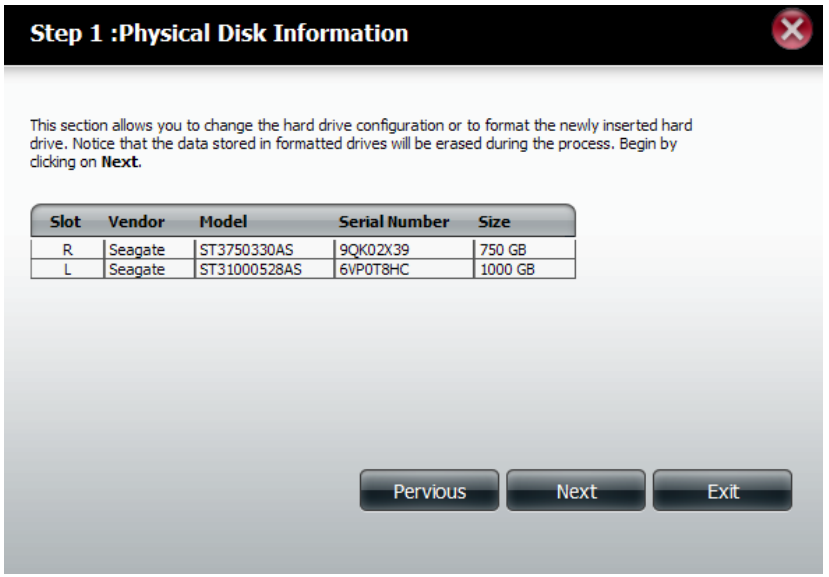


Hard Drive Configuration Wizard

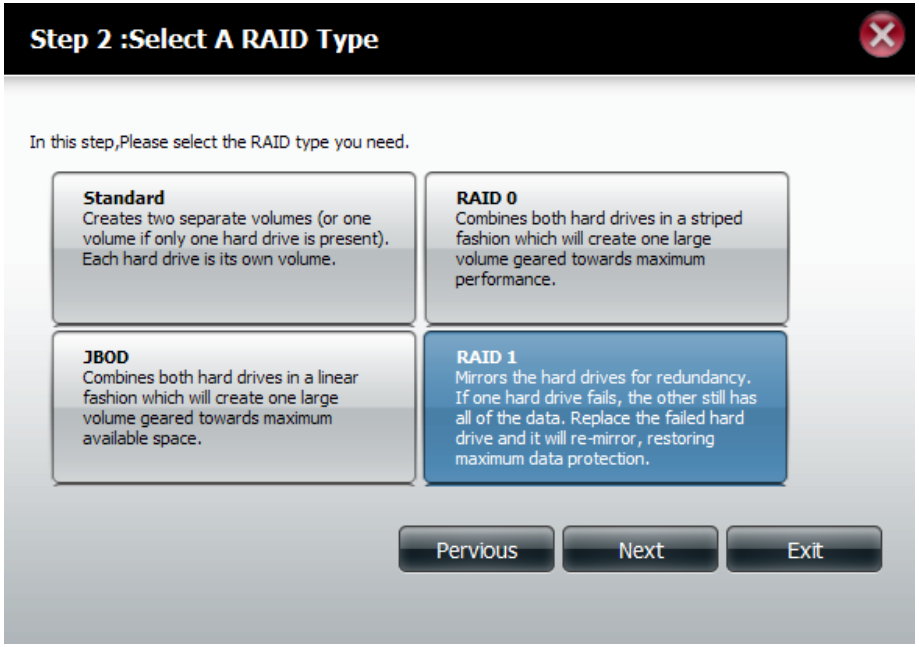
When you click the **Set RAID type and Re-Format** button in the Disk Management-Hard Drive Configuration menu, a wizard will launch allowing you to format your drives and create the RAID format. The following is an example of a RAID1 configuration:

Initially the steps of the configuration process are shown. You must decide on the RAID type you would like to format your HDDs with. Click the **Next** button to continue or click **Exit** to cancel.

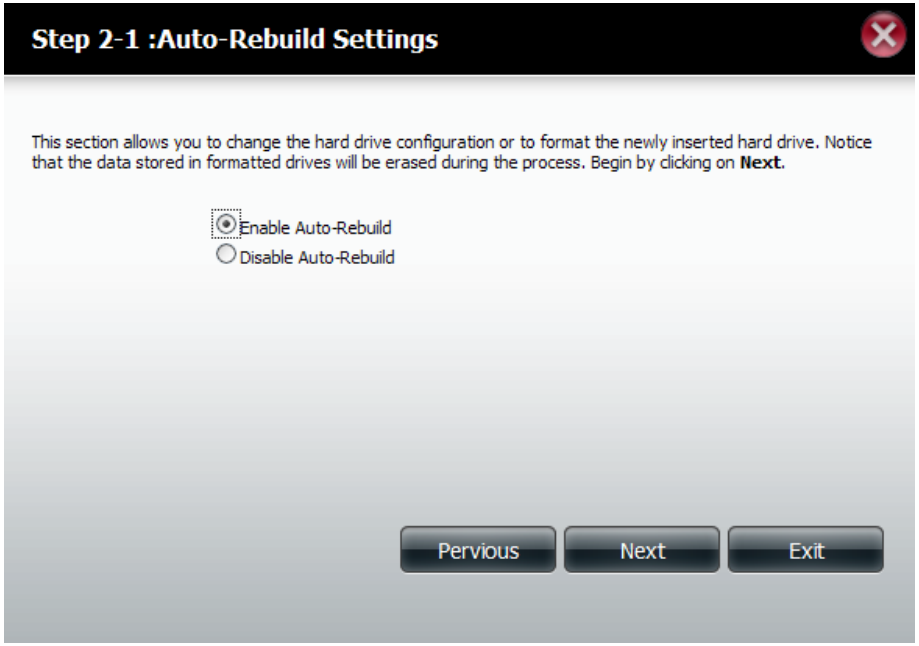
This screen displays the currently installed HDD information. Any data on the installed hard drives will be lost by the formatting. Click **Next** to continue.



Select the format desired by clicking on the RAID type box to highlight it in blue. In this example the maximum data protection option of RAID 1 is selected. Click **Next** to continue.

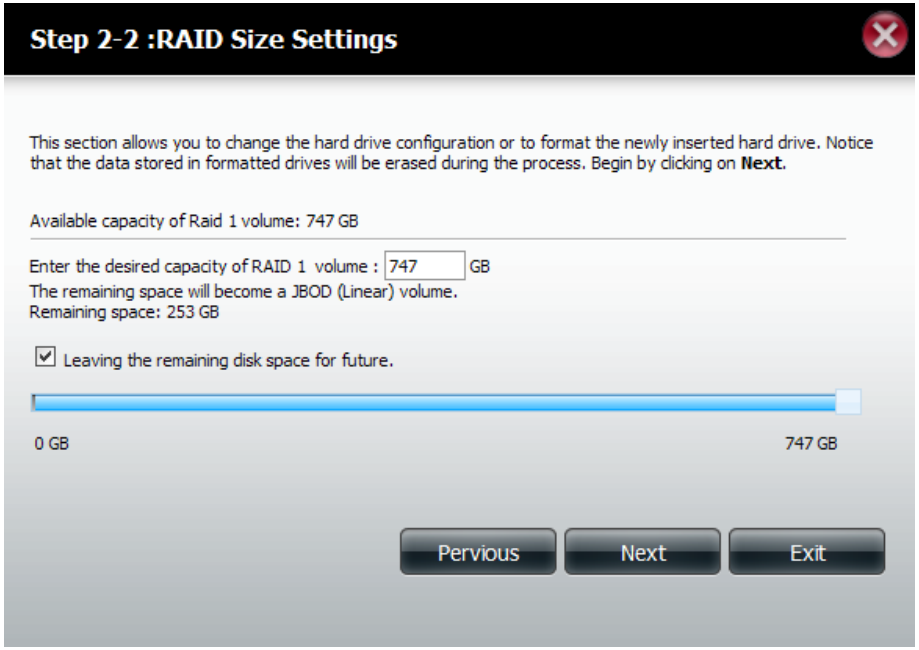


If you have selected RAID 1 then the wizard will display this step to enable or disable Auto-Rebuild. Auto-Rebuild will automatically rebuild a failed disk drive if it has been replaced with a new one. Set to disabled if you prefer to start this process manually. Click **Next** to continue.

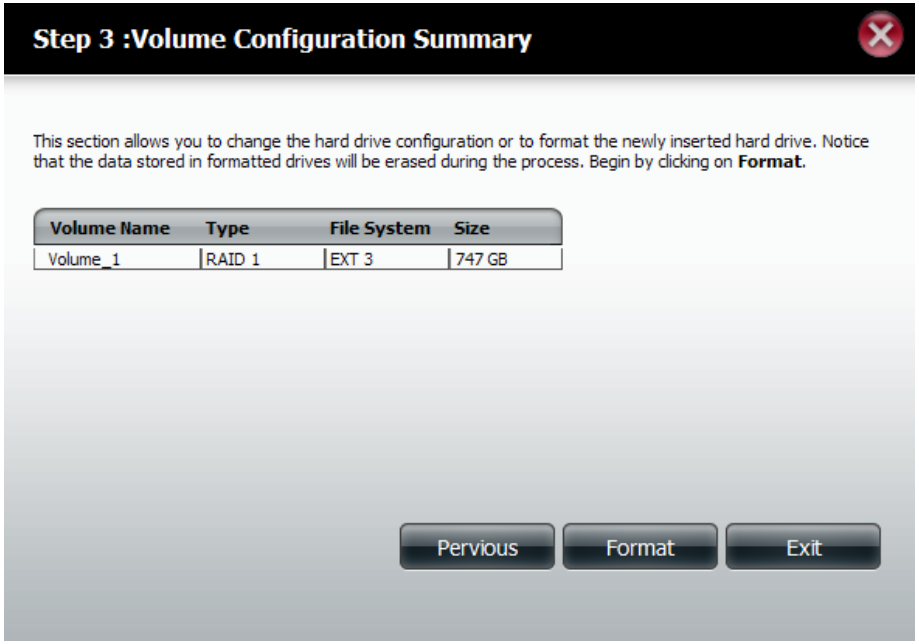


If you select a RAID 0 or 1 option then you need to determine the size of the RAID volume. Any extra space will be formatted as a JBOD volume. Click **Next** to continue.

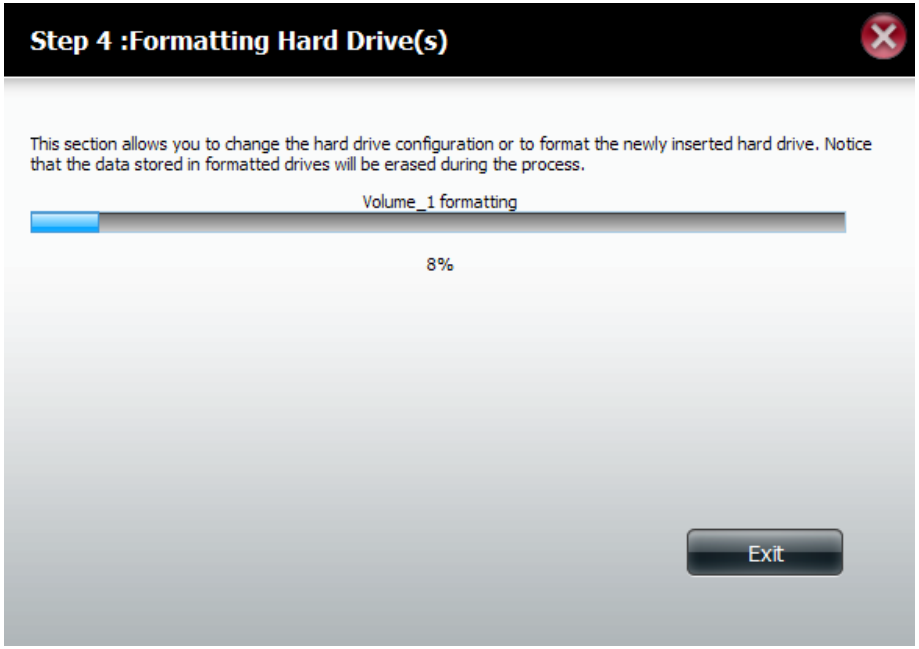
Note: If you select **Leaving the remaining disk space for future**, you can format the JBOD partition at a later time.



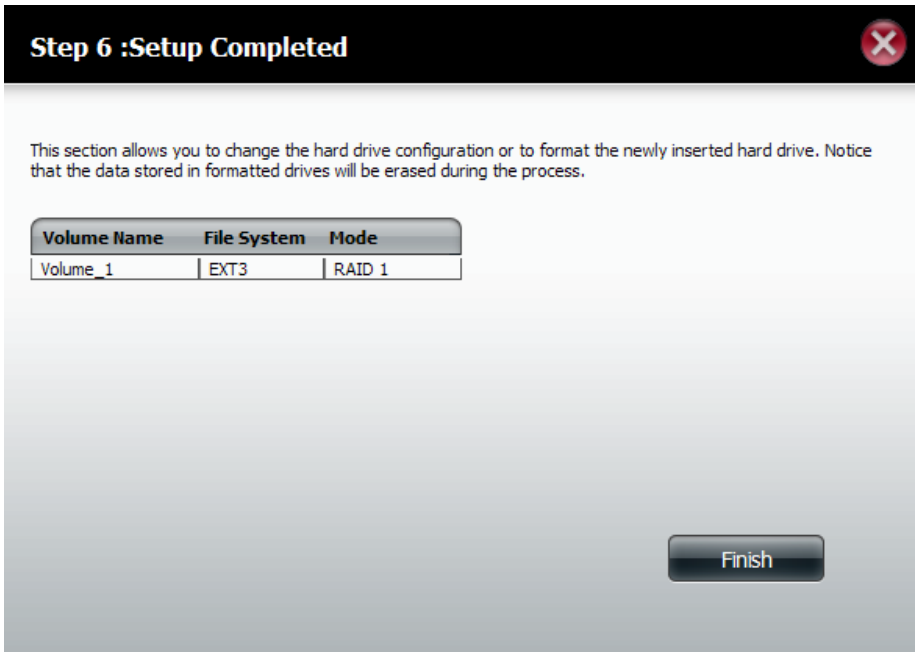
A Volume Configuration Summary is displayed. Check the table and click **Next** to format the drives. Otherwise click the **Previous** button to make changes to your configuration or click **Exit** to end the wizard.



During the formatting process a progress bar is displayed.



When the formatting is completed the wizard displays the finished Volume Configuration table. Click **Finish** to end the wizard.



S.M.A.R.T Test

S.M.A.R.T stands for "Self-Monitoring, Analysis, and Reporting Technology". This is a system on a hard drive used to monitor and report on the health of the drive. If the HD is grayed out, then it does not support S.M.A.R.T.

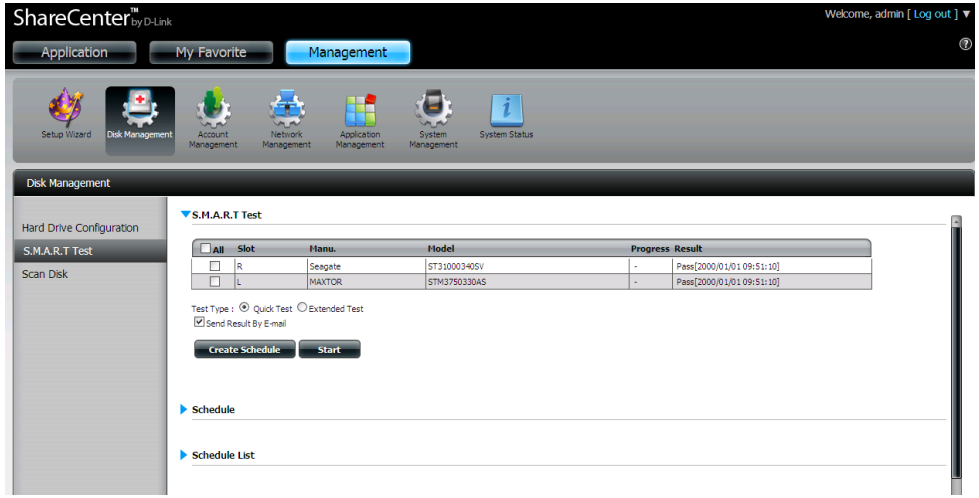
S.M.A.R.T Test: To run the S.M.A.R.T test, select the hard drive you wish to perform the S.M.A.R.T test on. Then select whether to run a Quick or Extended S.M.A.R.T test. Then click **Start** to run the test. Click the **Create Schedule** button to run the test at a pre-determined time and date.

Quick Test: Runs a quick S.M.A.R.T test. The test usually takes less than 10 minutes. This test will check the electrical, mechanical, and read performance of the hard drive. The results are displayed as Passed/Failed on the web UI and can also be sent as an e-mail alert.

Extended Test: Runs an extended S.M.A.R.T test. This test requires a lot more time to complete. However, it is a more thorough and complete test when compared to the Quick Test.

Send result by E-mail: Enable this function in order to have the results of the S.M.A.R.T test sent to you by e-mail.

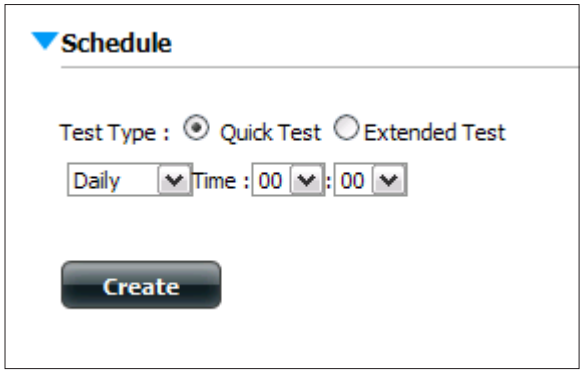
Create Schedule: Click on this button in order to create a scheduled S.M.A.R.T test. You will be able to schedule a test on a daily, weekly, and monthly basis.



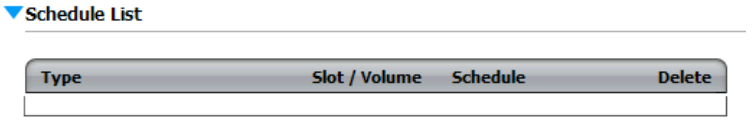
Schedule: By clicking the **Create Schedule** button the user can create a S.M.A.R.T. test schedule where this test will run automatically at the configured time.

Select the frequency (Daily, Weekly, Monthly) and the Time here. Click on the **Create** button to add a schedule.

Schedule List: In the window all the created schedule lists will be displayed.



Note: When performing a S.M.A.R.T. test, your hard drives will not be available over the network until it has completed testing.



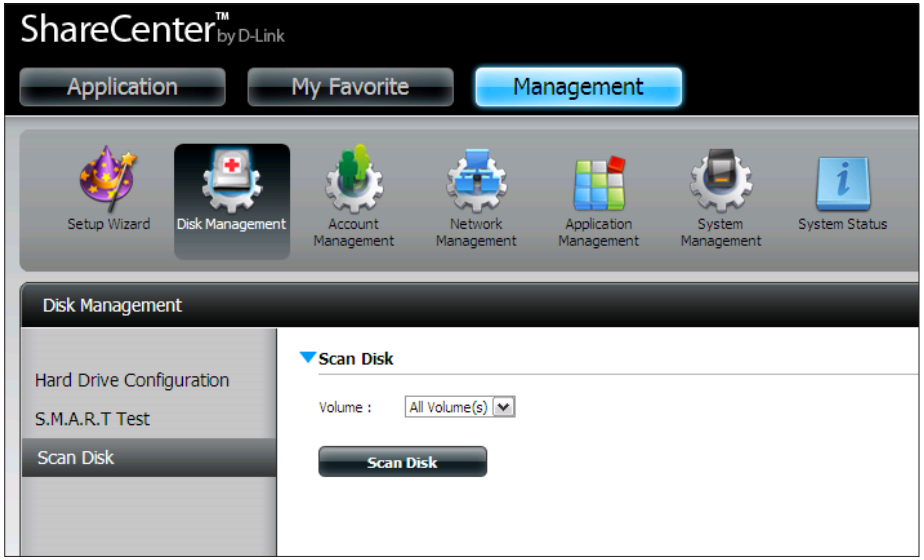
Scan Disk

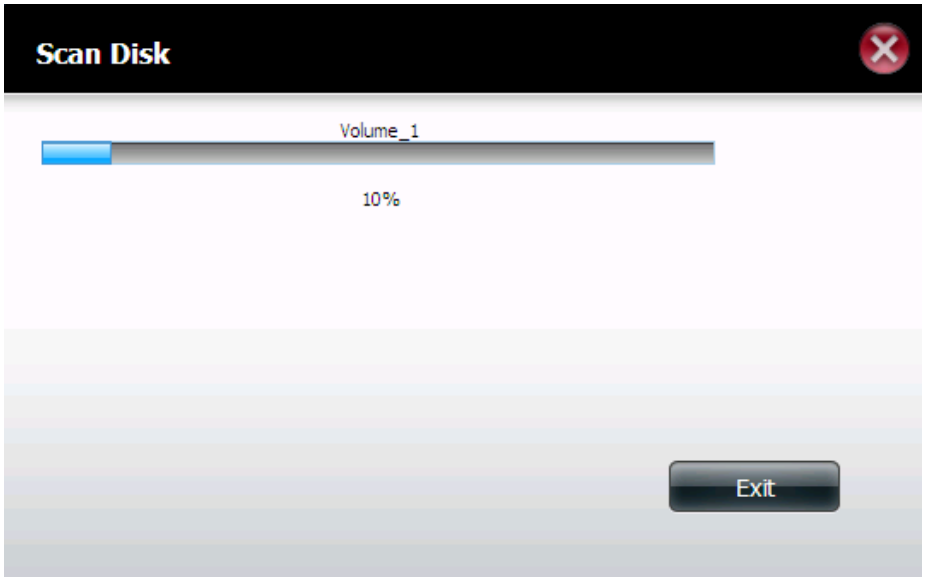
Scan disk provides a method to test the disk's file system in your ShareCenter.

Scan Disk: Scan Disk will scan your disks file system for errors and/or corruption. After completion, the test results will show Success or Failure. Click on the **Scan Disk** button to start the test. If the test fails you can try reformatting the drive and test again. Otherwise you will need 3rd party disk troubleshooting tools.

Volume: Use the drop-down menu to select the disk volume that you want to run the **Scan Disk** test on.

Scan Disk Progress Window: If you have started a Scan Disk test then a window with a progress bar will appear to monitor the test. Click the **Exit** button to abort the test if required or once the test has run 100 percent.





Account Management

Users / Groups

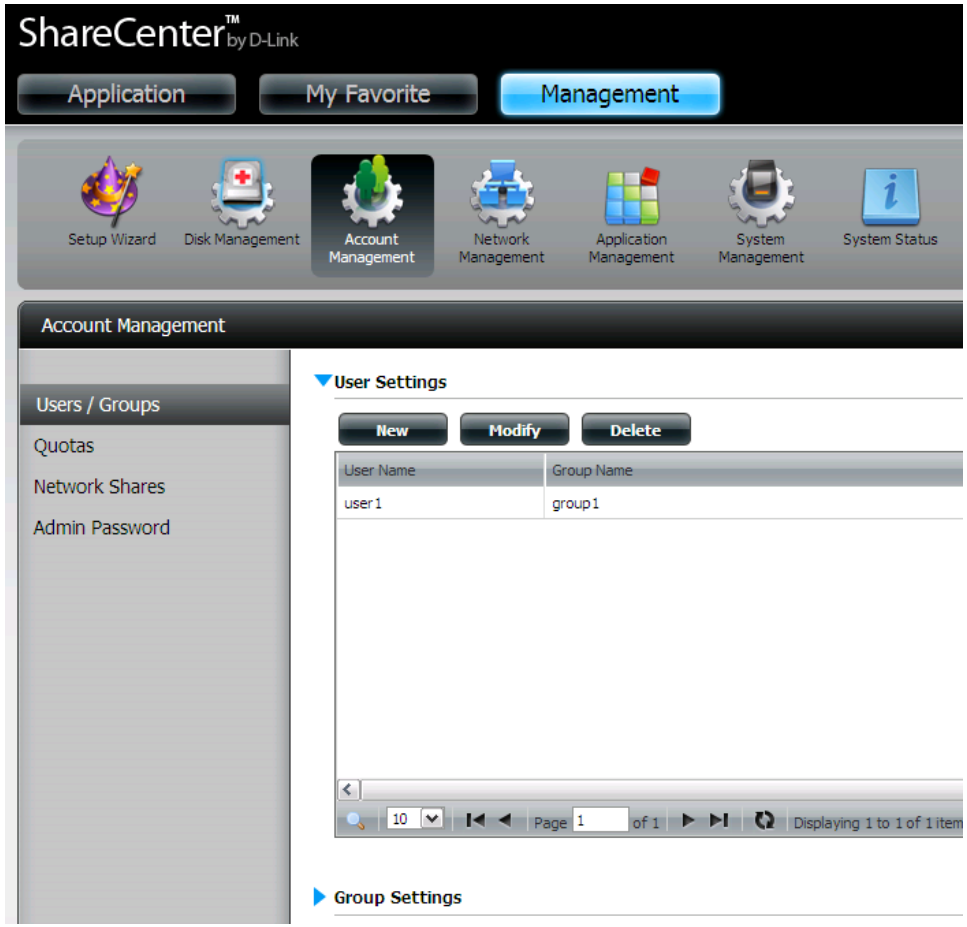
The Users / Groups menu is used to create and manage user and group accounts. Up to 256 users and 32 groups can be created. By default, all users have read and write access to all folders but access rules can be created in the Network Shares menu.

User Settings: Your hard drives can be configured and formatted in various RAID configurations here.

New: Click this button to launch a wizard that will walk you through adding a new user configuration.

Modify: Click on an existing user in the table so that it is highlighted in red and then click the **Modify** button to change the configuration of an existing user.

Delete: Click on an existing user in the table so that it is highlighted in red and then click the **Delete** button to remove a user from the configuration.



Adding New Users Wizard

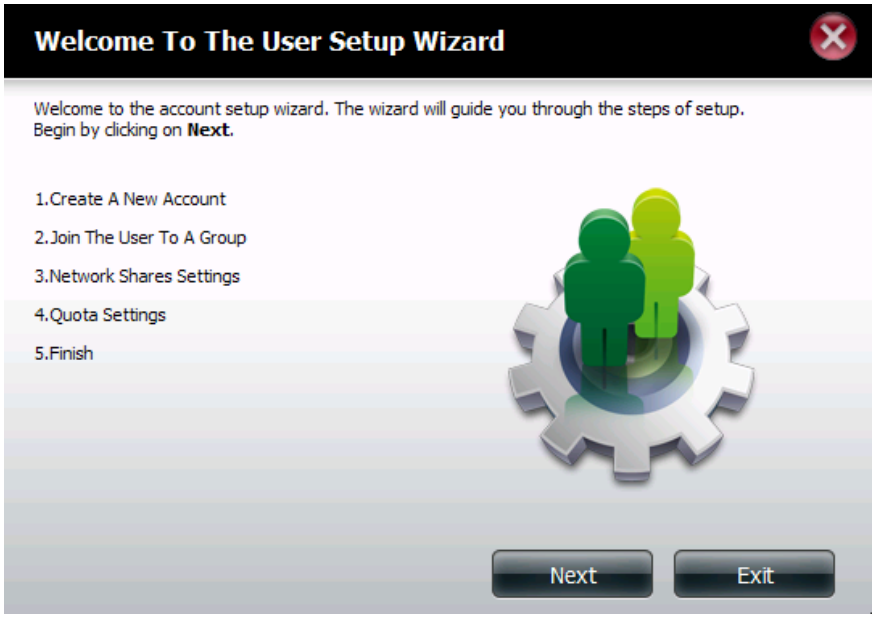
The following section will describe how to add a new user on this device. To add a user click on the **New** button. A easy to configure wizard will be launched and look like the following:

This window welcomes the user to the setup wizard for adding or modifying a user. This wizard will guide the user through the steps of setup.

In this wizard the user will be able to:

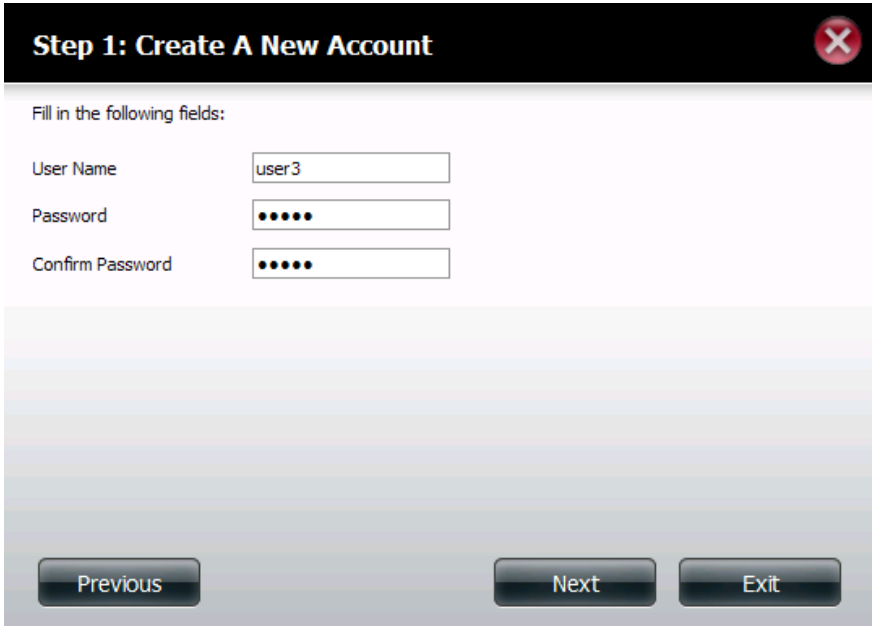
1) Create a new user account.
2) Join a group.
3) Configure the appropriate network shares settings.
4) Configure the user quota.
5) View a summary of the configuration before completing the addition.

Click on the **Next** button to continue.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



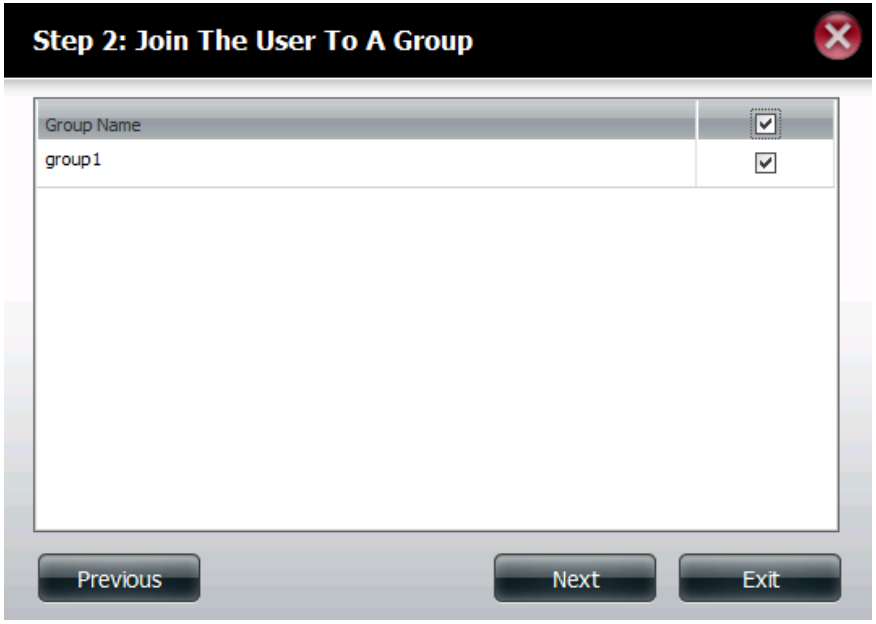
Step 1: Here you can enter the User Name and Password for the new user account. The password needs to be confirmed by re-entering the password in the Confirm Password field.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



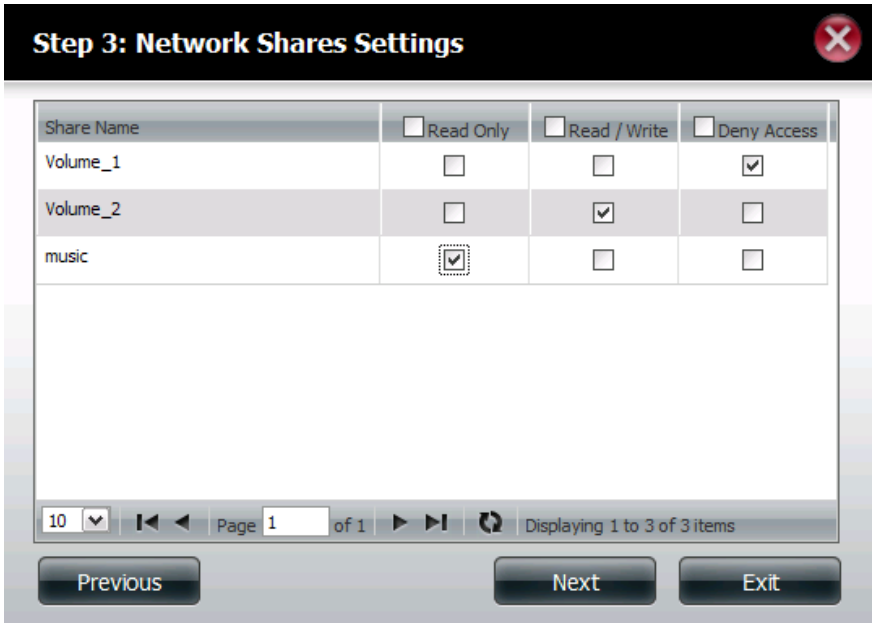
Step 2: Here you can add this user account to a group. Select the appropriate Group Name by clicking the check box.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 3: Here the user can configure the appropriate Network Access settings for the user by simply selecting one of the following options: **Read Only**, **Read/Write** or **Deny Access**.

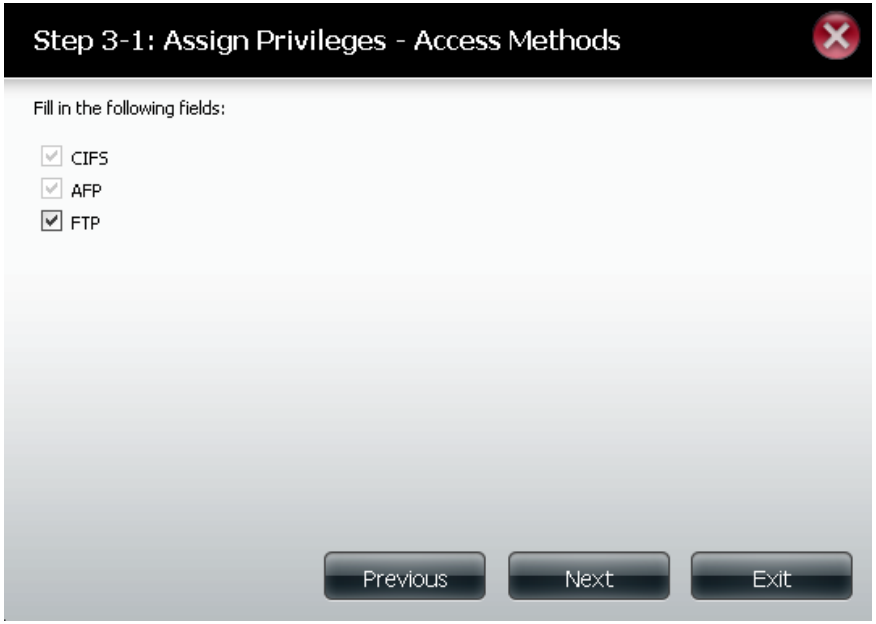
Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 3-1: Here the user can configure the application privileges assigned to this user. Select FTP. CIFs and AFP is set as default.

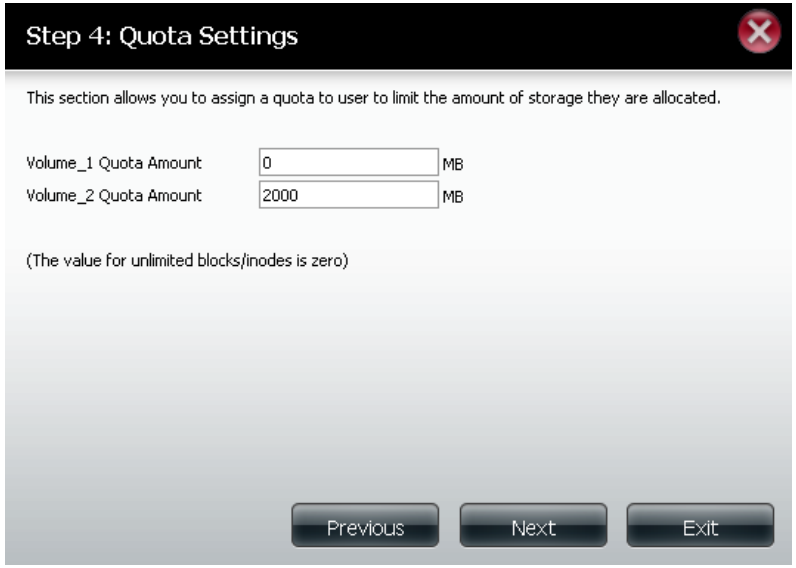
- **CIFS** is short for Common Internet File System.
- **AFP** is short for Apple Filing Protocol.
- **FTP** is short for File Transfer Protocol.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 4: Here you can configure the Quotas settings for the user account. Enter the quota amount in the block(s) indicated in Megabytes. By entering 0Mb the quota will be set to unlimited.

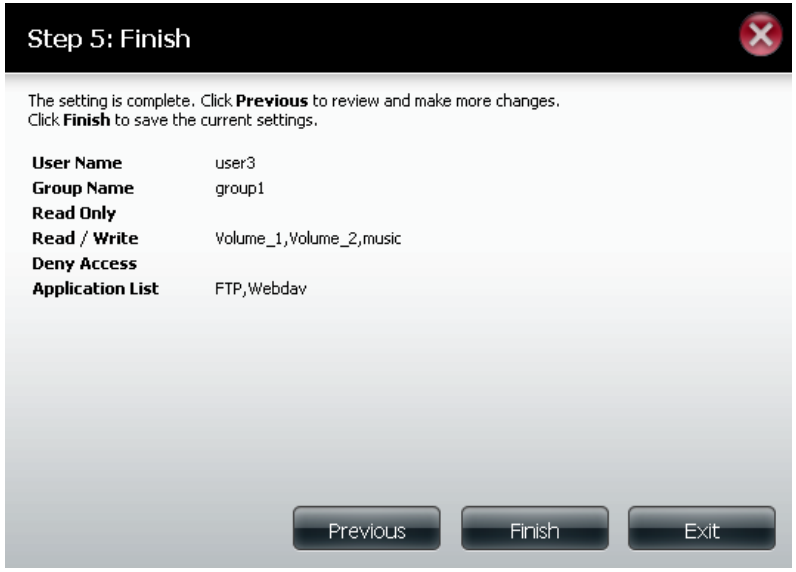
Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 5: Here you can confirm to create the new account.

Click on the **Previous** button to return to the previous window.
Click on the **Finish** button to accept the change and complete the wizard.
Click on the **Exit** button to discard the changes made and return to the User/Group window.

After the new account has been created, a window will appear that states the account was created successfully. Click on the **OK** button to continue.



Step 6: A final message appears indicating the user is successfully added to the ShareCenter configuration..

Adding New Groups Wizard

The following section will describe how to add a new group on this device. To add a group click on the **New** button. A wizard will be launched:

This window welcomes the user to the setup wizard for adding or modifying a group. This wizard will guide the user through the steps of setup.

In this wizard the user will be able to:

1) Create a new group.
2) Add a user to a group.
3) Configure the appropriate network shares settings.
4) Configure the quota settings.
5) View a summary of the configuration before completing the addition.

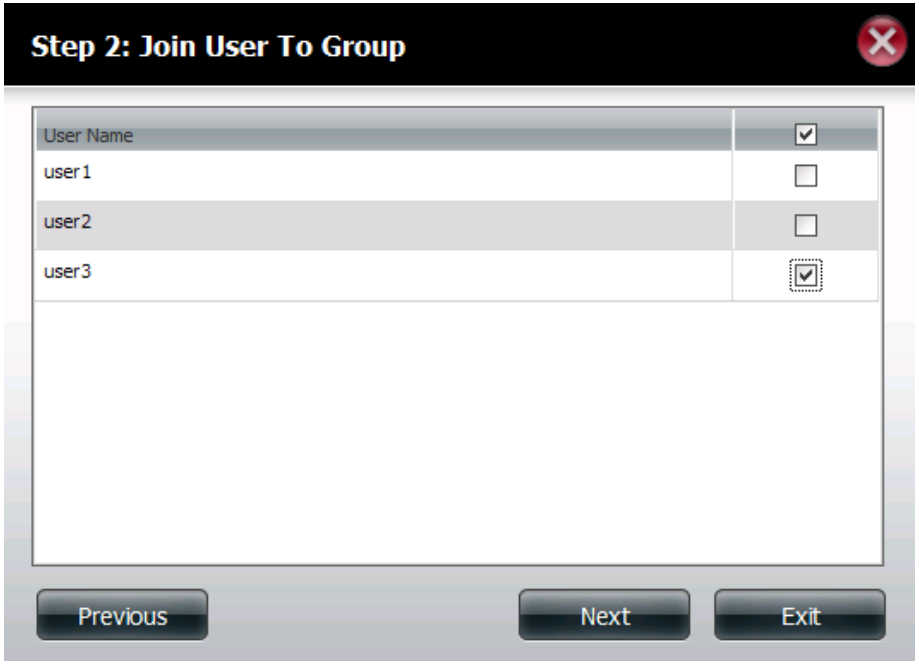
Click on the **Next** button to continue.
Click on the **Exit** button to discard the changes made and return to the User/Group window.

Step 1: Enter the name for your new group.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.

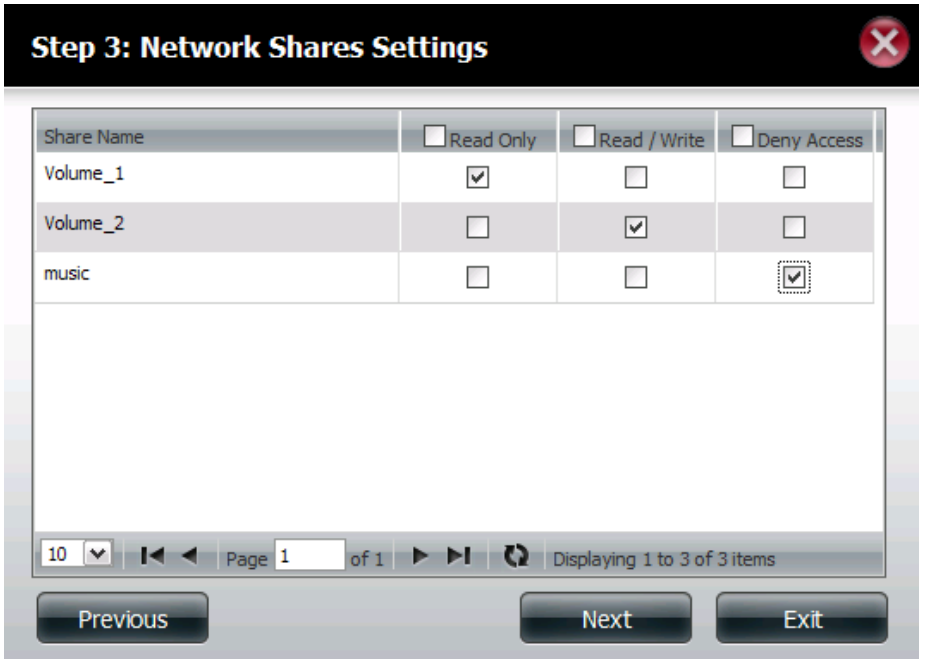
Step 2: Select the users you would like to add to your new group by checking the box.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 3: Assign the appropriate Network Access settings for this group by simply clicking one of the following options: **Read Only**, **Read Write** or **Deny Access**.

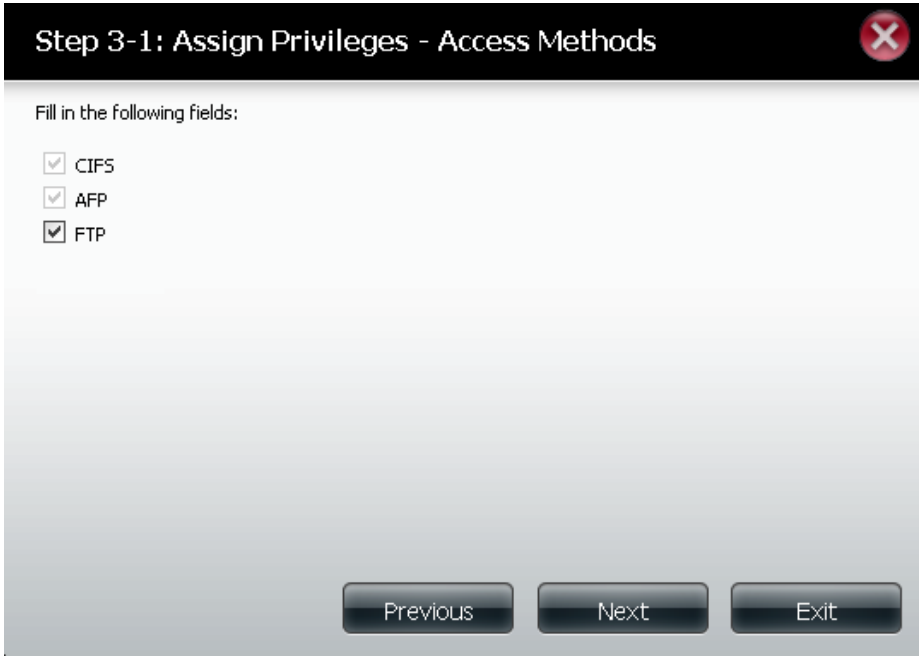
Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 3-1: Select the application privileges assigned to this group. Options to select are FTP. CIFS and AFP is set as default.

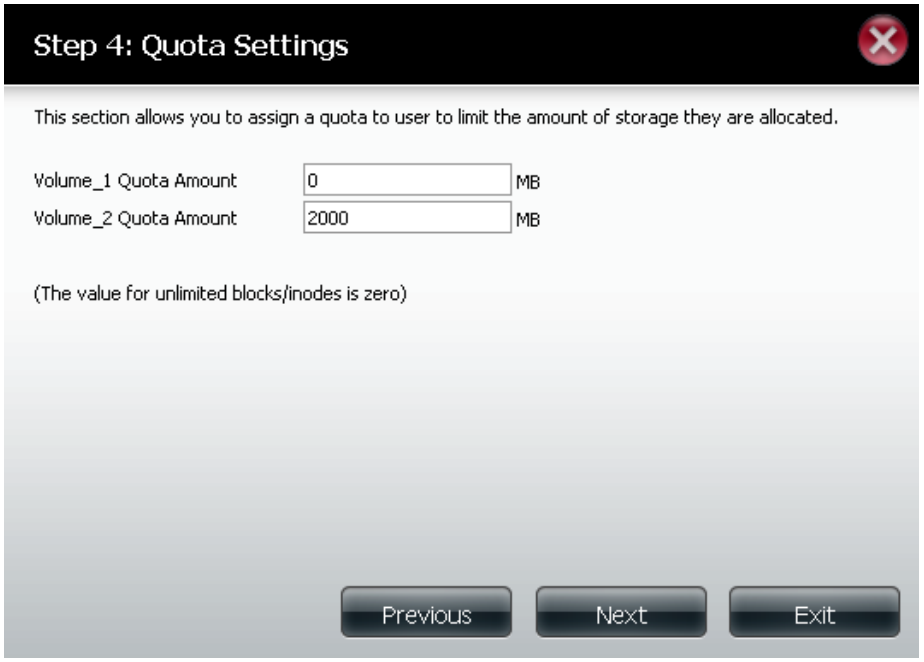
- **CIFS** is short for Common Internet File System.
- **AFP** is short for Apple Filing Protocol.
- **FTP** is short for File Transfer Protocol.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 4: Configure the Quotas settings for this group. Enter the quota amount in the block indicated in Megabytes. By entering 0Mb the quota will be set to unlimited.

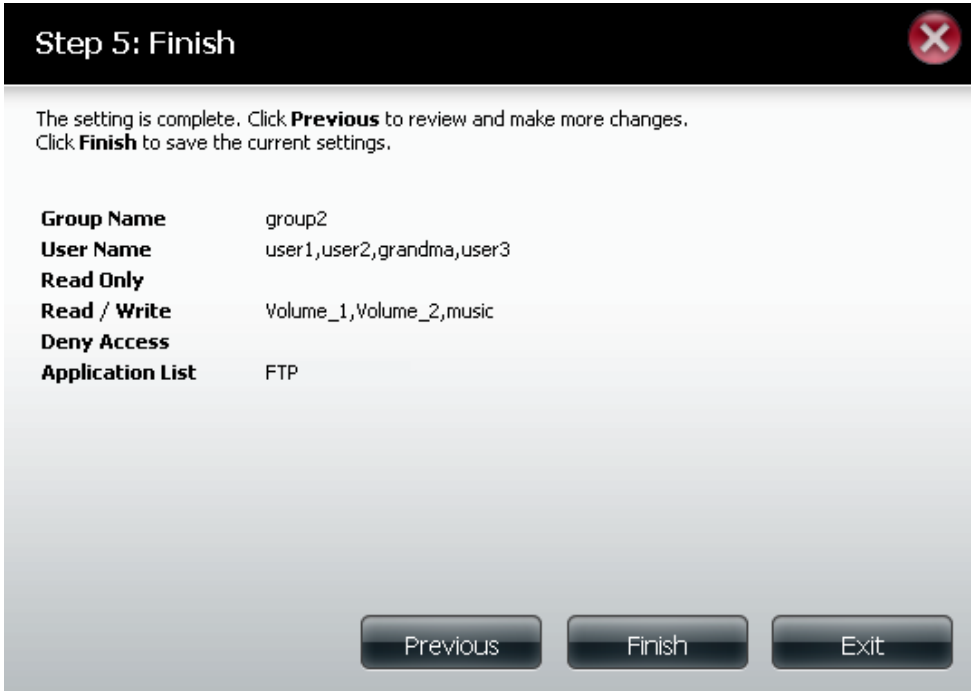
Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the User/Group window.



Step 5: Verify the settings and click **Finish**.

Click on the **Previous** button to return to the previous window.
Click on the **Finish** button to accept the change and completed the wizard.
Click on the **Exit** button to discard the changes made and return to the User/Group window.

After the new group has been created, a window will appear that states the group was created successfully. Click on the **OK** button to continue.

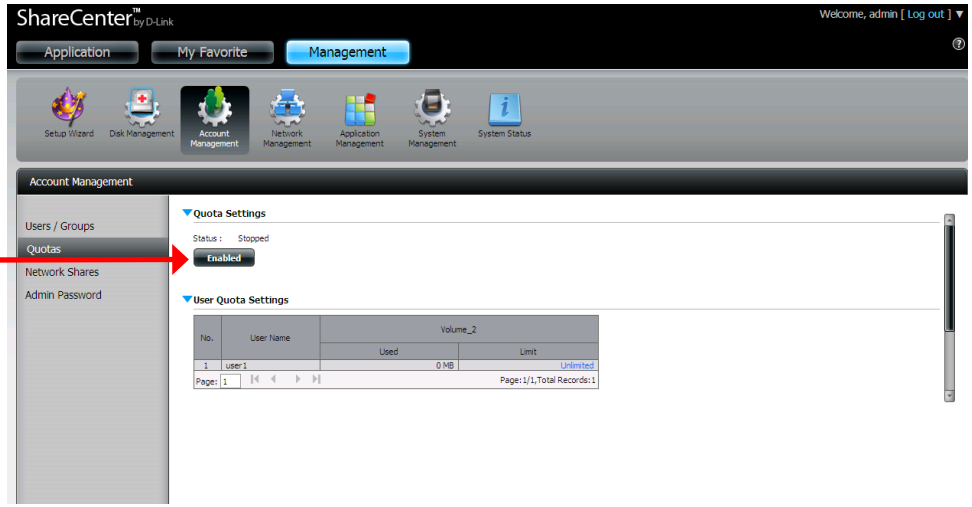


Success: A final message appears indicating the group was created successfully and added to the ShareCenter® configuration.

Quotas

The ShareCenter® supports storage quotas for both groups and individual users. Assigning a quota to a group or user will limit the amount of storage they are allocated. By default, users and groups do not have a quota.

Click the **Enabled** button to enforce the quotas that are set in the Users / Groups management or the tables below.



In the User Quota Settings table you can view the current user usage and limit setting. Click on the blue font to set usage limits.

User Quota Settings

No.	User Name	Volume_1		Volume_2	
		Used	Limit	Used	Limit
1	user1	0 MB	Unlimited	0 MB	Unlimited
2	user2	0 MB	Unlimited	0 MB	Unlimited
3	user3	0 MB	Unlimited	0 MB	2000 MB

Page: 1 Page: 1/1,Total Records:3

In the Group Quota Settings table you can view the current group usage and limit setting. Click on the blue font to set the limit.

Group Quota Settings

No.	Group Name	Volume_1		Volume_2	
		Used	Limit	Used	Limit
1	group1	0 MB	Unlimited	0 MB	Unlimited
2	group2	0 MB	1000 MB	0 MB	2000 MB

Network Shares

The Network Shares page allows the user to configure shared folders and rights to specific users and groups. To be able to create new network access rules, the default rule must first be removed by simply selecting it and clicking on the **Delete** button. You can also mount .iso files in the ISO Mount Shares Setting. If a user has access to a mounted .iso file then that user will be able to read all the files within it.

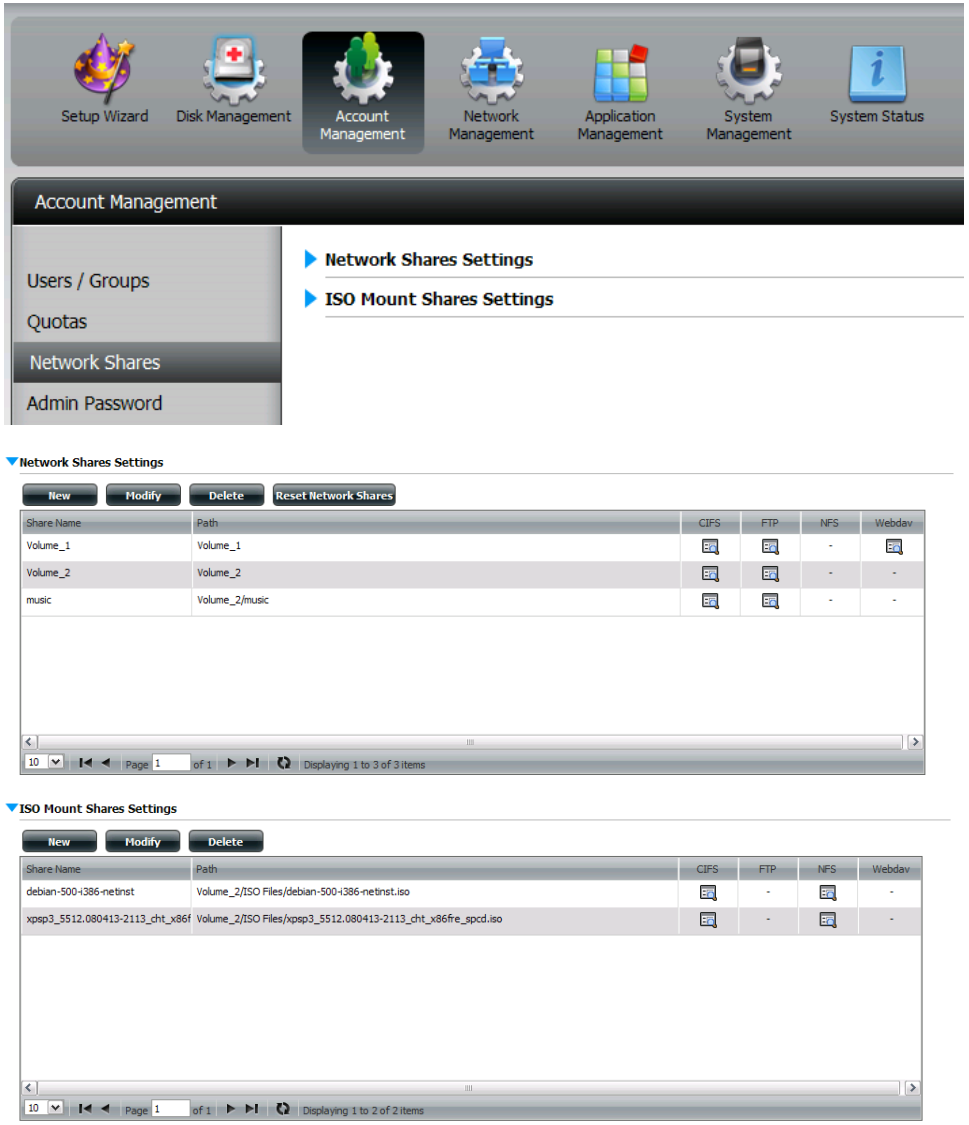
Network Shares: / ISO Mount Shares: The Network Shares Settings window allows you to add, modify and remove both new and existing Network Share and ISO Mount Share Settings.

To add a rule click on the **New** button. To modify an existing rule click on the **Modify** button. To remove a rule click on the **Delete** button.

To select a rule, simply click on the rule and the entry should change to red.

At the bottom of the table the user can navigate through pages and also refresh the window by click on the **Refresh** button.

If at any point the user wants to reset the network access list to the default configuration, click on the **Reset Network Shares** button.



Adding New Network Shares Wizard

The following section will describe how to add a new Network Share on the ShareCenter. To add a Network Share click on the **Add** button. A easy to configure wizard will be launched and look like the following:

Start: This window welcomes the user to the setup wizard for adding or modifying a network share.

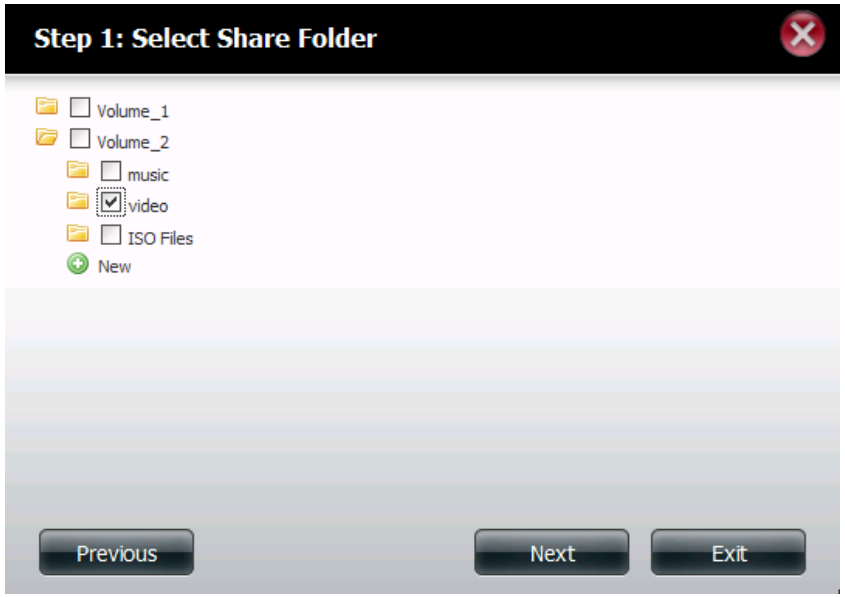
In this wizard the user will be able to:

1) Select share folders.
2) Configure shared folder access rights.
3) Configure network access settings.
4) View a summary of the configuration before completing.

Click on the **Next** button to continue.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.

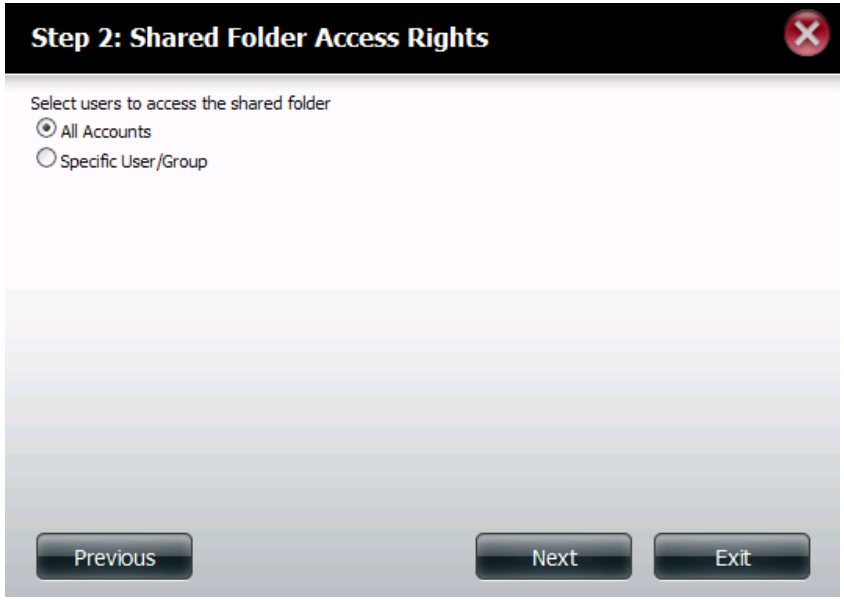
Step 1: Select the folder you want to include in this network share by checking the box.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 2: Select which user accounts or group are allowed to access this folder(s). Select **All Account** to allow all accounts access to this folder. Select **Specific User/Group** to only allow certain users or groups access to this folder.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.

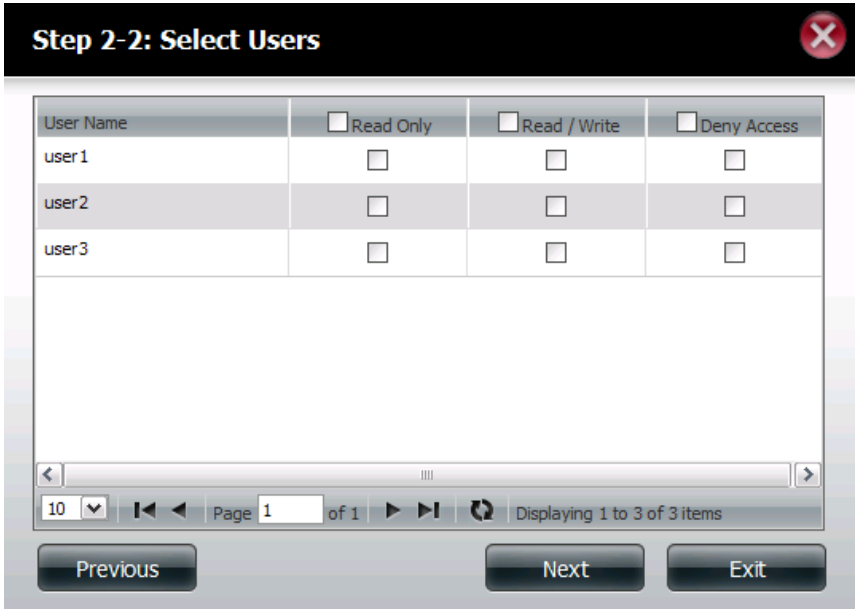


Step 2-1: Select the appropriate access rights for the share. Options to choose from are **Read Only**, **Read Write** and **Deny Access**. This procedure can also be used to block certain users from accessing certain folders.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.

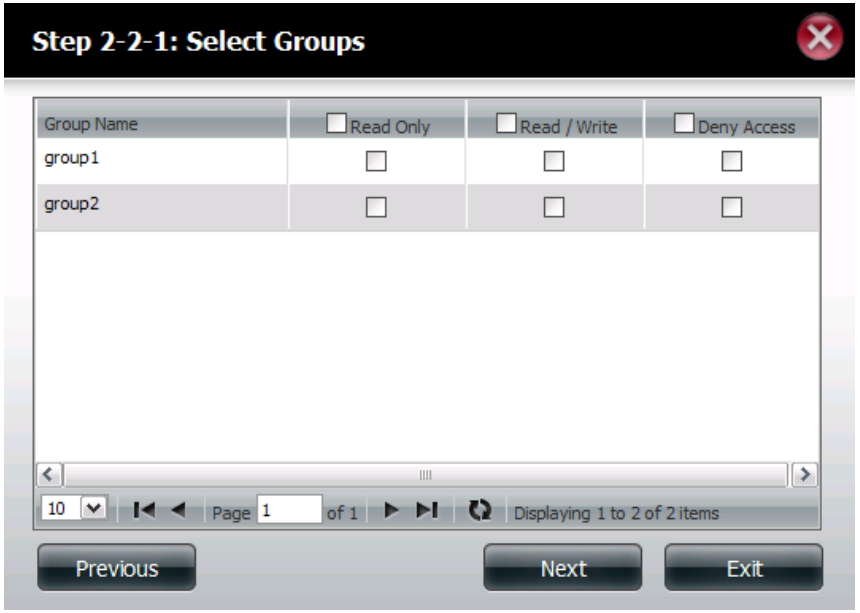
Step 2-2: If you select **Specific User/Group** in Step 2, then this step allows you to set the access rights for each **User** configured on the device.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.

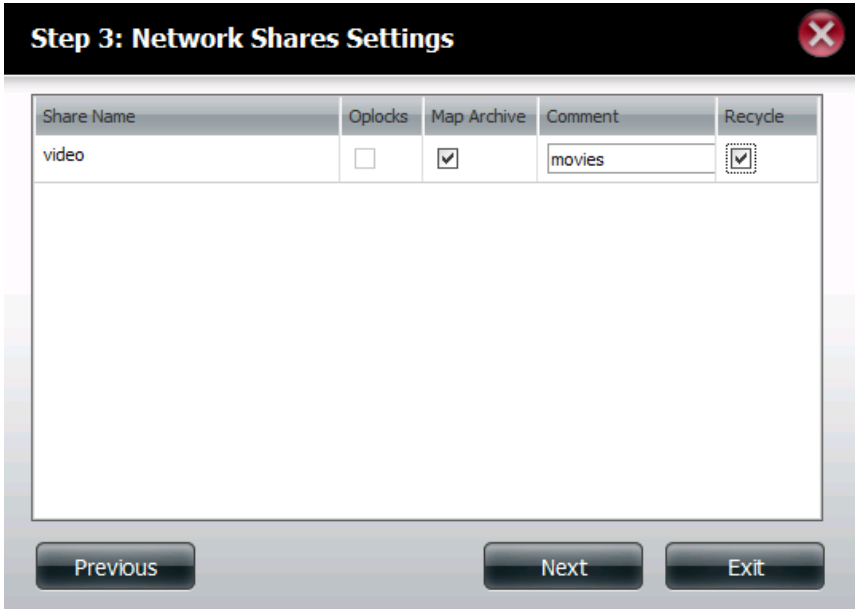


Step 2-2-1: If you select **Specific User/Group** in Step 2 then this step allows you to set the access rights for each **Group** configured on the device.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



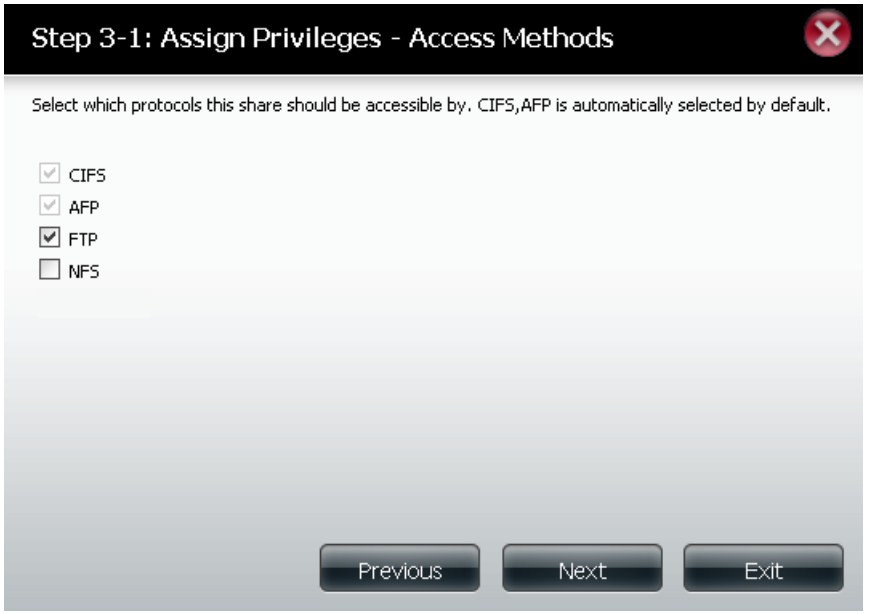
Step 3: This step allows you to assign privileges to this share. Opportunistic locks (oplocks) are a characteristic of the LAN Manager networking protocol implemented in the 32bit Windows family. Oplocks are guarantees made by a server for a shared logical volume to its clients. These guarantees inform the Client that a file's content will not be allowed to be changed by the server, or if some change is imminent, the client will be notified before the change is allowed to proceed. Oplocks are designed to increase network performance when it comes to network file sharing. However it is recommended to set the share oplocks to No (off) when using file-based database applications. When enabled, the file attribute "Map Archive" will be copied as the file is being stored on the device.



Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.

Step 3-1: Assign protocol privileges that a user can use to access this share. Options to choose from are FTP and NFS. CIFS and AFP are set as default.

- **CIFS** is short for Common Internet File System.
- **AFP** is short for Apple Filing Protocol.
- **FTP** is short for File Transfer Protocol.
- **NFS** is short for Network File System.

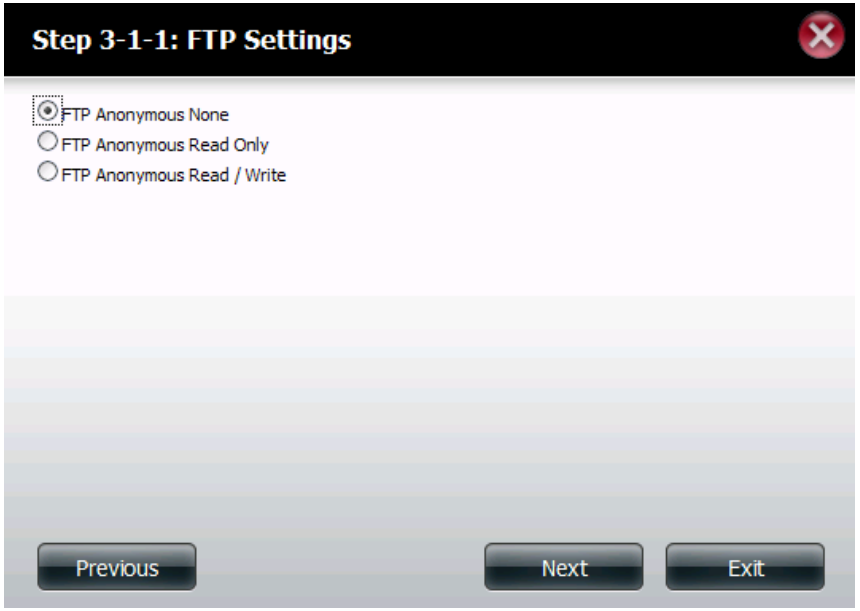


Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.

Step 3-1-1: Select the FTP settings for this share. FTP access can be:

1) FTP Anonymous None (No Access).
2) FTP Anonymous Read Only (Limited Access).
3) FTP Anonymous Read/Write (Full Access).

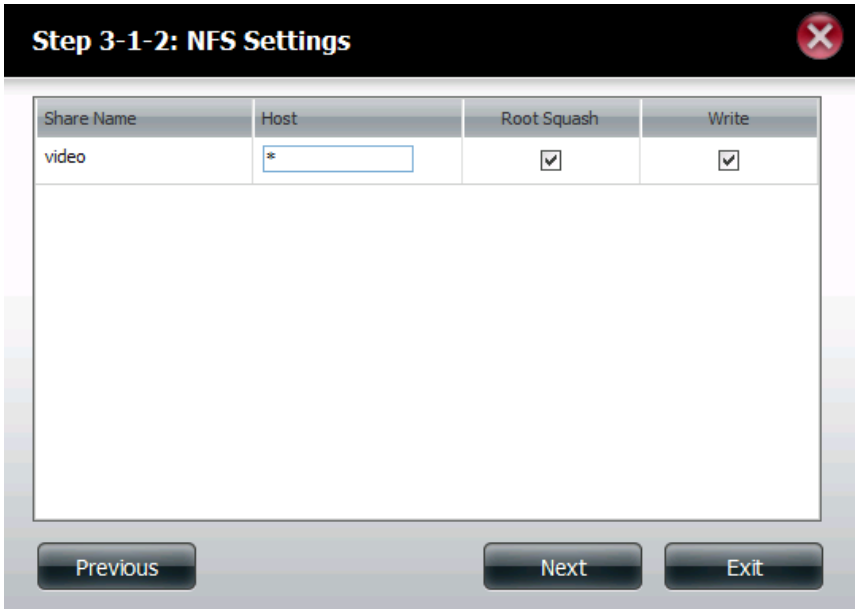
Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 3-1-2: If you selected **NFS** as an access method to your network share then set the parameters below:

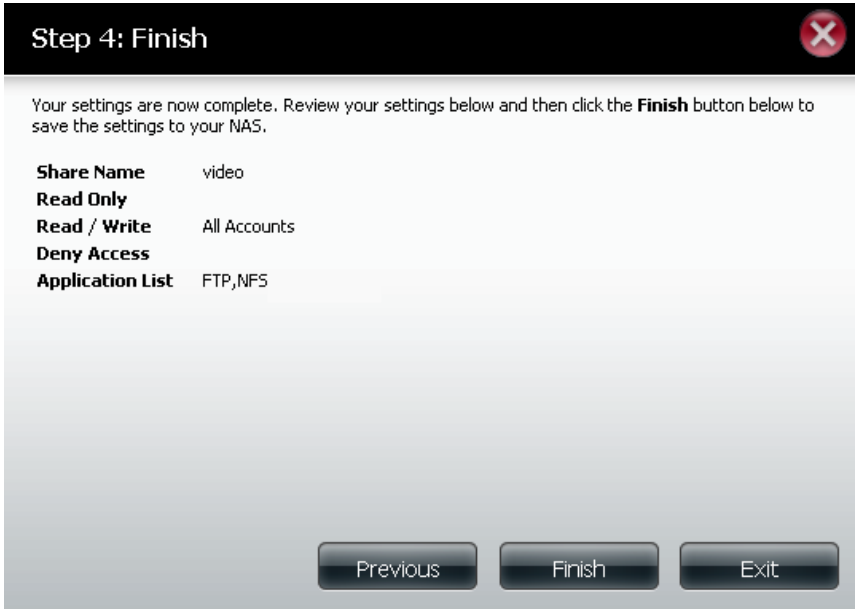
- **Host** - Allowable host address that can access using NFS (* indicates all hosts).
- **Root Squash** - Disables writing to the Root owned directories and files on the system when the user has root access privileges.
- **Write** - provide write permission to the file system.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 4: Click **Finish** to save your settings.

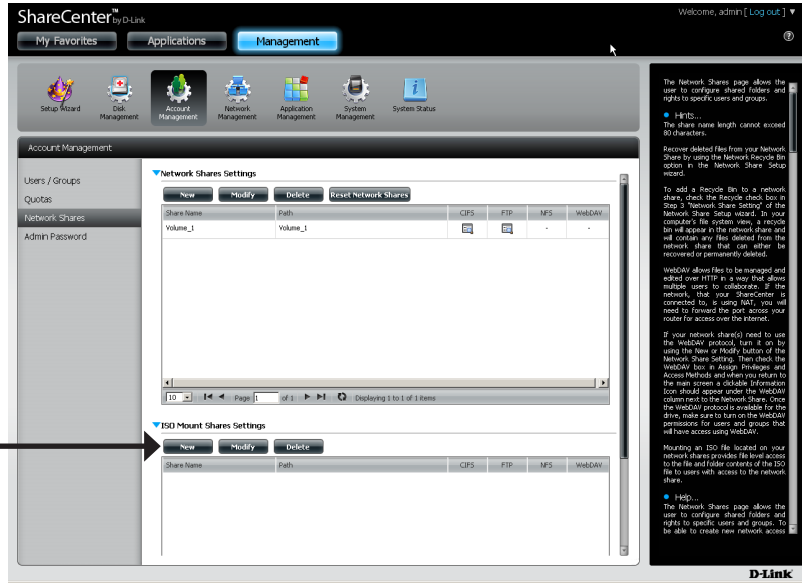
Click on the **Previous** button to return to the previous window.
Click on the **Finish** button to accept the change and complete the wizard.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Adding New ISO Mount Shares Wizard

The following section will describe how to add a new ISO mount on the ShareCenter. To add an ISO Mount click on the **New** button. A wizard will launch as shown below:

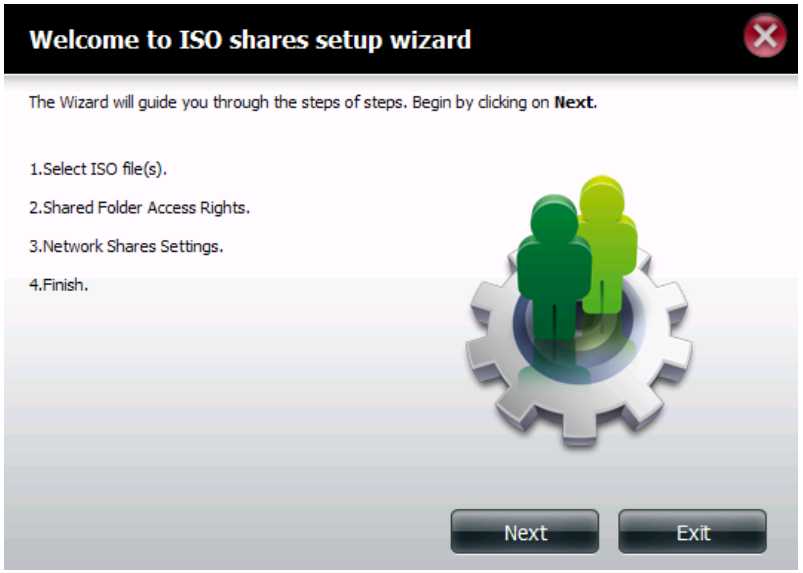
Click **New** to launch the ISO Share Setup Wizard



Setup: This wizard will guide the user through the steps of setup.

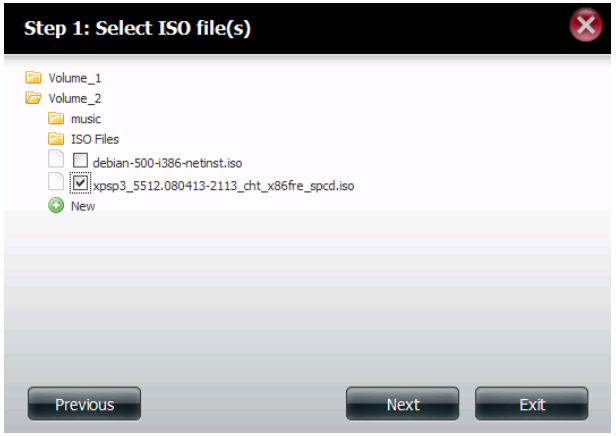
This wizard will allow you to:
1) Select an ISO file.
2) Share folder access rights.
3) Configure network access settings.
4) View a summary of the configuration before completing.

Click on the **Next** button to continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 1: Select the ISO file(s) to mount.

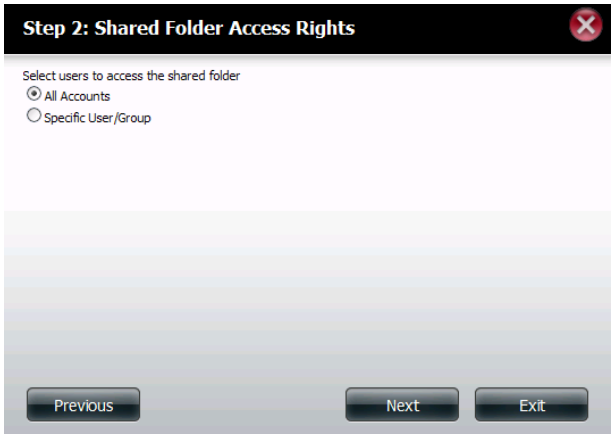
Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 2: Assign access privileges to this ISO Mount share.

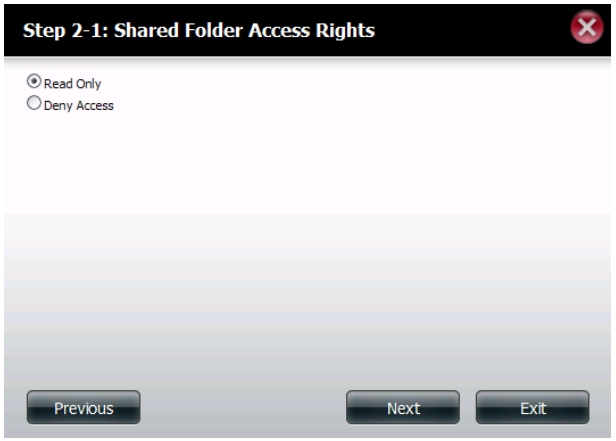
- Select All Accounts to assign the ISO Mount share read/deny privileges to all users.
- Select Specific User/Group in order to assign read/deny privileges to individual users and groups.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



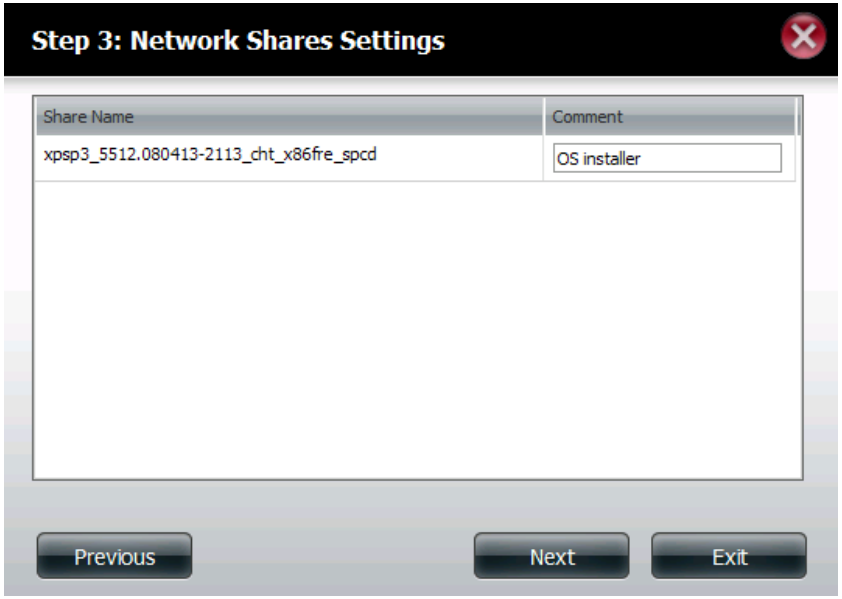
Step 2-1: You can assign **Read Only** or **Deny Access** privileges to the ISO Mount share here. Click on the appropriate radio button for the privileges you would like to assign.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 3: You may add a comment that describes the ISO Mount Share.

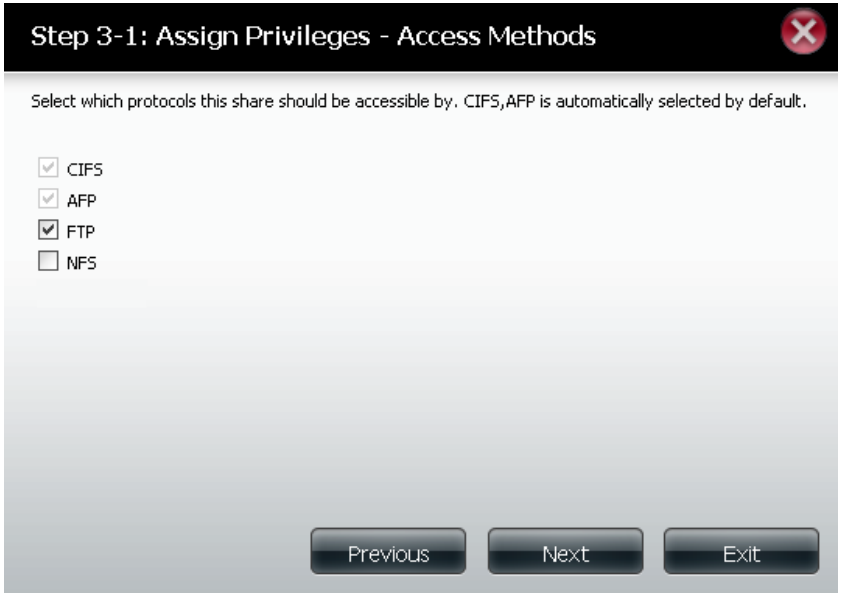
Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 3-1: Assign protocol privileges that a user can use to access this share. Options to choose from are FTP and NFS. CIFS and AFP are set as default.

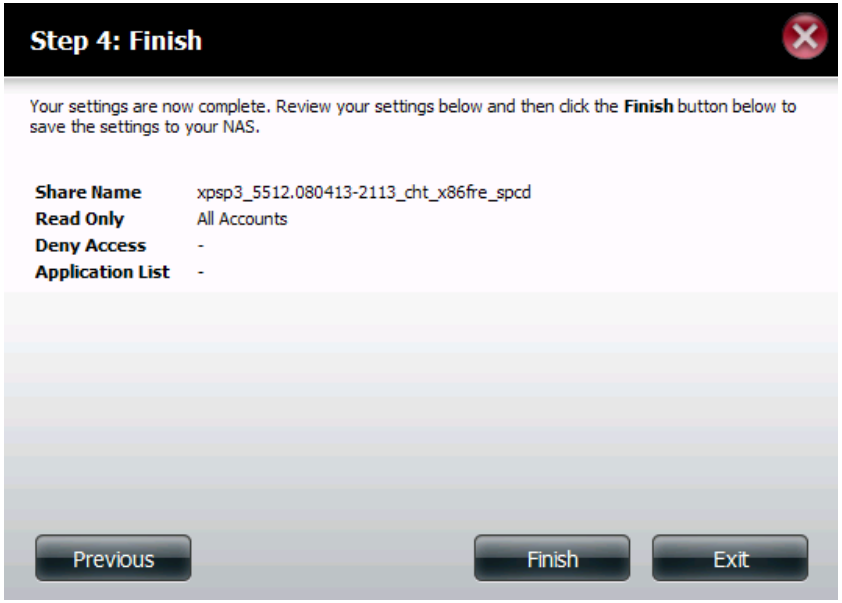
- **CIFS** is short for Common Internet File System.
- **AFP** is short for Apple Filing Protocol.
- **FTP** is short for File Transfer Protocol.
- **NFS** is short for Network File System.

Click on the **Previous** button to return to the previous window.
Click on the **Next** button to accept the change and continue to the next window.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.

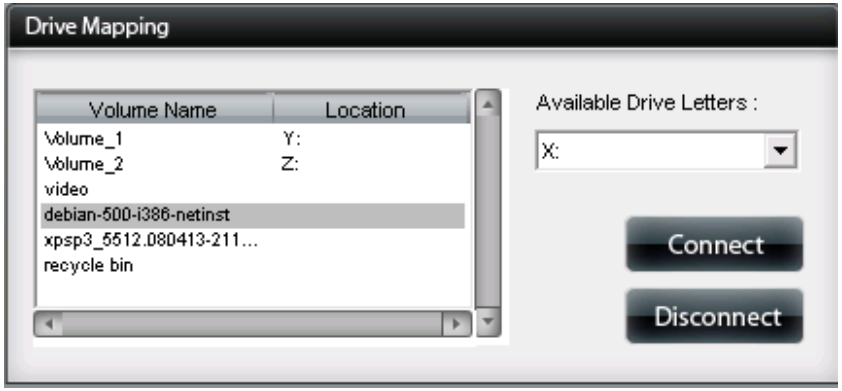


Step 4: Click **Finish** to save your settings.

Click on the **Previous** button to return to the previous window.
Click on the **Finish** button to accept the change and complete the wizard.
Click on the **Exit** button to discard the changes made and return to the Network Shares Page.



Step 5: Using the D-Link Storage Utility the ISO Mount Share can now be mapped to your computer so that you can access it.



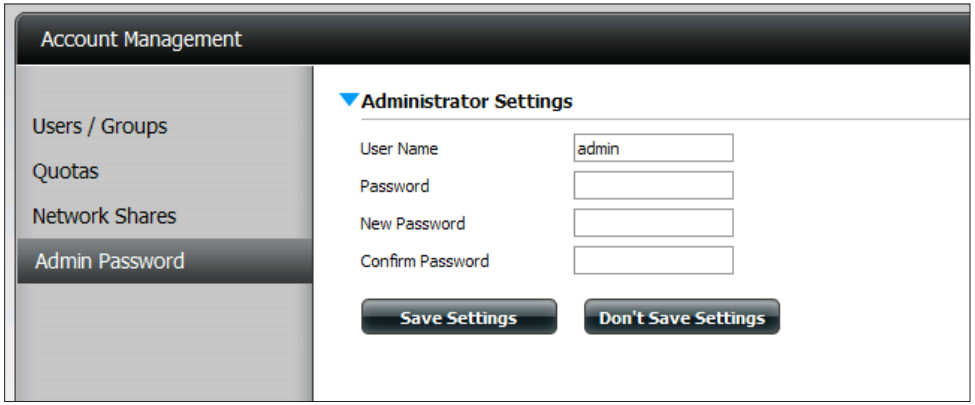
Admin Password

Username: The administrator user name is **admin**, and this cannot be changed.

Password: Enter the current password. (Leave this blank if you have not set a password yet.)

New Password: Enter a new password.

Confirm Password: Enter the new password again for confirmation.



Network Management
LAN Setup

The LAN Settings allows you to enable LLTD and to configure the Link Speed and the IP address as a DHCP client or Static IP.

IP Settings

DHCP Client: Selecting DHCP Client will cause the DNS-320 to obtain an IP address from the local DHCP server.

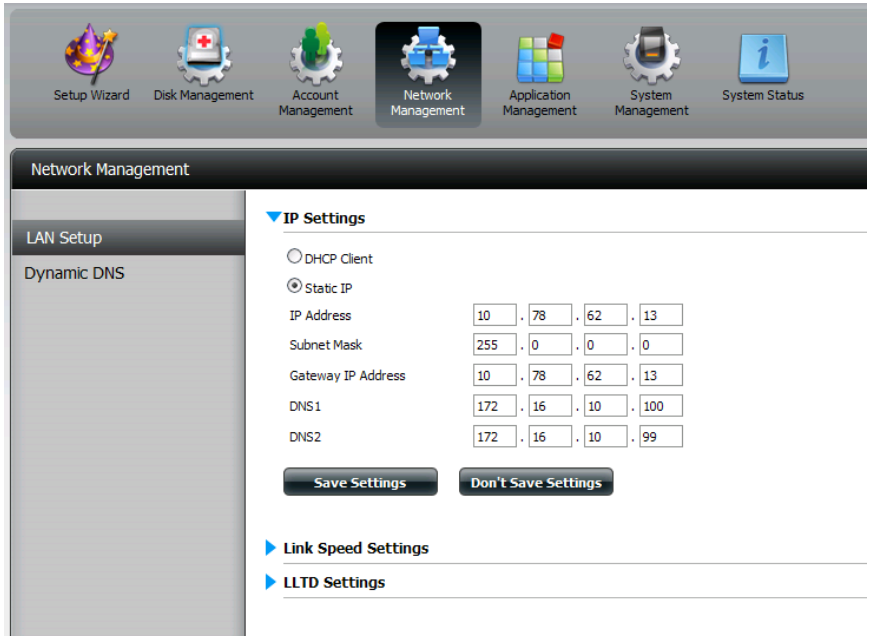
Static IP: Selecting Static IP requires you to assign the IP information for the DNS-320 manually.

IP Address: Enter an IP address for your device. The IP address of each device on the local area network must be within the same IP address range and subnet mask.

Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

Gateway IP Address: Enter the Gateway IP Address for the device. The Gateway IP Address is almost always the LAN address of your router. Most D-Link routers have a default LAN IP address of 192.168.0.1.

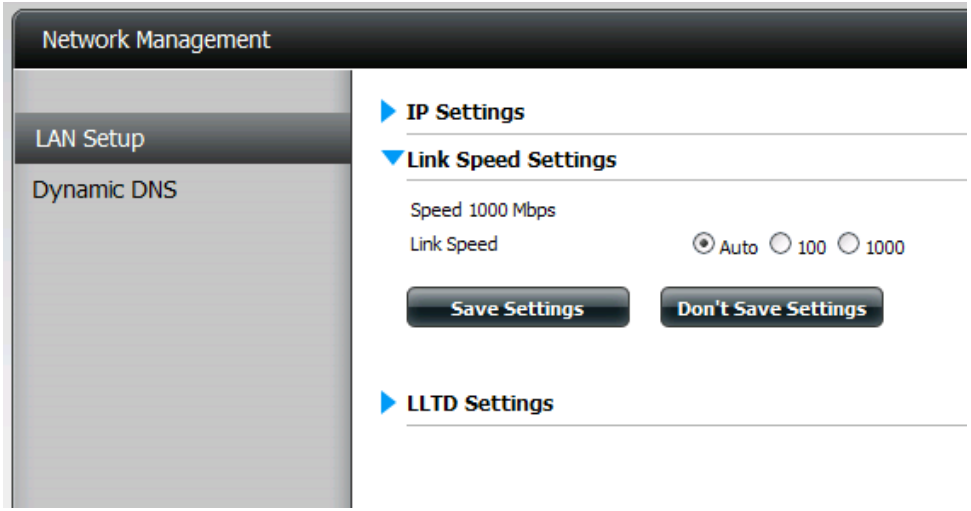
DNS1/ DNS2: Specify the first and second DNS Addresses for the device. The first DNS address is usually the LAN address of your router. A DNS Address will allow the device to resolve names into IP addresses. Click **Save Settings** when finished



Link Speed and LLTD Settings

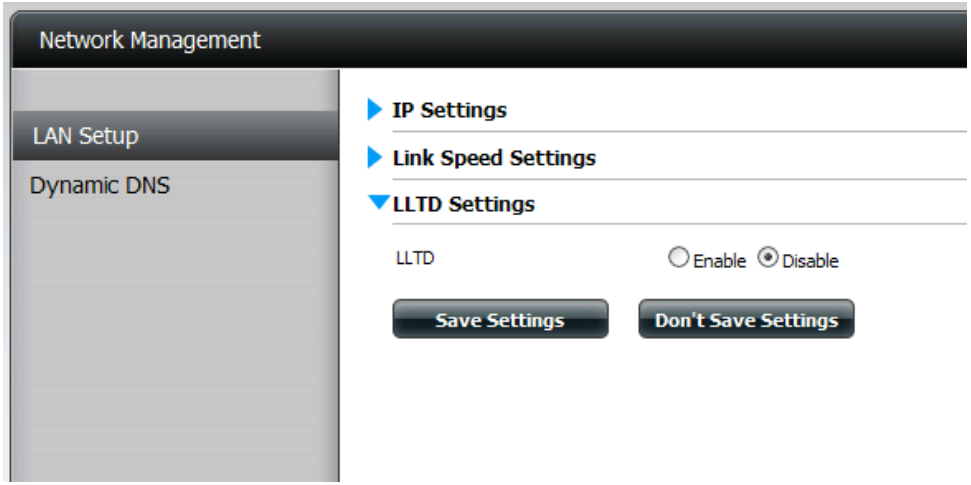
Speed: Displays the current Ethernet bit rate in Megabits per second.

Link Speed: Select either Auto (Auto-Negotiate), 100 Mbps, or 1000 Mbps by clicking the appropriate radio button. Then click the **Save Settings** button to save the new settings.



LLTD: The device supports LLTD (Link Layer Topology Discovery) and is used by the Network Map application that is included in Windows Vista® and Windows® 7.

Select to enable or disable LLTD.



Dynamic DNS

The DDNS feature allows the user to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your domain name to connect to your server regardless of your IP address.

DDNS Settings

DDNS: Select **Enable** or **Disable**.

Server Address: Select a DDNS Server from the combo box on the right hand-side, or type in the server address manually.

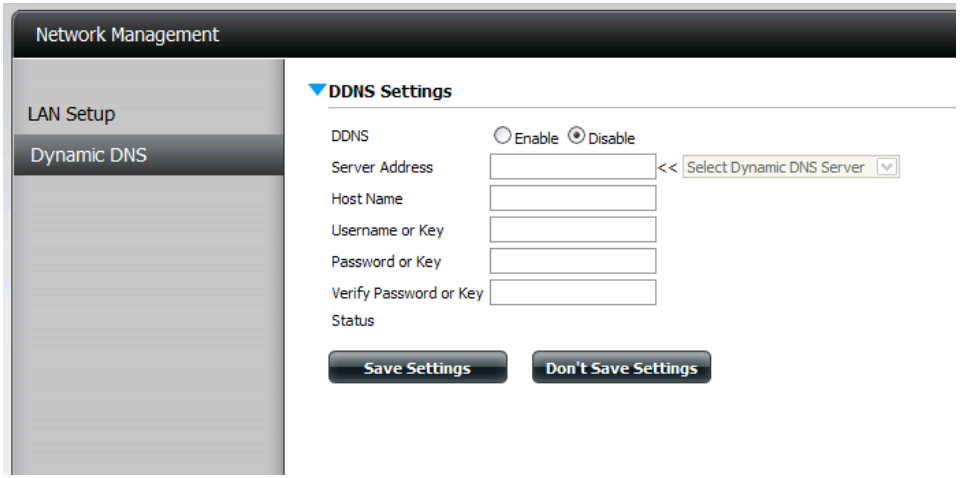
Host Name: Enter your DDNS host name.

Username or Key: Enter your DDNS username or key.

Password or Key: Enter your DDNS password or key.

Verify Password or Key: Re-enter your password or key.

Status: Displays your DDNS status.



When the user clicks on the "Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com" link, the user will be re-directed to the D-Link DDNS page.

Here the user can create or modify a D-Link DDNS account to use in this configuration.

Application Management

FTP Server

The device is equipped with a built in FTP Server. The server is easy to configure and allows users access to important data whether they are on the local network or at a remote location. The FTP server can be configured to allow user access to specific directories, and will allow up to 10 users to access the device simultaneously.

Max. User: Set the maximum amount of users that can connect to the FTP server.

Idle Time: Set the amount of time a user can remain idle before being disconnected.

Port: Set the FTP port. Default is 21. If you are behind a router, you will need to forward the FTP port from the router to the device. Additional filtering and firewall settings may need to be modified on your router to allow FTP Access to the device from the Internet. Once the port has been forwarded on the router, users from the Internet will access the FTP server through the WAN IP address of the router.

Passive Mode: In situations where the device is behind a firewall and unable to accept incoming TCP connections, passive mode must be used.

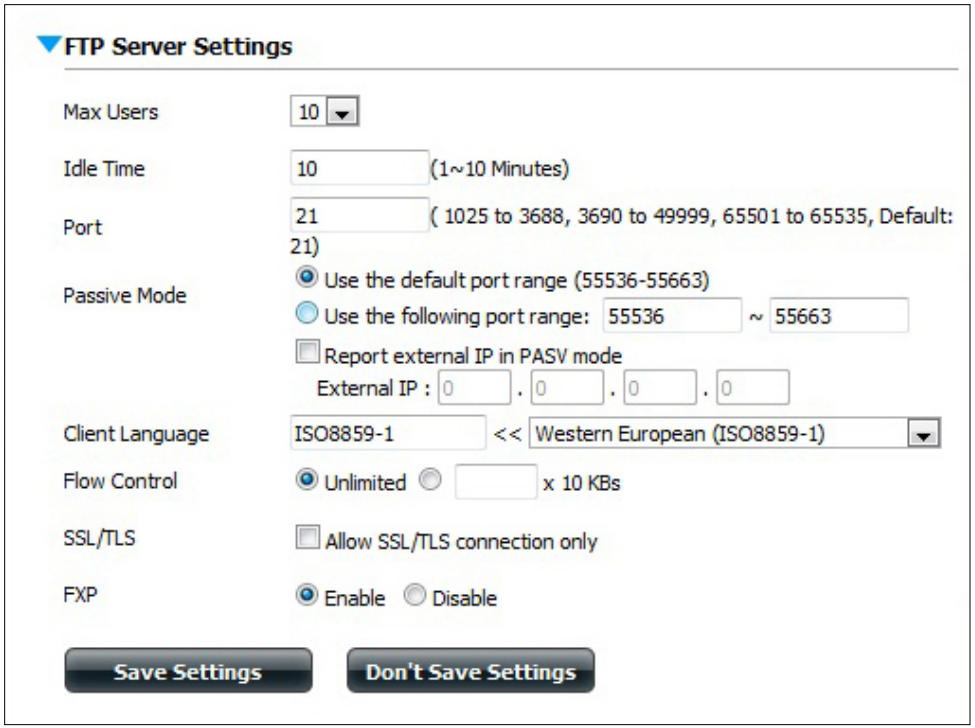
Client Language: Most standard FTP clients like Windows FTP, only support Western European code page when transferring files. Support has been added for non standard FTP clients that are capable of supporting these character sets.

Flow Control: Allow you to limit the amount of bandwidth available for each user.

SSL/TLS: Here the user can enable the SSL/TLS connection only.

FXP: Enable or Disable File eXhange Protocol to transfer files from one FTP server to another.

Note: In order to use FXP (File Exchange Protocol) for server-to-server data transfer, make sure to change the port from 21 to some other port as listed in the Port section of the Web UI. Also, make sure to open the corresponding port on your router and forward that port from your router to the device.



UPnP AV Server

The device features a UPnP AV Server. This server provides the ability to stream photos, music and videos to UPnP AV compatible network media players. If the server is enabled, the device will be automatically detected by UPnP AV compatible media players on your local network.

Click the **Refresh All** button to update all the shared files and folder lists.

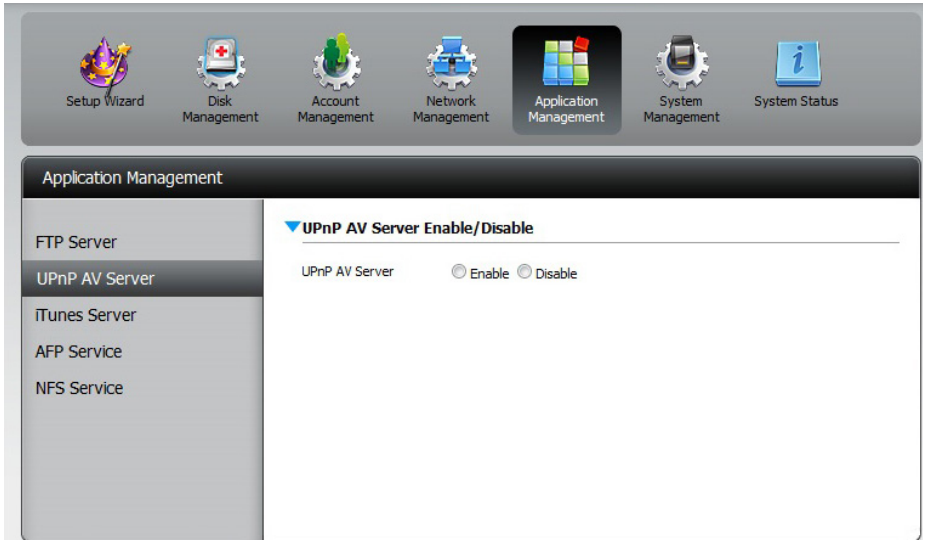
UPnP AV Server: Select **Enable** or **Disable**.

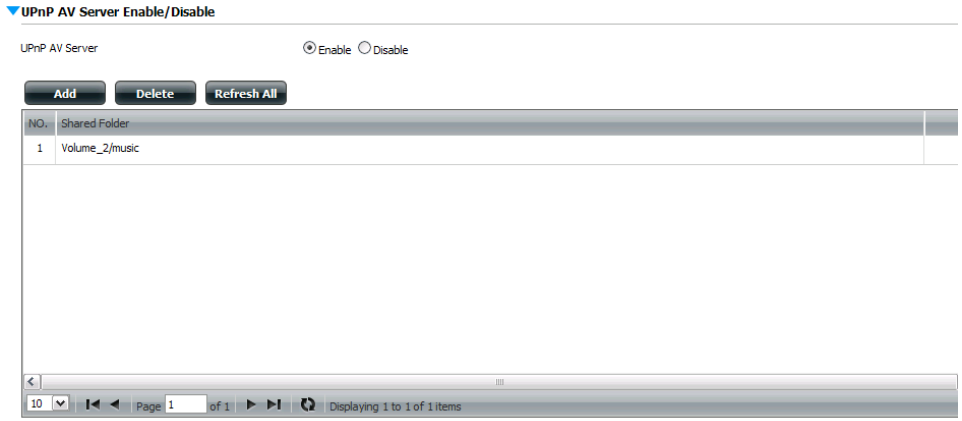
After enabling the UPnP AV Server option, the following window will appear.

In the window you will be able to add, delete and view existing UPnP AV Server shared folders.

Add, Delete: To add a new folder to the shared list, click on the **Add** button. To delete an existing folder, click on the **Delete** button. To refresh the list, click on the **Refresh** button.

Refresh All: Click the **Refresh All** button after adding new files to be used by UPnP AV compatible devices.





iTunes Server

The DNS-320 features an iTunes Server. This server provides the ability to share music and videos to computers on the local network running iTunes. If the server is enabled, the device will be automatically detected by the iTunes program and the music and videos contained in the specified directory will be available to stream over the network. Click the **Refresh All** button to update all the shared files and folder lists.

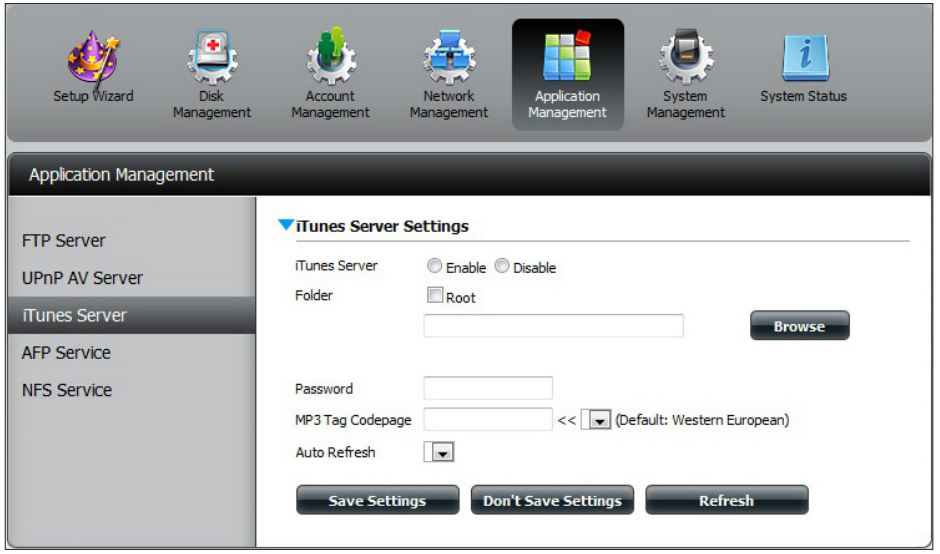
iTunes Server: Select to enable or disable the iTunes Server.

Folder: Specifies the folder or directory that will be shared by the iTunes server. Select root to share all files on all volumes, or click **Browse** to select a specific folders.

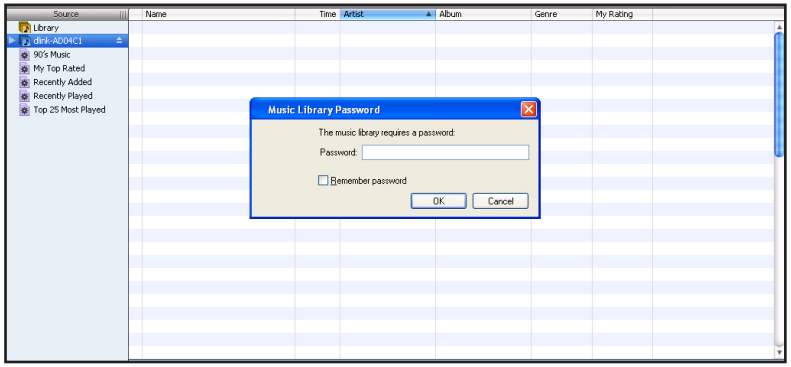
Password: Sets password for the iTunes server. (Optional)

MP3 Tag Codepage: Here the user can select the MP3 Tag Codepage used by this device. Currently the Codepage is set to Western European.

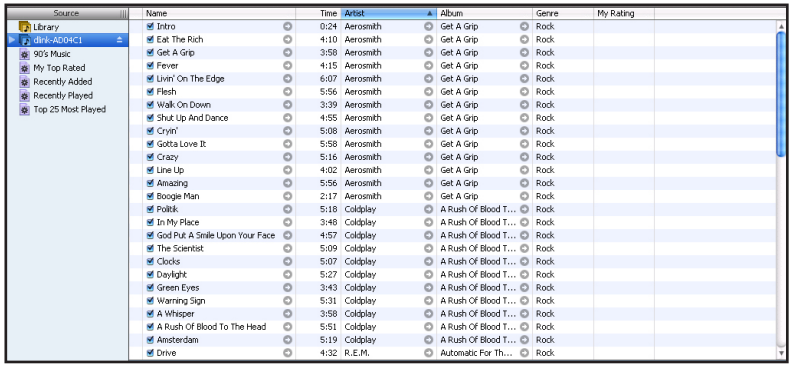
Auto Refresh: Here the user can select the Automatically Refresh time.



After enabling the iTunes server on the device, launch iTunes. In your iTunes utility, select the device and enter the iTunes server password if required.



Select the device When prompted, enter in the iTunes server password. Click **OK**.



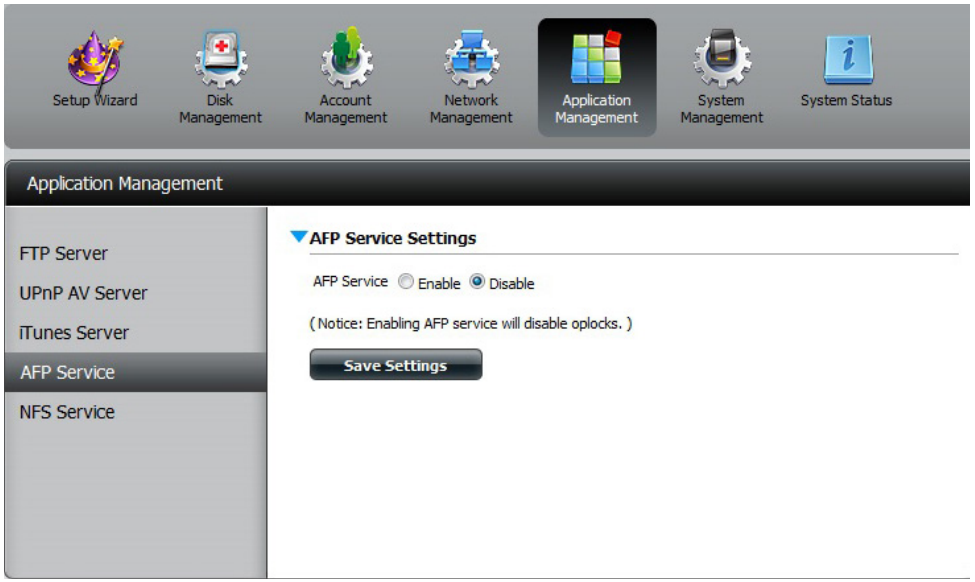
Media stored on the device will then be available for use in iTunes.

AFP Service

The ShareCenter supports Apple Filing Service for connectivity with MAC OS based computers. If you need to use AFP service enable it here otherwise leave it disabled to reduce CPU resource overhead.

AFP Service: Select enable to allow MAC OS based systems connect to your device using AFP protocol. Select disable to prevent unnecessary CPU resource depletion when AFP is not being used.

Save Settings: Click to save your AFP settings.



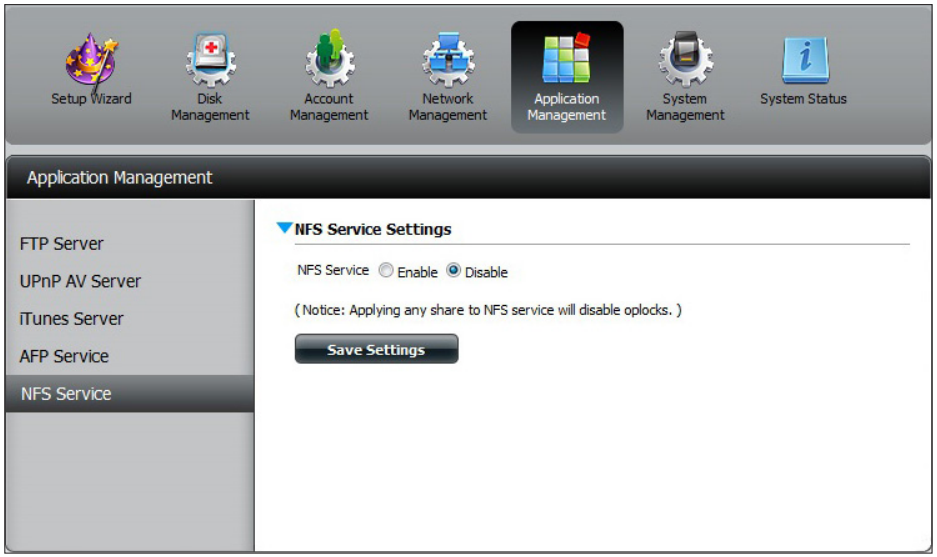
Note: Enabling AFP service will disable oplocks.

NFS Service

The device supports Network File System (NFS) service. To enable this multi-platform file system on your device enable it here. Otherwise disable the option to prevent unnecessary CPU overhead.

NFS Service: Select **Enable** to allow systems that support NFS to connect to your device using NFS protocol. Select **Disable** to prevent unnecessary CPU resource depletion when NFS is not being used.

Save Settings: Click to save your NFS settings.



Note: Applying NFS service to any Share will disable oplocks.

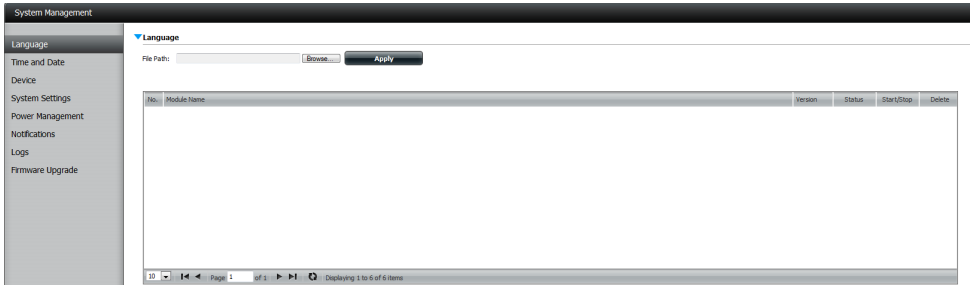
System Management

Language

This menu item allows you to install language packages onto your system. In addition, you can also install language packages to suit your local language needs.

Languages: Click on **Browse** to search for the specific language pack you want to install. After selecting the language pack, then click **Apply** to install the language pack.

Language Pack List: In the languages window you will see a table where the loaded language packs will be displayed and can be enabled at will by simply clicking the (>) "play" button. More than one language pack can be installed, but only one language pack can be used at a time.



Time and Date

The Time and Date page contains several different options for setting the device's internal clock. It is important to set an accurate time so that backups and downloads can be accurately scheduled.

System Time Settings: Displays the current date, time and time zone settings of the device.

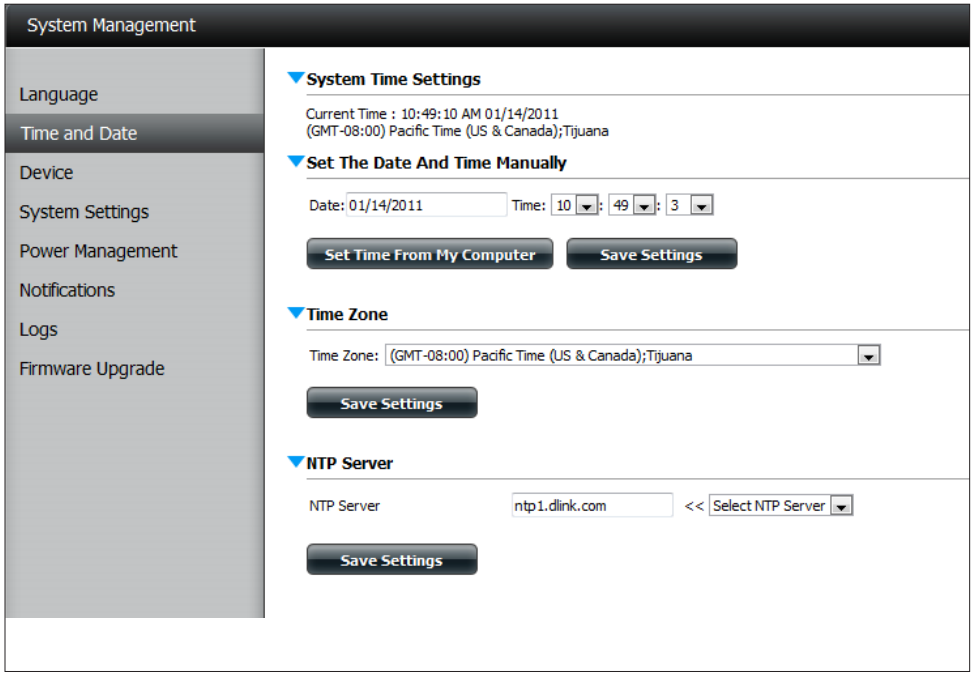
Manually: Enter the complete time and date settings manually. Click **Save Settings** to apply these settings. To synchronize the device clock with your computer, click the **Set time from my computer** button.

Time Zone: Select your time zone from the drop-down menu. Click **Save Settings** after selecting your time zone

NTP Server: Network Time Protocol (NTP) synchronizes the device with an Internet time server.

D-Link provides two time servers for your convenience. Select the one closest to your location.

Click **Save Settings** to accept these changes.



Device

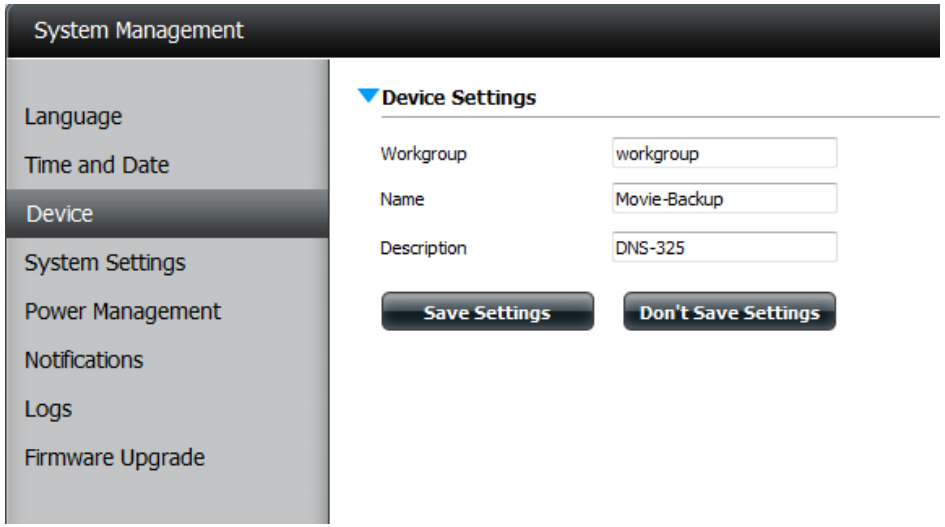
The device settings page allows you to assign a workgroup, name and description to the device. You can access this device by typing the host name in the URL section of your web browser. For example: http://dlink-d10001.

Workgroup: Enter your Workgroup name here. The workgroup name should be the same as the computers on the network. Devices using the same workgroup will have additional file sharing methods available.

Name: Enter your device name here. This name is what the device will appear as on the network. By default, the device name is dlink-xxxxxx, where xxxxxx is the last six digits of the MAC address.

Description: Assign a device description to the device.

Click **Save Settings** to accept these changes.

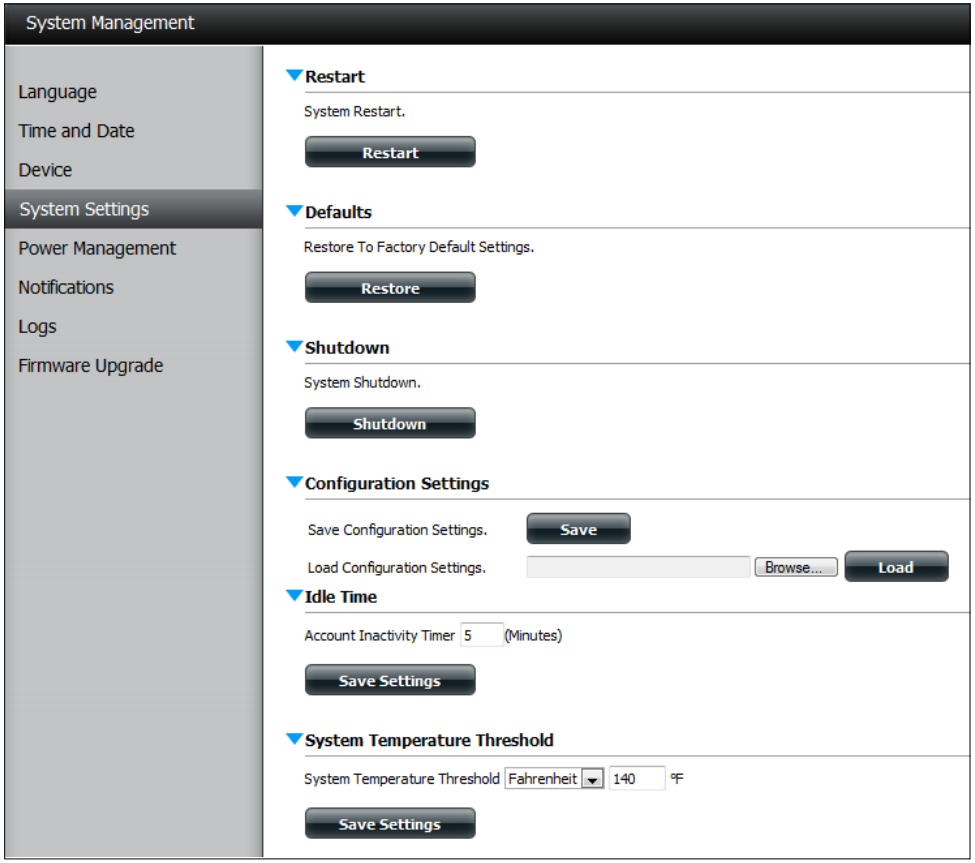


System Settings

Restart: Clicking to reboot the device.

Default: Click to restore the device back to the factory default settings. All previous settings that have been configured will be erased.

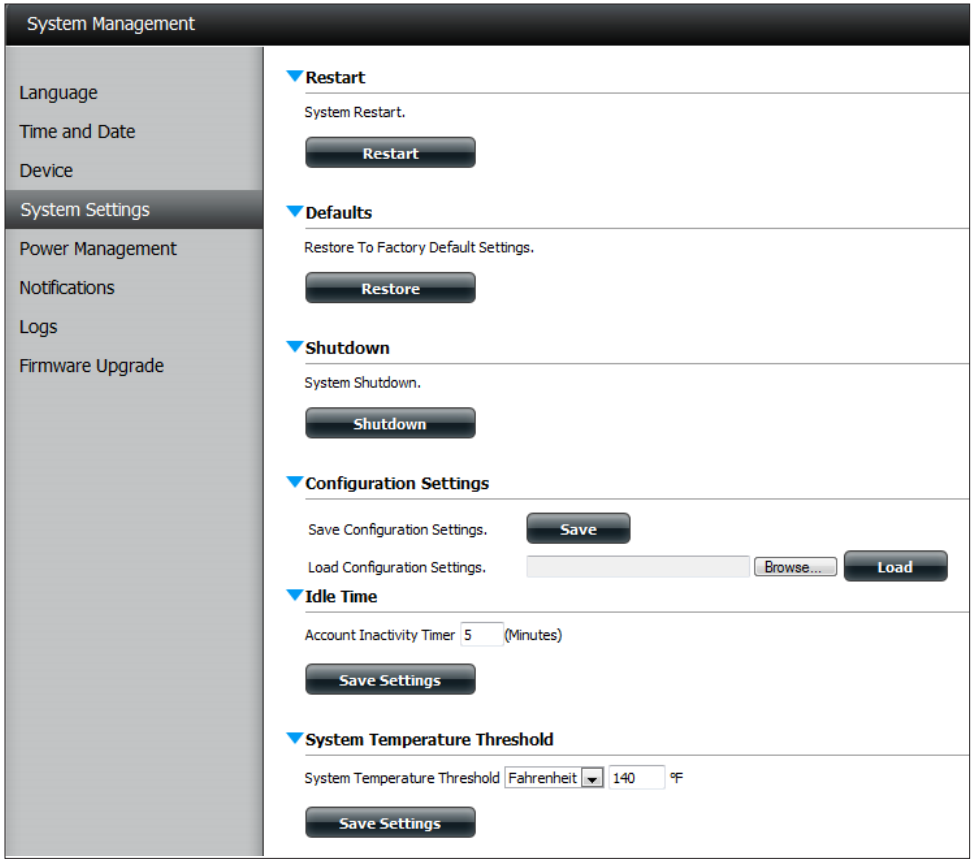
Shutdown: Click to turn off the device.



Configuration Settings: Click on the **Save** button to save the current configuration settings to a file on your computer. If at a later time you need to reload this configuration after a system reset, browse to the file and click **Load**.

Idle Time: Enter the time (in minutes) that the administrator and users will be allowed to remain idle while accessing the web UI.

System Temperature Threshold: Here the user can configure the system temperature threshold value. This value can be set in Fahrenheit or Celsius. The device will automatically shutdown when it reaches the temperature set here.



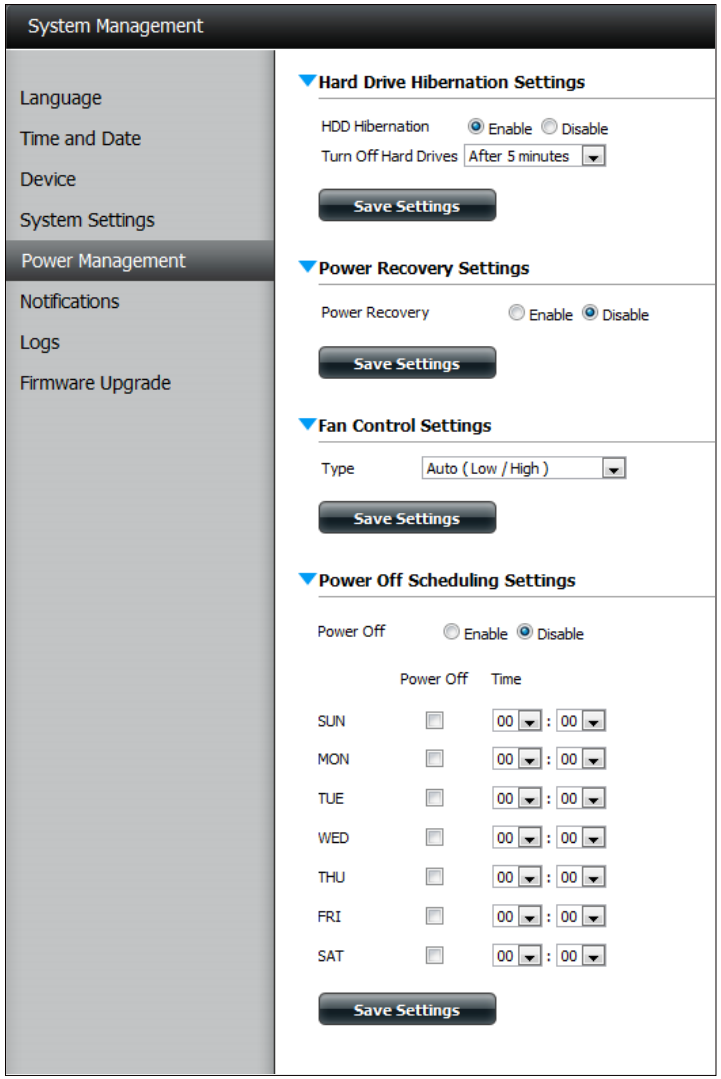
Power Management

The device Power Management feature allows you to configure the drives to shut down while power remains constant to the device. The drives will power up again when data is accessed.

HDD Hibernation: Click **Enable** or **Disable**.

Turn Off Hard Drive: Set the amount of idle time before the drives go into hibernation.

Power Recover: Click **Enable** or **Disable**. The Power Recovery feature will automatically restart your device from a previously unexpected shutdown due to a power failure.

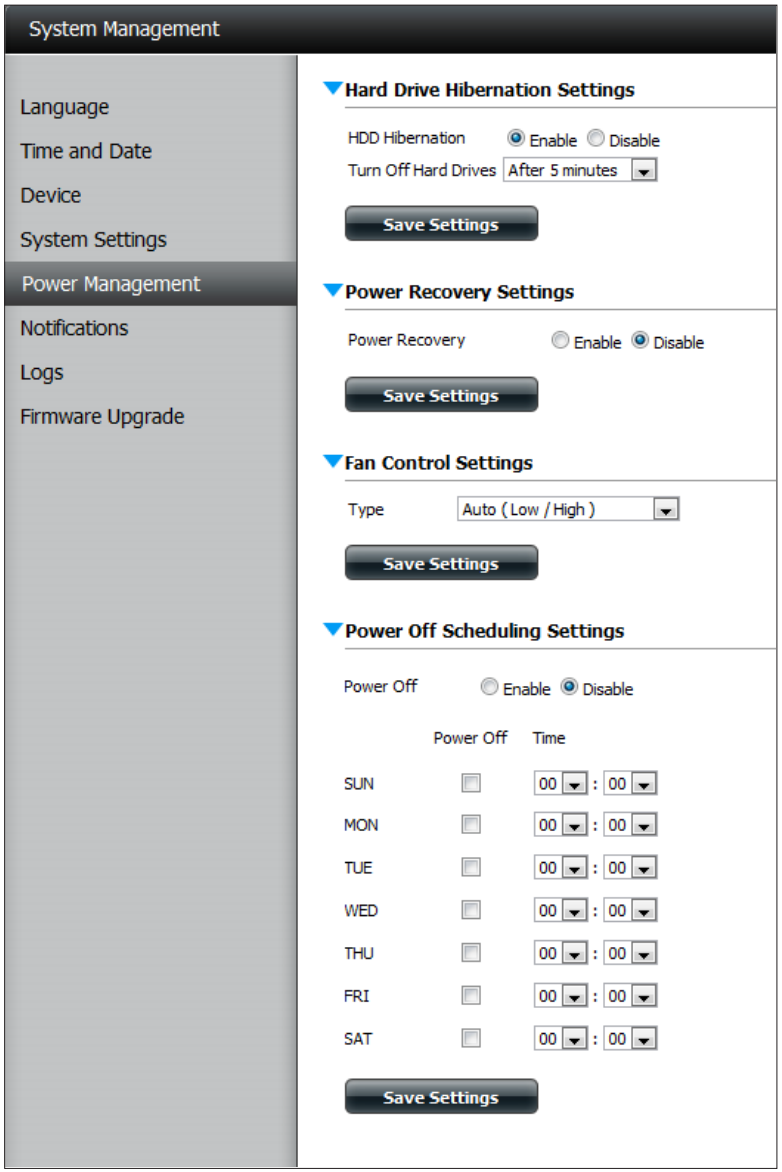


You can also control the speed of the fan using three different settings and you can power off the device at scheduled times for each day of the week.

Fan Control: The speed of the fan can be controlled from this section.

If you select **Auto** mode, the speed of the fan will change (Off/Low/High) depending on the internal temperature of the enclosure.

Power Off Scheduling: Click **Enable** to turn on this function. Enable or disable the power off days using the check box and configure the time for each day that the power off will occur.



Notifications
Email Settings

With E-Mail Alerts, you can configure e-mails to be sent to you that alert you to certain operational conditions and drive status conditions. These alerts can prove helpful with the management and safeguarding of important data.

Login Method: Select either **Account** or **Anonymous**. Choosing Anonymous does not require a User Name or Password.

Username: Enter the appropriate user name for your e-mail account.

Password: Enter the appropriate password for your e-mail account.

Port: Enter the SMTP port number used here.

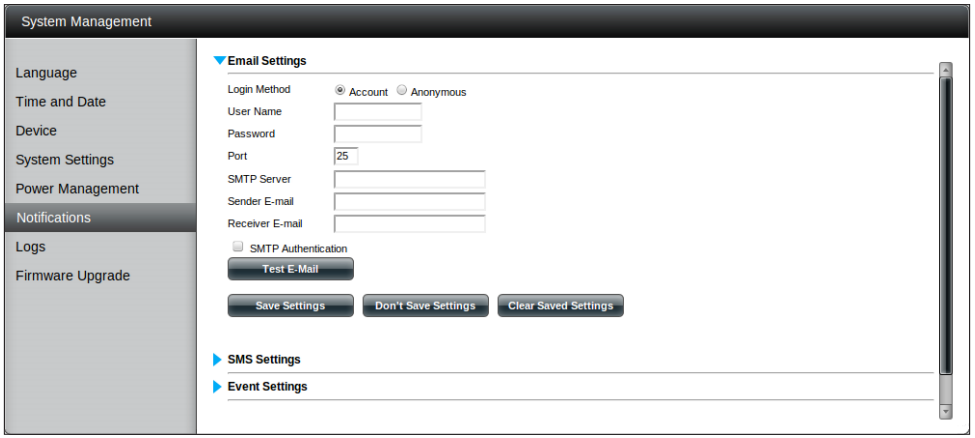
SMTP Server: Enter the IP address or domain name of your outgoing mail server. If you are unsure of this value, contact your e-mail provider.

Sender E-mail: Enter the "from" e-mail address (e.g. alerts@share.com). This field does not require a valid e-mail address. However, if your e-mail client is filtering spam, make sure you allow this address to be received.

Receiver E-mail: Enter the e-mail address you want to send the alerts to. This address must correspond with the SMTP server configured above.

SMTP Authentication: Click this option to use SMTP authentication.

Test E-Mail: Click the **Test E-Mail** button to send a test alert and confirm your settings are correct.



SMS Settings

The same alerts of system conditions that can be sent to an email box can also be sent to a mobile phone or by SMS text messages. You need to have an agreement with a SMS service gateway that the device can then be configured to send the alerts to. The service provider then sends the received alerts to the configured mobiles as text messages.

Enable SMS Notifications: Check this box to enable SMS alerts to be sent to your mobile phone.

SMS Service Provider: Select from the drop-down list your SMS service provider you would like to use (these are added with the **Add** button)

Add button: Click on the **Add** button and enter the information into the appropriate fields that your provider has given you to use for the configuration.

Delete button: Remove the selected Service Provider from the configuration.

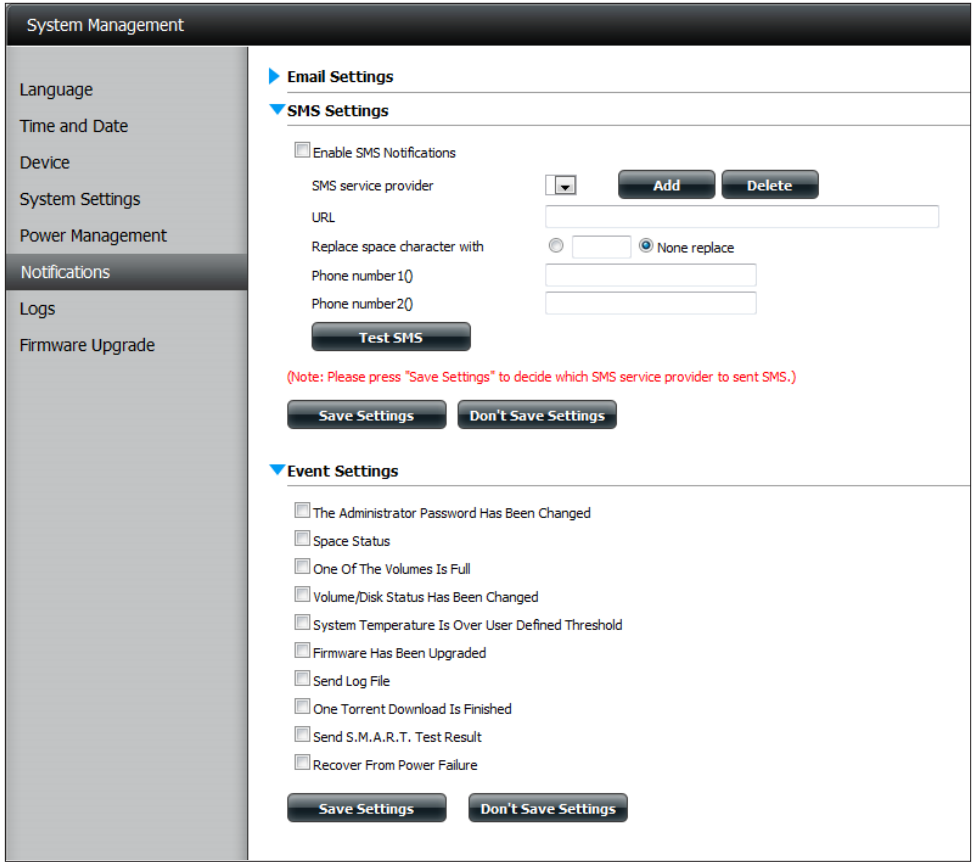
URL: The specific service provider URL provided and added in the Add procedure.

Replace space character with: If required by your service provider enter a character that will be used for the space.

Phone Number 1: Automatically populated from the **Add** button function.

Phone Number 2: Enter a second mobile telephone number. Verify that the number input is according to the configuration instructions from your Mobile Service Provider.

Test SMS button: Click this button to send a test message to your mobile phone to verify the settings are correct and the API URL is functioning with your provider.

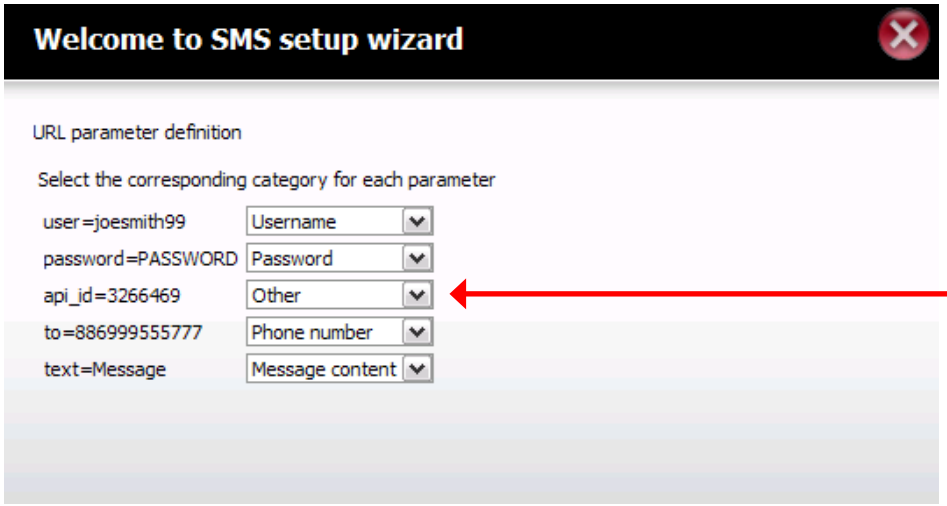


Adding an SMS Service Provider

Once you have a SMS Service provide you with a HTTP API URL, enter it into the Add SMS Service Provider wizard. Enter the URL in the first window with an appropriate Provider Name. In the next window select the appropriate HTTP API URL parameter types definitions from the drop-down menus next to the parsed fields of the URL.

Enter your SMS Provider name here.

Enter the HTTP API URL provided to you.

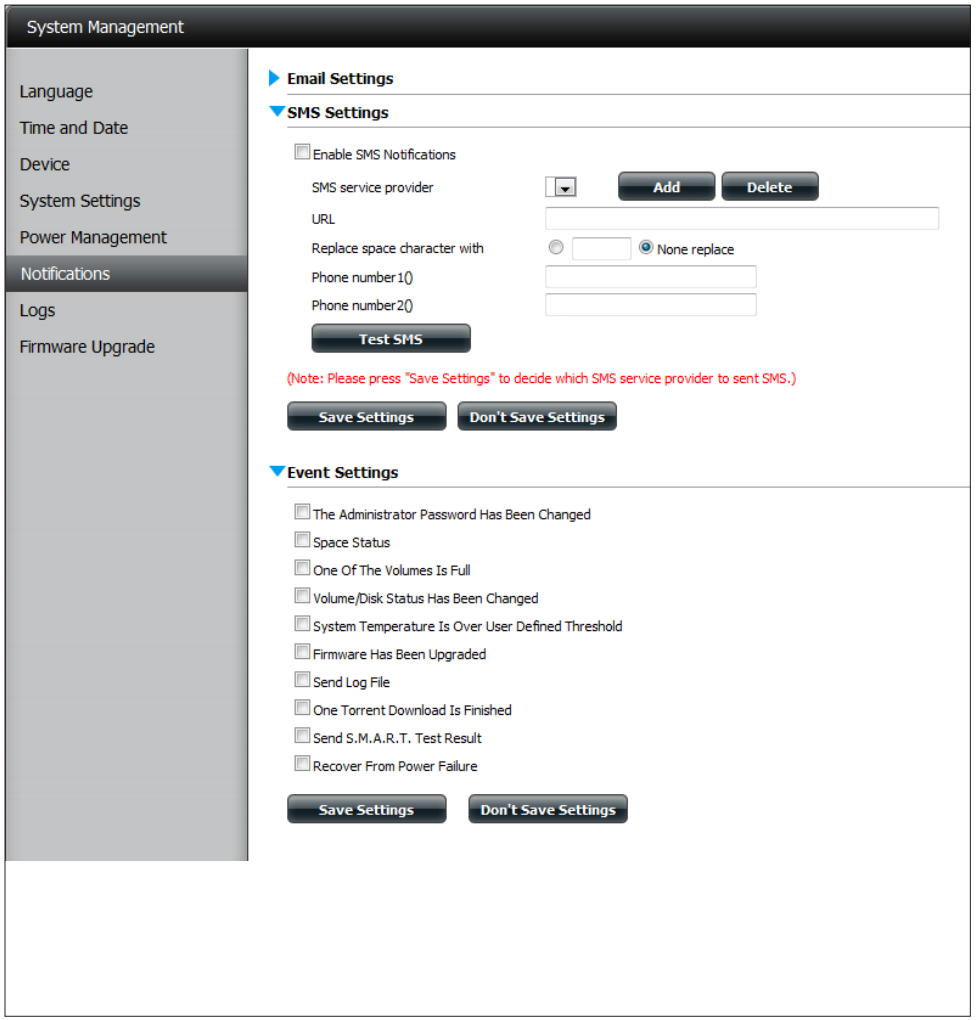


Choose the appropriate type parameter in the drop-down menu for the parsed parameters of the URL on the left.

Event Settings

You can limit which events are sent as alerts to the Email or SMS settings by checking the events here.

Event Settings: Select the information you want e-mailed to the above address or sent over SMS messages to the above mobile number. The items checked will be sent when necessary.



Logs

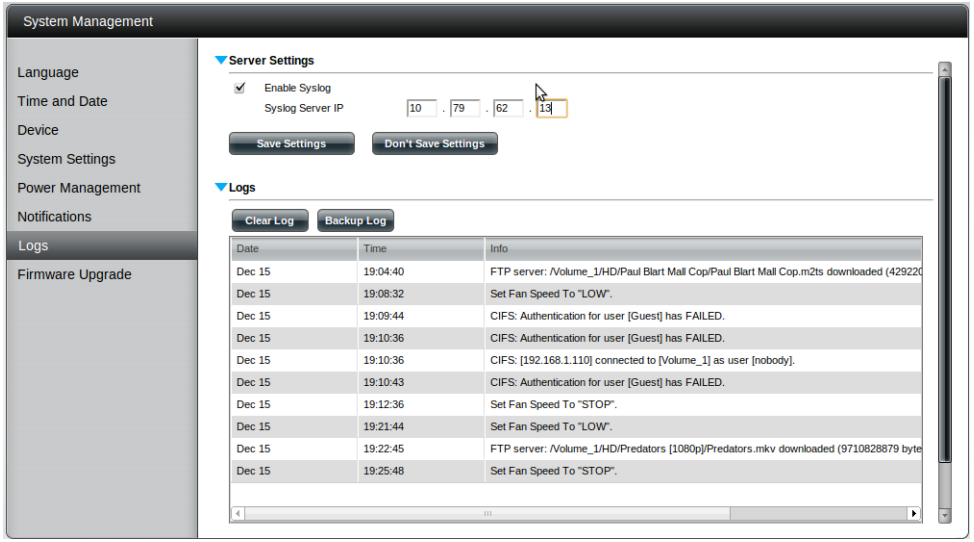
Within the Logs menu item you can setup your device to receive Log Events from other ShareCenters or send the log events to another ShareCenter or SysLog server. You can also view the NAS system logs and the FTP logs here.

Enable Syslog: Click to activate the Syslog server functionality of your device to be able to receive logs from other ShareCenters.

Syslog Server IP: Enter the IP address of an external Syslog server that you wish to send the logs of this device to.

Clear Log: Click **Clear Log** to delete all the existing logs.

Backup Log: Click **Backup Log** to save the existing logs to a text file on your computer.



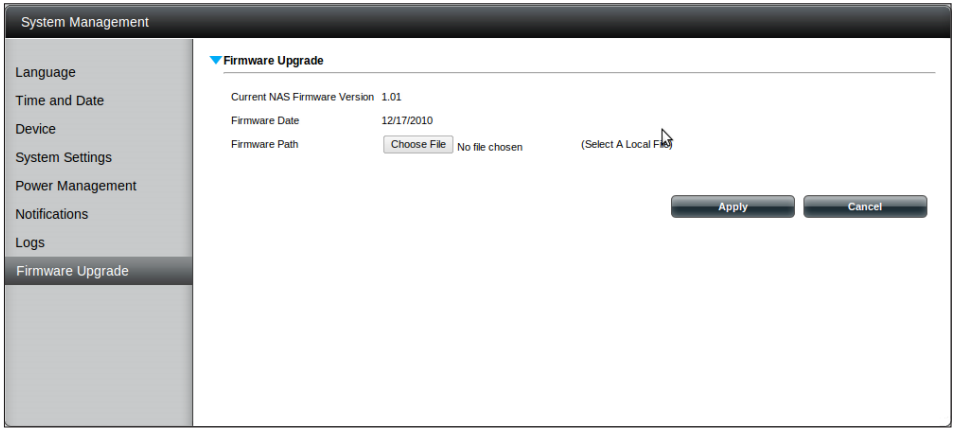
Firmware Upgrade

The Firmware Upgrade Page makes it simple to check for new firmware releases and upload them to the device. This section provides a link to check for new firmware on the D-Link support website. If a new firmware is available, download the file to your local computer.

Current Firmware Version: Displays the current firmware version on your ShareCenter® device.

Firmware Date: Displays the date of when the firmware was created.

Firmware Upload: When upgrading the firmware, click **Browse** to select the new firmware file on your local computer and then click **Apply** to begin the firmware upgrade process.



Status

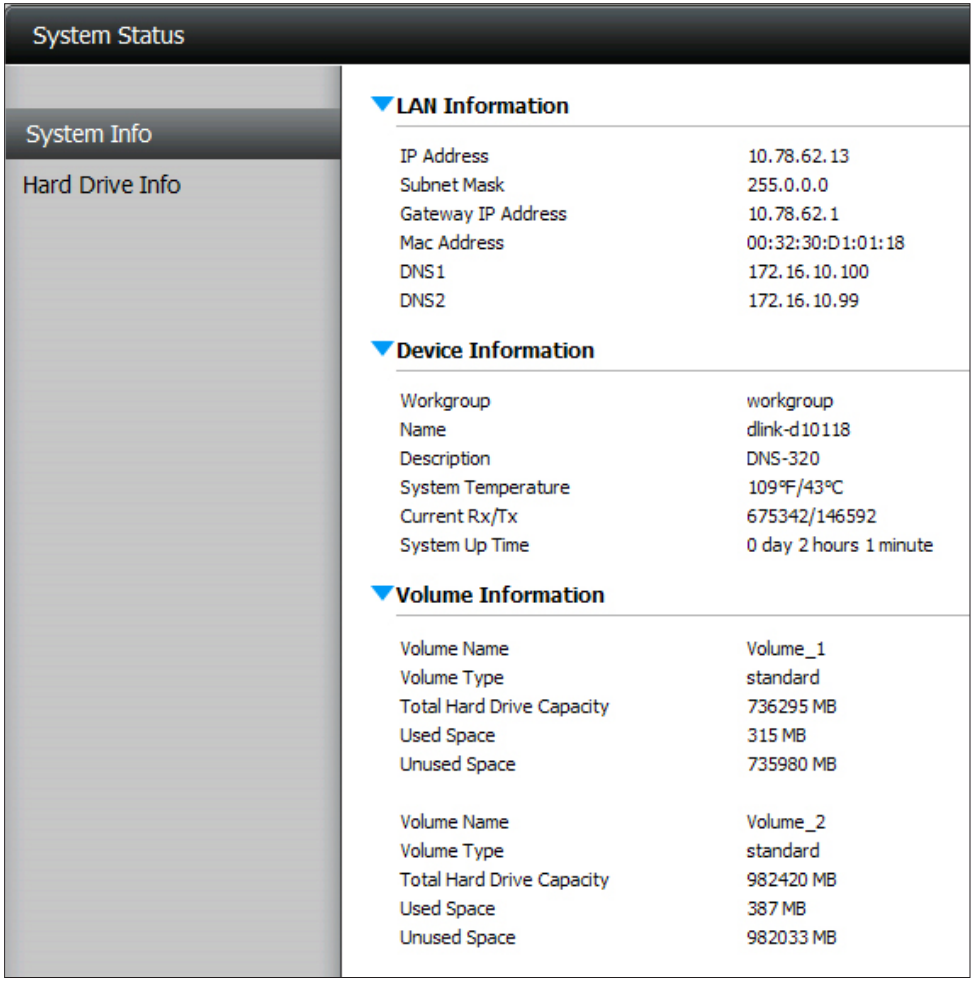
System Info

Here you can view various system information some of which is static and others dynamic.

LAN Information: Displays the local network settings of your device.

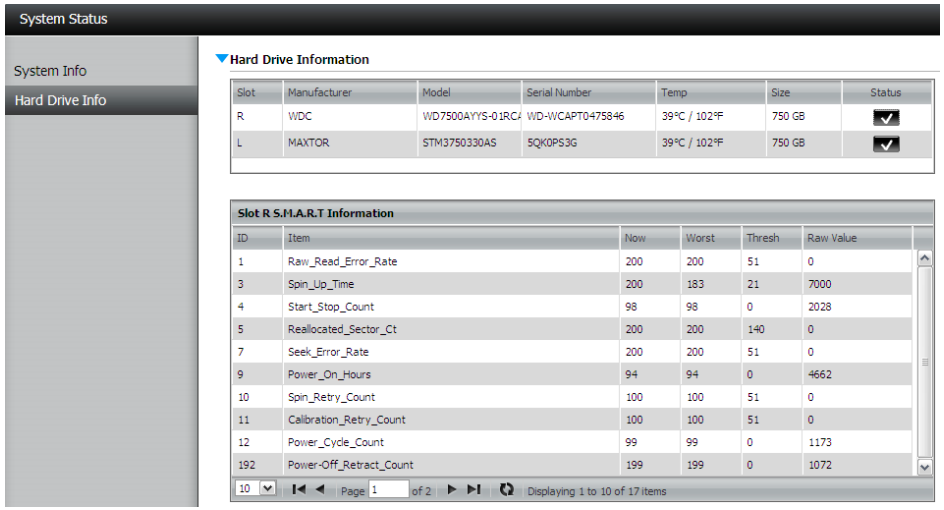
Device Information: Displays the workgroup, name, description, current temperature, packet counts, and system uptime.

Volume Information: Displays the hard drive information, including the disk mode, total size, used and remaining drive space.



Hard Drive Info

This section will display a summary of the hard drive(s) currently installed. The summary will include information such as the hard drive manufacturer, model, serial number, temperature, total capacity size, and status. The "Status" of the hard drive will display the health of the hard drive. If your hard drive is healthy, the status will display "Normal". If your hard drive is not healthy, the status will display "Abnormal". At any time, if you wish to view the S.M.A.R.T table of the hard drive, you can press the "Normal/Abnormal" button. After pressing the button a table appears with the S.M.A.R.T. data below the table of the Hard Drives installed.



Applications

FTP/HTTP Downloads

Schedule file and folder backups from an FTP server, web server, or local network share. Always test the URL before applying changes. This will help to ensure a successful download.

Category: Use the radio buttons to select the type of server that the source files/folders for the Schedule Downloads are located on. Click the **HTTP** radio button to specify that the source files are located on a web server. Click the FTP radio button to specify that the source files/ folders are located on an FTP server.

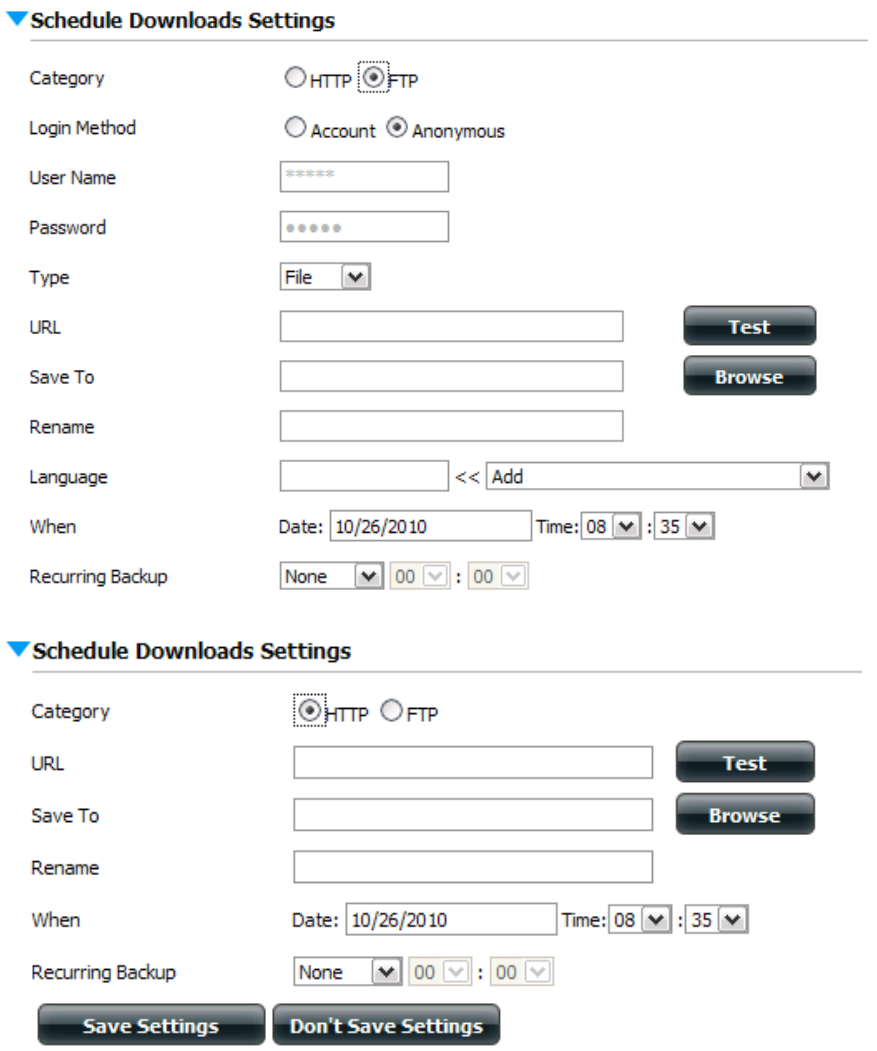
Login Method: Enter the login information for the site that contains the files that you want to schedule for downloading. If no password is required, select **Anonymous**. If a password is required, select **Account** and provide the user name and password.

Username: Enter the user name here.

Password: Enter the password here.

Type: Select either **File** or **Folder** from the drop-down list depending on whether you wish to download a file or a folder. Select **File** if you wish to download a specific file. Select **Folder** if you wish to download all the files in a specific folder.

URL: Enter the FTP/ HTTP site address for the scheduled download. Click on **Test** to verify access to the site address and file/folder. If you have chosen **File** from the above drop-down list, you must specify the exact file in the URL path, including the file extension. (e.g. http://example.com/test/testfile.txt).



Save To: Enter the specific destination on the internal drives for the downloaded files or folders to be saved to. Click **Browse** to browse the internal drives.

Rename: If you would like to rename a file after it has been downloaded from the specified HTTP/FTP server, enter the name you would like the file to be renamed to in this field.

Language: Use the drop-down menu to select the language used in the file or folder that you are trying to download.

When: Select the date and time for the download to occur.

Recurring: If you wish to schedule a recurring backup, select the desired interval (daily, weekly, or monthly) and the time you want the backup to start.

Incremental Backup: This type of backup, if used, will compare files of identical names on both the source and destination folders. If the source file was modified later than the destination file, the source file will overwrite the existing (old) destination file. If the source file is the same as the destination file, no action will be taken.

Schedule Download List: Pending and completed download events will be listed here. The current status for each event is displayed here. In addition, there is an option to delete a download event at anytime. Current download statistics, such as % completed and download speed, are displayed for each event. A refresh button is also provided to produce updated listings at any time.

Remote Backups

Remote Backups allows you to back up your device to another ShareCenter or Linux Server or vice versa from a remote ShareCenter or Linux Server to your device. Click the **Create** button in the remote backups list to start a wizard where you can configure the Remote Backup functionality.

Enable remote backup service: Check this box to enable the remote backup server functionality to that a remote NAS or Linux.

Note: If you are not using the Remote Backup functionality leave this box unchecked so that your device performance will not be affected by the additional overhead used by this process.

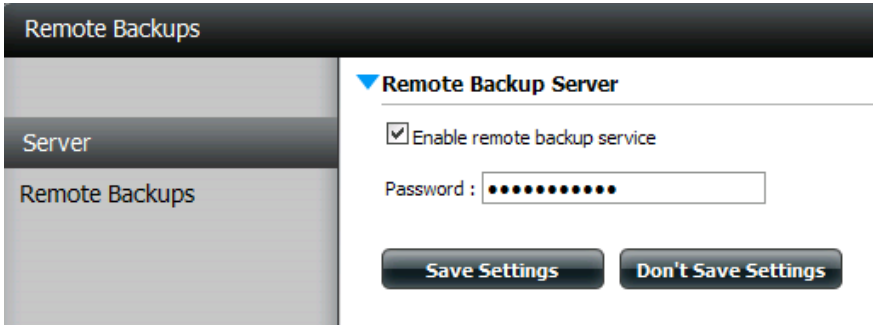
Password: Enter a password that the remote client will use.

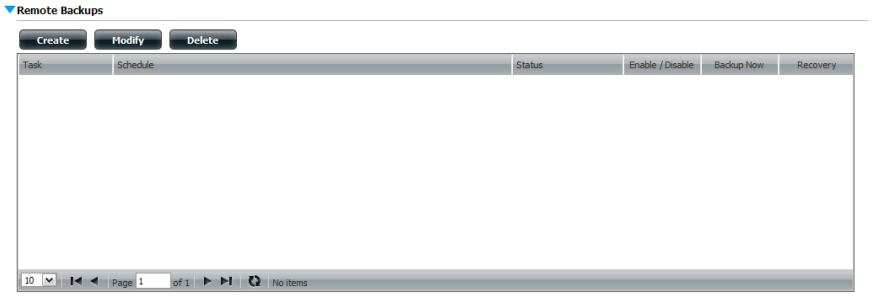
Remote Backups list: This is the list of remote backup jobs built by pressing the **Create** button above the list to configure each job.

Create: Click the **Create** button to build a new remote backup job.

Modify: Click to make changes to your existing Remote Backup jobs in the Remote Backup list. You must select the remote backup job first and then click the **Modify** button.

Delete: To remove a Remote Backup job select the job in the list and then click the **Delete** button.

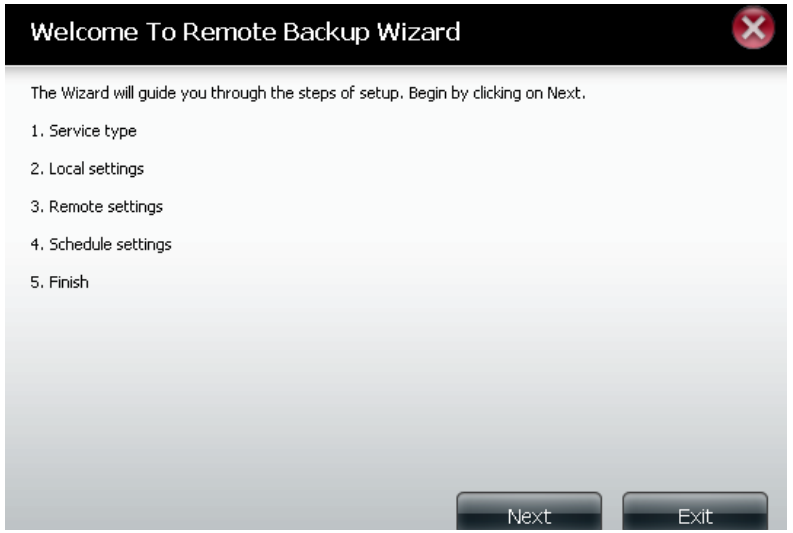




Remote Backups - Create wizard

When you click the **Create** Button above the Remote Backup list this wizard will launch allowing you to configure a new Remote Backup job.

Wecome: Displays the steps of the wizard.

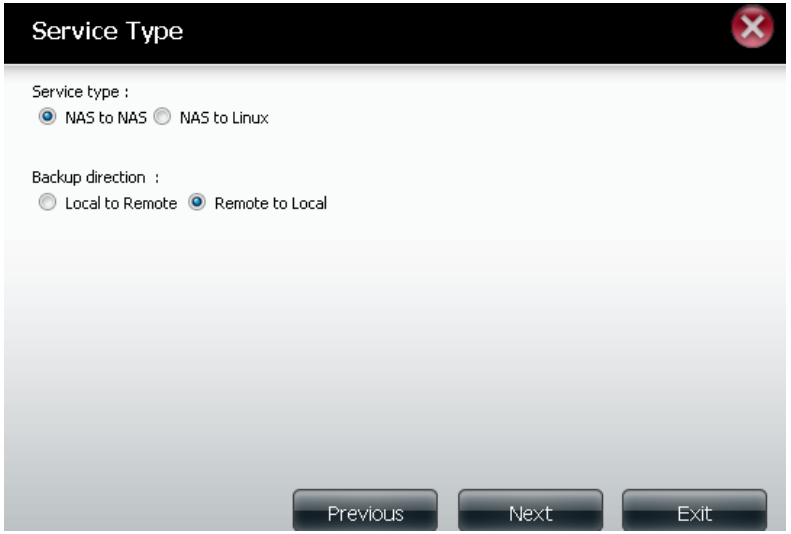


Service Type: **NAS to NAS**: Backup from the local NAS to a remote NAS or vice versa.

NAS to Linux: Backup from the local NAS to a Linux file system or vice versa.

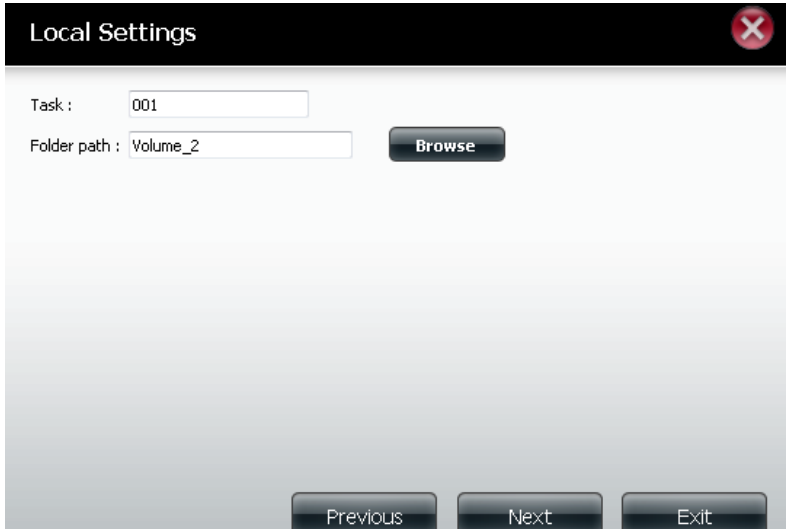
Local to Remote: Sets the backup source as the local NAS and the target destination for the backup files as the remote NAS or Linux file system.

Remote To Local: Sets the backup source as the remote NAS or Linux file system and the target destination for the backup files as the local NAS.



Local Settings: **Task (Name):** The name used to refer to the backup job which will be listed later in the Remote Backup list.

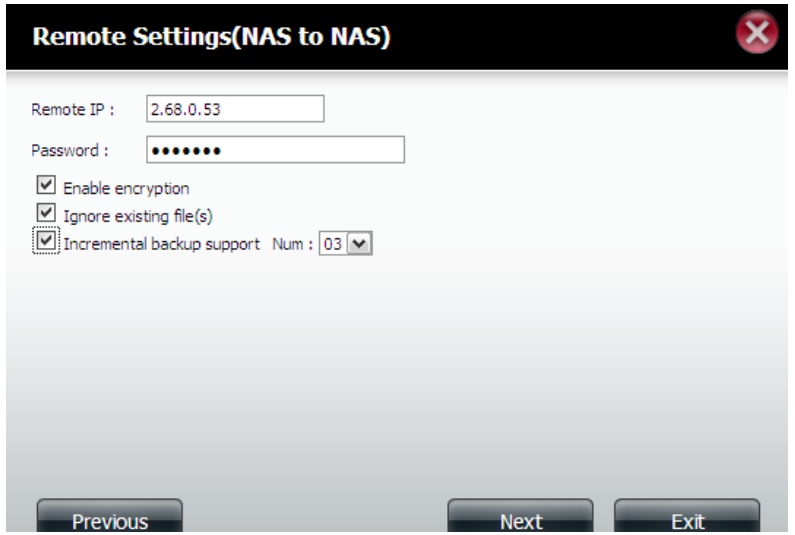
Folder Path: Select a local network share folder or file as the target or source for the backup job.



Remote Settings: **Remote IP:** The backup process uses Rsync protocol and needs to know the IP address of the destination source or target device for the backup. Input the IP of the remote NAS or Linux file system.

Enable Encryption: Checking this box will enable SSH encryption of the files that are transferred (backed up) over the network between the local and remote devices.

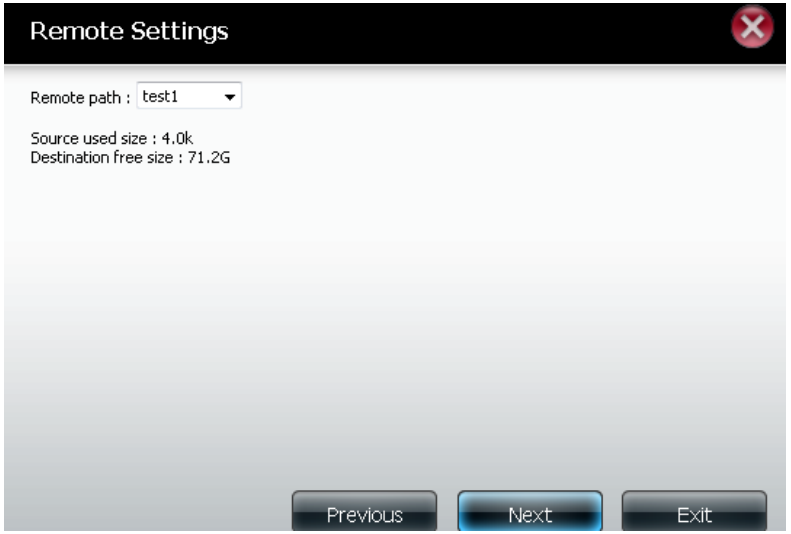
Ignore existing file(s): Checking this box prevents the backup process from writing over any files in the target file system that are not part of the backup files or folders. Therefore any existing files in the target system are preserved.



Incremental backup support Num (#): Checking this box provides multiple backup-capability at scheduled times. The first backup in an incremental series captures all the files for backup. Subsequent backups are incremental in that only the files and the folders that have changed in the backup source since the last incremental backup will need to be backed up. Each incremental backup builds a complete snapshot of the backup source however only the initial backup contains all the original files and folders. The subsequent backups in the incremental series contain new files and folders plus the links to the first incremental backup.

Remote Settings:

Remote Path: Using the drop-down menu, select the file system (folder) path to the remote target or source system for backup.

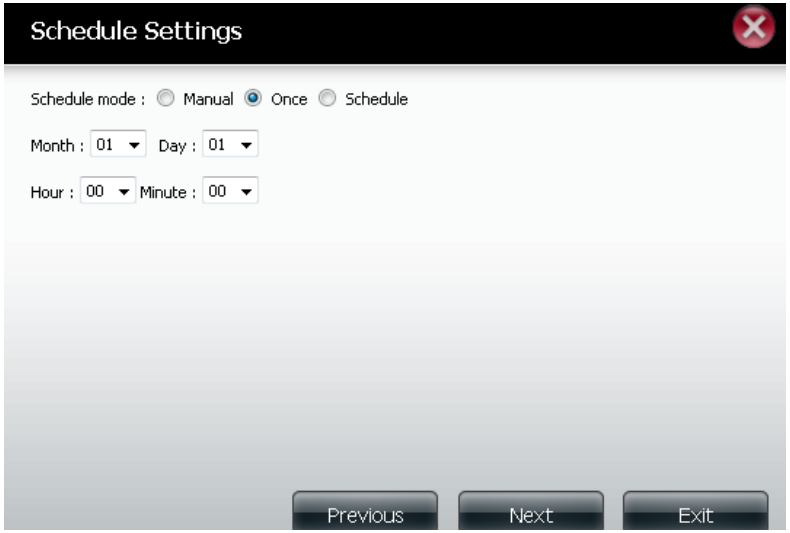


Schedule Settings:

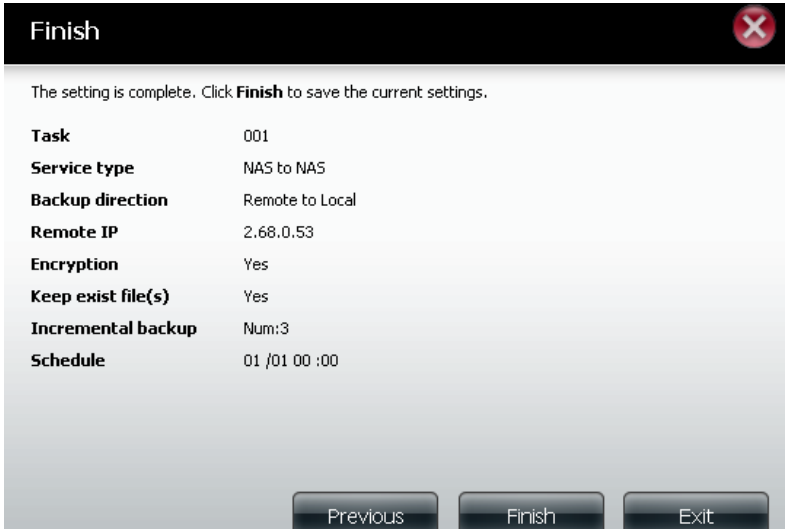
Manual: Check either **Yes** or **No** selection below to start the backup (yes) immediately on completion of the wizard or (no) manually start the backup from the Remote Backup list.

Once - Select this option to run the Remote Backup once at a specific date and time set.

Scheduled: Select this option to set the backup to occur daily, weekly, or monthly per a specific schedule.



Finished: Click on **Finish** if you are satisfied with all the settings of the Backup job created. Otherwise click on the **Previous** button to go back and make changes. Alternatively click on **Exit** to end the configuration without adding a Remote Backup job.



Remote Backups list:

Task: The name of the Remote Backup job.

Schedule: When the Remote Backup job will execute.

Status: Current status which can be

- Ready the remote backup job is ready to be executed.
- Finished the remote backup job has executed completely and successfully.
- Failed the Remote backup job was unsuccessful during execution.

Enable/Disable: If the button shows a red circle the remote backup job is enabled. Click the red button to disable the remote backup job and the button will change to a green triangle. Clicking the green triangle will enable the job again.

Backup now: Click to execute the backup job immediately as long as the job is enabled.

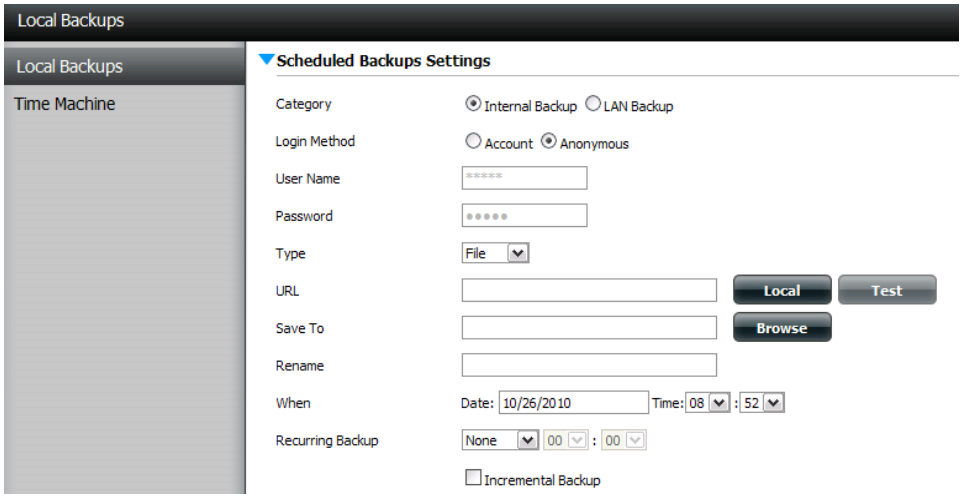
Recovery: Click to write the backup files and folders back into the source file system from the backup target system (reverse the file direction).

Navigation buttons: Use these buttons to move up and down in the list when there are multiple jobs configured.

Refresh Button: Click this button during a backup or recovery process to monitor the progress by updating the progress completed bar.

Local Backups

Schedule local file and folder backups from the local network share of the device or from the local computer. Always test the URL before applying changes. This will help to ensure a successful download.



Category: Use the radio buttons to select the backup method. If your NAS device has two volumes you can click the Internal Backup radio button to backup the data from the first volume to the second volume and vice-versa. The Internal Backup feature also allows you to backup an existing folder on a volume to another folder on the same volume but nested folders in the same volume are not allowed.
If you want to backup the data from your PC or another NAS device to your NAS device, click the LAN Backup radio button.

Login Method: Enter the login information for the site that contains the files that you want to schedule downloads from. If no password is required, select **Anonymous**. If a password is required select **Account** and provide the user name and password. This option is only available for LAN Backups.

Username: Enter the user name.

Password: Enter the password.

Type: Select **File** or **Folder**, depending on what you want to download or backup.

URL: Enter the URL of the site or server you are initiating a transfer from. E.g. ftp://123.456.789/Test or ftp://123.456.789/test.txt

Save To: Enter a valid destination drive on the device, or click **Browse** to select the destination.

Rename: Enter the renamed file name here.

When: Enter the date and time you want the scheduled backup or download to initiate.

Recurring Backup: Designate the interval and time you want the backup or download to run unattended.

Incremental Backup: By default all local backups and file/folder downloads are in Overwrite mode, meaning that identical files in the destination folder will be overwritten by the source files. Checking Incremental Backup will have the device compare identical file names at the source and destination. Files will only be overwritten if the source file is more recent.

Local Backups - Time Machine

This section allows the user to configure the device so that it becomes a backup destination in the Mac OS X Time Machine. In order to use this function, the AFP service is required. The AFP service will start automatically as soon as this function is enabled.

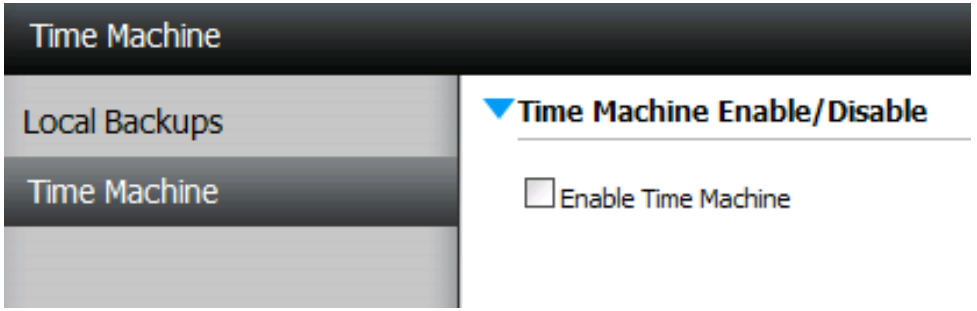
Enable Time Machine: Click this to enable the Time Machine function to work with a MAC OS X Time Machine. The Time Machine Settings list will appear when this checkbox is ticked.

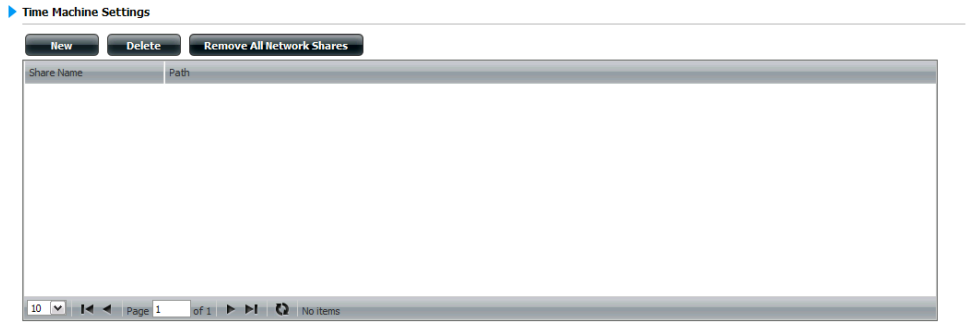
Time Machine Settings list: A list of destination folders on the Network Shares associated with the Time Machine backup.

New: Click to add a NAS folder as a Time Machine destination.

Delete: Click to delete a NAS folder setup.

Remove all Network Shares: Deletes all of the NAS folders in the list.





P2P Downloads - Settings

Within this menu you can configure the P2P download management settings.

P2P: Select **Enable** or **Disable**.

Disable: In the block provided the user can configure the running schedule for P2P downloads. Simply select the Start and Stop block for the appropriate day and time.

Auto Download: Select **Enable** or **Disable**.

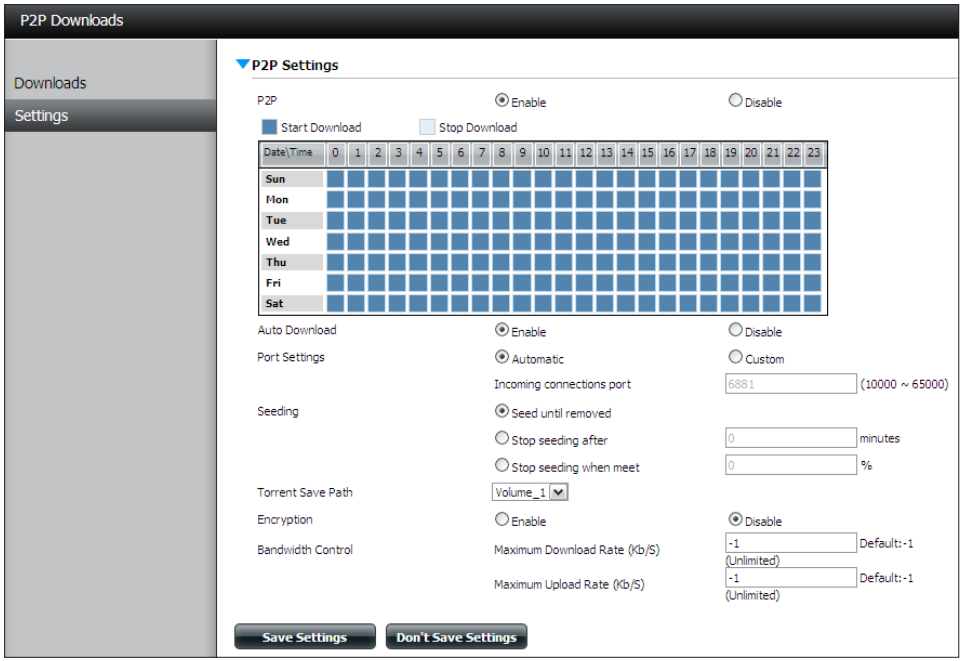
Port Settings: Click Enable to allow the device to automatically choose incoming connection port or click **Custom** and configure the incoming connection port manually.

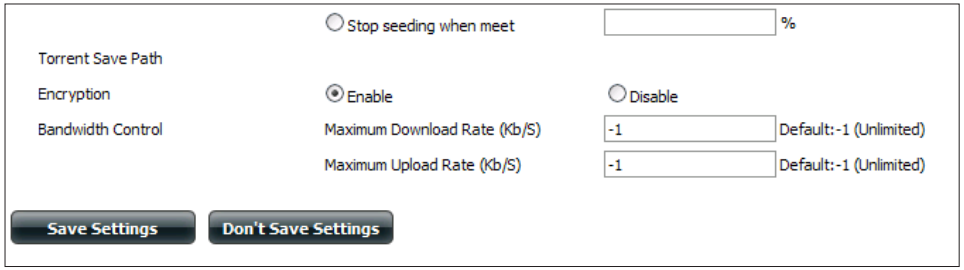
Seeding: Select one of the three seeding options.

Torrent Save Path: Displays the volume where the Torrent will be saved.

Encryption: Select **Enable** or **Disable**.

Bandwidth Control: Configure the maximum download rate and maximum upload rate. Enter **-1** to set the respective field to *unlimited*.





P2P Downloads - Downloads

Configure the Peer-to-Peer download manager settings.

Add Torrent from URL: In the field provided you can copy and paste a link to a torrent file hosted on the Internet. The P2P download manager will add the torrent file to the download manager and download your files.

Add Torrent from File: Browse for a torrent file you have downloaded onto your PC.

P2P Downloads list: This window will display all the running tasks.

Remove Completed: The user can click on the **Remove Completed** button to remove completed downloads.

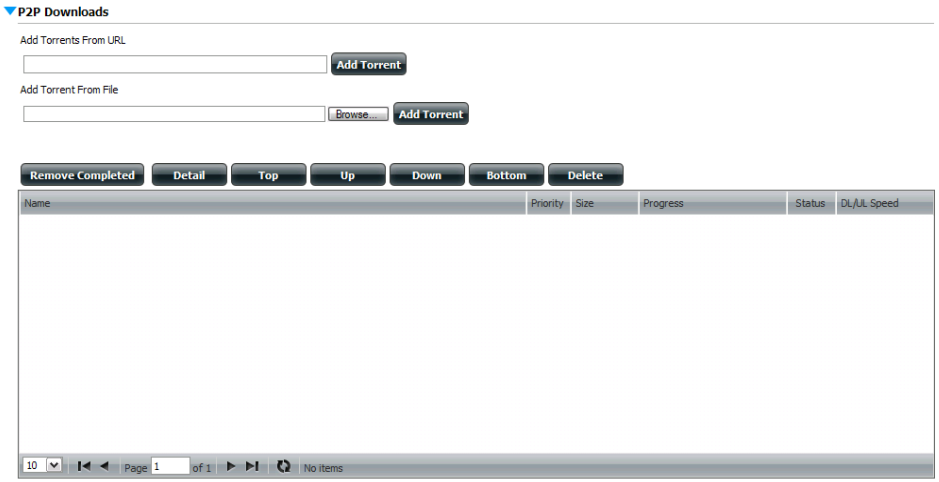
Detail: Click **Detail** to view the files that are being downloaded for each torrent.

Top, Up, Down, Bottom: Click **Top**, **Up**, **Down** and **Bottom** buttons allows the user to move the selected P2P download in the task list. The downloads at the top of the list have a higher priority than the ones listed below them.

Delete: Click **Delete** to remove a selected download. This will remove not only the torrent file, but also the partially downloaded files too.

Start / Stop: The start and stop button allows the user to start and stop selected P2P downloads in the task list.

Torrent Scheduling: Click the **Torrent Scheduling** button to configure a scheduling rule for the select P2P downloading task.



Navigation: At the bottom of the P2P Task window there are a couple of navigation controls. When multiple tasks exist, the user can select how many tasks will be displayed by using the drop-down menu. The user can also navigate to next pages when more than one page exist.

Refresh: Click **Refresh** to refresh the P2P task list to display the most updated statistics.

Web File Server

Whenever you cannot mount the network shares of your NAS, use the Web File Server to access the files using a browser over the Internet. If the network that your device is connected to is using NAT, you will need to forward HTTP port 80 across your router for access over the Internet.

Up: Click the **Up** button to go up (or back) one directory in the folder structure of the network share selected.

Upload: Select a destination folder in a network share by navigating in the folder view on the left. Click the **Upload** button to open a dialogue window where you can browse to select a file on your computer for uploading to the selected destination folder.

Download: Select a file for download to your computer by navigating in the folder view on the left. Click on the file. Once the text turns red, click on the **Download** button and save or open the file as needed. You may select multiple files at the same time by holding the CTRL key and clicking on the files you want to download.

Refresh: Click the **Refresh** button to update the folder and file view of the Web File Server.

Download: Downloads the selected file to your computer.

Copy: Click to copy the file to the clipboard. A wizard will launch and allow you to select the folder to paste the copy of the file to. Once you have selected the folder, click **OK** to paste the file in that folder.

Move: Moves the file to a new folder.

Delete: Removes the selected file.

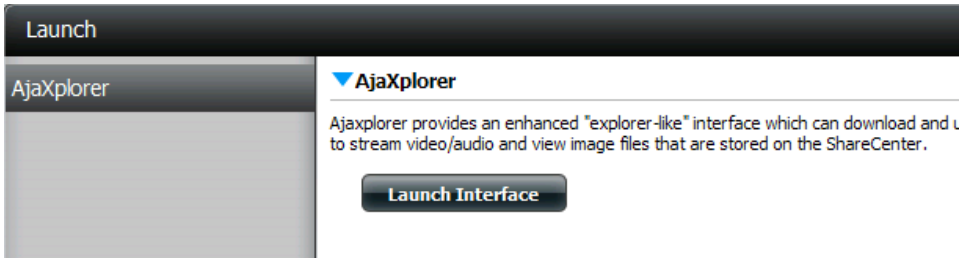
Rename: Allows you to configure a new file name for the selected file.

Properties: Displays the file properties such as ownership, access rights and modify time.

AjaXplorer

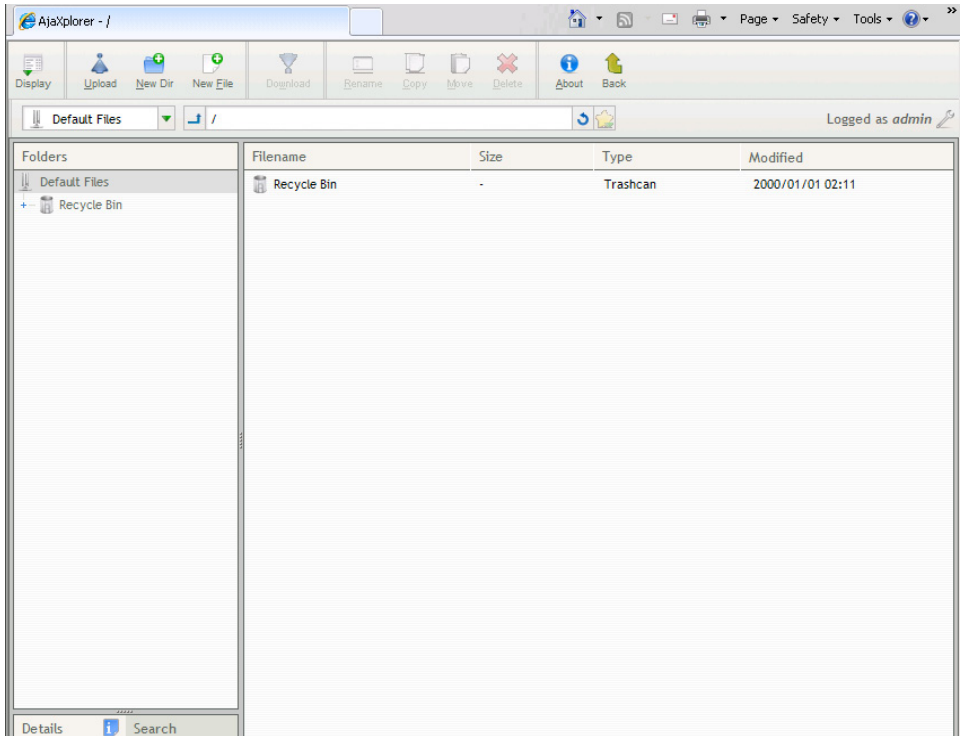
This section allows you to configure the AjaXplorer function. AjaXplorer is a file explorer that allows you to remotely manage the files stored under the AjaXplorer folder by using a web browser.

Launch Interface: This launches your browser with the Ajaxplorer file system interface to the ShareCenter®.



Documentation: Information regarding using the Ajaxplorer application can be found here:

http://www.ajaxplorer.info/



Administrator: If you launched the interface as the admin user in your ShareCenter® then you will have administrator rights within the AjaXplorer interface. As the admin user you will have read write access to all areas of the files systems as well.

User: If you launched the interface as a configured user in your ShareCenter® then you will have the users rights within the AjaXplorer interface. That users read/write access privileges to the shares of the ShareCenter® will be applicable within the AjaXplorer interface as well.

My Favorites

The My Favorites tab allows you to add any icon you routinely access from the Applications or Management Tab in one convenient location for easy and quick access. You can add icons to the My Favorites tab using two different methods:

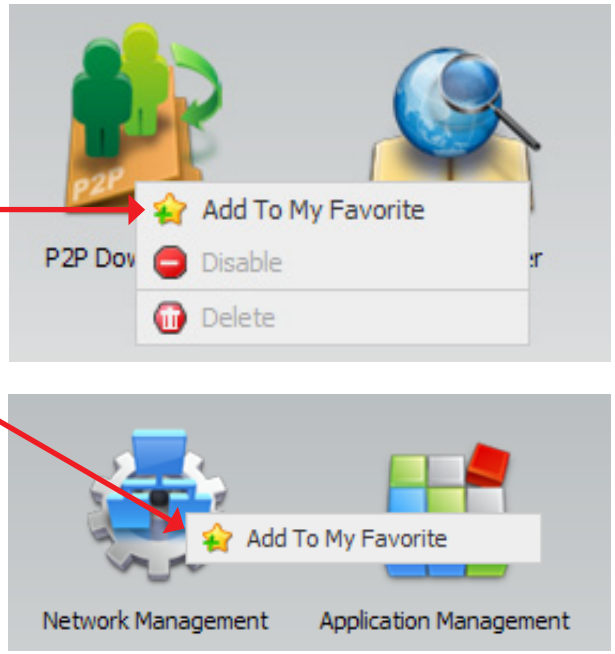
Re-arranging the My Favorites View

Within the My Favorites tab you can arrange the layout of the icon order according to your needs. To move the position of an icon, click and drag the icon to a new position anywhere in the current icon locations. Once you have dragged the icon to the new location, release the mouse button and the other icons will automatically reorder themselves.

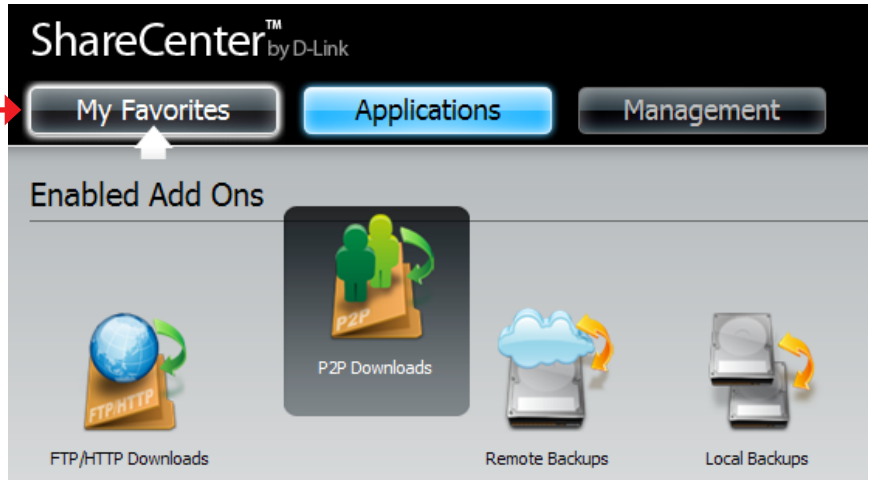
Add an Icon to My Favorites

There are two methods to add an icon alias to My Favorites. You can either right-click the icon and select **Add to My Favorites** or use the Drag and Drop method as per item 2 below.

1. Right-click on an icon in the applications or management tab and click on the **Add to My Favorite** menu item from the command list that appears.



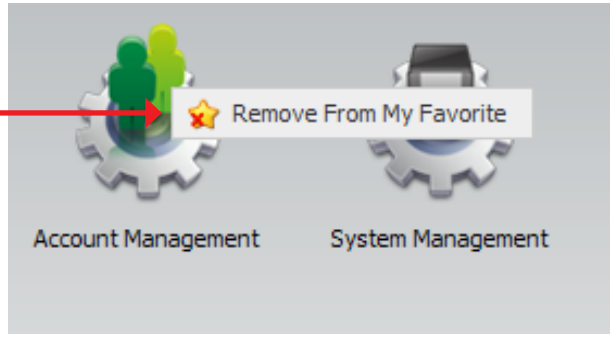
2. While holding the left button down over the icon drag it over the My Favorites tab (drag and drop method). You will see an white arrow pointing to the My Favorites tab which is highlighted when you start to drag the icon



Remove an Icon from My Favorites

To remove an icon alias from the My Favorites tab simply right-click on it and select **Remove From My Favorite** in the context selection that appears.

Right-click an Icon alias in the My Favorites tab and select **Remove From My Favorite** option. The Icon alias should disappear from the My Favorites tab view.



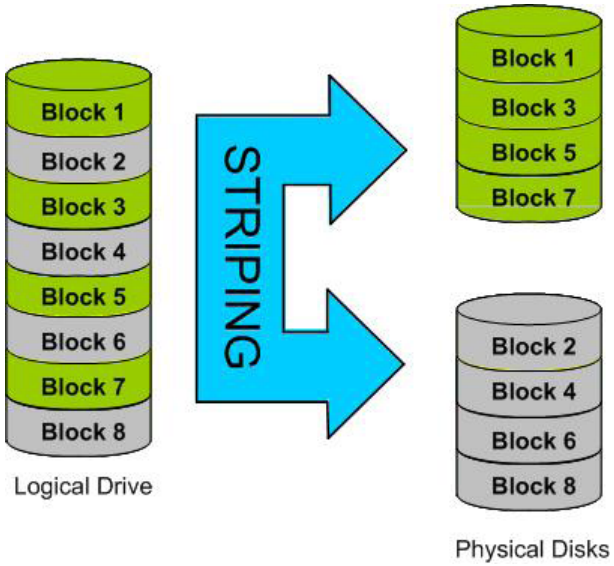
Knowledge Base

What is RAID?

RAID, short for Redundant Array of Independent Disks, is a combination of two or more disks with the aim of providing fault tolerance and improving performance. There are several different levels of RAID, with each one providing a different method of sharing or distributing data among the drives. The device supports JBOD, RAID 0, RAID 1, and Standalone.

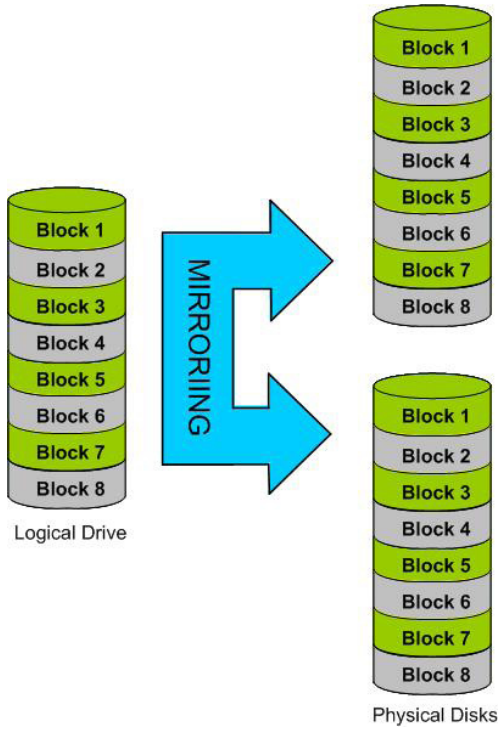
RAID 0 RAID 0 provides data striping, which spreads out blocks of data over all drives, but does not provide data redundancy.

Although performance is improved, the lack of fault tolerance means that if one drive fails, all data in the array will be lost.



RAID 1 RAID 1 provides mirroring over multiple disks, with the same read/write speed of a single disk. A RAID 1 array can only be as large as it's smallest member disk.

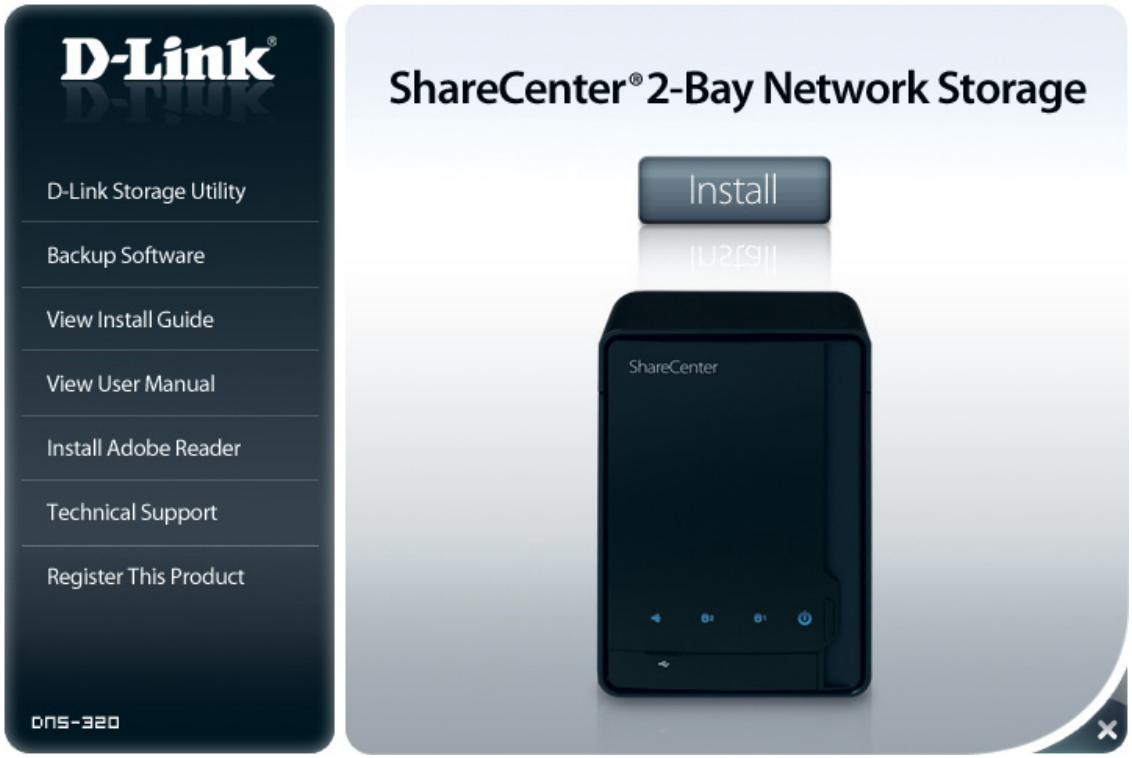
Because the data is stored on multiple disks, RAID 1 provides fault tolerance and protection, in addition to performance advantages.



Mapping a Drive

You can use the D-Link Storage Utility to map drives to your computer. Insert the ShareCenter® CD into your CD-ROM drive.

Click **D-Link Storage Utility**



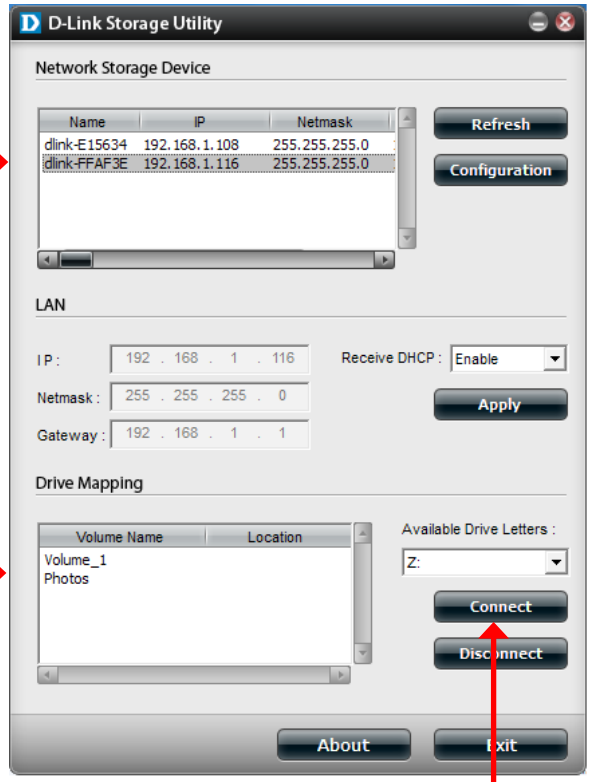
The Storage Utility will load and detect any ShareCenter® devices that are on the local network.

If the device you are working with does not show up in the device list, click **Refresh**.

Highlight an available device.

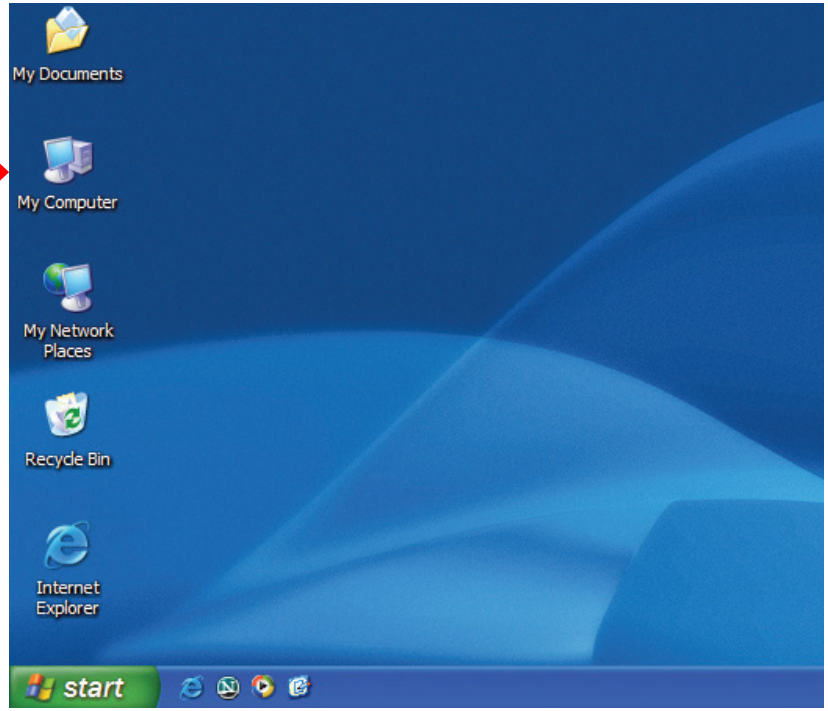
Available volumes will be displayed under Drive Mapping. Highlight the volume you want to map.

Select an available drive letter from the drop-down menu and click **Connect**.

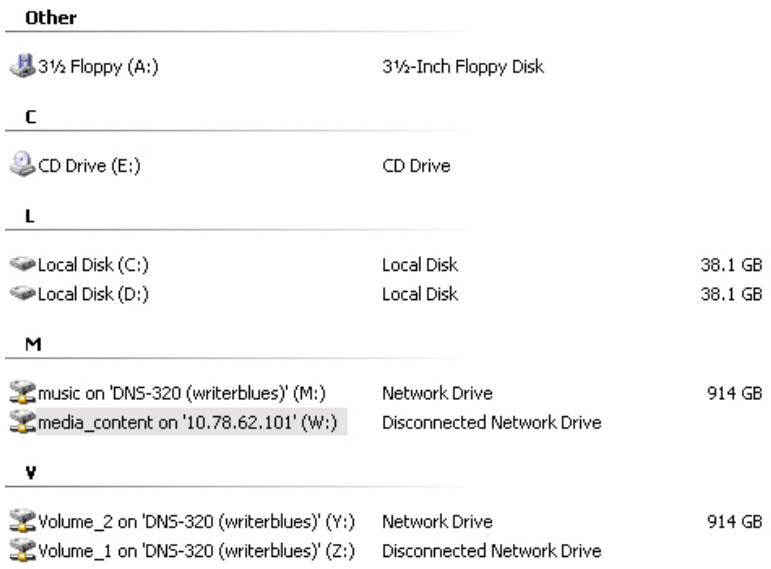


Once connected, your mapped drive(s) will appear in My Computer.

Double-click the **My Computer** icon on your desktop.



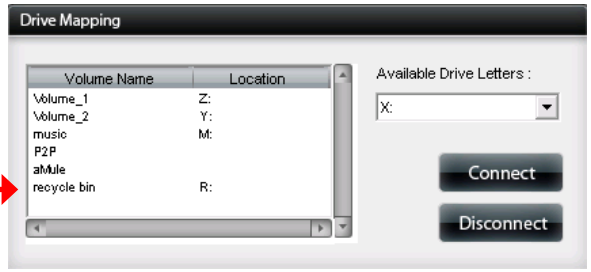
Double-click the mapped drive to access the files and folders.



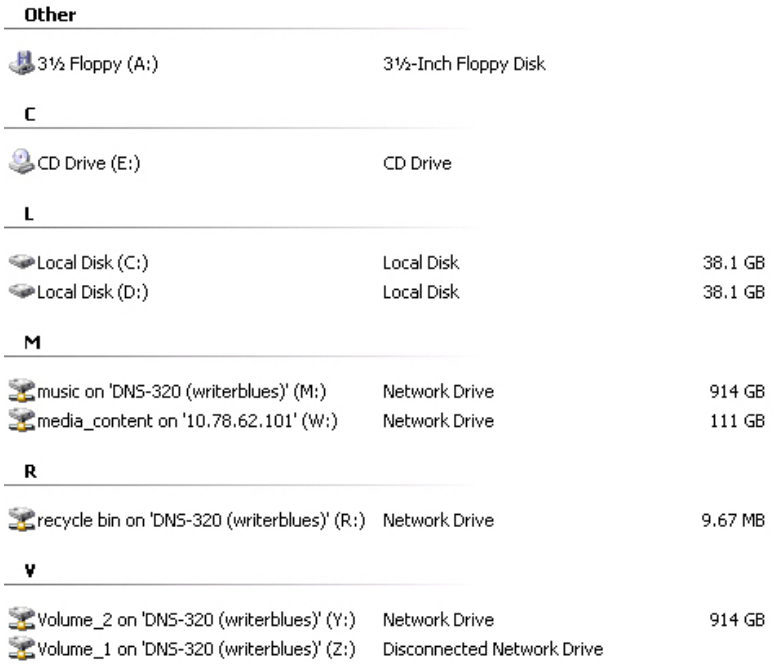
Mapping the Recycle Bin

If you have turned on the Recycle Bin option with any of your Network Shares created, then you can map the recycle bin as a Network Drive to have access to it.

The Recycle Bin will appear in the drive mapping area of the Storage Utility.



Once connected the Recycle Bin of the device will appear as a Network Drive.

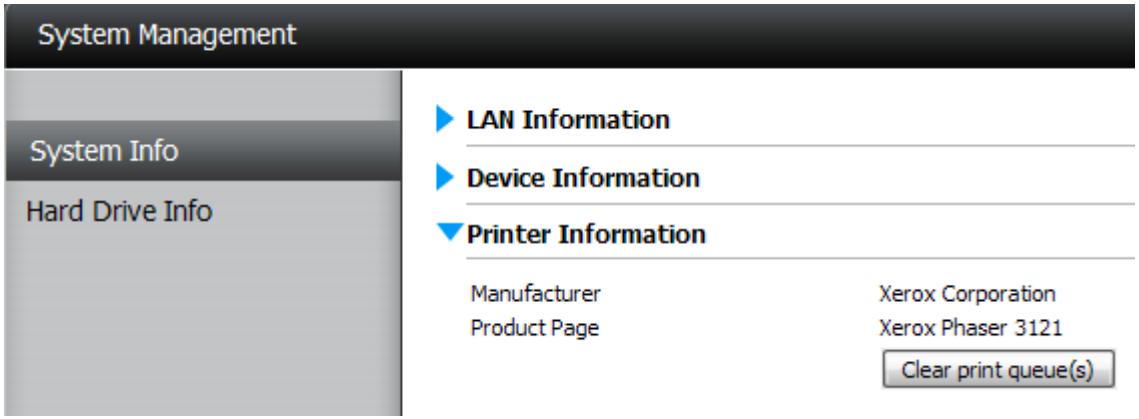


USB Print Server

The device features a built-in USB print server, giving users the ability to share a printer on their local network. Connect a USB printer to the USB port on the back of the device. It is important to ensure that any of the printer manufacturer's drivers are already installed or available on any computer you want to print from.

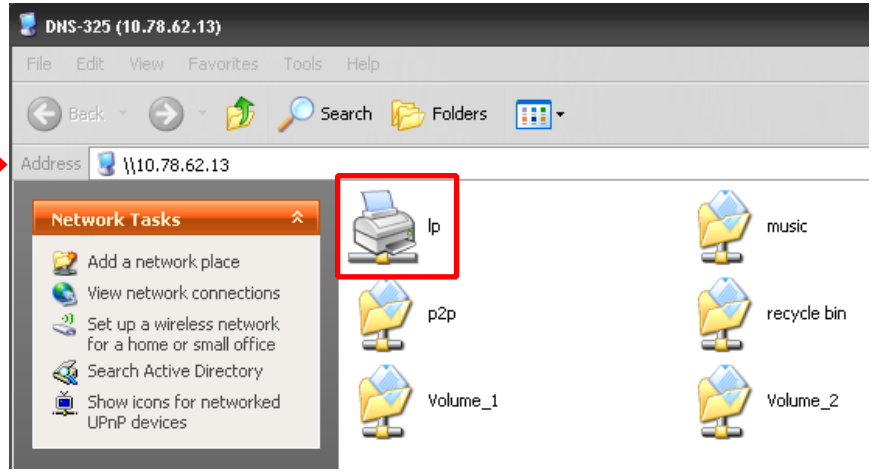
Note: Only the print function is supported. The device does not support the copy and scan functions of Multi-Function Printers.

To add a printer, connect your printer via USB cable to the USB port of your device:



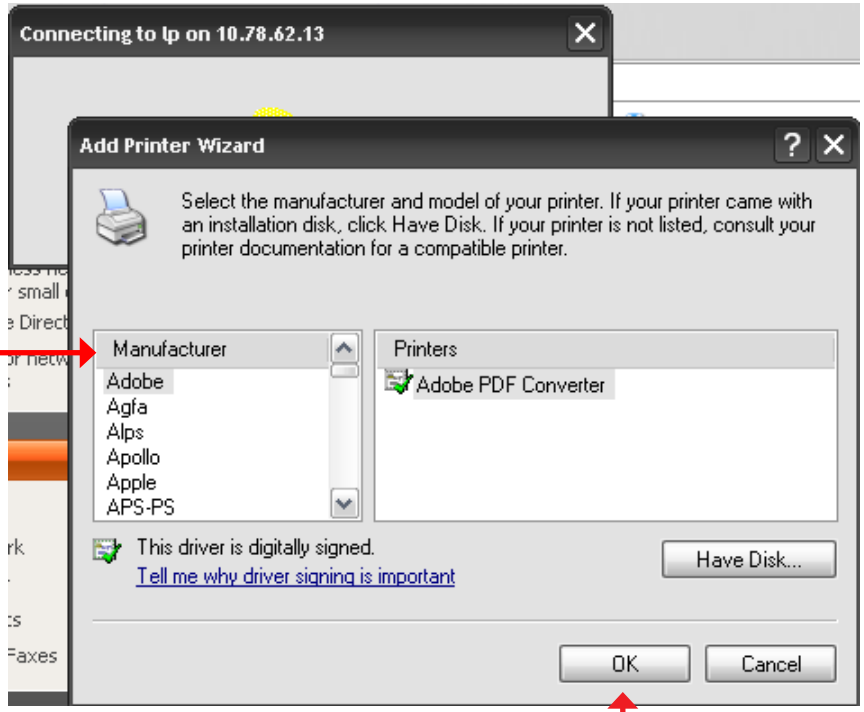
The printer should appear in your in the System Info menu of the Status icon.

Connect to your device with Samba and then double-click the lp icon.

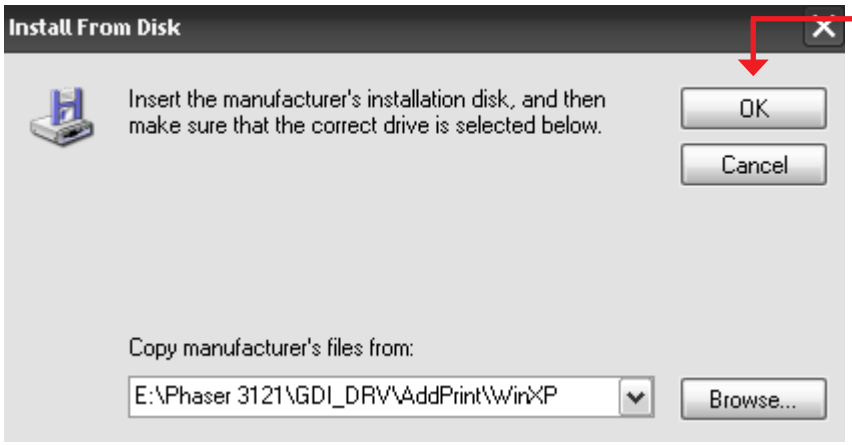


The Windows® Add Printer Wizard will launch:

Select the printer driver from the installed Manufacturer list or use the **Have Disk** button to browse for the printer driver file.

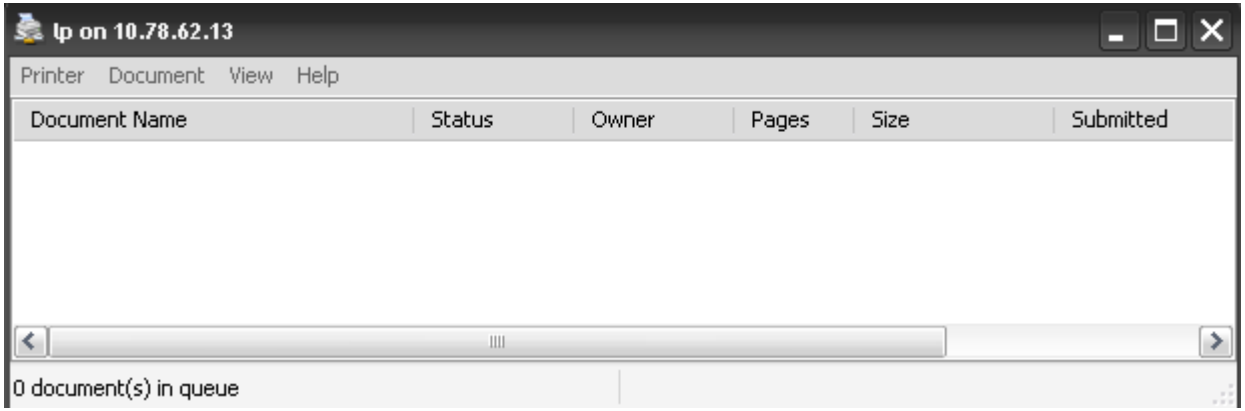


Click **OK** to continue.



Once you have selected the proper driver as shown in the browse list then click **OK** to install the printer.

The printer is now installed and the printer queue will appear.

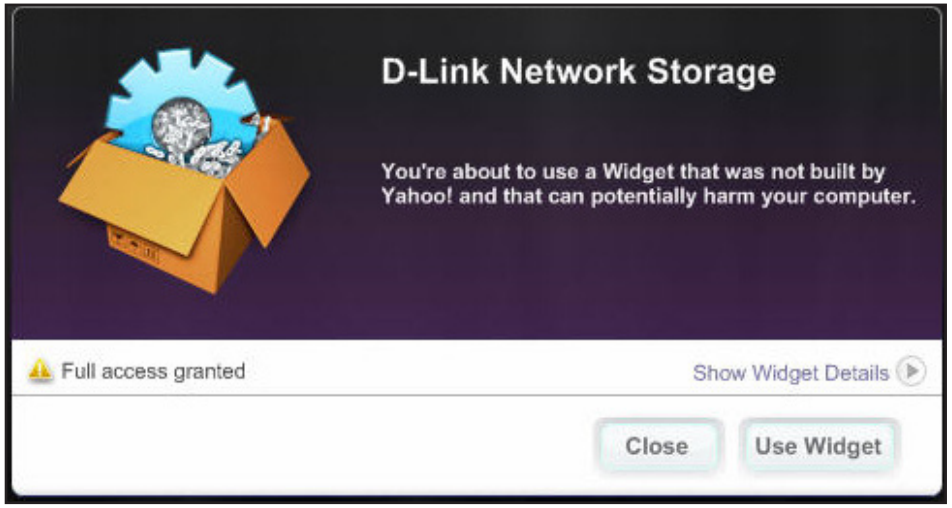


Yahoo! Widget Installation

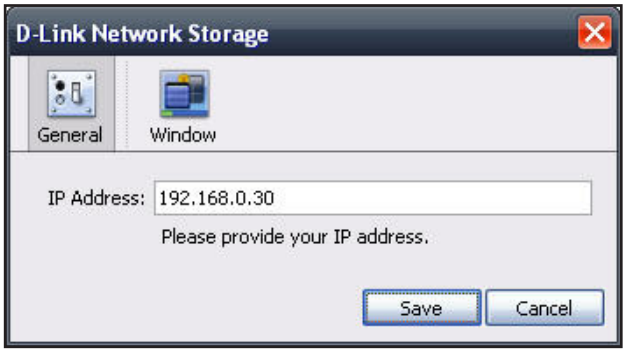
D-Link provides an added feature called a Yahoo! Widget.

What is a Yahoo Widget?
Yahoo! Widgets are free application platforms that can be used in Microsoft Windows and Mac OS X. The engine uses a JavaScript runtime environment combined with an XML interpreter to run small applications referred to as widgets, and hence is part of a class of software applications called widget engines.

Step 1: Install the Yahoo! Widget. Once the Yahoo! Widget is installed a D-Link icon will appear in your Widget Dock. Once you hover with your mouse over the D-Link Widget you'll be able to click the configuration button.



Step 2: Click the configuration button to configure the Widget. Enter the IP Address of your device and click the **Save** button. Now you are ready to use your new D-Link Yahoo! Widget!



Yahoo! Widget Display

The D-Link Widget is mainly used for monitoring the activities taking place.

System: In the System window information about your Computer, DNS-320, IP Address, Firmware Version and Current Operational Temperature are displayed.

Hard Drive: In the Hard Drive window information about the storage space of your device is displayed.

Server: In the Server window information about the USB Device, UPnP Server, ITunes and FTP Server configured is displayed.

Download: When the P2P Application is loaded, you can monitor your P2P download status here.

USB Copy Function

The DNS-320 supports on option where the user can enter a USB storage medium in to the USB port and with a click of a button automatically copy the contents of the USB storage medium into a folder on the device

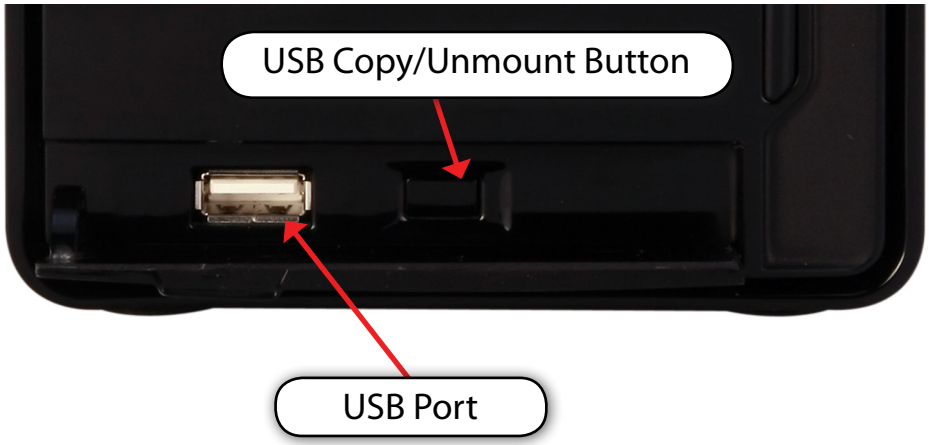
Step 1: Insert a USB storage device into the USB port, located on the front panel of the device. The USB Light on the front panel will start to flicker. Once the light is on solid, then the USB storage is ready for use.

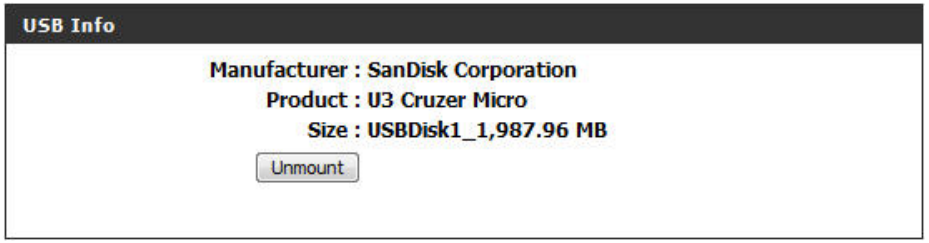
Step 2: To copy the contents of the USB storage to a folder on the device, press and hold the **USB Copy/Unmount Button** button for 1-3 seconds. The device will create a new folder in the Volume 1 folder and will copy all the files from the USB storage to this folder.

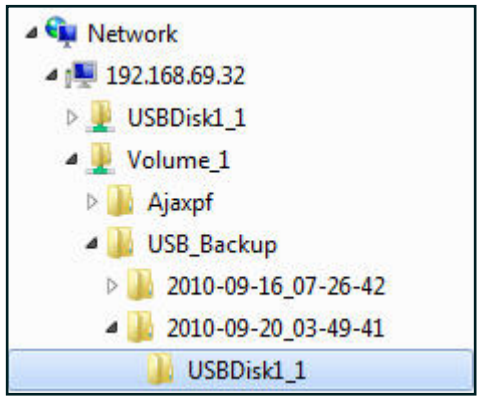
Step 3: To **unmount** the USB storage device after the copy is complete, press and hold the **USB Copy/Unmount Button** button for 5 seconds. When the USB light has switched off, then the USB storage un-mounted successfully and is ready to be removed.

To check whether the USB storage device is connected successfully, the user can navigate to the **System Info** menu of the **System Status** icon in the Management Tab of the Web GUI of the device and view the **USB Information** section.

Note: It is a very good practice to un-mount an USB storage device before removing it from a USB port.







Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DNS-320)
- Hardware Revision (located on the label on the bottom of the switch (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the device).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

For customers within the United States:

Phone Support:
(877) 453-5465

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(800) 361-5265

Internet Support:
http://support.dlink.ca

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor.
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware (excluding power supplies): Three (3) years
- Free Technical Support - Basic Installation: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim:

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.• The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:

The Limited Warranty provided herein by D-Link does not cover:
Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks:

D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright ©2011 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Registration

Register your product at http://registration.dlink.com

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0
January 14, 2011