freedom™

freeStor 4020

4-bay Desktop Network Storage

USER'S MANUAL

Rev. 2.0

P/N: N0042000

Copyright and Trademark Information

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

The freeStor 4020 is an intelligent network storage solution for small office, medium office, and home network environments. The freeStor 4020 features an integrated file server with system backup, system recovery, and managed shared files by user names or groups. The freeStor 4020 can connect to a Gigabit Ethernet network and can support up to 4 3.5" SATA (serial advanced technology attachment) hard disk drives (HDD). Its high performance is ideal for protecting valuable company data, and quickly restoring files from a backup. The freeStor 4020 offers a convenient graphical web user interface, and provides security by limiting access to shared folders by user or group level authentication.

The freeStor 4020 provides a complete and advanced data backup/protection solution including RAID and DiskSafe Express (DSE). The freeStor 4020 supports standard RAID levels 0, 1, 5 and 10. DSE is a powerful function to provide entire system backup and recovery for clients running Windows 2000, Windows XP or Windows Server 2003 in the event of hard disk failure in the client.

1.1 Terminology

For clarity, the OS X operating system will be referred to as "OS X" and Mac 9.0 and earlier operating systems will be referred to as "Mac" throughout the manual.

1.2 System Benefits and Key Features

- Music, Video, and Data file sharing among Windows, Linux, Unix and Macintosh users with username and password protected and managed access.

- Can act as a DHCP server or DHCP client for easy network configuration.

- Easy file sharing management via a user-friendly graphical web interface.

- Setup wizard for easy initial configuration.

- DSE provides system and data backup, remote boot and system and data restoration for Windows 2000, Windows XP and Windows Server 2003 clients.

- Built-in FTP server provides convenient high-speed file transfers.

- System software upgrade via web interface.

- RAID 0, 1, 5, and 10 support.

- System information for disk usage, service status, RAID, system log and current

connections.

1.3   Product Specifications

Hardware Specifications

Processor	Intel IOP80219 400MHz
Memory	DDR 256 MB
Flash	8 MB NOR Flash
HDD	Up to four 3.5" SATA Hard Disks from 80GB to 500GB
Maximum Capacity	Up to 2.0TB
Network	One Intel gigabit LAN port interface
SATA Controller	Intel SATA Controller
USB	2 x USB 2.0 connectors
EMI Safety	CE/FCC Class B
System Power	200W PSU
Operating Temperature	32ºF to 104ºF (0ºC to 40ºC)
Operating Humidity	10% to 90% relative humidity
Non-Operating Temperature	32ºF to 104ºF (0ºC to 40ºC)
Storage Temperature	-4ºF to 158ºF (-20ºC to 70ºC)
Storage Humidity	5% to 90% non-condensing

Software Specifications

Operating System	Linux Kernel 2.6
Network Service	DHCP Client/Server (default is DHCP client, with a static IP address of 192.168.0.101 if a DHCP server cannot be found)
Supported Web Browsers	Microsoft Internet Explorer 6.0 or newer Mozilla Firefox 1.06 or newer
RAID	RAID 0, 1, 5, 10
File-Sharing Protocols	CIFS/SMB, NFS, FTP, HTTP, HTTPS
Access Control	Users have read-only or read/write access to shared folders CIFS users access shared folders using passwords

USB printer limitations

The storage system is designed to work with up to two USB printers. However, the following printers are not supported:

- Multi-function printers (such as printers that perform copying, scanning, or faxing in

addition to printing)

- Windows Printing System (WPS)

- Non-PostScript printing (Mac)

- Duplex-only (two-way) communication

    Note: Refer to your printer's documentation for information about disabling duplex communication. With some duplex printers, printing might complete successfully, although errors might occur. In addition, some features (such as the printer reporting low ink levels) might not function since two-way communication is not supported.

1.4 Package Contents

- freeStor 4020 unit

- One power cord

- One RJ-45 cable

- DSE Boot CD

- Device management utility, DSE client, firmware and user's manual CD

1.5 Front Panel

The front panel (Figure 1-1) contains the power button, hard disks, and status LEDs.
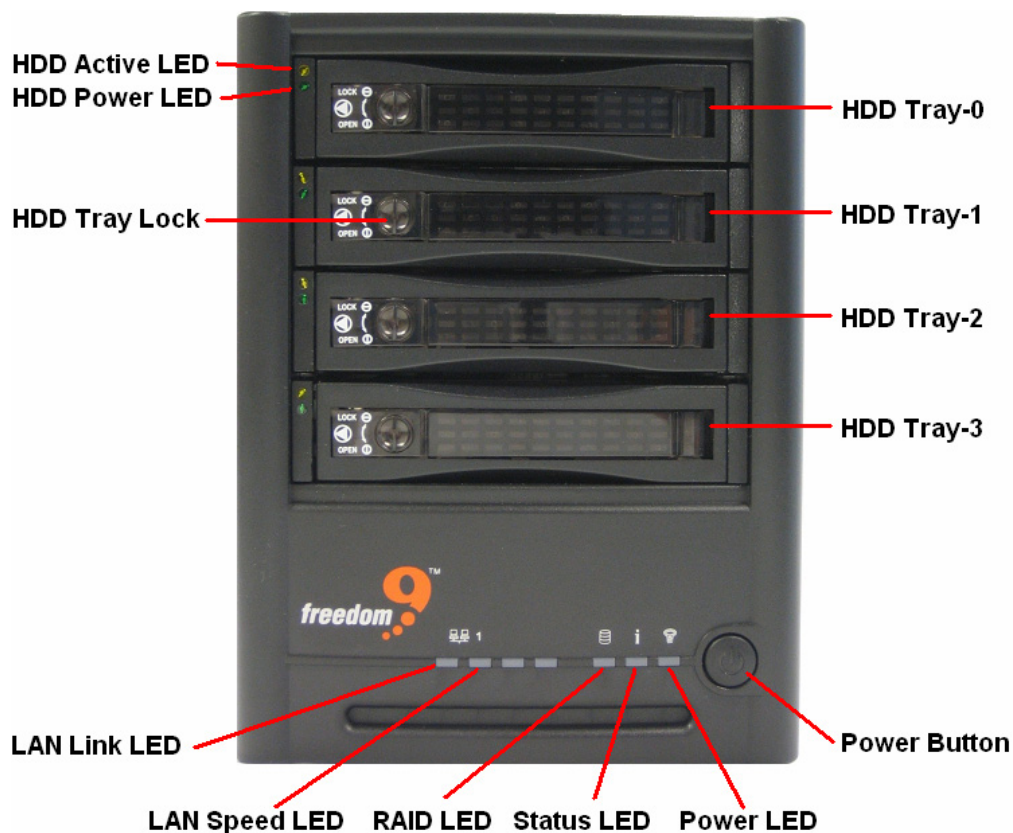
Figure 1-1: Front Panel

HDD Active LED	This LED flashes GREEN when the HDD is active.
HDD Power LED	This LED lights up GREEN when the HDD is installed properly.
HDD tray lock	Turn the lock horizontally to lock the tray in place, or vertically to unlock it.
LAN Link LED	This LED will flash ORANGE if the network interface is being used.
LAN Speed LED	This LED will light up ORANGE when connected to a gigabit connection, and GREEN when connected to a 10/100 Mbps connection.
HDD Trays	Four 3.5-inch SATA HDD trays.
Power LED	This LED lights up BLUE when the system is powered on.
Power button	Press this to turn the unit on, and press and hold until the Status and RAID LEDs start flashing to turn it off.
Status LED	This LED lights up BLUE when the hard disks reach their maximum storage capacity.
RAID LED	This LED lights up RED when RAID 0 is used, ORANGE when RAID

	1 or RAID 10 is used, GREEN when RAID 5 is used, and is off if no RAID is used.

1.6 Rear Panel

The rear panel (Figure 1-2) contains the system fan, power supply, USB 2.0 ports, gigabit LAN port, power cord connection, and reset button.
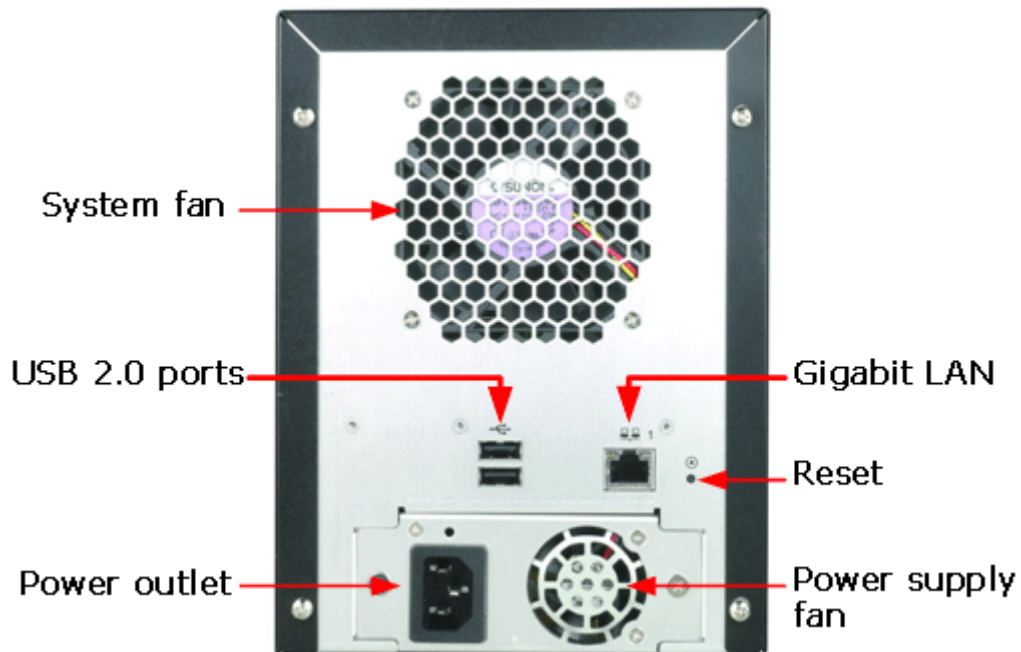
Figure 1-2: Rear Panel

USB 2.0 Ports	The USB ports can be used to connect USB printers and external storage to the freeStor 4020. USB hubs are not supported by these USB ports.
Power Outlet	Supplies power to the device.
Gigabit LAN Port	Gigabit Ethernet connection. The right LED lights up GREEN when connected to a 10/100 Mbps network, and ORANGE when connected to a gigabit network.
Reset Button	Press the "Reset" button for three seconds the unit to system defaults.

1.7 Requirements

Before using the freeStor 4020, the following minimum requirements must be met:

Web Browser	Microsoft Internet Explorer 6.0 or above or Mozilla Firefox 1.06 or above
Network Environment	TCP/IP network environment

Serial ATA hard disk	At least one Serial ATA HDD installed with at least 80GB capacity

All clients using DSE must meet the following requirements:

BIOS	Client PCs must be able to boot from a CD
Operating System	Windows Server 2003, Windows XP, or Windows 2000 (Professional, Server, or Advanced Server) with Service Pack 2 or above. **Note:** The operating system must be installed on the first partition (Drive C).
LAN port	At least one wired NIC

2 Installation and Setup

2.1 Hard Drive Installation

It is highly recommended that all of the hard drives used are the same size. However, if they are different sizes, it is recommended that the drives are placed from largest to smallest from the top tray to the bottom tray.

> **Note:** At least one SATA hard disk with at least 80 GB capacity must be installed before the unit can be used. The unit does not ship with any hard drives installed.

Follow these steps to install a hard drive into the unit:

1. Remove the topmost hard drive tray (Figure 2-1) from the freeStor 4020.

> **Note:** Ensure that the hard drive is a SATA drive (Figure 2-2) and not an ATA or SCSI drive.

Figure 2-1: Hard Drive Tray
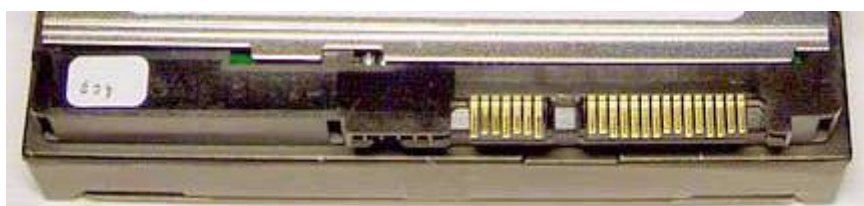
Figure 2-2: SATA Connector

2. Slide the new hard drive into the tray and fasten the screws underneath the tray (Figure 2-3).
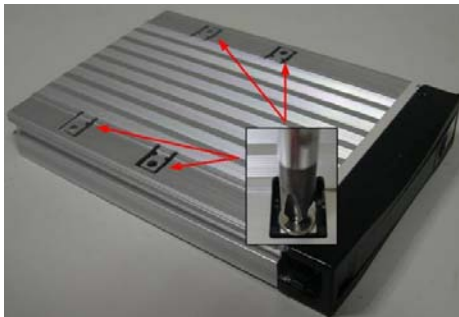
Figure 2-3: Attaching the Hard Drive to the Tray

3. Pull out the handle before inserting the hard drive tray into the freeStor 4020.

4. After the tray has been inserted, push the handle back into position to lock the tray in place.

5. Repeat steps 1-4 for the remaining hard drives that need to be installed.

6. Connect the power cable to the back of the freeStor 4020 and plug the other end of the cable into a power socket.

7. Press the power button on the front of the freeStor 4020.

8. The Status LED will flash while the unit is booting up. Once the unit has finished booting up, the Status LED will turn off.

9. Once the unit has powered up, the hard drive LED will flash green and the power LED will light up blue on the drive tray. If the hard drive LED is flashing red, there is a problem with the drive installation and the drive should be removed, tested, and reinstalled again using the above procedure.

   Notes:

   - If you replace all of the drives with higher capacity, you have to go to Administrator to login and format the drives. This will cause all data and backups to be deleted.

   - It is recommended that the freeStor 4020 be plugged into a surge protector or uninterruptible power supply (UPS) to prevent damage to the unit from power surges.

2.2 Storage System Console Installation

The Storage System Console is a Windows application included with the freeStor 4020. The software allows you to discover and access all freeStor 4020's on the network. Although not required, the Storage System Console makes configuring and managing the units much easier.

The Storage System Console runs on the following operating systems: Microsoft Windows 2000 with Service Pack 2 or higher, Microsoft Windows XP, Microsoft Windows Server 2003.

To install the Storage System Console, follow these steps:

1. Insert the Installation CD into your CD-ROM drive.

2. In Windows Explorer, open the "StorageSystemConsole" folder on the installation CD. Double-click the "Setup.exe" file to begin installation of the software.

3. On the welcome page (Figure 2-4), click "Next".
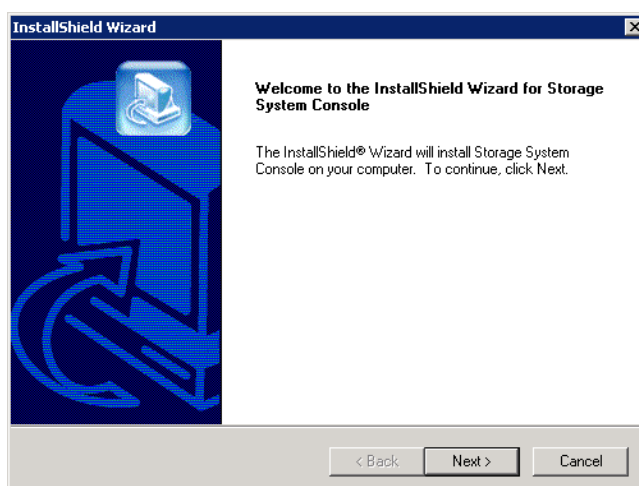
Figure 2-4: Welcome Page

4. Click "Yes" if you agree to the terms of the license agreement. If you do not agree to the terms, you cannot install the software.

5. On the next page (Figure 2-5), enter your name and company name and then click "Next".
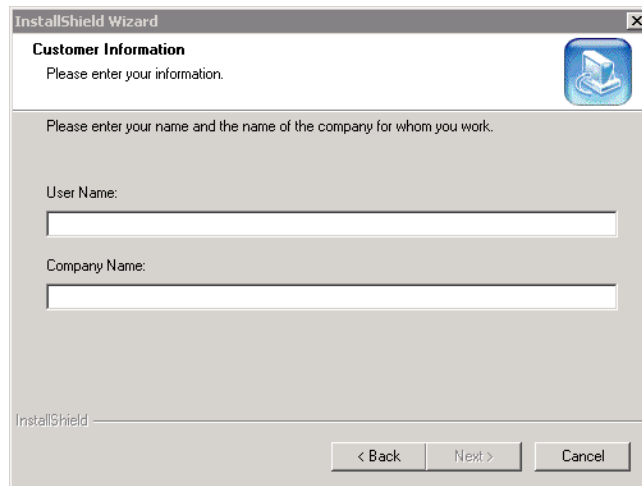
Figure 2-5: Customer Information

6. On the following page (Figure 2-6), click "Next" to install the Storage System Console in the displayed location, or click "Browse…" to select or specify a different location and then click "Next".
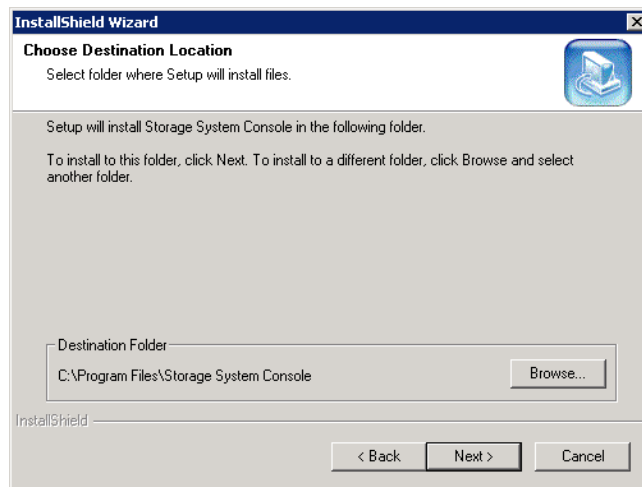
Figure 2-6: Destination Location

7. Review your selections and click "Next" to proceed (Figure 2-7).

16
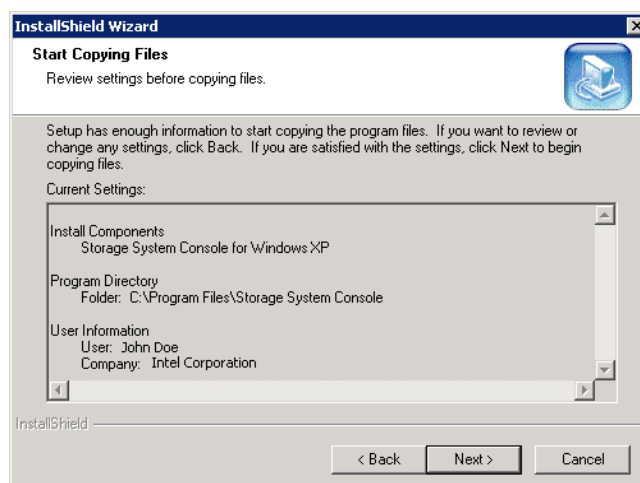
Figure 2-7: Summary

8. To complete the installation, click "Finish" (Figure 2-8).
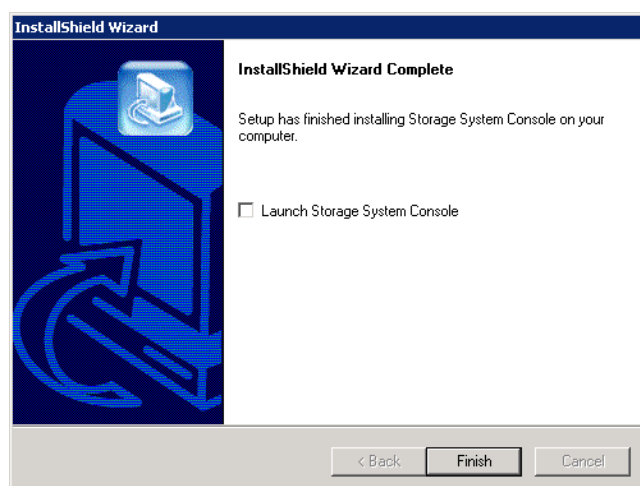
Figure 2-8: Installation Complete

Once the Storage System Console has been installed, run the program from the Start Menu (Start → Programs → Storage System Console).

When the Storage System Console starts, it will automatically scan the network for freeStor 4020 devices. After the scan is complete, the devices found will be listed in the left pane (Figure 2-9).
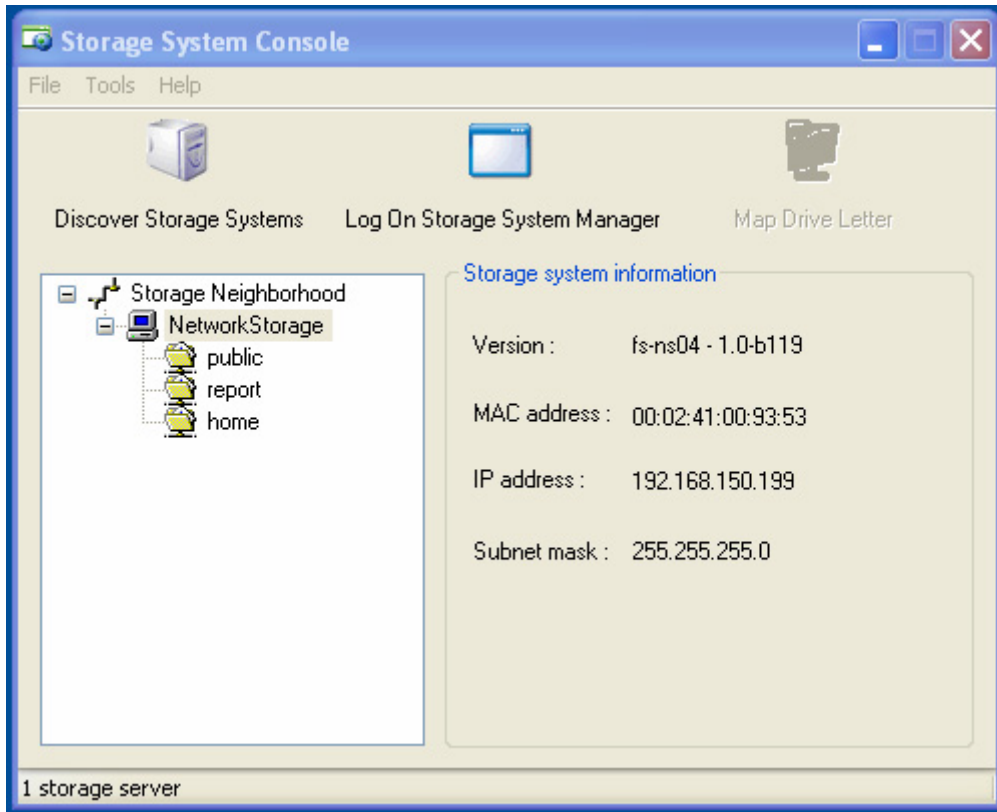
Figure 2-9: Storage System Console

In the left pane, select the name of the new unit and click "Log On Storage System Manager" to access the web interface of the device.

If any freeStor 4020 units are added to the network after the software has started, click "Discover Storage Systems" to rescan the network for the new units.

2.3 System Setup

Once the hard drives have been successfully installed, the freeStor 4020 will have to be configured before it can be used. Follow these steps to configure the device.

1. Connect the freeStor 4020 to your network. If your network has a DHCP server, the freeStor 4020 will automatically get an IP address from the DHCP server. Otherwise, the freeStor 4020 will default to an IP address of 192.168.0.101.

2. Using a computer on the same network as the freeStor 4020, change the IP address of the computer to match the freeStor 4020 (e.g. if the freeStor 4020's IP address is 192.168.0.101, the computer's IP address should be 192.168.0.X where X is between 1 and 254 and not the same as the freeStor 4020). For instructions on changing your computer's IP address.

3. Plug in and power on the freeStor 4020.

4. The web interface of the freeStor 4020 can be accessed by using the Storage System Console (see Section 2.2) or by using a web browser. For access using a web browser, open up a web browser (Internet Explorer 6.0 or higher or Mozilla Firefox 1.06 or higher) and enter the IP address of the unit in the address bar.

5. For both connection methods, the web browser will be connected to the freeStor 4020 and the System Initialization screen will be displayed (Figure 2-10).
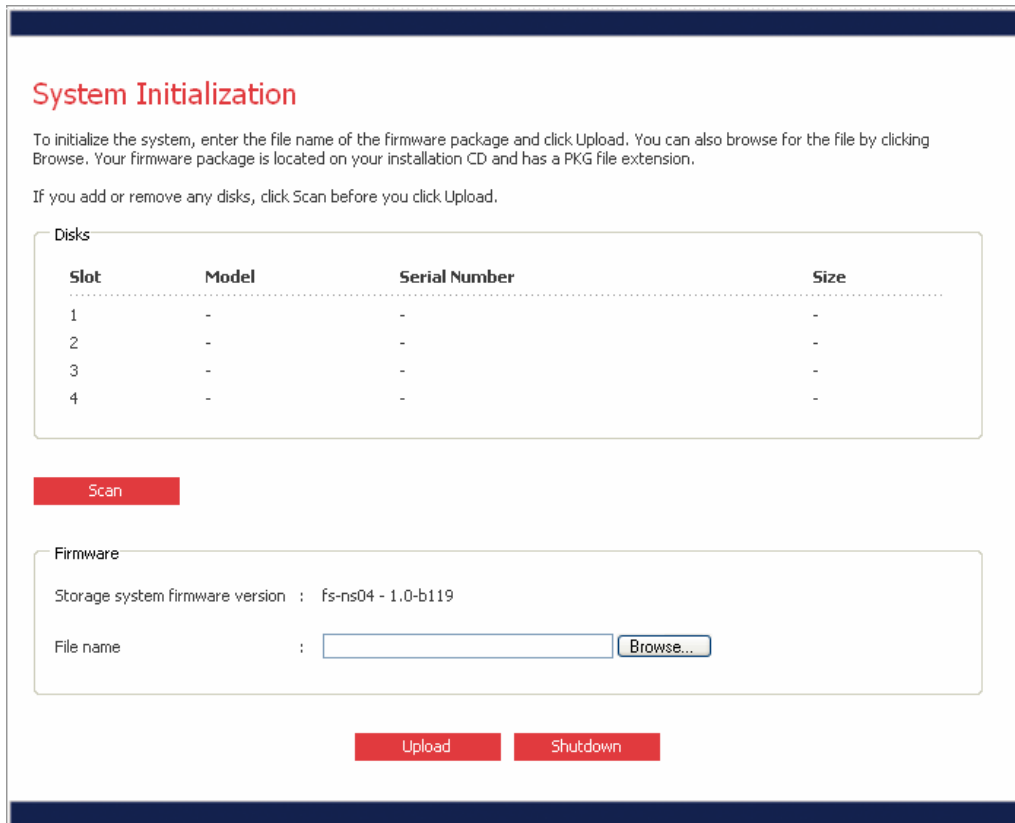
Figure 2-10: System Initialization Screen

6. The System Initialization screen will list the model, serial number, and size of the hard drives installed in the unit. If a hard drive is added or removed after loading this page, click "Scan" to refresh the list of hard drives.

7. Click "Browse" and navigate to the firmware file on the CD-ROM. The firmware has a file extension of ".pkg". Select the file and click "Open".

8. Click "Upload" to upload the firmware to the hard disks in the unit. Once the firmware has finished uploading, the unit will automatically restart.

9. After the unit has restarted, connect to the device again using steps 7 through 9.

10. Once the web browser is open, a welcome screen will be displayed (Figure 2-11).
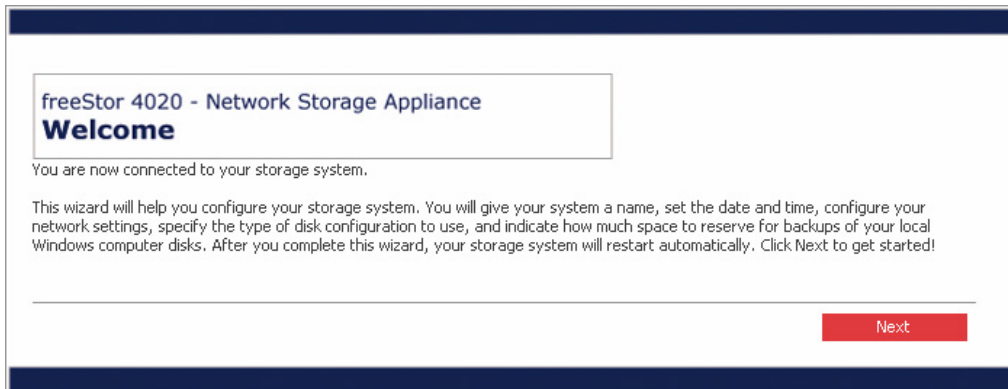
Figure 2-11: Welcome Screen

11. Click "Next" to proceed to the next page.

12. The next page contains the End User Software License Agreement (Figure 2-12). If you agree to the terms, click on the "I accept the license agreement" check box and click "Next".

   Note: You cannot use the freeStor 4020 if you do not agree to the terms in the End User Software License Agreement.
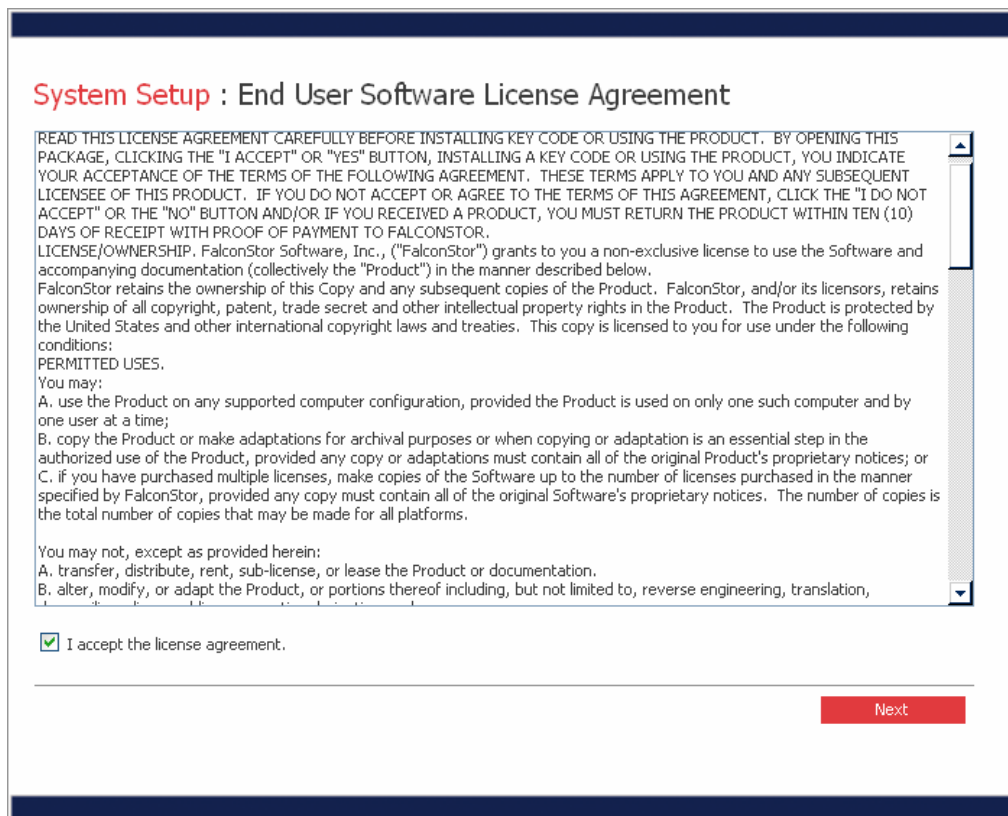
Figure 2-12: End User Software License Agreement

13. On the next page, enter a host name to identify the freeStor 4020 on the network (Figure 2-13). The system name can be up to 15 characters long and can only include letters,
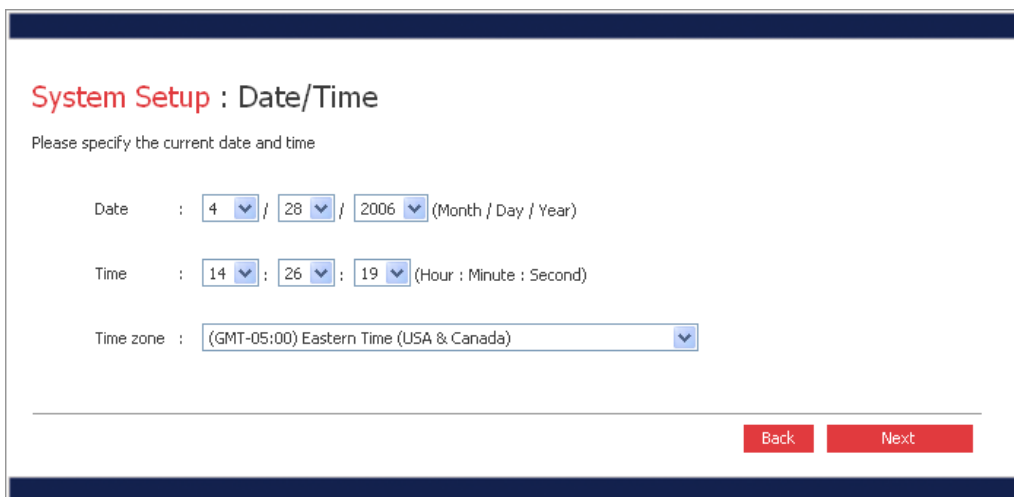
numbers, and hyphens. To proceed, click "Next".

Figure 2-13: Host Name

14. On the next page, enter the current date and time (Figure 2-14). The time must be entered in 24-hour notation (2:15 PM should be entered as 14:15). After entering the date and time, click "Next".

Figure 2-14: Date/Time

15. On the next page, enter the network settings of the freeStor 4020 (Figure 2-15). If the network has an existing DHCP server, select "Get an IP address automatically". Otherwise, select "Use this IP address" and enter the desired IP address below. After entering the network settings, click "Next".
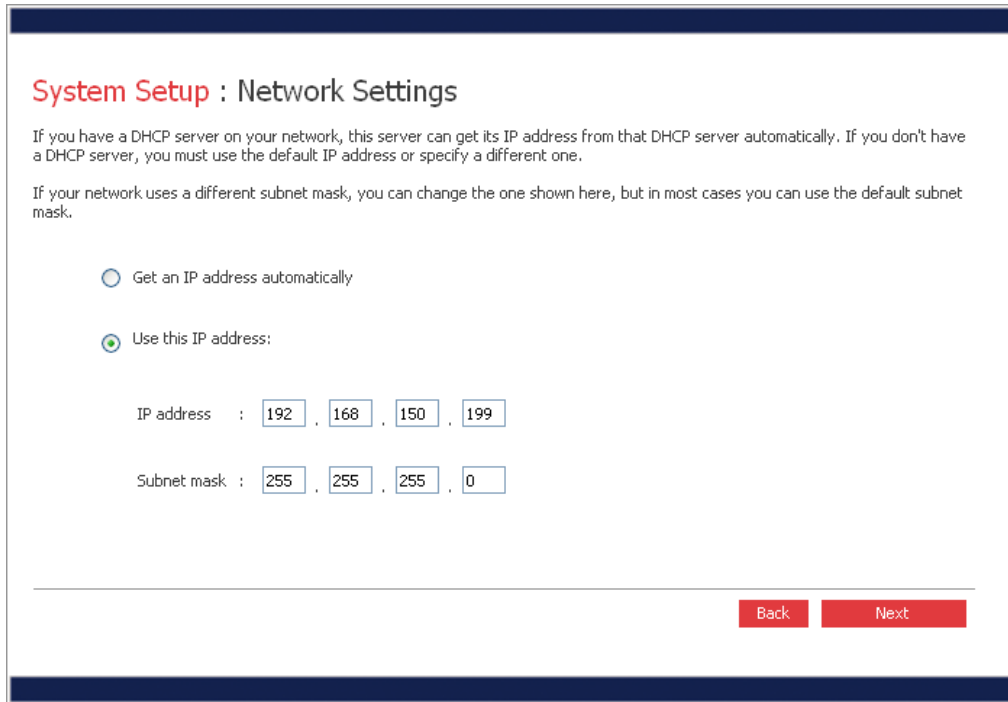
Figure 2-15: Network Settings

16. The next page will ask for the disk configuration to use for the freeStor 4020 (Figure 2-16). The options presented on the page vary depending on the number of hard drives in the unit.
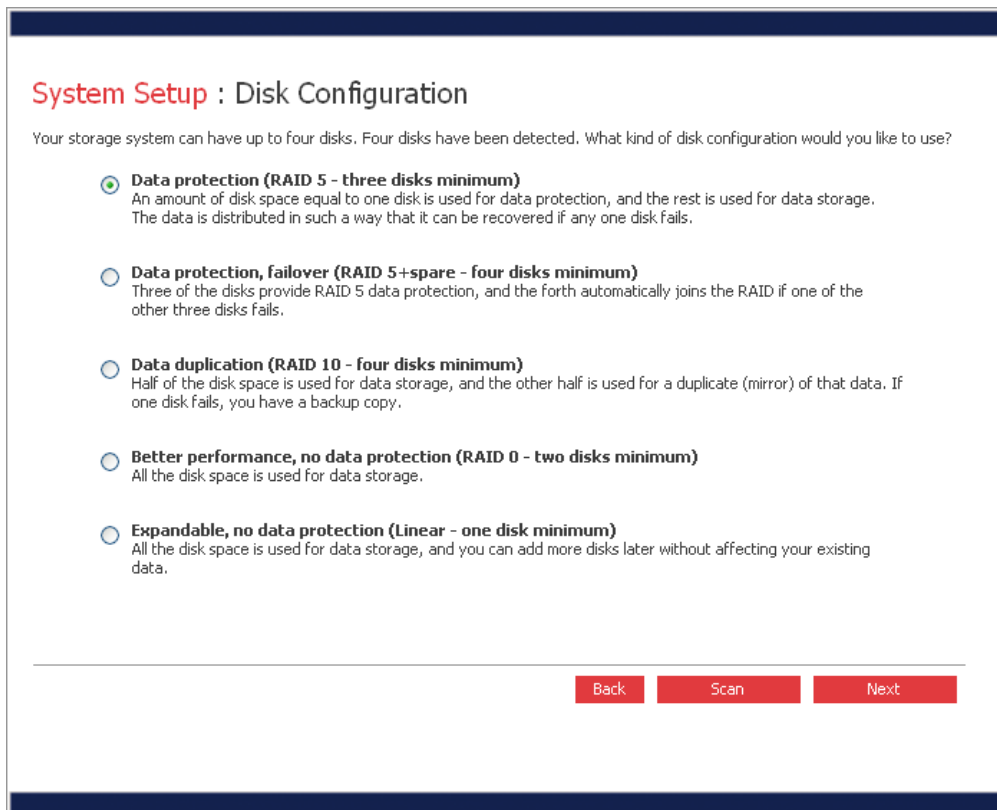
Figure 2-16: Disk Configuration

22

17. To add or remove hard drives from the freeStor 4020 at this time, add or remove one drive at a time, and click "Scan" before adding or removing the next drive.

   Note: It is strongly recommended that all of the drives that are to be used in the final configuration be installed at this time. Adding or removing drives after this step could require drive reconfiguration and data loss.

18. To accept the default disk configuration (which will provide the best level of data protection available for the number of hard disks currently installed), click "Next". By default, a linear disk configuration is used for a single hard disk, RAID 1 is used for two hard disks, and RAID 5 is used for three or four hard disks.

19. To change the disk configuration, select the desired RAID level and then click "Next".

20. The next page will assist in determining the amount of space required for storing DiskSafe backups (Figure 2-17). If you do not wish to use the system backup capabilities of the freeStor 4020, select "0" and click "Next" and proceed to step 27. To calculate the amount of space required, select the number of disks that will be backed up.

   Note: A single computer with two hard drives or one hard drive with two partitions will count as two disks, not one.

21. After selecting the number of disks, a list will appear below with text boxes labeled "Disk 1", "Disk 2", etc. Enter the total capacity of each disk that will be backed up. To determine the size of a hard drive, open Windows Explorer and right-click on a hard drive (e.g. "C:") and select "Properties". Be sure to enter the total capacity and not just the used space. Click "Next".
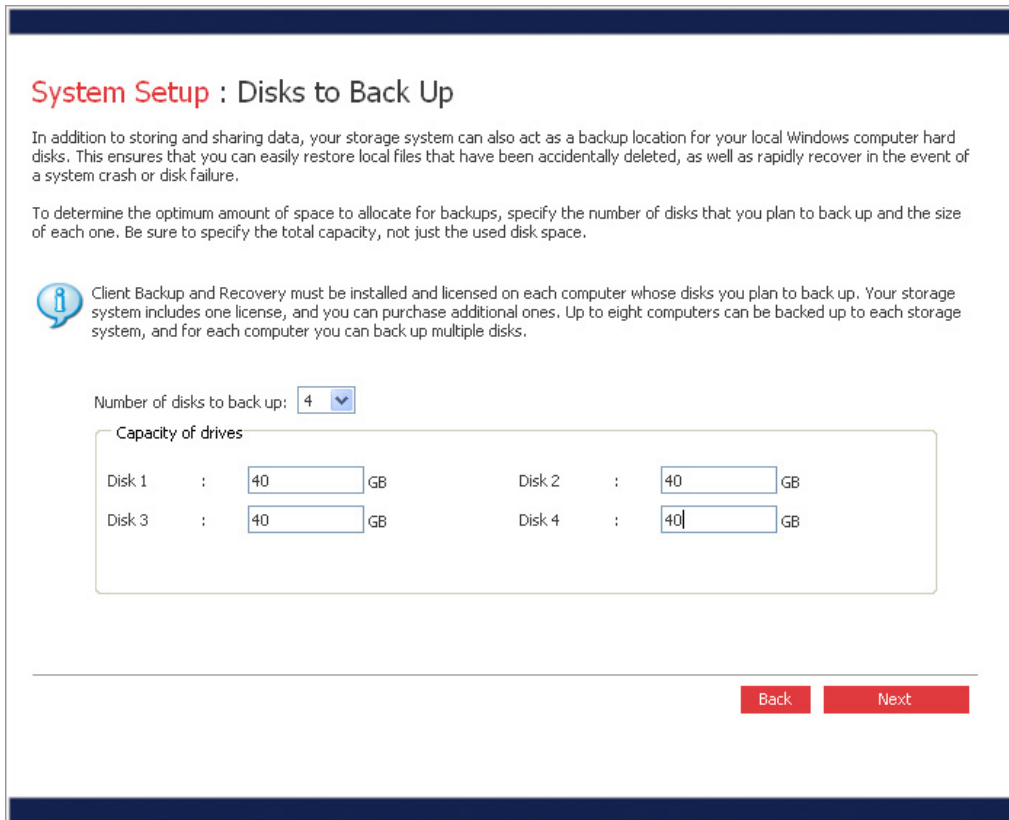
Figure 2-17: Backup Calculator

22. On the following page, you can select how much space to allocate to backups and how much to shared folders (Figure 2-18). Based on the information provided on the previous page, the suggested percentage of backup space will be automatically entered in the text box. To change the percentages, select a text box and enter a new percentage. Once one value is changed, the other will automatically be updated so that the total of the two boxes is 100%.

Notes:

- Once the wizard is completed, changing the disk allocation in the future will result in the deletion of all data on the freeStor 4020.

- The maximum space which can be used for backups is 99%. If the amount of space needed exceeds this limit, then some disks cannot be backed up. Click "Finish" when ready to proceed.
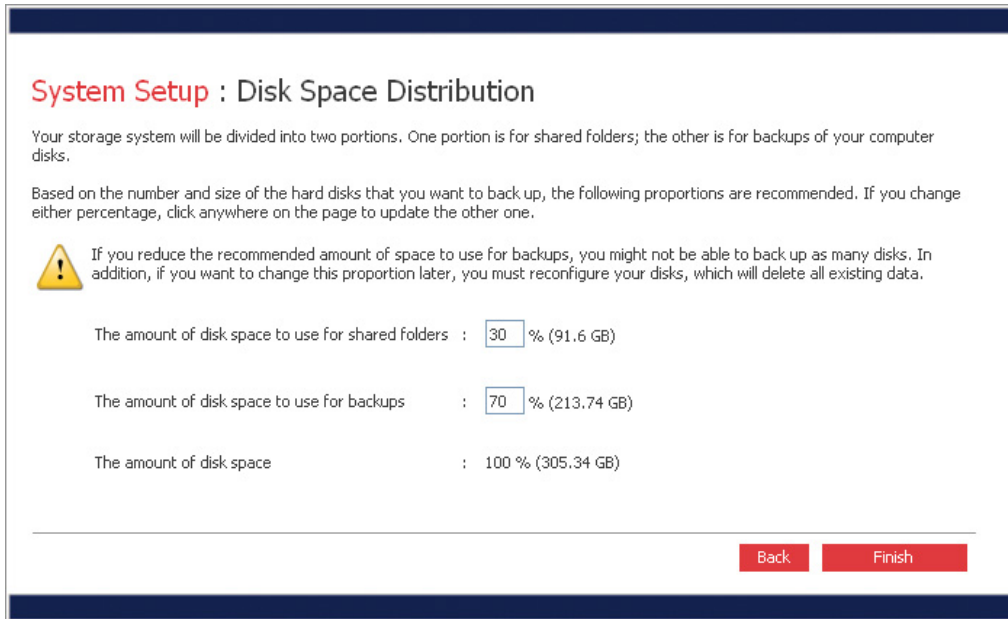
Figure 2-18: Disk Space Distribution

23. Confirm that all of the settings are correct and click "OK" when the confirmation page appears. The configuration page (Figure 2-19) will appear to show the progress of the system setup. Once the setup is complete, the system will restart automatically.
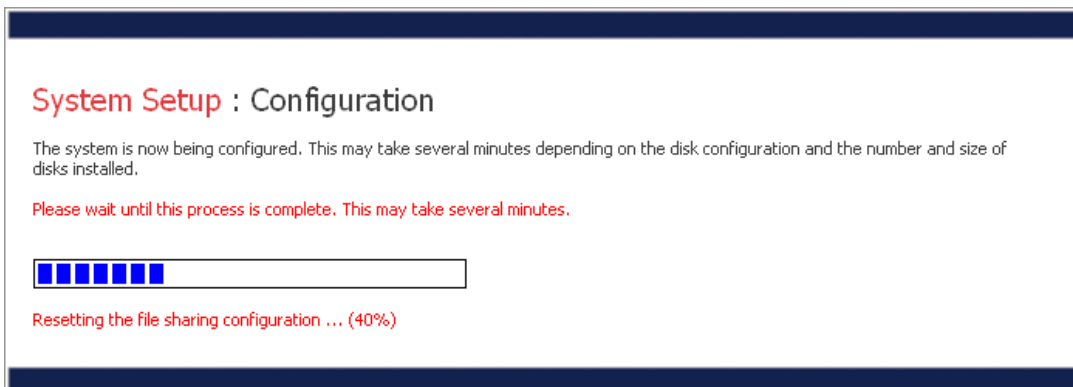
Figure 2-19: System Configuration

After the unit restarts, the web management interface can be used to add users and create shared folders to start using the freeStor 4020.

3 Web Management Interface

The web management interface can be accessed using a web browser directly connecting to the IP address of the freeStor 4020, or the Storage System Console (see Section 2.2).

When first accessing the web interface, the login screen (Figure 3-1) will appear. Enter the user name and password and click "Login". The default user name is "admin" and the default password is "storage". It is recommended that the password be changed as soon as possible for security reasons.

Figure 3-1: Login Screen

3.1   Main Menu

After logging in, the Home page will be displayed on the screen. The main menu (Figure 3-2) is displayed along the top of every page and allows you to access all of the freeStor 4020's features. The main menu has the following items:

Figure 3-2: Main Menu

- **Home:** Displays information about the total storage capacity on the storage system, how much disk space is allocated for shared folders, how much is allocated for backups, and how much is used for each. This page also displays the total number of shared folders and the number of networked computers (backup clients) that have backed up one or more disks on the storage system.

- **Users:** Displays a list of all currently configured users and lets you add, modify, and remove users. For Windows and OS X users, this area also lets you add, modify, and remove groups.

- **Shared Folders:** Displays a list of all currently configured shared folders and lets you add shared folders, change which users can access them, and remove them.

- **Backups:** Displays a list of all computer disk backups that currently exist and lets you change the recovery CD password or delete the backups for a particular computer hard disk.

- **Advanced:** Provides access to advanced storage system configuration options, such as setting up e-mail alerts; upgrading the firmware; removing USB devices; changing the system, network, or disk configuration settings; viewing information about system events; and shutting down the system remotely.

- **Contact Us:** Provides contact information about freedom9.

- **Log Out:** Logs you out of the web interface.

3.2   Home

The Home Page (Figure 3-3) displays summary information about the device. The Storage Status page displays the space allocated and used for file sharing and backups by the freeStor 4020.

> **Note:** The total storage capacity will be less than the total size of all of the hard

disks because some of the disk space is needed for the operating system and management software. In addition, the amount of used backup capacity will be greater than the total size of all the disks listed on the Backups page because additional storage space is needed for the data that has changed between backups.
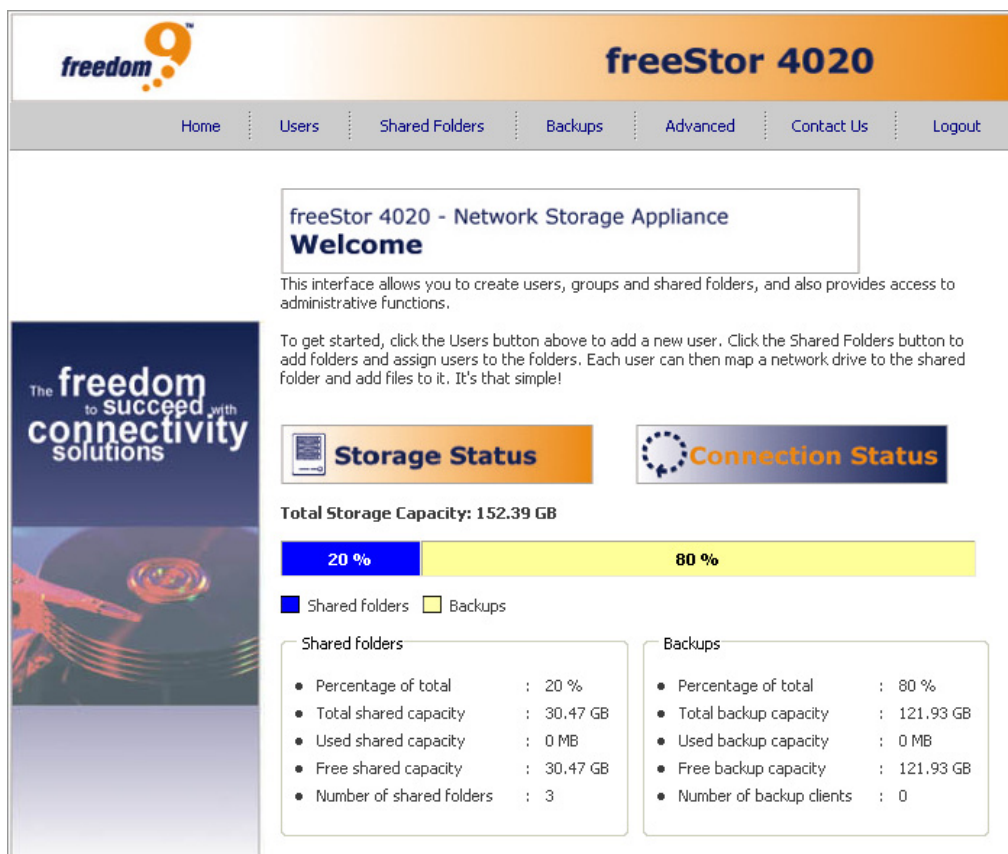
Figure 3-3: Home Page

Clicking on the Connection Status button will display a list of users and the shared folders they are connected to (Figure 3-4). Due to the nature of the NFS protocol, Linux and Mac connections are not listed on this page. Likewise, ongoing backup or recovery activities do not appear on this page.

This page indicates only that a connection with a shared folder has been established; this does not necessarily mean that the user has opened any files in the shared folder.

> **Note:** If a user accesses a shared folder using the "guest" user name, the name guest appears in the Users column, followed by the user's computer name in parentheses.

Figure 3-3: Connections Page

3.3   Users

Clicking on the "Users" button in the menu will open the Users Page (Figure 3-5) which allows you to manage the users on the freeStor 4020.
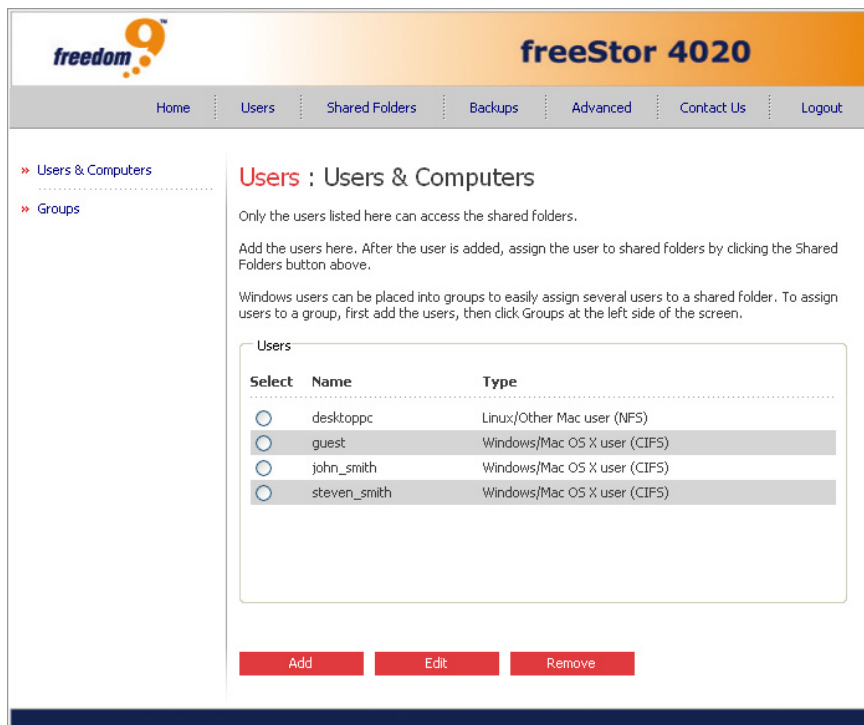
Figure 3-5: Users Page

29

By default, the freeStor 4020 includes a user named "guest" that has a password of "guest". Windows and OS X users can access all shared folders that the user "guest" is authorized to access. However, for increased security, it is advised that additional users are added as well. For example, to restrict access to a shared folder that contains confidential information, you would add at least one user and authorize that user to access that shared folder and not authorize the "guest" user to access it. Adding a user for each individual or computer in the network provides maximum flexibility and security, enabling you to control exactly who can access what information.

In addition, only Windows and OS X users can use the "guest" user account. If there are Linux users or Mac users on the network, you must add users to allow these computers to access any shared folders.

When you add a Windows or OS X user, a folder with the same name as that person's user name is automatically created on the storage system. Only that person can access that folder, and that person has full read/write access to it. In the Storage System Console, this folder is identified as the home folder.

Up to 64 Windows or OS X users, and up to 64 Linux or Mac users (for a total of up to 128 users) can be added to the freeStor 4020.

> **Note:** Since each Linux or Mac user can represent multiple users, the number of actual users can be higher.

To add a new user:

1. Click "Add" to open the Add User page (Figure 3-6). Select the type of operating system used by the user and click "Next".

   > **Note:** Linux and Mac users must use Network File System (NFS) to access the freeStor 4020 are given access based on the computer and not the individual users on the computer.
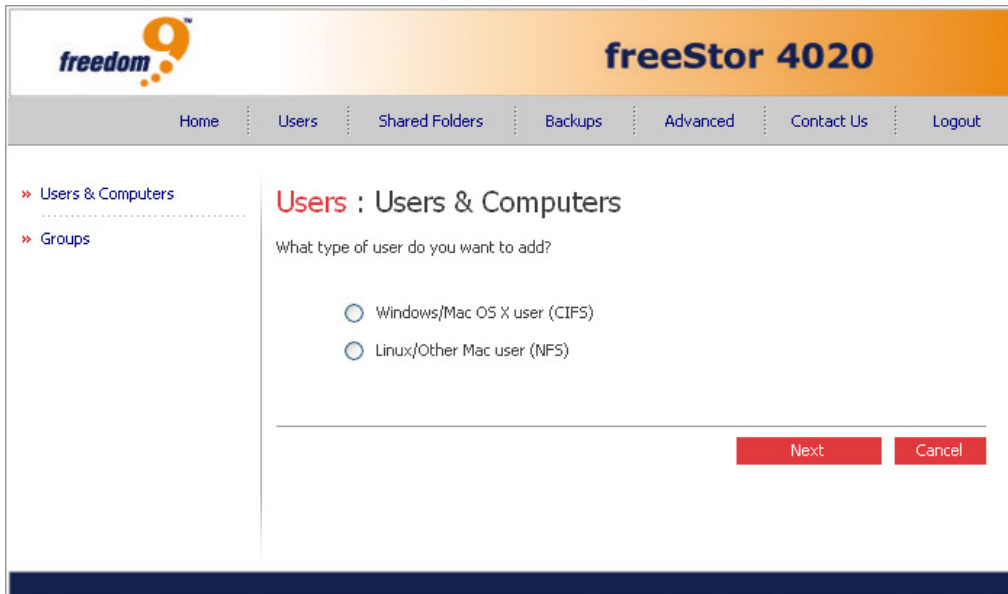
Figure 3-6: Add User Page

2. The next page that is displayed depends on the type of user being added. For Windows and OS X users, the page shown in Figure 3-7 will be displayed, and for Linux and Mac users, the page shown in Figure 3-8 will be displayed.
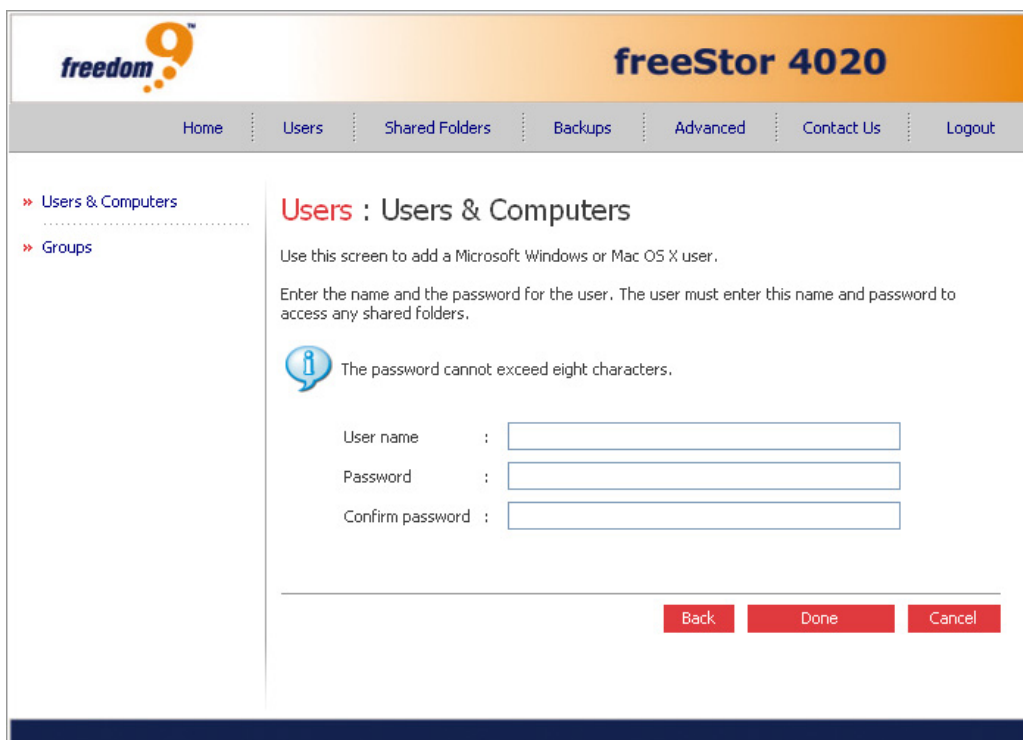
Figure 3-7: CIFS Add User Page
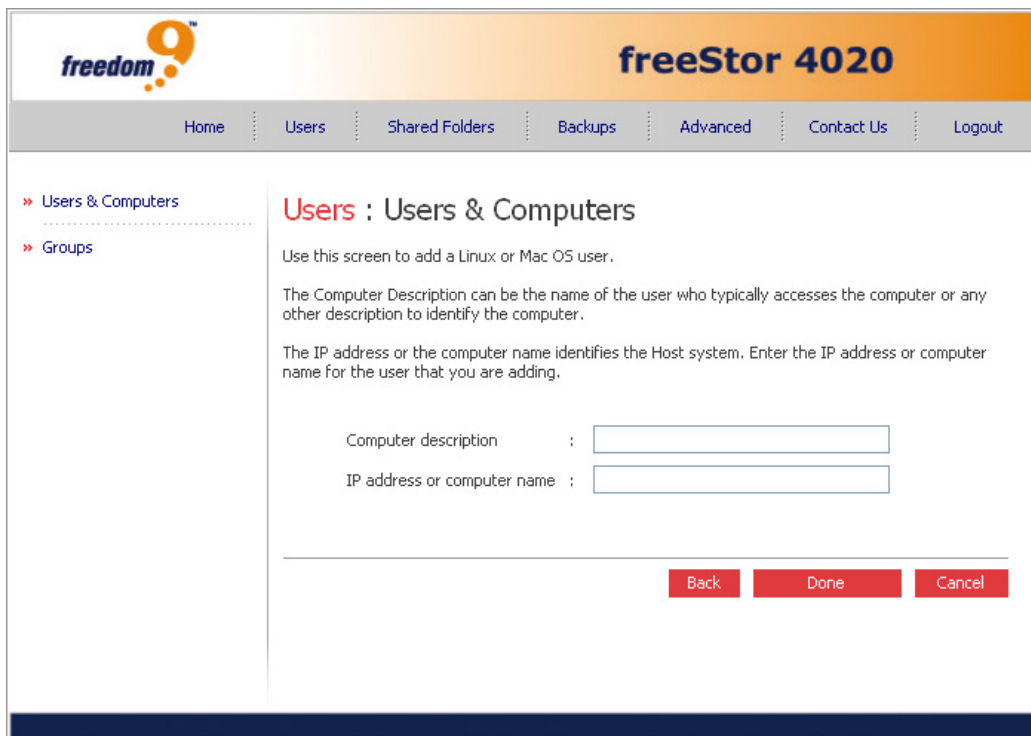
Figure 3-8: NFS Add User Page

3. For Windows and OS X users, enter the user name and password users have to enter to access their account. Re-enter the password in the last field and click "Done" to continue. The user name can be up to 20 characters long and must consist of letters and numbers only.

> **Note:** If the user name and password specified here are the same as the person's Windows user name and password, the person will not be prompted to provide a user name and password when accessing the shared folder.

4. For Linux and Mac users, enter a description of the computer(s) being used to access the freeStor 4020. The description can be up to 15 characters long. Next, enter the IP address or the actual computer's name in the system configuration of the computer(s) that are allowed to use this user account.

> **Note:** You can create a single user account that represents multiple computers. In the "IP address or computer name" textbox, you can use the wildcard characters ***** and **?** to represent multiple client machines (e.g. "client*" and "client?" will match any computer in the subnet with a name starting with "client". "*.company.com" would include all computers in the domain "company.com"). The wildcards can only be used with computer names and not IP addresses.

To edit an existing user:

1. Click the radio button beside the user to edit and click "Edit". For Windows and OS X users, the page shown in Figure 3-7 will be displayed. Only the password used to access the shared folders can be changed, but not the user name. This change will not affect current connections, but will take effect the next time someone tries to connect to a shared folder.

2. For Linux and other Mac users, the page shown in Figure 3-8 will be displayed. The IP address or computer name can be changed, but not the computer description. Changing this information immediately disconnects that computer from the shared folders.

To remove an existing user:

Click the radio button beside the user to remove and click "Remove". When prompted to confirm the removal, click "Yes".

> **Warning:** When removing a Windows/OS X user, that user's personal (home) folder is automatically deleted. It is recommended that the user copy any data from this folder to another location to ensure that it is not lost before removing the user.

3.4 Groups

Windows and OS X users can be put into groups, which makes it easier to give several users access to the same shared folder at once.

When you click "Users" in the main menu and click "Groups" in the left menu, the page displays a list of all currently configured groups (Figure 3-9). When you select a group in the Groups list, the members of that group appear in the adjacent Members list.
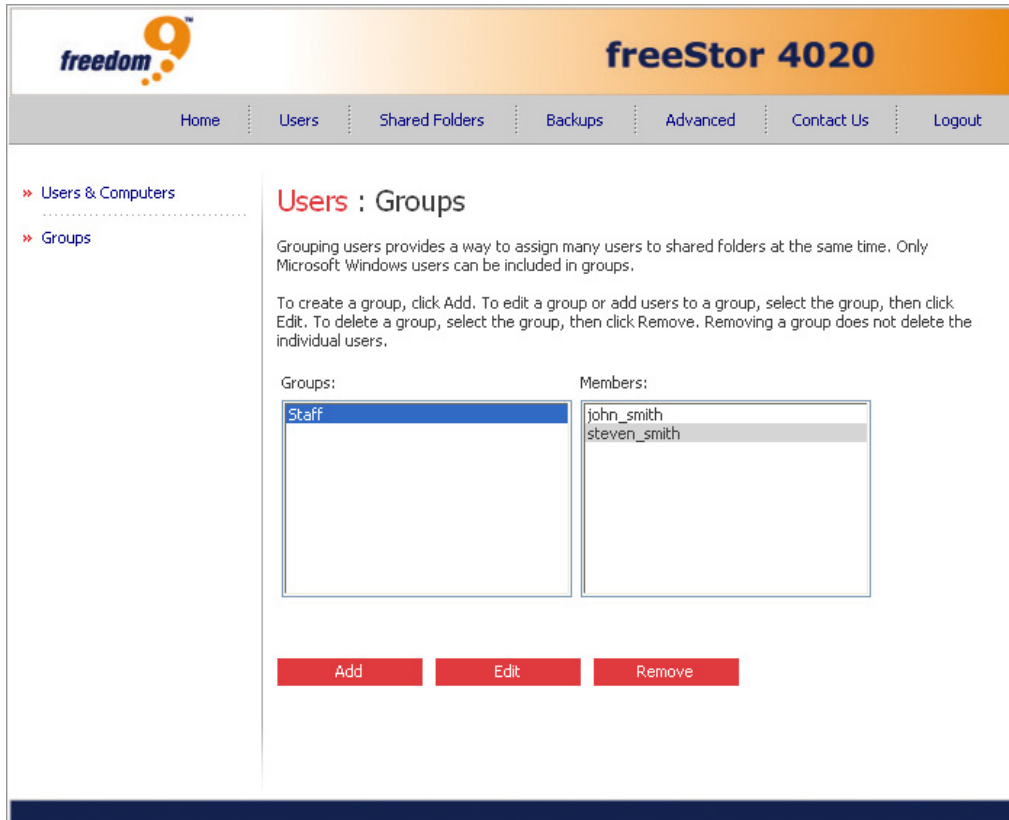
Figure 3-9: Groups Page

To add a new group:

When you create a group, you typically specify which users should be members of that group, although you can create an empty group and add users later. A user must be created from the Users page before being added to a group.

Each user can be a member of multiple groups. For example, the user Alice might be a member of both the Marketing and Executives groups.

The freeStor 4020 supports up to 16 groups at any one time.

To add a group:

1. In the navigation bar, click "Users".

2. In the left pane, click "Groups".

3. Click "Add" to open the add groups page shown in Figure 3-10.
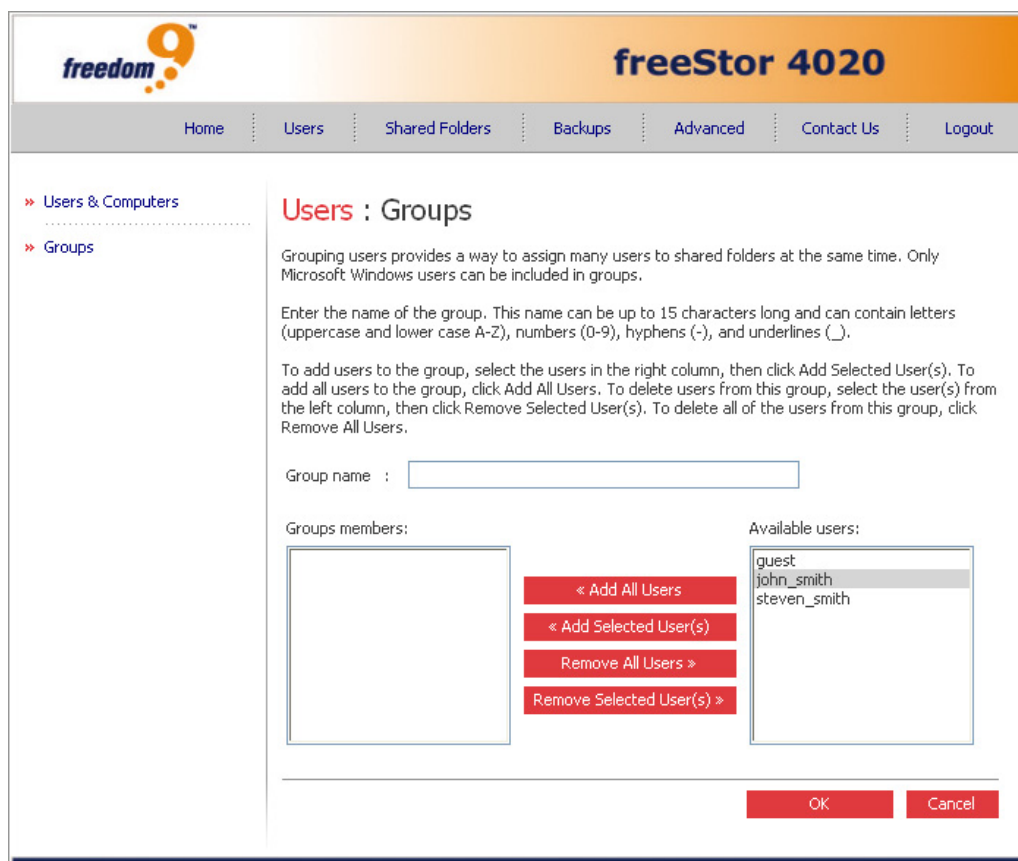
Figure 3-10: Add Group Page

4. In the "Group name" text box, enter a unique name for the group. This name can be up to 15 characters long and can include letters, numbers, hyphens, and underscores.

5. Specify which users should belong to this group, and then click "OK": To select multiple, contiguous users, hold down the Shift key and select the first user, then select the last user. All users between the first and last selected user are selected. To select multiple, non-contiguous users, hold down the Ctrl key as you select each user.

> **Add All Users:** All users from the Available users list are added to the group.

> **Add Selected User(s):** All selected users from the Available users list are added to the group.

> **Remove All Users:** All users from the Group members list are removed from the group.

> **Remove Selected User(s):** All selected users from the Group members list are removed from the group.

To edit an existing group:

You can change which users are members of each group at any time. When you add a user to

a group, that user immediately has access to all the shared folders that the group is authorized to access. However, if you remove a user from a group, the change does not take effect until that user disconnects from the shared folder or shuts down the computer.

For example, the user Alice might be a member of both the Marketing and Executives groups. The Marketing group might have read-only access to the Budget shared folder, while the Executives group might have read/write access. As a member of the Executives group, Alice would have read/write access to that shared folder. If Alice is currently connected to that shared folder and you subsequently remove her from the Executives group, she will continue to have read/write access to that folder until she disconnects or shuts down her computer. The next time she connects, she will continue to have access to the shared folder (since she is still a member of the Marketing group), but she will be able to only view the files there; she will not be able to add, modify, or delete any files.

To edit a group:

1. In the navigation bar, click Users.

2. In the left pane, click Groups.

3. In the Groups list, select the group whose membership you want to change and click "Edit".

4. The Edit Group page (Figure 3-10) will be displayed.

5. The Edit Group page functions the same way as the Add Group page. On the Groups page, when you select this group in the Groups list, the Members list will immediately reflect the changes you just made.

Removing an existing group:

Removing a group does not remove the users that are members of that group; it simply means that the group will no longer appear in the Groups list on the Groups page. The users remain listed on the Users & Computers page.

However, removing a group can affect access to shared folders. When you remove a group, the members of that group will no longer have access to any shared folders that the group was authorized to access unless they were granted individual access as well.

For example, the Executives group might include Alice, Bob, and Carlos, and that group might have read/write access to the Budget shared folder. If you remove the Executives group, Alice, Bob, and Carlos remain users, but they will no longer have any access to that shared folder.

On the other hand, if the Executives group had read/write access to the Budget shared folder, but Alice had read-only access, when you remove the group, Bob and Carlos will no longer

have access to the Budget shared folder (since their access rights were determined by their group membership), but Alice will continue to have read-only access, since that access right was granted to her on a user level.

To remove a group:

1. In the navigation bar, click Users.

2. In the left pane, click Groups.

3. In the Groups list, select the group that you want to remove.

4. Click "Remove".

5. When prompted to confirm the removal, click "Yes".

The group no longer appears in the Groups list.

3.5 Shared Folders

Clicking on the "Shared Folders" button in the menu will open the Shared Folders Page (Figure 3-11) which allows you to manage the shared folders on the freeStor 4020.
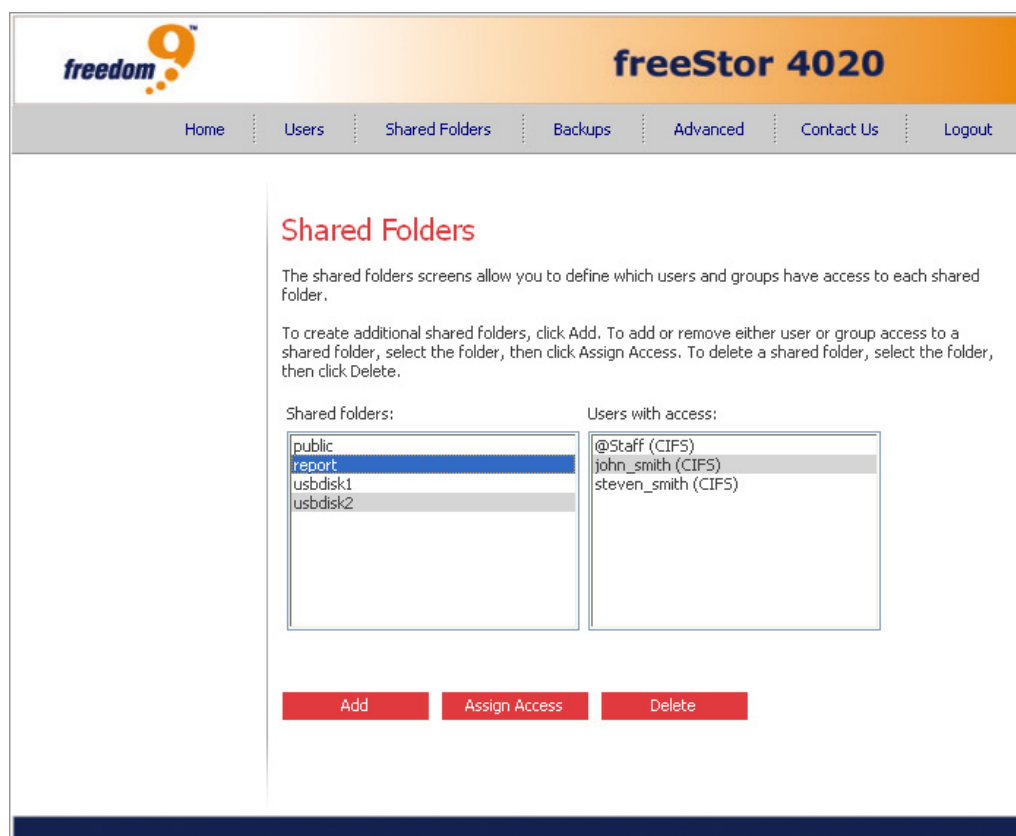
Figure 3-11: Shared Folders Page

By default, the freeStor 4020 includes a shared folder named public, and all Windows and OS X users can access it and create, modify, or delete files in the folder unless you change the list of authorized users or their access rights.

In addition, when a Windows or OS X user is added, the storage system automatically creates a shared folder with the same name as the person's user name. Only that user can access that shared folder.

However, additional shared folders can also be created for specific users or for better organization. For example, in an office environment, you might want to create a shared folder for company policies that everyone can only view and not write to, and separate shared folders for confidential business files that only selected individuals or departments can view and change. In a home environment, you might want to create separate folders for different types of files, like photos, videos, or music. In addition, since only Windows and OS X users can access the public folder, you would have to create shared folders if your network includes Linux or Mac users.

Up to 32 shared folders can be created. Users who can access and write to these shared folders can create additional sub-folders for organizing the files they store there.

Notes:

- The Shared folders list includes usbdisk1 and usbdisk2, whether or not any USB disks have been connected to the storage system.

- Shared folders created as a result of creating Windows/OS X users do not appear in the Shared folders list.

To add a new shared folder:

1. Click the "Add" button. The page shown in Figure 3-12 will be displayed. Select the type of user that will be accessing this shared folder and click "Next". The operating system running on the user's computer determines which option you should choose (Windows/OS X users (CIFS) or Linux/Mac users (NFS)).
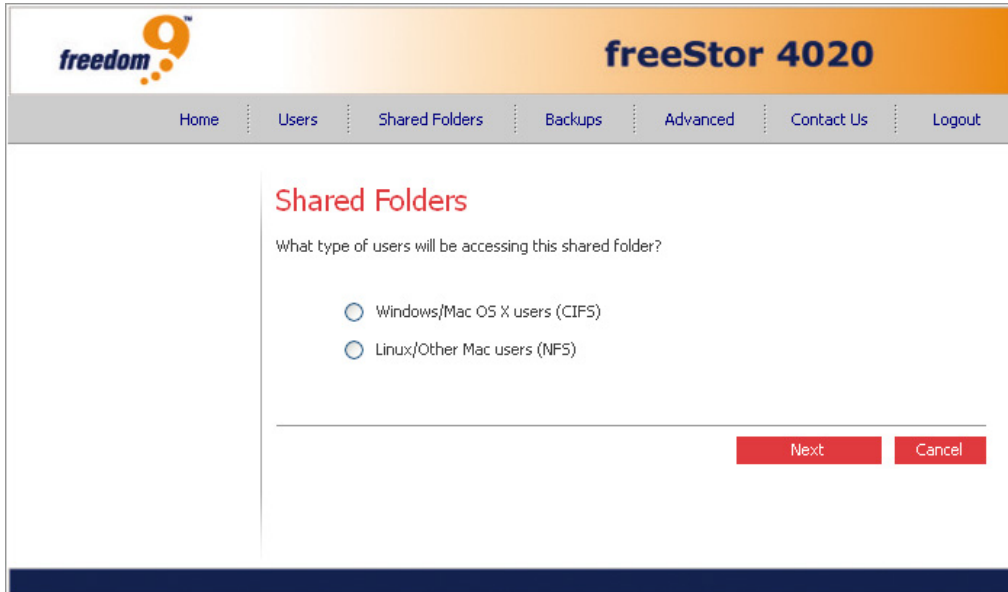
Figure 3-12: Add Shared Folder Page

2. The next page that is displayed depends on the type of used that was selected. For Windows and OS X users, the page shown in Figure 3-13 will be displayed, and for Linux and Mac users, the page shown in Figure 3-14 will be displayed.
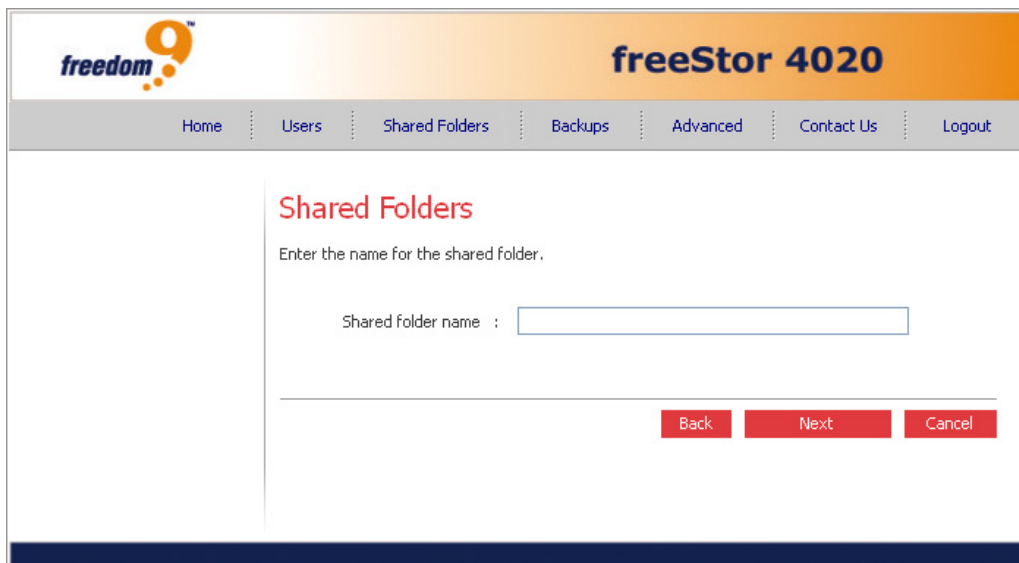
Figure 3-13: CIFS Add Shared Folder Page
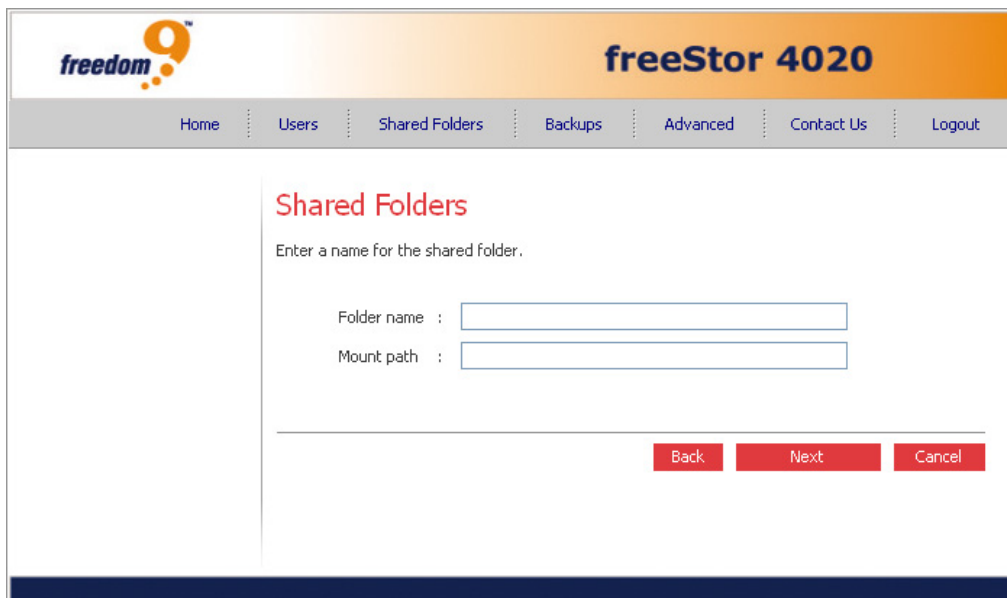
Figure 3-14: NFS Add Shared Folder Page

3. In the Shared folder name text box, enter a unique name for the shared folder, and then click "Next". This name can be up to 64 characters long and can contain letters, numbers, hyphens, underlines, and spaces.

> **Note:** Each shared folder name must be unique. For example, if you create a shared folder named Photos for Windows/OS X users, you cannot subsequently create a shared folder named Photos for Linux/Mac users. In addition, the shared folder name cannot be the same as any Windows/OS X user name.

4. For Linux/Mac users, the Mount path indicates the path that those users will specify when accessing the shared folder. As you enter a shared folder name in the text box, the same name is appended to the mount path. (You cannot change the first part of the mount path—/nas/NASDisk-00002/).

5. The page that appears next varies, depending on the user type selected. For Windows and OS X users, the page shown in Figure 3-15 will be displayed, and for Linux and Mac users, the page shown in Figure 3-16 will be displayed.

Figure 3-15: CIFS Define Folder Permissions Page
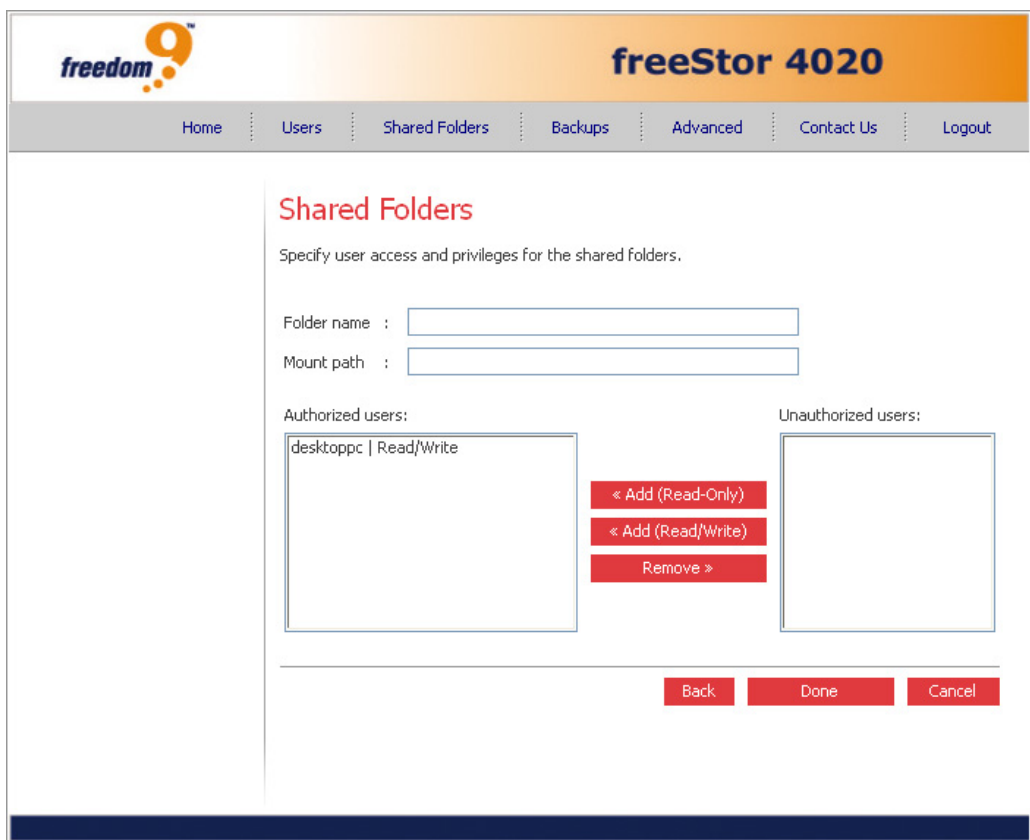
Figure 3-16: NFS Define Folder Permissions Page

6. From the Unauthorized users list, select the name of the user(s) who should be given access this shared folder. To select multiple, contiguous users, hold down the Shift key and select the first user, then select the last user. All users between the first and last selected user are selected. To select multiple, non-contiguous users, hold down the Ctrl key as you select each user. Then click the "Add" button corresponding to the access rights that the selected user(s) should have:

Read-Only: Only read the files in the shared folder and its subfolders.

Read/Write: Read, add, modify, and delete the folders and files in the shared folder.

7. The selected user(s) will then move from the Unauthorized users list to the Authorized users list along with the type of access granted to the user(s). If you accidentally add a user that you didn't mean to add, select the user in the Authorized users list and click "Remove". The user will then return to the Unauthorized users list.

Note: The same procedure can be performed for groups as well If groups have been created. For CIFS users, the page shows all existing groups and users. For example, if you created a group named Group1, and added User2 and User3 to that group, the Unauthorized groups list includes Group1, and the

Unauthorized users list includes User2 and User3. If you select Group1 and click "Add (Read-Only)", Group1 moves to the Authorized groups list, but User2 and User3 do not move to the Authorized users list. This allows you to specify unique access rights for those users. For example, you could select User3 and click "Add (Read/Write)". This willl mean that everyone in Group1 will have read-only access to the shared folder except User3, who will have read/write access to it. On the Shared Folders page, the group name in the Users with access column is preceded by an @ symbol.

To edit an existing shared folder:

For any shared folder that appears in the Shared folders list or any USB disk, you can change which users can access it and what level of access they have. Shared folders that are created as a result of creating Windows/OS X users do not appear in the Shared folders list and cannot be modified. These folders automatically provide only the associated user with read/write access to that folder.

> **Note:** By default, all users have read/write access to the public folder. You can change the user assignments or access rights for the public folder.

When you add a user to the list of authorized users for a shared folder or USB disk, that change takes effect immediately. However, if you remove a user from the list of authorized users, or if you change the user's access rights, the change does not take effect until that user disconnects from the shared folder or USB disk, or shuts down the computer.

For example, the user Alice might have read/write access to the Budget shared folder. If Alice is currently connected to that shared folder and you subsequently remove her from the list of authorized users or change her access level to read-only, she will continue to have read/write access to that folder until she disconnects or shuts down her computer. The next time she connects, she will either not have access (if she was removed from the list of authorized users), or she will be able to only view the files there (if her access level was changed).

To change user access to shared folders and USB disks:

1. In the Shared folders list, select the shared folder or USB disk whose user access you want to change.

2. Click "Assign Access".

3. If you selected a shared folder or a USB disk to which you previously assigned users, go to step 6.

4. If you selected a USB disk to which you did not previously assign users, select the type of

user that you want to assign to this USB disk, and then click "Next".

5. The operating system used by the user determines which option you should choose - Windows/OS X user (CIFS) or Linux/Mac user (NFS).

> **Note:** Linux and Mac users access shared folders using NFS. In this environment, access to shared folders is given to entire computers, not to individual users of those computers. However, in Windows and OS X environments, each computer user can have individual access to a shared folder.

6. Return to step 5 of the previous section (To add a new shared folder) and follow the remaining steps to make changes to the selected shared folder.

To delete an existing shared folder:

Once you have created a shared folder, you can delete it at any time. When you delete a shared folder, any users who are currently accessing it are immediately disconnected from it.

> **Warning:** Deleting a shared folder deletes all the subfolders and files in that shared folder. If you want to delete only selected subfolders or files, access the shared folder and delete the desired items.

To delete a shared folder:

1. In the Shared folders list, select the shared folder that you want to delete.

2. Click "Delete".

3. When prompted to confirm the deletion, click "Yes".

The shared folder no longer appears in the Shared folders list, and all associated subfolders and files are deleted.

3.6 Managing Backups

Once the users have used DiskSafe Express to back up their computer hard disks to the storage system, clicking on the "Backups" button in the menu will open the Backups Page (Figure 3-17) which displays a list of each computer that has performed a backup, the size of each protected disk, the date and time of the last four backups, and the backup disk ID (the number used to identify the backup on both the storage system and on the Status page in DiskSafe Express).
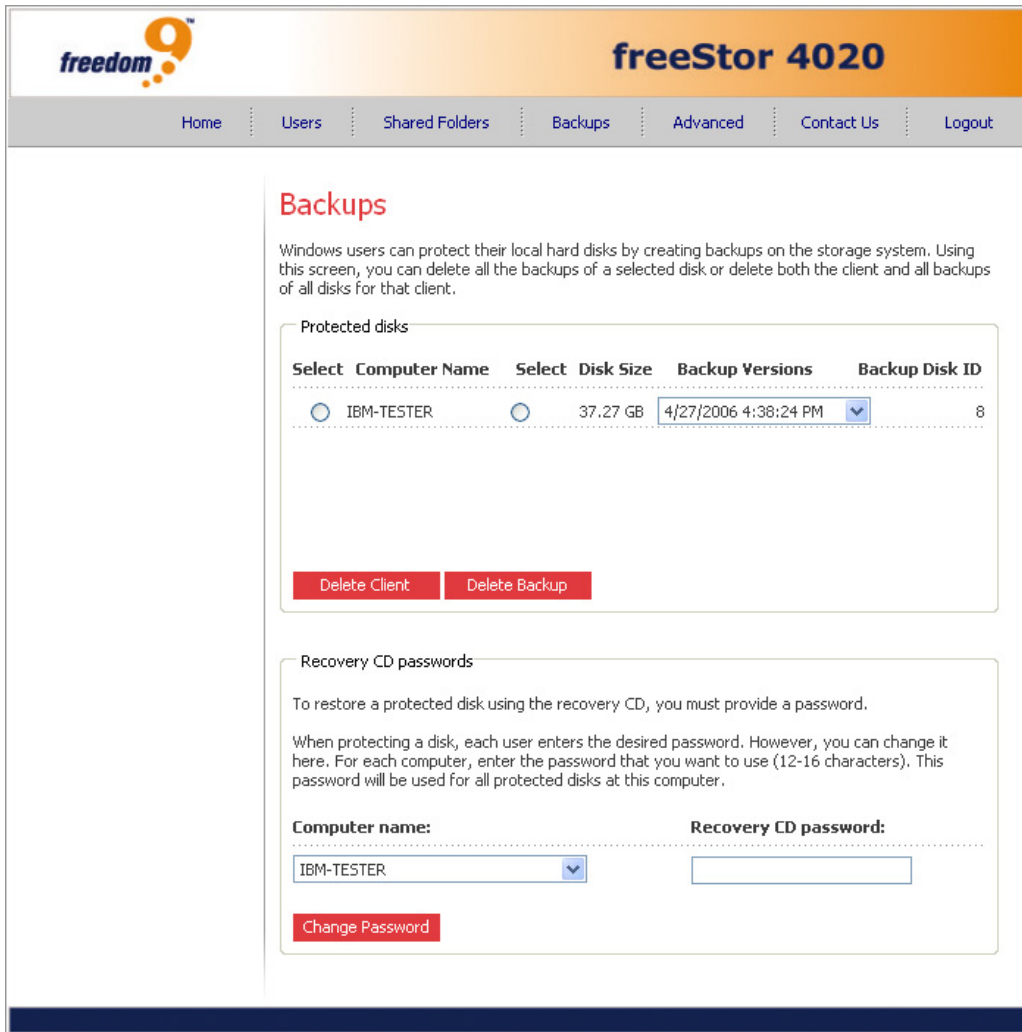
Figure 3-17: Backups Page

When the user first performs a backup, the user must enter a password which is used to perform a recovery of the backup. If the user forgets the password, it can be changed on the page. When a user removes protection for a disk, the existing backups are not deleted. The user can re-use the allocated space for new backups, or the backups can be deleted manually using the Backups page.

To change the recovery CD password:

1. In the Computer name list, select the name of the computer whose recovery CD password is to be changed.

2. In the Recovery CD password text box, type the password to use. (This password must be 12–16 characters long.)

3. Click "Change Password".

The user must provide this password when recovering a disk from this storage system using the recovery CD.

Deleting backups

You can delete all backups of a given disk, but you cannot delete just an individual backup from a specific date and time.

> **Note:** If you delete all backups of all disks for a particular computer, that computer no longer appears on the Backups page. However, that computer name remains in the storage system and counts toward the total number of computers that are allowed to back up to the storage system. If you want to delete all backups of all disks and the computer name, refer to the next section, "Deleting a client."

To delete all backups of a disk:

1. Select the radio button adjacent to the disk whose backups you want to delete (in the second Select column).

2. Click "Delete Backup".

3. When prompted to confirm the deletion, click "Yes".

The disk no longer appears on the Backups page, and all backup versions are deleted. If only one disk was protected, the computer name disappears from the page as well.

> **Note:** If you delete a backup and the user did not previously remove protection for that disk, when the user subsequently accesses DiskSafe Express, the Status page will indicate that the backup of the protected disk is offline. To back up the disk once again, the user must remove protection and then protect the disk again.

Deleting a client

If you remove DiskSafe Express from a particular computer, or if you change the computer name, the original computer name remains on the storage system and counts toward the total number of computers that are allowed to back up to the storage system. To both delete all backups of all disks for a particular computer and the computer name, you must delete the client itself.

To delete a client:

1. Select the radio button to the left of the computer whose backups and computer name you want to delete from the storage system (in the first Select column).

2. Click "Delete Client".

3. When prompted to confirm the deletion, click "Yes".

All backups of all disks associated with this computer are deleted, and the computer name is also deleted from the storage system.

> **Note:** If you delete a client and the user did not previously remove protection for that disk, when the user subsequently accesses DiskSafe Express, the Status page will indicate that the backup of the protected disk is offline. To back up the disk once again, the user must remove protection and then protect the disk again.

3.7   Email Alerts

Clicking on the "Advanced" button in the menu will open the Alerts page (Figure 3-18) which allows you to set up the storage system to send notification emails to up to three email addresses if a problem occurs—for example, if one of the disks fails, or if insufficient space is available for creating new files or performing a backup. To take advantage of this feature, you must have access to an SMTP e-mail server, either within your own network or through an Internet service provider.

> **Note:** The e-mail might not be sent immediately when the problem occurs, but will be sent within an hour of the event. In addition, if the problem is fixed within an hour of its occurrence – for example, if you replace the disk that failed – the alert will not be sent.
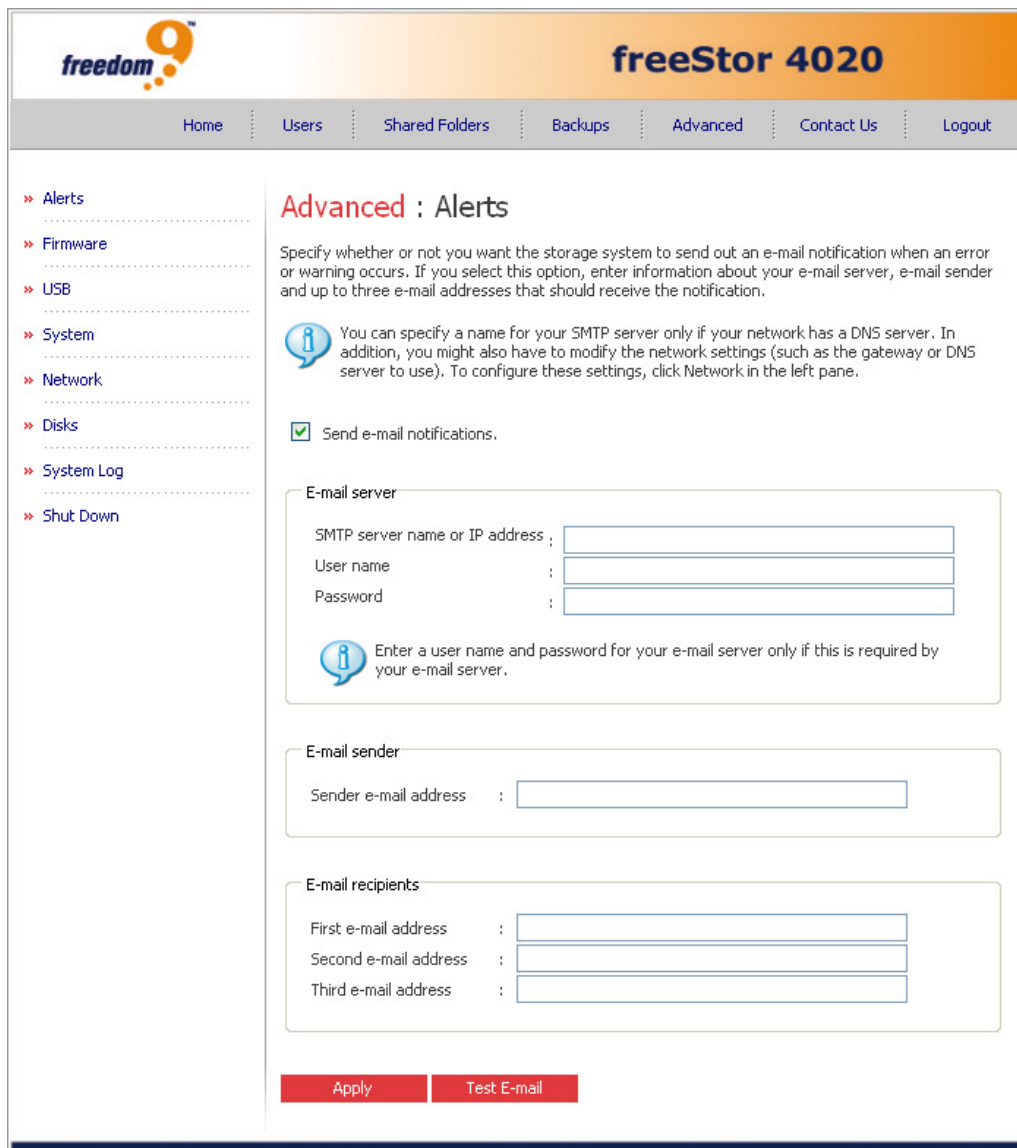
Figure 3-18: Alerts Page

To set up e-mail alerts:

1. Specify whether or not the storage system should send e-mail notifications when a problem occurs by selecting or clearing the "Send e-mail notifications" check box.

2. If you select this option, enter the fully qualified domain name or IP address of your email server and at least one email address.

3. If you clear this option, e-mail notifications will not be sent, and all the related fields on this page appear dimmed. However, if you previously entered information on this page, that information is retained so that you can easily re-enable email notifications later. If you clear this option, you do not have to complete the rest of this procedure; simply click "Apply".

4. In the SMTP server name or IP address text box, enter the fully qualified domain name or

IP address of your email server.

5. If required by your email server, enter a user name and password for logging into that server in the User name and Password text boxes.

6. If your email server cannot use the default sender email address (root@localhost), or if you want the individuals who receive email notifications to be able to reply to the alert, enter the address that you want to appear as the return address in the Sender e-mail address text box. For example, you could enter your own e-mail address (such as MyName@MyCompany.com).

7. In the First e-mail address text box, enter the eemail address of an individual who should receive e-mail notifications when a problem occurs.

8. The email address can be up to 128 characters long and must include the @ symbol (for example, MyName@MyCompany.com).

9. If you want email notifications to be sent to other individuals as well, enter the appropriate e-mail addresses in the Second e-mail address and Third e-mail address text boxes.

10. Click "Apply".

11. When the confirmation message appears, click "OK".

To confirm that the configuration is correct, click "Test E-mail", and click "OK" when the confirmation message appears. This sends a test message to the specified recipients. If they do not receive the test message, make sure that all the entries on this page are correct. You might also have to modify the network settings (such as the gateway to use).

3.8   Firmware Upgrades

Clicking on the "Advanced" button in the menu, then clicking "Firmware" on the left menu will open the Firmware page (Figure 3-19) which displays the current version of the firmware that is installed on your storage system. It also allows you to upgrade it if newer firmware becomes available.   For additional security, you must enter your administrator password in order to upgrade the firmware.

> **Warning:** When you upgrade the firmware, the storage system restarts, and access to the Manager is temporarily interrupted. Users will not be able to access the shared folders while the system restarts. If users have shared files open, data might be lost. Be sure to have all users save their changes and close any open files before you upgrade the firmware.

Restarting the storage system when a backup is occurring will not have any adverse effect; the backup will resume automatically when the storage server resumes operation. However, restarting the storage system when a disk is being recovered can potentially corrupt the user's operating system, and the user will have to recover the system disk using the recovery CD (or, if the system disk was not protected, re-install the operating system). Be sure to upgrade the firmware only when DiskSafe Express recovery is not occurring.
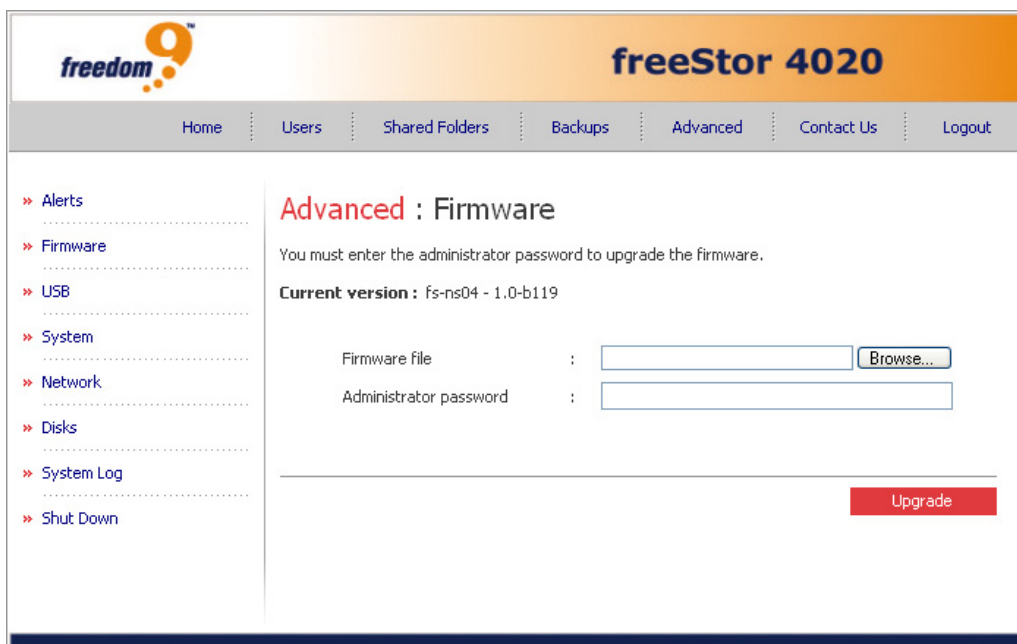
Figure 3-19: Firmware Page

To upgrade the firmware:

1. In the Firmware file text box, enter the path and file name for the firmware package (which typically ends in ".pkg"), or click "Browse" and select the file from the displayed list.

2. In the Administrator password text box, enter the password that you use for logging in to the Manager.

3. Click "Upgrade".

4. When the confirmation message appears, click "OK".

3.9   USB Devices

Clicking on the "Advanced" button in the menu, then clicking "USB" on the left menu will open the USB page (Figure 3-20) which displays a list of all USB devices that are currently attached to the storage system, including the type of device it is, the manufacturer, and the name. USB

disks are identified by the names usbdisk1 and usbdisk2. USB printers are identified by the names usbprinter1 and usbprinter2. These names cannot be changed.
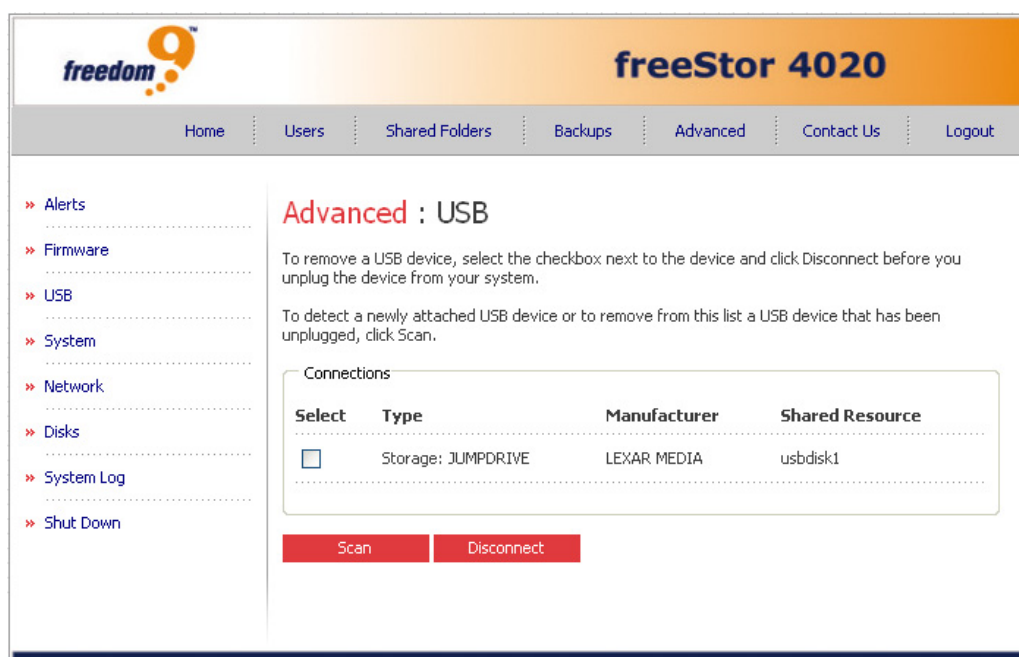
Figure 3-20: USB Page

When you plug a USB device into the storage system, the storage system automatically detects it and adds that device to the USB page. (You might need to click "Scan" to update the display.)

However, when you want to unplug a USB device from the storage system, you must first use the Manager to disconnect it. This prevents data corruption and other potential problems with the device. Once the USB device has been disconnected via the Manager, you can unplug it.

To disconnect a USB device:

1. In the list of USB devices, select the device(s) that you want to disconnect.

2. Click "Disconnect".

3. When the confirmation message appears, click "OK".

You can now unplug the USB device.

> **Note:** If you inadvertently disconnect a USB device that you want to retain, unplug it from the storage system, plug it back in, and then click "Scan". This reactivates the USB device. Since the USB device always remains on the Shared Folders page, any user assignments are always retained. If you remove one USB device and insert another one into the same port, the permission will be carried over from the previous device to the new one.

3.10 System Settings

Clicking on the "Advanced" button in the menu, then clicking "System" on the left menu will open the System page (Figure 3-21) which displays the settings that you specified when you initially configured the storage system, such as the storage system name, and the current date and time.

> **Note:** Changing the storage system name might affect access to shared folders or backups, depending on how your network is configured and how users access the storage system.
>
> For example, if users connected to the storage system using its IP address, changing the name has no effect. However, if they connected using the name, they must disconnect from their shared folders and then access the shared folders again using the new name.
>
> If the DiskSafe Express users connected to the storage system using its name, they must remove protection from all disks that connected to this storage system and protect their disks again, using the new name.
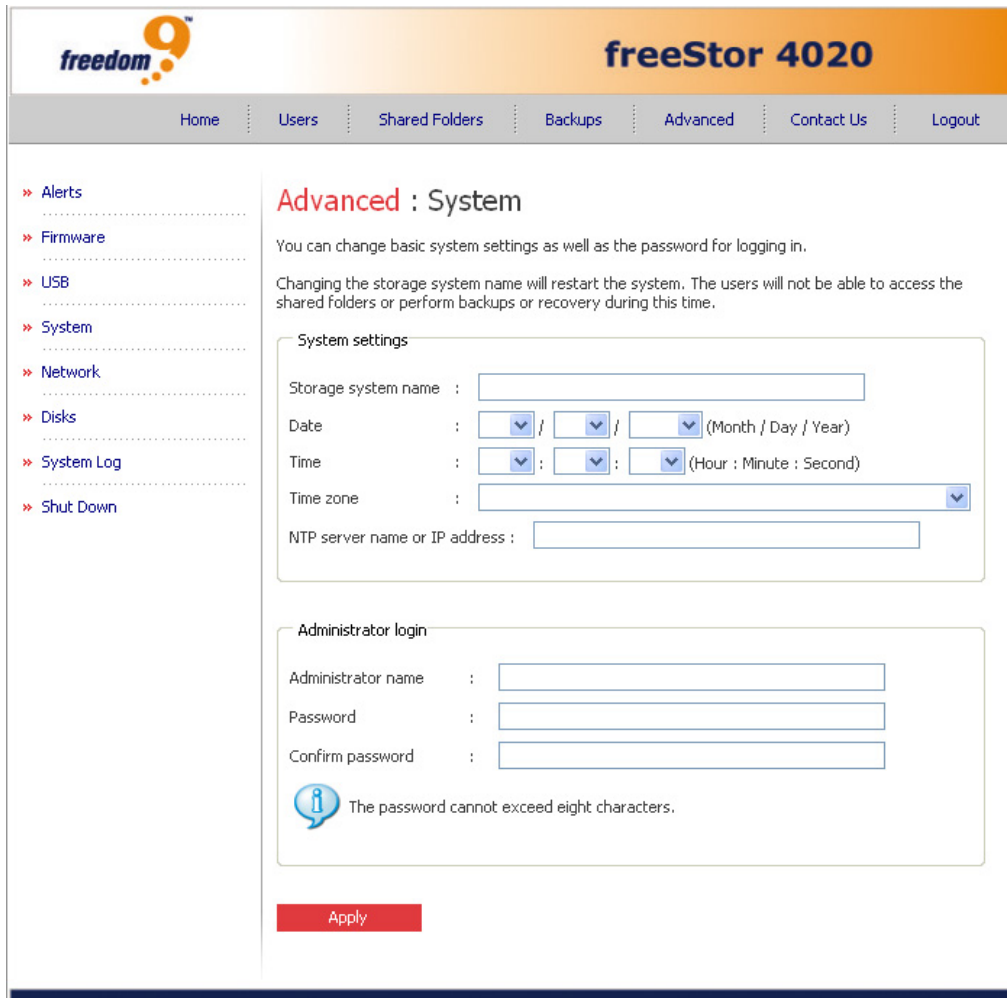
Figure 3-21: System Page

Using the System page, you can also change the administrator name and password to use for logging in to the Manager.

To change any of the system settings:

1. Make the desired changes based on the following options:

- Storage system name: The name of the freeStor 4020 used on the network. This name can be up to 15 characters long and can include letters, numbers, and hyphens.

- Date: The current date.

- Time: The current time.

- Time zone: The local time zone.

- NTP server name or IP address: If using an NTP (Network Time Protocol) server to set the time, enter its IP address here. You can use a name only if it is resolvable.

- Administrator name: The name used to log into the web interface.

- Password: The password used to log into the web interface.

- Confirm password: If changing the password, must match the password entered in the Password textbox.

The user name and password are case-sensitive.

2. Click "Apply".

3. When the confirmation message appears, click "OK".

3.11 Network Settings

Clicking on the "Advanced" button in the menu, then clicking "Network" on the left menu will open the Network page (Figure 3-22) which displays the network settings that were set when you initially configured the storage system.

> **Note:** Changing the IP address or subnet mask can have several effects. If you access the Manager using the Storage System Console or using the storage system's IP address, access to the Manager will be disrupted and you will have to access it again using the new IP address. Users who accessed the shared folders using the previous IP address will be disconnected and must access them again using the new IP address. Users who backed up their disks to the storage system using the previous IP address must remove protection for all affected disks and protect their disks again, removing the storage system from the list of backup locations and adding it again using the new IP address.
>
> Users who backed up their disks to the storage system using the storage system name do not have to remove protection from their disks or remove the storage system from the list of backup locations. However, they must start DiskSafe Express so that it can retrieve the new IP address.
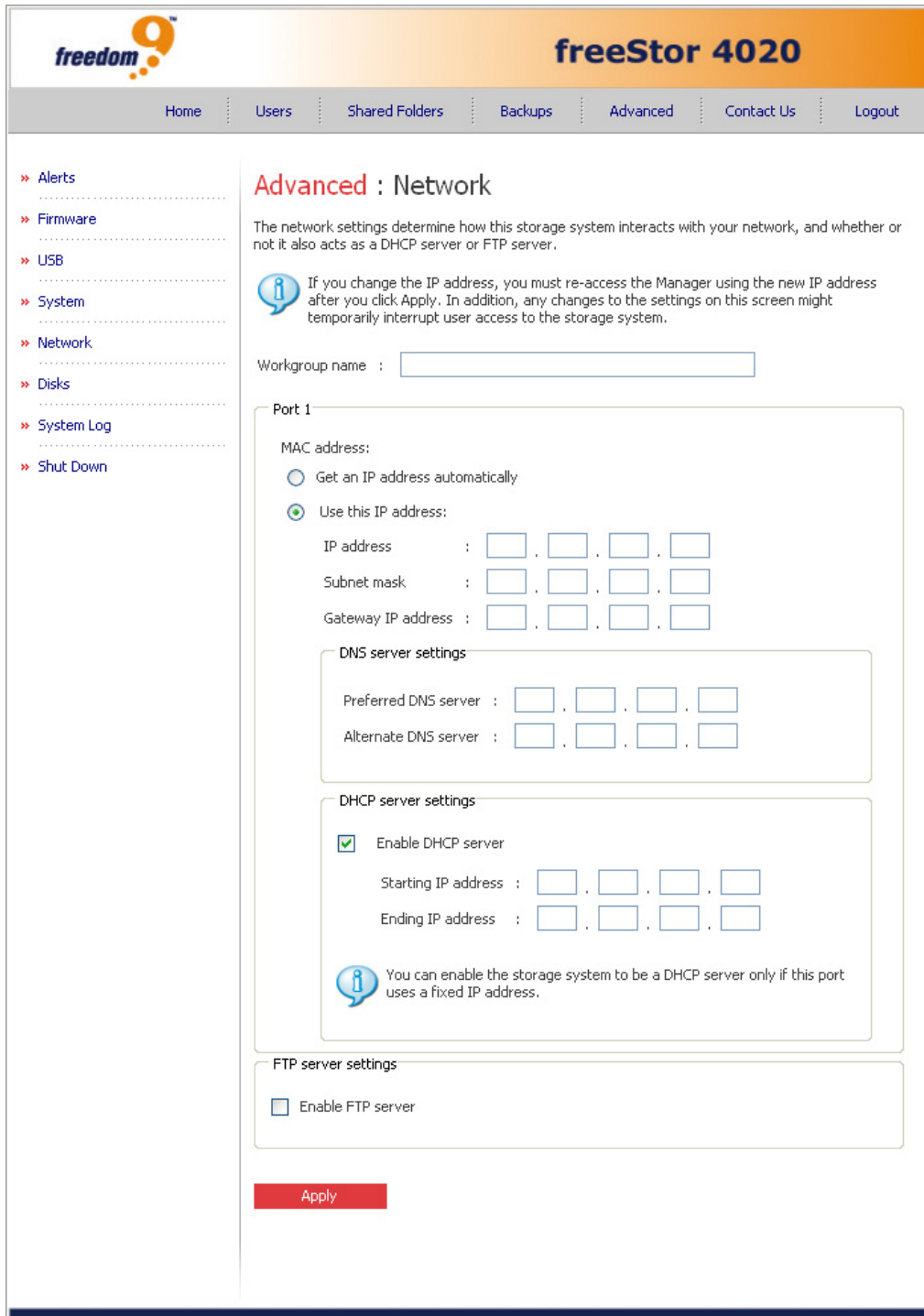
Figure 3-22: Network Page

You can also configure the storage system to act as a DHCP server. In other words, the storage system can assign IP addresses to other computers in your network, simplifying the network configuration of each individual system.

In addition, your storage system can act as an FTP server. This allows all Windows/OS X users to use a Web browser or FTP client to access the public folder. They can also access their personal folder that was created automatically when their user name was added to the

storage system. For more information, refer to "Accessing the storage system using FTP".

To change any of the network settings:

1. Make the desired changes based on the following options:

- **Workgroup name:** The workgroup to which the storage system belongs on the network. In the Workgroup name text box, enter the name of the workgroup. This name can be up to 15 characters long.

- **Get an IP address automatically:** Instructs the freeStor 4020 to obtain an IP address from a DHCP server on the network.

- **Use this IP address:** Sets the IP address of the freeStor 4020 manually based on the fields below.

- **IP address:** The IP address of the device (if set to manual IP mode).

- **Subnet mask:** The subnet mask of the device (if set to manual IP mode).

- **Gateway IP address:** The gateway IP address of the device (if set to manual IP mode).

- **Preferred DNS server:** The primary DNS server's IP address for the device to use (if set to manual IP mode).

- **Alternate DNS server:** The secondary DNS server's IP address for the device to use (if set to manual IP mode).

- **Enable DHCP server:** Enables the DHCP server on the freeStor 4020. It is important to note that only one DHCP server should be active on the network at any one time to prevent conflicts.

- **Starting IP address:** The start of the IP address range to be assigned by the DHCP server.

- **Ending IP address:** The end of the IP address range to be assigned by the DHCP server.

2. Click "Apply".

3. When the confirmation message appears, click "OK".

   Note: If you changed the IP address of the storage system, you must now access the Manager using the new IP address.

3.12 Disk Configuration

Clicking on the "Advanced" button in the menu, then clicking "Disks" on the left menu will open the Disks page (Figure 3-23) which displays information about all the hard disks that are currently installed in your storage system.
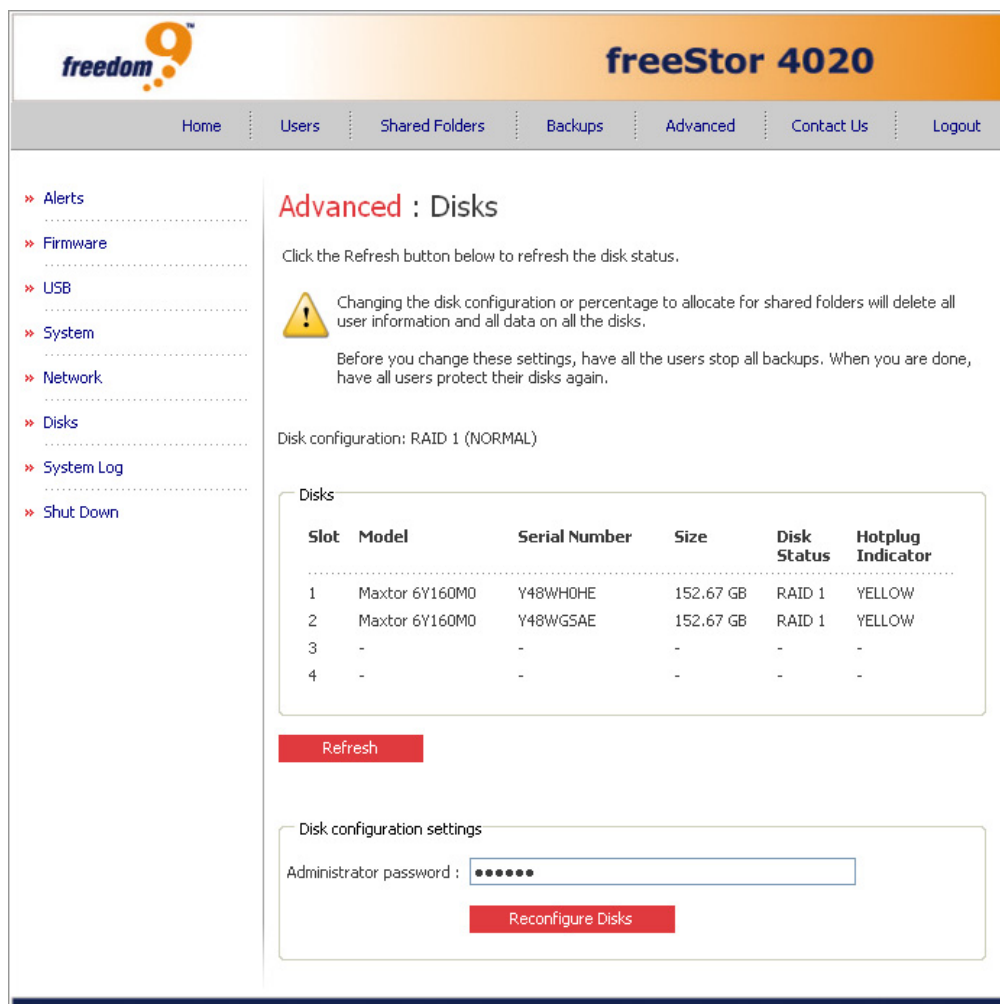
Figure 3-23: Disks Page

This page includes the following details:

- The disk configuration (that is, whether the disks use a linear or RAID configuration, and the RAID level)

- The overall status of the disks:

  o Normal – All the disks are working properly.

  o Degraded – One or more disks have failed but all the data is still available.

  o Failed – The storage system has stopped working properly.

- The slot where each hard disk resides.

- The model number, serial number, and size of each hard disk.

- The current status of each disk:

  o RAID – The disk is working properly as part of the specified RAID level.

  o New – The disk has been added to the storage system but is not part of a RAID.

  o Spare – The disk is acting as a spare disk for the RAID.

  o Rebuilding – The disk is being rebuilt (for example, when a failed disk is replaced)

- N/A – The disk is detected but not available for use (for example, when it has failed)

- The hotplug indicator:

  o RED – Removing the disk will cause the RAID to fail.

  o YELLOW – Removing the disk will cause RAID degradation.

  o GREEN – Removing the disk will not affect the RAID.

  Note: Whenever a disk is added or removed from the storage system, you must click "Refresh" to update this page.

You can change the disk configuration or percentage of the storage space that is allocated for shared folders at any time. However, for additional security, you must enter your administrator password to be able to make these changes.

  Warning: Changing the disk configuration or percentage to allocate for shared folders will delete all user information and all data on all the disks. Before you change these settings, have all the users disconnect from all shared folders and remove protection from all disks. When you are done, you must re-add all users, create new shared folders, and have all users once again access the shared folders and protect their disks.

To change the disk configuration or storage space allocation:

1. In the Administrator password text box, enter your password for logging in to the Manager.

2. Click "Reconfigure Disks".

3. When the confirmation message appears, click "OK".

4. The Disk Configuration page (Figure 3-24) appears. (The options that appear on this page vary, depending on the number of hard disks that are currently installed in the system.)
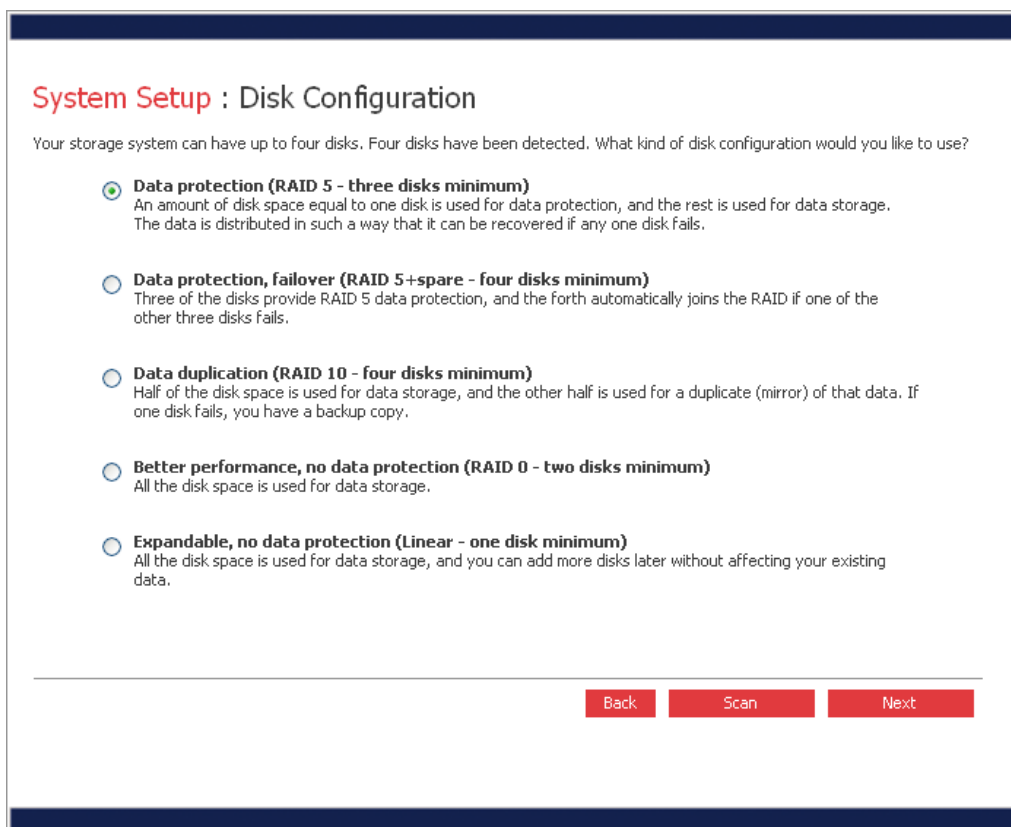
Figure 3-24: Disk Configuration Page

5. If you want to add or remove hard disks, do so one at a time and click "Scan" after each action.

6. To accept the default disk configuration (which will provide the best level of data protection available for the number of hard disks currently installed), click "Next". By default, a linear disk configuration is used for a single hard disk, RAID 1 is used for two hard disks, and RAID 5 is used for three or four hard disks.

7. If you want to change the disk configuration, select the desired RAID level and then click "Next".

8. The Disks to Back Up page (Figure 3-25) appears.
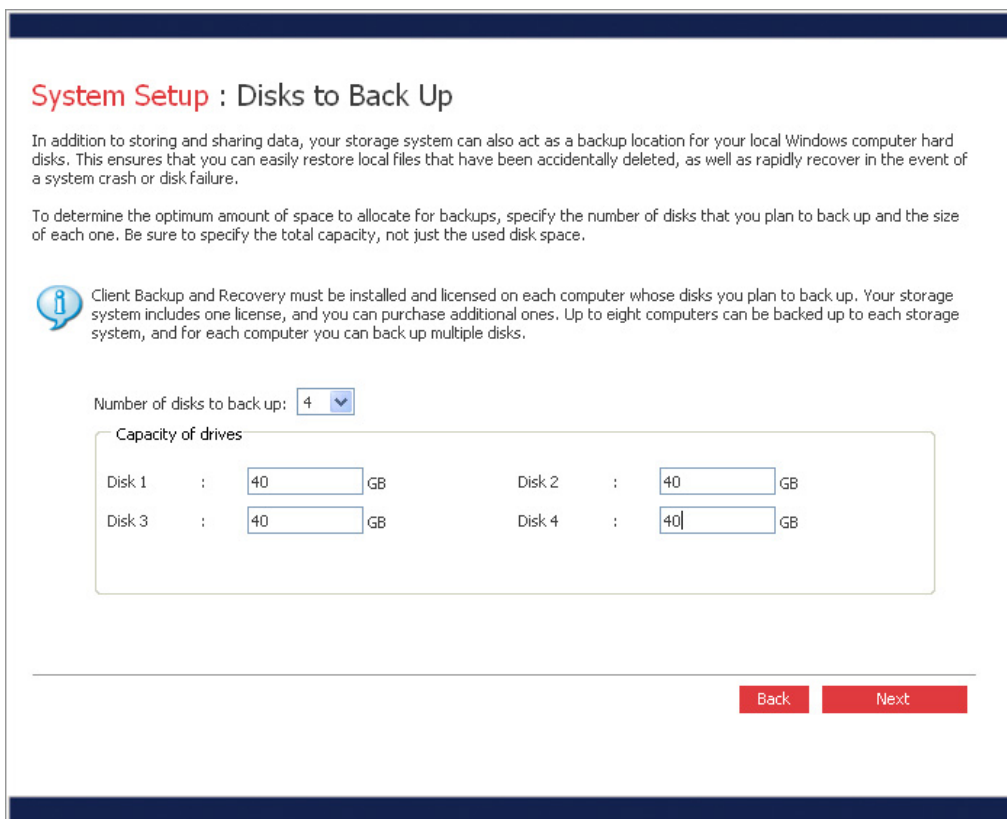
Figure 3-25: Disks to Back Up Page

9. In the Number of disks to back up list, select the total number of disks that you plan to back up to this storage system.

10. If some computers have multiple disks, be sure to select the total number of disks that you plan to back up. For example, if your network has five computers and each computer has two hard disks, you would select 10.

11. When you select a number from this list box, a corresponding number of text boxes (Disk 1, Disk 2, etc.) appear in the Capacity of drives group box.

12. If you don't plan to back up any disks, select 0, click "Next", and go to step 18.

13. The maximum number of disks you can back up is 25.

14. If you leave this field blank, 70% of your storage space will be allocated for backups, and 30% will be allocated for shared folders.

15. In each text box, enter the size of each disk that you plan to back up (in gigabytes).

16. To determine the size of a disk, open My Computer or Windows Explorer on that computer, right-click the disk, and then click Properties. Be sure to enter the entire capacity of each disk, not just the amount of used disk space.

17. If a disk is smaller than 1 GB, divide the number of megabytes by 1024. For example, a

512-MB disk would be .5 GB (512 divided by 1024 is .5).

> **Note:** Only 99% of the available storage space can be allocated for backups. If the amount of disk space you need exceeds that limit, you will not be able to back up all the disks.

18. The Disk Space Distribution page (Figure 3-26) appears:
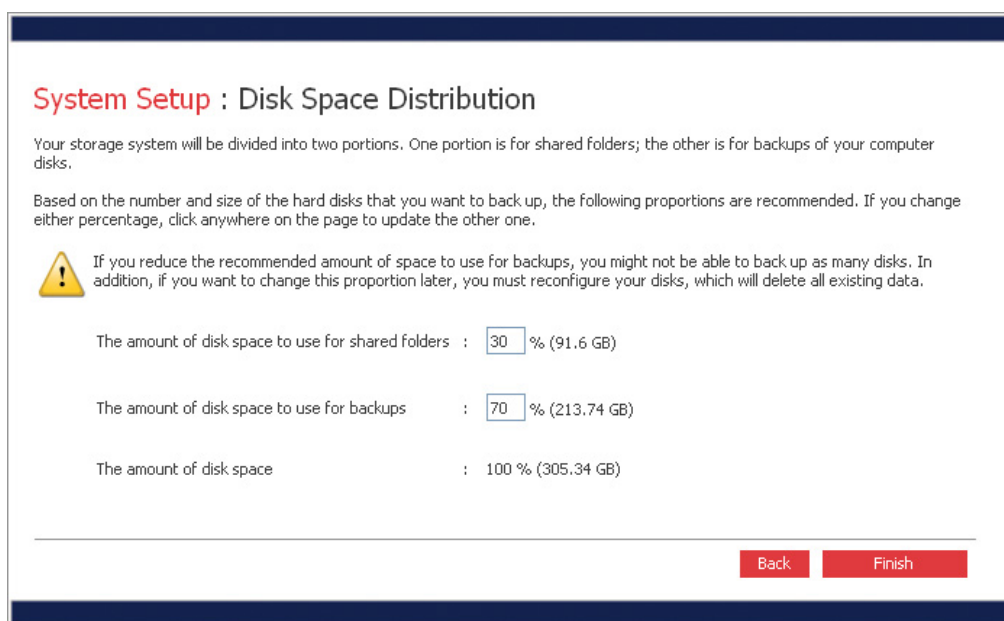
Figure 3-26: Disk Space Distribution Page

19. To change the percentage of space allocated for shared folders and backups, enter the desired percentage for each usage type. (The percentages must add up to 100%.) Then click "Reconfigure Disks".

20. When the confirmation message appears, click "OK".

21. The Disk Configuration Status page (Figure 3-27) displays the progress of the process:
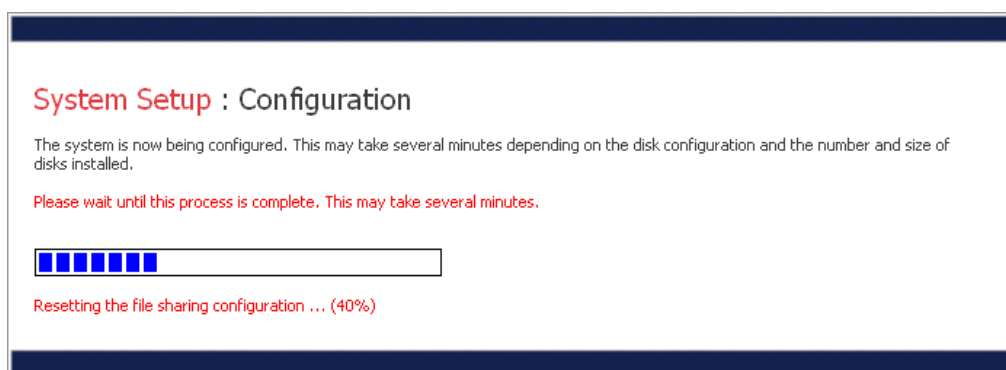
Figure 3-27: Disk Configuration Status Page

22. When this process is complete, the Disk Configuration Completion page (Figure 3-28) will

be displayed and the storage system will restart.
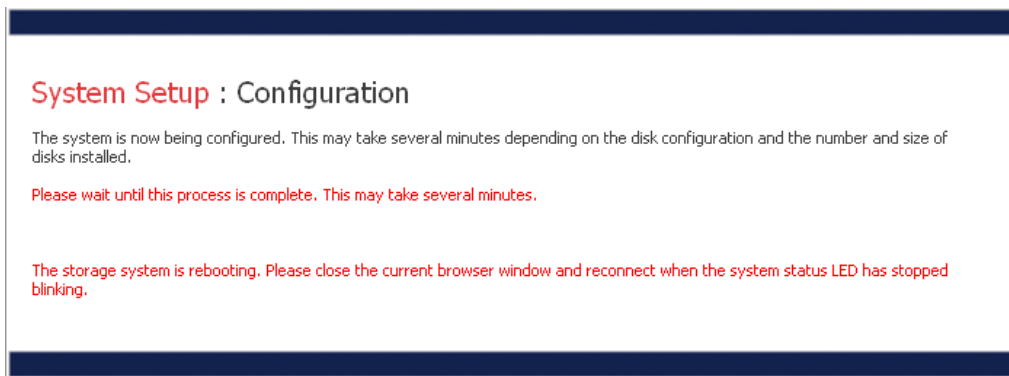
Figure 3-28: Disk Configuration Completion Page

23. Close the browser window.

24. After the system has restarted, you can access the Manager and re-create your users and shared folders.

3.13 Logging Out

When you have finished using the Manager, it is recommended that you log out to ensure that unauthorized individuals do not make changes to the storage system.

To log out:

1. Clicking on the "Log Out" button in the menu.

2. When the confirmation message appears, click "OK". The Log Out page appears.

3. To log back in to the Manager later, click "Log In".

3.14 Shutting Down

Clicking on the "Advanced" button in the menu, then clicking "Shut Down" on the left menu will open the Shut Down page (Figure 3-29) which allows you to shut down the unit from the web interface. To ensure that you don't shut down the system accidentally, you must enter your administrator password to shut down the device.
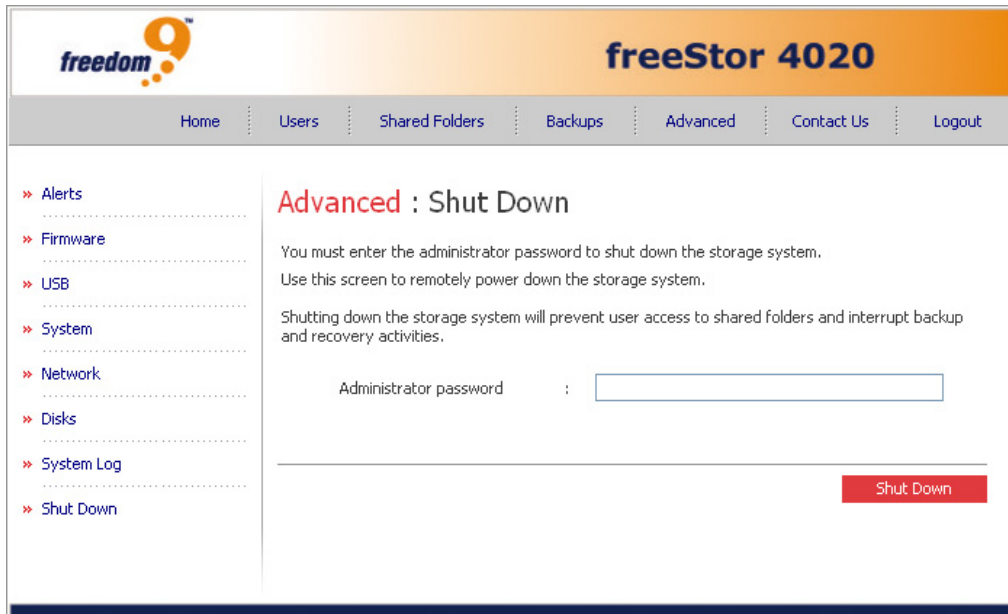
Figure 3-29: Shut Down Page

Warning: If you shut down the storage system, users will no longer be able to access the shared folders on the storage system. If users have shared files open, data might be lost. Be sure to have all users save their changes and close any open files before you shut down the storage system.

Shutting down the storage system when a backup is occurring will not have any adverse effect; the backup will resume automatically when the storage server is powered on again. However, shutting down the storage system when a disk is being recovered can potentially corrupt the user's operating system, and the user will have to recover the system disk using the recovery CD (or, if the system disk was not protected, re-install the operating system).

To shut down the storage system using the Manager:

1. In the Administrator password text box, enter the password for logging in to the Manager.

2. Click "Shut Down".

A message appears, indicating that the system is shutting down.

Once the storage system shuts down, if you refresh the browser window, it will be blank. If you subsequently try to access the Manager, an error message will appear, since the storage system will no longer be running.

4 File Sharing and System Backup

4.1 File Sharing

The freeStor 4020 allows users to share files quickly and easily, using multiple operating systems. By default, there is one shared folder called "public" that is accessible by all users. Additional shared folders can be created by using the Web Management Interface. The procedure for accessing shared folders depends on the operating system being used.

4.1.1 Windows Clients

If you're using Windows, you have two options for accessing shared folders: you can use My Computer or Windows Explorer to map a drive letter to the shared folder, or you can install the Storage System Console and use that utility to map a drive letter to the shared folder (see Section 2.2 for instructions on installing the console). With the Storage System Console, you don't have to worry about remembering the name of the storage server or the shared folders; it displays them automatically. However, the computer where you install the Storage System Console must be on the same subnet as the storage system.

Using My Computer or Windows Explorer

To access a shared folder using My Computer or Windows Explorer:

1. Open My Computer or Windows Explorer.

2. From the Tools menu, click Map Network Drive to open the Map Network Drive dialog box (Figure 4-1).
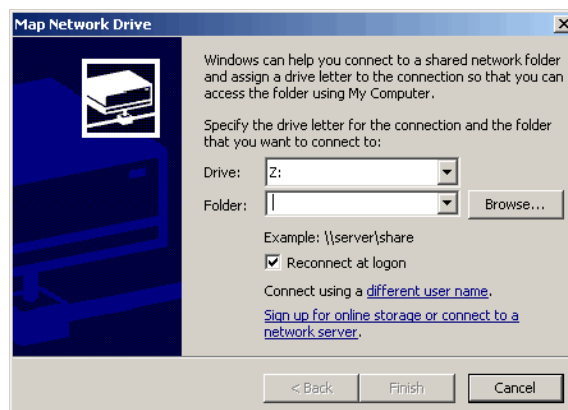
Figure 4-1: Map Network Drive

3. In the Drive list, select the drive letter that you want to assign to the shared folder.

4. In the Folder text box, enter the following: "\\storage_system\shared_folder" where storage_system is the name or IP address of the storage system, and shared_folder is the name of the shared folder. For example, if the storage system name is Storage and the shared folder name is Photos, you would enter the following: "\\Storage\Photos". Alternatively, you can click Browse and select the shared folder from the Microsoft Windows Network.

> **Note:** You can use the storage system name only if that name is registered with a DNS server on your network.

5. To automatically connect to this shared folder each time you log on to Windows, select "Reconnect at logon".

6. If you clear this option, you must repeat this procedure each time you want to access the shared folder.

7. Click "Finish".

8. If prompted, enter your user name and password for accessing this shared folder, and then click "OK".

> **Note:** If the user name and password for accessing the shared folder are the same as your Windows user name and password, you will not be prompted to provide a user name and password to access the shared folder.
>
> In addition, once you provide your user name and password for accessing one shared folder, you are not prompted to provide it again when you access other shared folders to which you have access rights.

If the guest user has access to this shared folder, you can use guest as both the user name and password.

You can now access the shared folder from My Computer or Windows Explorer.

Using the Storage System Console

To access a shared folder using the Storage System Console:

1. Install the Storage System Console (as described in Section 2.2).

2. Click Start → Programs → Storage System Console.

3. As soon as you start the Storage System Console, it automatically scans the network for

storage systems. This might take a few minutes. As soon as the scan is complete, the left pane displays a tree view of all the storage systems it found:

> **Note:** If you connect a storage system to the network after the Storage System Console has already scanned it, or if you change the IP address of the storage system, you must click Discover Storage Systems to scan the network again and update the tree in the left pane.

4. In the left pane, double-click the name of the storage system that contains the shared folders that you want to access.

5. The storage system name expands to display all the available shared folders. Those shared folders that can be accessed using the guest user name and password are listed first.

6. In the left pane, select the shared folder that you want to access and then click "Map Drive Letter".

> Note: The home item provides only you with access to a shared folder that is unique to your user name.

7. Go to Step 3 in the previous section (Using My Computer or Windows Explorer) and continue to the end of the procedure.

4.1.2   Linux Clients

To access a shared folder on a computer running Linux:

1. Create a directory by entering the following command at the command prompt: "mkdir /my_directory" where my_directory is the name of the directory. Be sure to include the full path to the directory (for example, "/mnt/my_directory").

2. If desired, display a list of all the available shared folders by entering the following command: "showmount -e storage_system" where storage_system is the name or IP address of the storage system.

> **Note:** You can use the storage system name only if that name is registered with a DNS server on your network.

3. Mount the desired shared folder by entering the following command: "mount storage_system:/nas/NASDisk-00002/folder /my_directory" where storage_system is the name or IP address of the storage system, folder is the name of the shared folder, and my_directory is the name of the directory that you created in step 1. If you included a full path when creating the directory, be sure to include the full path with this command (for

example, "mount storage_system:/nas /NASDisk-00002/folder /mnt/my_directory").

4. Repeat steps 1 through 3 for each shared folder that you want to access.

4.1.3   Macintosh Clients

The procedure for accessing a shared folder on a Mac varies, depending on whether the Mac is running OS X or an older operating system. (Macs running OS X can access the same shared CIFS folders as Windows users. Mac running older operating systems can access the same shared NFS folders as Linux users.)

OS X

To access a shared folder on a Mac running OS X:

1. From the Go menu, click "Connect to Server".

2. In the Address text box, enter the following and click Connect: "smb://storage_system" where storage_system is the name or IP address of the storage system.

    Note: You can use the storage system name only if that name is registered with a DNS server on your network.

3. In the Select a share list, select the name of the shared folder that you want to access and then click "OK".

4. Enter the user name and password for accessing this shared folder, and then click "OK". If the guest user has access to this shared folder, you can use guest as both the user name and password. An icon with the name of the shared folder is created on the desktop.

5. Repeat steps 1 through 4 for each shared folder that you want to access.

6. To access the shared folder, double-click the icon on the desktop.

Other Mac operating systems

For information about accessing a shared folder using NFS on a Mac running an operating system older than OS X, please refer to your Mac documentation.

4.1.4   FTP Clients

If you enabled the storage system to act as an FTP server, all Windows/OS X users can use a Web browser to access the public folder. They can also access their personal folder that was created automatically when their user name was added to the storage system.

    Note: Even if you changed the access rights to the public folder (for example,

to prevent a particular user from accessing it altogether or to limit a user to read-only access), all existing users have full read/write access to the public folder when accessing it via FTP.

To access the storage system using FTP:

1. At any Windows or OS X computer, open a Web browser, enter the following in the address bar, and press Enter: "ftp://user_name@storage_system" where user_name is the user name as defined on the storage system and storage_system is the name or IP address of the storage system (for example, "ftp://user1@storage" or "ftp://user1@192.168.0.101"). You can use guest as the user name, but you will be able to access only the public folder.

   .**Note:** You can use the storage system name only if that name is registered with a DNS server on your network.

2. If prompted, enter your user name and password for accessing shared folders, and then click "OK". If you used the guest user name, the password is also guest.

3. Double-click any of the displayed folders or files to open them. You have full read/write access to all the folders and files in both the public folder and your personal folder, and you can create new ones. If you browse to other websites, you will remain logged in until you close the browser window. (That is, you can return to the FTP site using the Back button in your browser window.)

   Note: Files copied to or from the storage system using FTP can be no larger than 2 GB.

4.2   System Backups with DiskSafe Express

Even if most of your data is stored and protected on your storage system, your operating system files, applications, and many other files still reside on each individual computer in your network. If one of those local disks fails, it can take many hours to re-install and reconfigure the operating system and applications on a new or repaired hard disk, and some files might be completely lost.

DiskSafe Express is a software application designed to address this issue. On each computer where it is installed, DiskSafe Express provides reliable data protection and rapid data recovery in the event of a system crash or disk failure.

DiskSafe Express protects Windows desktops and laptops by backing up their local disks or partitions to the storage system. To make sure that you have recent copies of your local disk,

DiskSafe Express can automatically perform a backup at regularly scheduled intervals – either once a day or once a week. (You can also disable automatic backups and just perform backups manually at a time of your choosing.) Up to four backups are saved on the storage system for each computer; each time a new backup is performed, the oldest backup is automatically deleted.

To ensure that valuable storage space isn't used up by duplicate data, when DiskSafe Express performs each subsequent backup, it copies only the data that has changed since the last time a backup was performed. This also minimizes the impact on your network. Yet through unique technology on the storage system, each backup is a complete point-in-time image. You can view or recover the entire disk or partition exactly as it existed at a particular date and time.

Whenever you want to recover data from the storage system, you can do so quickly and easily. If you need to recover just a few folders or files, you can access the desired backup and copy what you need back to your local disk. If the protected disk isn't your system disk (that is, the disk that contains the Windows operating system files that the computer uses when it runs), and you need to recover the whole disk, you can do so using DiskSafe Express. And if the protected disk is your system disk, and you need to recover the whole disk, you can do so using the recovery CD included with the freeStor 4020. Recovering the whole disk restores the disk with exactly the same data that it contained at the time the backup was performed – you don't have to reinstall or reconfigure the operating system or applications.

4.2.1   System Requirements

Each computer where DiskSafe Express is installed must meet the following system requirements:

- One of the following operating systems:

  o Microsoft Windows XP Home Edition or Professional with Service Pack 2 or higher

  o Microsoft Windows Server 2003

  o Microsoft Windows 2000 Professional, Server, or Advanced Server with Service Pack 4 or higher

- Microsoft iSCSI Initiator 2.0

- 20 MB free hard disk space

For information about downloading and installing the iSCSI Initiator 2.0, refer to the next section.

> **Note:**   DiskSafe Express requires the Intelligent Management Agent (IMA),

which is installed automatically if it is not already installed. IMA requires an additional 5 MB of free hard disk space (for both the application and associated log file data).

Microsoft .NET Framework 1.1 is also required and installed automatically if it is not already installed. The .NET Framework requires approximately 40 MB of additional free hard disk space.

In addition, if your computer name includes any characters other than letters (A–Z or a–z), numbers (0–9), hyphens (-), colons (:), or periods (.), you must change the computer name before you use DiskSafe Express to protect a disk.

If you are using a firewall on the computer that you plan to protect, TCP port 11762 must be open on the firewall to allow DiskSafe Express to communicate with the storage system.

4.2.2   Installing the Microsoft iSCSI Initiator

Before you can install DiskSafe Express, you must download and install the Microsoft iSCSI Initiator 2.0.

To download and install this initiator:

1. Open a Web browser, enter the following in the address bar, and press Enter: http://www.microsoft.com/downloads/details.aspx?FamilyID=12cb3c1a-15d6-4585-b385-b efd1319f825&DisplayLang=en

2. Scroll down to the Files in This Download section and click "iSCSI-2.0-x86fre.exe".

3. Select the option to run the file (Run, Open, or Run this program from its current location).

4. If a security warning appears, click "Run".

5. When the installation wizard starts, click "Next" on the first page.

6. On the page with installation options, click "Next". (Initiator Service and Software Initiator are selected by default.)

7. If a message box appears telling you to configure the settings in the Control Panel, click "OK".

    Note: You do not have to configure the Microsoft iSCSI Initiator. DiskSafe Express will configure it for you automatically.

8. If you agree to the terms of the license agreement, select "I Agree" and then click "Next".

9. When the installation completes, click "Finish".

After your computer restarts, you can install DiskSafe Express.

4.2.3   Installing DiskSafe Express

You must install DiskSafe Express on each computer whose local disks you want to protect.

To install DiskSafe Express:

1. Ensure the Microsoft iSCSI Initiator 2.0 is already installed by following the steps in the previous section.

2. Insert the Installation CD into your CD-ROM drive.

3. In Windows Explorer, open the "DiskSafeExpress" folder on the installation CD. Double-click the "DSESetup.exe" file to begin installation of the software.

4. If Microsoft iSCSI Initiator 2.0 is not installed on the computer, the warning message in Figure 4-2 will be displayed. If this appears, install the Microsoft iSCSI Initiator 2.0 by following the previous section before proceeding.
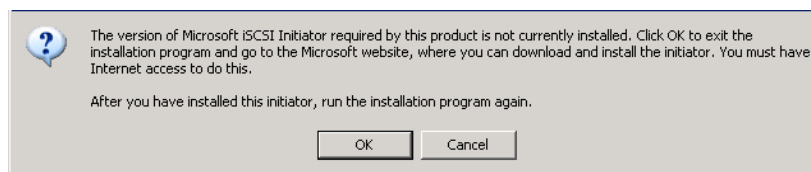
Figure 4-2: iSCSI Initiator Warning

5. If Microsoft .NET Framework 1.1 is already installed, go to the step 11. If this component is not currently installed, the following prompt appears (Figure 4-3).
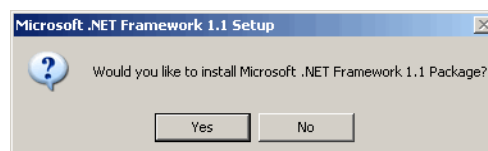
Figure 4-3: .NET Framework Warning

6. Click "Yes" to install the .NET Framework 1.1 component. You cannot install DiskSafe Express without first installing Microsoft .NET Framework 1.1.

7. When you click "Yes", the setup utility for Microsoft .NET Framework 1.1 starts (Figure 4-4).
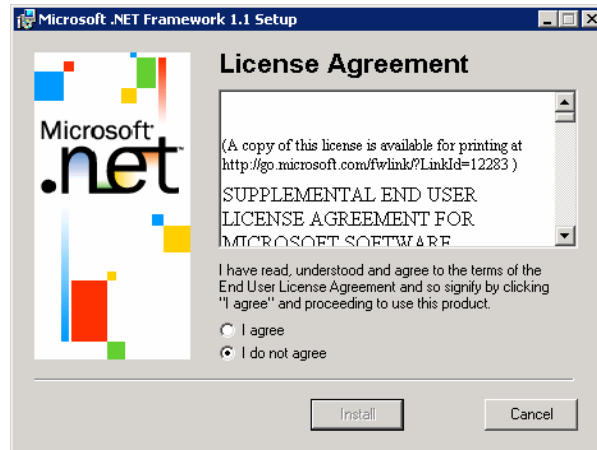
Figure 4-4: .NET Framework License Agreement

8. If you agree to the terms of the license agreement, select "I agree" and then click "Install".

9. It might take some time to copy and configure the associated files.

   Note: The remaining time might be reported as 0 and it might appear that no progress is occurring. However, configuration is occurring in the background.

10. When a message appears, indicating that the installation of Microsoft .NET Framework 1.1 is complete, click "OK".

11. After you click OK, the Intelligent Management Agent is installed automatically (if it is not already installed), and the welcome page for installing DiskSafe Express appears (Figure 4-5).
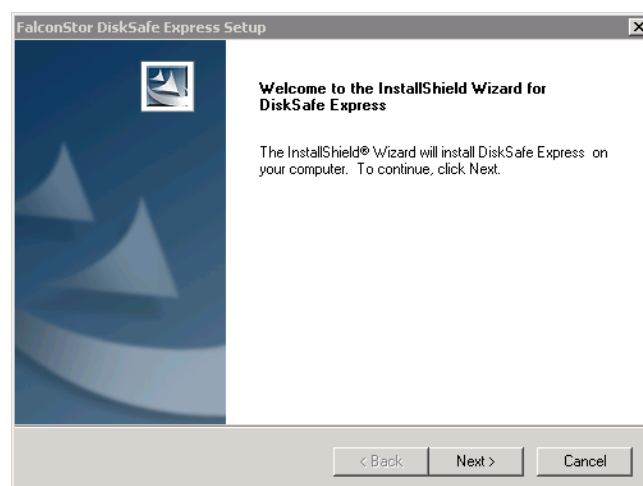
Figure 4-5: DiskSafe Express Welcome Page

12. On the welcome page, click "Next" and the License Agreement page will appear (Figure

4-6).
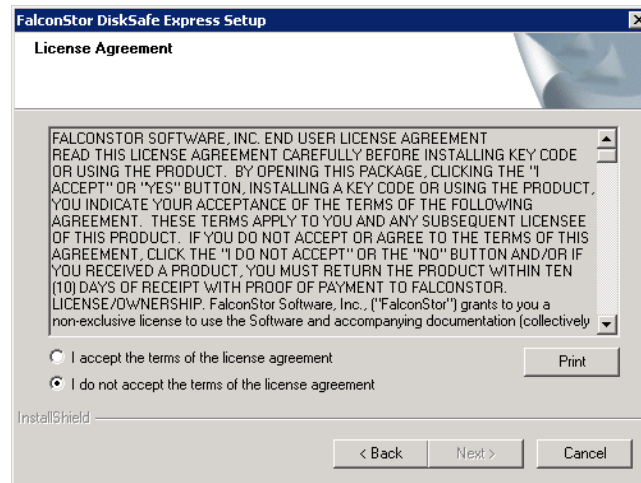
Figure 4-6: DiskSafe Express License Agreement

13. If you agree to the terms of the license agreement, select "I accept the terms of the license agreement" and then click "Next".

14. On the next page (Figure 4-7), click "Next" to install DiskSafe Express in the displayed location. Alternatively, you can click "Browse", select or enter a different location, click "OK", and then click "Next".

> **Note:** You must install DiskSafe Express on the drive that you boot from (that is, where Windows is installed, typically C:).
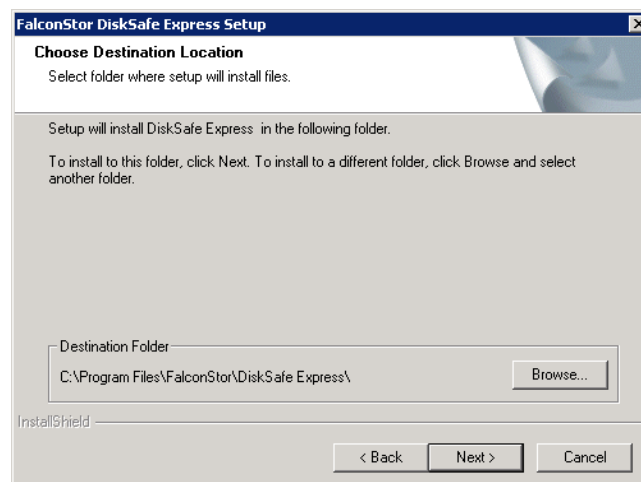
Figure 4-7: DiskSafe Express Destination Folder

15. To complete the installation and restart your computer, click "Finish" on the next page (Figure 4-8).
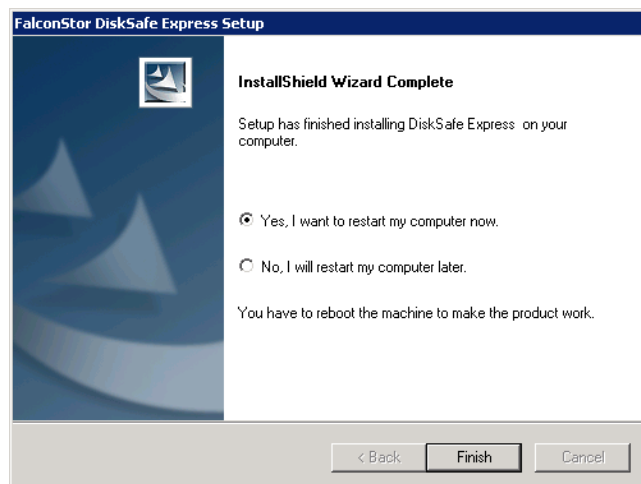
Figure 4-8: DiskSafe Express Installation Completed

16. If you do not want to restart your computer at this time, select "No, I will restart my computer later" and then click "Finish". You do not have to restart the computer immediately after installation, but you do have to restart it before running DiskSafe Express.

17. After you restart the computer, the License dialog box appears (Figure 4-9).
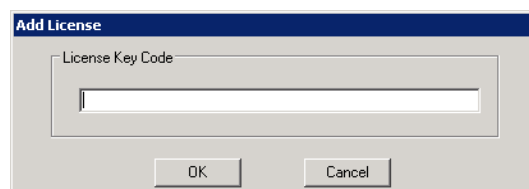
Figure 4-9: DiskSafe Express License Dialog

18. Type the key code for licensing the product and click "OK". If your computer has an Internet connection, the license is activated automatically. When you click OK on the confirmation message, the Protect a Disk wizard starts. For information about this wizard, refer to Section 4.2.6.

> Note: If you previously used this key code on a different computer, an error message appears, and you must re-activate your license. For more information, refer to Section 4.2.5.
>
> If your Internet connection is temporarily down, or if this computer doesn't have an Internet connection, click "OK" on the warning message. The Protect a Disk wizard still starts, but after 30 days you will no longer be able to perform backups or recovery until you activate the license. For more information, refer

to Section 4.2.5.

4.2.4   Starting DiskSafe Express

To start DiskSafe Express, click Start → Programs → DiskSafe Express.

If you did not protect a disk after installing DiskSafe Express and restarting your computer, you will be prompted to do so the first time you run this application. For information about this wizard, refer to Section 4.2.6.

If you already protected a disk, the application window appears (Figure 4-10).
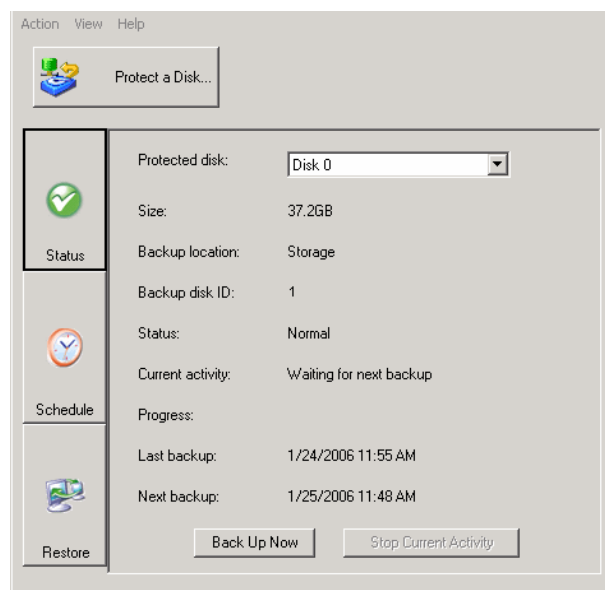
Figure 4-10: DiskSafe Express Application

The "Status" page displays the name of the disk that you protected and related information, such as the size of the disk, the name of the storage system where the backup resides, the number used to identify the backup disk on the storage system (Backup disk ID), the current status, information about any ongoing activity, and the date and time of the last backup and next scheduled backup If any.

> **Note:** If your license is not currently activated, a message appears, advising you of this. You must activate your license within 30 days of installing DiskSafe Express. After that time, you will no longer be able to perform backups or recoveries. For more information, refer to Section 4.2.6.

4.2.5   Activating Your License Key

When you install DiskSafe Express and restart your computer, you will be prompted to license

the product. If your computer has an Internet connection, the license is activated automatically. However, if your Internet connection was temporarily down or if your computer has no Internet connection, your license will not be activated. You must activate your license within 30 days of installing DiskSafe Express; otherwise you will not be able to perform a backup or recovery after that time.

If your Internet connection was temporarily down, your license will be activated automatically the next time you run DiskSafe Express with a restored Internet connection.

However, if your computer has no Internet connection, you must perform offline activation (as described in the next section).

> **Note:** The license activation is tied to your computer's hardware. Once you have activated a particular license, if your computer hardware changes, or if you install DiskSafe Express on a different computer using the same key code, an error message will appear. You must export your current license data (Action → License → Offline Activation → Export License Data) and e-mail the license file to "dsekeycode@freedom9.com", indicating that your hardware has changed. When you receive confirmation that your license has been re-activated, you can continue to use the product.

Activating your license without an Internet connection

If your license wasn't activated because your computer has no Internet connection, you must obtain an activation code using another computer that does have both an Internet connection and e-mail.

To activate your license without an Internet connection:

1. From the Action menu, click License → Offline Activation to open the Offline Activation dialog box.

2. Click "Export License Data".

3. On the Save As dialog box, select one of the following locations and then click Save:

- A shared folder accessible to both your computer and a computer that has Internet and e-mail access

- A floppy disk

- A USB disk

4. If you did not save the file to a shared folder, take the floppy disk or USB disk to a

computer with Internet and e-mail access. If you used a shared folder, access that folder from a computer with Internet and e-mail access.

5. From the computer that has Internet and e-mail access, e-mail the license file to the following address: "dsekeycode@freedom9.com".

6. When you receive an e-mail response, save the returned license file back to the shared folder, floppy disk, or USB disk.

7. If you did not save the file to a shared folder, take the floppy disk or USB disk back to the computer where DiskSafe Express is installed. If you used a shared folder, access that folder from the computer where DiskSafe Express is installed.

8. From the Action menu, click License → Offline Activation.

9. Click "Import Activation Code".

10. On the Open dialog box, browse to the location where the returned license file exists and double-click it.

11. On the confirmation message, click "OK".

12. The license is now activated and you can continue to back up and recover your disks.

13. To Close the dialog box, click "Exit".

Replacing your existing license

To replace your existing license:

1. From the Action menu, click License → Add License.

2. The Add License dialog box displays your current license key code.

3. In the License key code text box, enter the new key code.

4. Click "OK".

5. When the confirmation message appears, click "OK".

If your computer has an Internet connection, the license is activated automatically. If your Internet connection is temporarily down, your license will be activated automatically the next time you run DiskSafe Express with a restored Internet connection. If this computer does not have an Internet connection, you must perform offline activation (as described in the previous section).

4.2.6   Protecting Your Disks

After you install DiskSafe Express and restart your computer, the Protect a Disk wizard runs automatically. Using this wizard, you can specify which disk or partition you want to back up, where the backups should be stored, when automatic backups (if any) should occur, and what password you want to use for the recovery CD. If you cancel this wizard, you can start it again at any time using the following procedure.

To protect a disk:

1. Click "Protect a Disk" to run the Protect a Disk wizard.

2. In the Available disks list (Figure 4-11), select the disk or partition that you want to protect.
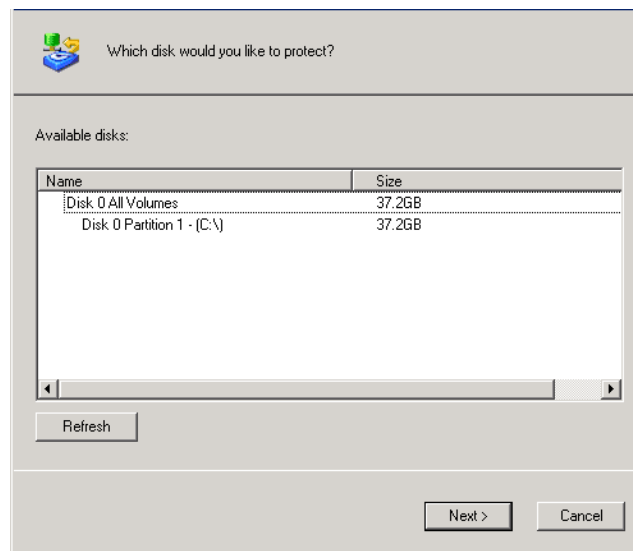
Figure 4-11: DiskSafe Express Disk Selection

If your computer has only one hard disk, there will still be two items in this list. The first item represents the entire hard disk, and the second item represents the partition on that disk. (If there's only one partition on the disk, the partition is the same as the entire disk.)

If your hard disk is divided into multiple partitions, this list displays one item for the entire hard disk, and one item for each partition. If your computer has multiple hard disks, this list displays an item for each disk and an item for each partition on each disk. Each partition is identified by its drive letter.

> **Note:** Dynamic disks are not supported.

If you select an entire disk, all the partitions on that disk are protected as a single entity. This means that you can't later recover only one partition; you have to recover the entire disk. If you select just a partition, you can subsequently recover just that partition.

In addition, you can recover a data disk or partition using DiskSafe Express, but you can recover a system disk or partition only using the recovery CD, so if you have separate partitions for your system information and your data, you might want to protect each one separately.

> **Recommendations:**
>
> - If your computer has only one disk with one partition, select the disk.
>
> - If your disk has a system partition and a data partition, select one of the partitions and complete the wizard. Then run the wizard again and protect the other partition. This provides complete protection with maximum flexibility.
>
> - If you have several disks and several partitions on each, select either one of the disks or one of the partitions and complete the wizard. Then run the wizard again and protect another disk or partition.

If you have never previously completed the Protect a Disk wizard, go to Step 3.

If you have previously completed the Protect a Disk wizard and connected to a storage system, go to Step 4.

If you have previously protected this disk and removed protection as described in Removing protection, go to Step 5.

3. When the Add Storage System dialog box appears, DiskSafe Express automatically scans your subnet for storage systems. Any storage systems that are detected appear in the Discovered Storage Systems List (Figure 4-12).
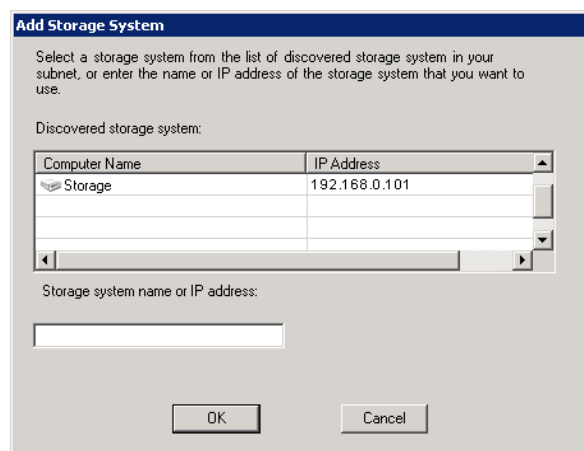
Figure 4-12: Add Storage System Page

From the Discovered storage systems list, select the storage system where you want to back up the selected disk. The name of the storage system automatically appears in the Storage system name or IP address text box.

If no storage systems are automatically discovered, or if you want to back up your disk to a different storage system, enter the name or IP address of the desired storage system in the Storage system name or IP address text box.   Click "OK".

> **Note:** If an authentication error occurs, make sure the name or IP address of the storage system is correct, and that your computer is connected to the network.

4. From the Backup locations list (Figure 4-13), select the storage system to use for backups of this disk or partition. (The first backup location in the list is selected by default.)
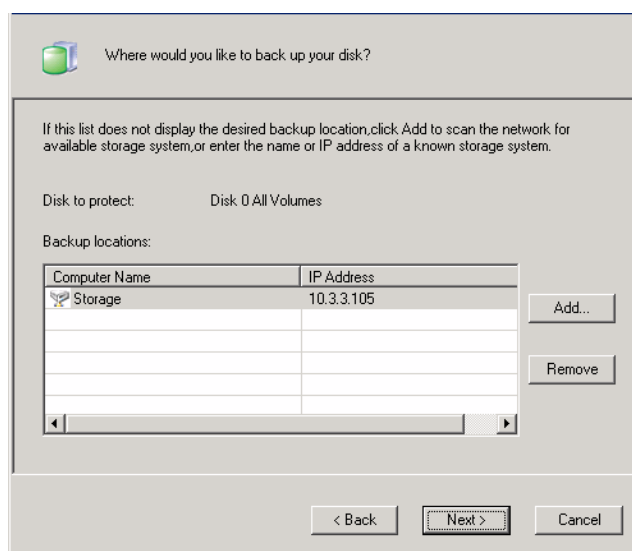
Figure 4-13: Storage System Selection Page

If you want to scan the network for new storage systems, or add a new one manually, click Add and repeat step 3.

If you want to remove a storage system that's not valid or that you no longer want to use, select the storage system from the Backup locations list, click "Remove", and then click "Yes" to confirm the removal. (You can remove a storage system only if it is not currently being used to protect another disk.)

Once you have selected the desired backup location, click "Next" and go to step 6.

5. If you previously protected this disk and removed protection, specify whether or not you want to re-use the existing backup or create a new one on the previously backed up page

(Figure 4-14).
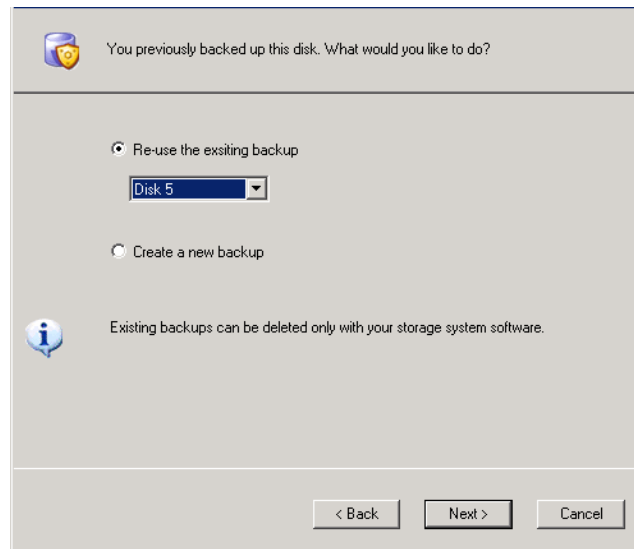
Figure 4-14: Previously Backed Up Page

If you select Re-use the existing backup, you must select which backup to reuse from the list. Then click "Next" and go to the next step.

If you select Create a new backup and click "Next", you must select the desired backup location as described in step 4.

6. Specify when you want backups to occur in the Backup Schedule page (Figure 4-15).
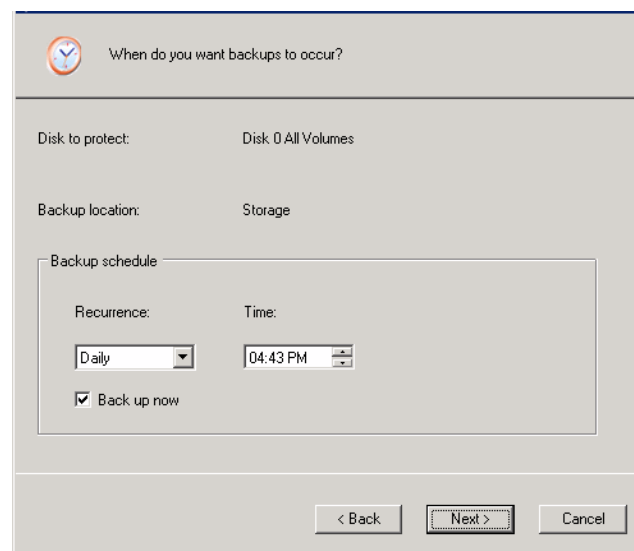
Figure 4-15: Backup Schedule Page

For example, if you want backups to occur every day, select "Daily" from the Recurrence

list. If you want backups to occur once a week, select the day of the week from the Recurrence list. Then select the time.

If you don't want backups to occur automatically, select "Not Scheduled" from the Recurrence list (the Time field will be dimmed). Backups will occur only when you start one manually.

Notes:

- Only four backups of each protected disk or partition are saved on the storage system, so if you back up your disk every day, you'll be able to recover data from only the last four days. If you back up your disk once a week, you'll be able to recover data from four weeks ago, but the most recent backup might be as many as six days old.

- Although DiskSafe Express is specifically designed to perform backups without affecting your other computer activities, you might want to schedule backups for a time when they'll have the least impact on your system, like during lunch or after business hours (if you leave your computer running overnight). If you're protecting multiple disks or partitions, it is recommended that you schedule each backup to occur at a different time.

- Once you complete this wizard, if a backup does not occur at its scheduled time for any reason, a message will appear, advising you of this and giving you the option to perform the backup immediately or wait until the next scheduled backup.

7. Specify whether or not to back up your disk as soon as you finish the wizard by selecting or clearing the Back up now check box, and then click "Next".

If you clear this option, the disk will be backed up at the next scheduled time or the next time you perform a manual backup.

8. If you ever need to recover your disk using the recovery CD, you'll be prompted for a password. In the Recovery CD password text box (Figure 4-16), enter the password that you'd like to use, enter it again in the Retype your password text box, and then click "Next". Notes:

Notes:

- The recovery CD password must be 12–16 characters long.

- The same password is used for all disks backed up to the same storage system. If you subsequently protect a second disk using the same storage

system, you will not be prompted to provide this password again. However, if you protect a second disk using a different storage system, you will be prompted to provide a password for that storage system.

- You can change this password later using DiskSafe Express.
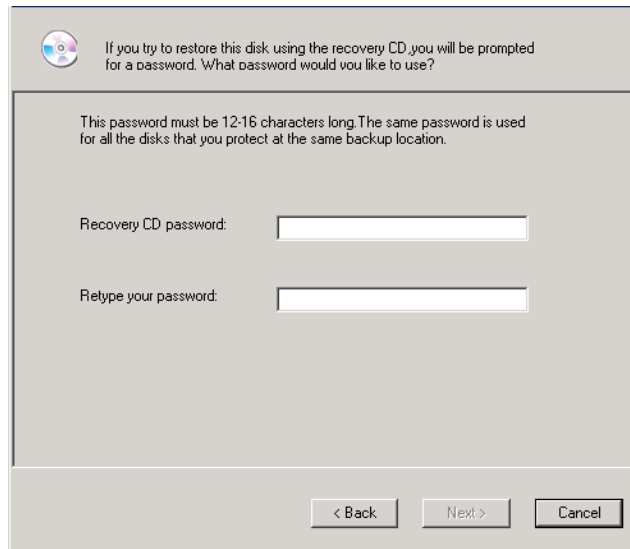
Figure 4-16: Recover CD Password Page

9. Review all your selections and click "Finish" on the next page (Figure 4-17).
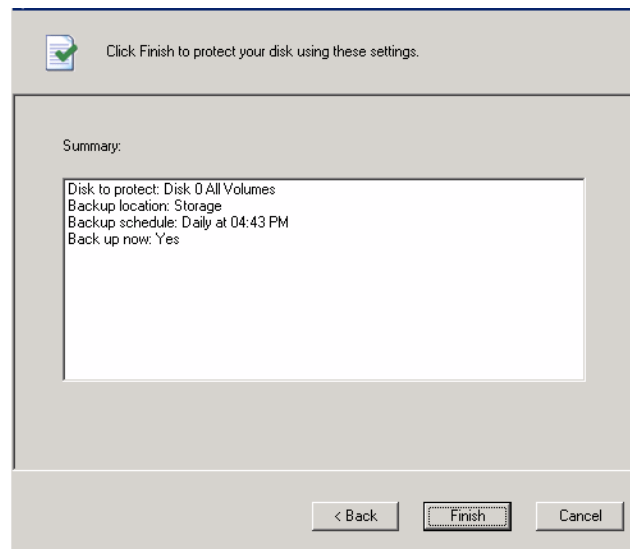
Figure 4-17: DiskSafe Express Completion Page

If you selected the "Back up now" check box, the backup will begin as soon as you click Finish, and you can review its progress on the Status page in DiskSafe Express.

If you want to protect additional disks or partitions, repeat this procedure for each one.

Note: If you subsequently change the drive letter of a protected disk or partition, you must restart DiskSafe Express to update this application..

4.2.7   Manually Backing Up Your Disk

Once you protect a disk, it is automatically backed up at regular intervals (unless you chose Not Scheduled from the Recurrence list when you completed the schedule). However, you can also back up a disk manually at almost any time. For example, if you're about to install a new application, you might want to back up your disk right before you do that so that if any problems occur, you can recover your disk to the state it was in immediately before you installed the application.

Note: You can manually back up a disk only if a backup or recovery is not currently occurring.

To manually back up a disk:

1. In the DiskSafe Express utility, click Status.

2. In the Protected disk list, select the disk that you want to back up.

3. Click "Back Up Now".

The Current activity area displays information about what's happening, the percentage of the backup that has completed, and the speed at which the data is being sent over the network. The Progress bar graphically indicates how much of the backup is complete.

To stop a backup in progress, click "Stop Current Activity".

4.2.8   Stopping a Backup or Recovery in Progress

Once a backup or recovery starts, you can stop it at any time. When you stop a backup in progress, that backup won't appear in the list of backups on the Restore page, and any changed data that was not copied to the storage system will be copied during the next backup.

When you stop a recovery in progress, the local disk or partition is left in an incomplete state, and you must recover it again later before you can use it.

To stop a backup or recovery in progress:

1. In the DiskSafe Express utility, click Status.

2. In the Protected disk list, select the disk whose backup or recovery you want to stop.

3. Click "Stop Current Activity".

4. If you're stopping a backup, the backup stops immediately.

5. If you're stopping a recovery, a confirmation message appears. Click "OK" to stop the recovery now, or click "Cancel" to proceed with it.

4.2.9 Changing the Backup Schedule

When you protect a disk, you specify when you want backups to occur. However, you can change this schedule at any time.

To change the backup schedule:

1. In the DiskSafe Express utility, click "Schedule".

2. In the Protected disk list, select the disk whose backup schedule you want to change.

3. Specify when you want backups to occur.

4. For example, if you want backups to occur every day, select Daily from the Recurrence list. If you want backups to occur once a week, select the day of the week from the Recurrence list. Then select the time.

5. If you don't want backups to occur automatically, select Not Scheduled from the Recurrence list. (The Time list appears dimmed.) Backups will occur only when you start one manually (as described in Manually backing up your disk).

6. Click "Apply".

7. The schedule change takes effect immediately, and the date and time of the next scheduled backup appears in the Next backup area.

4.2.10 Changing the Recovery CD Password

When you protect a disk, you specify what password to use for recovering the disk using the recovery CD. However, you can change this password at any time.

> **Note:** The same password is used for all disks backed up to the same storage system. If you backed up multiple disks to the same location and change the password for one, the password is changed for all of them. However, if you backed up one disk to one storage system and a different disk to a different storage system, each disk can have a different recovery CD password.

To change the recovery CD password:

1. In the DiskSafe Express utility, click "Restore".

2. In the Protected disk list, select a disk whose backup resides on the storage system whose recovery CD password you want to change.

    To double-check your selection, click "Status". The name of the storage system appears in the Backup location area. Then click "Restore" to return to the Restore page.

3. Click "Recovery CD Password" to open the dialog box to change the password (Figure 4-18).
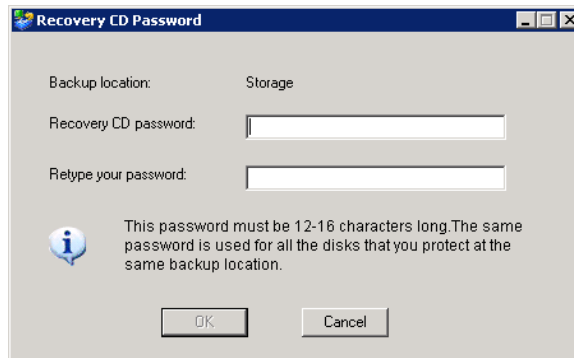
Figure 4-18: Changing Recovery CD Password Dialog

4. In the Recovery CD password text box, enter the desired password. This password must be 12-16 characters long.

5. In the Retype your password text box, enter the password again.

6. Click "OK".

4.3   System Restoration with DiskSafe Express

With DiskSafe Express, there are several ways to recover data from your backups. The best method to use depends on what you want to do:

*   **Recovering selected folders, files, or sections of files:** If you accidentally permanently deleted a folder or file that you want to recover, or if you just want to retrieve some information from a file that you changed, you can access the backup that contains the desired data and copy it to your local disk.

    You can also use this procedure to try out different "what if" scenarios—for example, changing the format of the data in a file—without adversely affecting the data on your local disk.

    For more information, refer to Section 4.3.1.

- **Recovering an entire non-system disk or partition**: If you protected a disk or partition that isn't being used to run the operating system, you can recover that disk or partition using DiskSafe Express. You might need to do this if the disk has become corrupted or the data has been extensively damaged. The entire disk or partition will be restored to its exact state at the time of the selected backup.

   > **Warning:** When you recover non-system disks or partitions, you will lose any data that was written to the disk after the time of the selected backup, as well as any backups that were performed after the backup you're recovering. It is recommended that you copy any newer files that you want to keep to another disk before you recover the disk. To copy files from a backup, refer to Section 4.3.1.

   In addition, if network errors occur or the storage system shuts down during recovery, your operating system might become unstable, and you will have to recover it using the recovery CD (or re-install the operating system if you did not protect your system disk). Be sure to recover your disks or partitions only when your environment is stable.

   You can continue to use your computer for other tasks while the data is being recovered, although not any applications or files located on the disk or partition that you're recovering.

   For more information, refer to Section 4.3.2.

- **Recovering an entire system disk or partition:** If you need to recover your system disk or partition - that is, the disk or partition used to run the operating system - you can do so using the recovery CD. This is particularly useful if the hard disk has failed and has been repaired or replaced, or if you want to duplicate an existing disk configuration for another computer. The entire disk or partition will be recovered to its exact state at the time of the selected backup. However, you won't be able to use your computer until all this process is complete.

   For more information, refer to Section 4.3.3.

4.3.1   Recovering Files From a Backup

To recover selected folders, files, or sections of files from a backup:

1. In the DiskSafe Express utility, click "Restore".

2. In the Protected disk list, select the disk that contains the folders or files that you want to recover.

3. In the Backups list, select the backup from the desired date and time. You can select only a

backup for which No appears in the Backup View Open column.

4. Click "View Backup".

5. When the confirmation message appears, click "OK".

After a few moments, a window opens automatically, displaying all the data associated with the selected backup. You can now open the folders and files in the backup view to make sure they contain the information you want, and copy any of the data to your local disk.

Warning: You can open and change the files in the backup view, and even create new folders or files. However, as soon as you close the view (as described in the next step), all the changes will be lost. The next time you view the backup, it will appear the way it existed at the time the backup was created.

Notes:

*   If the first drive letter after your local disks is mapped to a shared network folder, you must use Disk Management to change the drive letter assigned to the backup view so that you can access it.

*   For example, if your system disk is mapped to C:, your CD-ROM drive is mapped to D:, and a shared network folder is mapped to E:, and you view a backup, you will continue to see the shared network folder when you explore E:, and you will not see a new drive letter for the backup view. (Internally, the backup view is also mapped to E:, since that was the first drive letter after the local disks.) However, when you use Disk Management to change the drive letter for the backup view from E: to F:, you will be able to see both the shared network folder (E:) and the backup view (F:).

*   To change the drive letter, right-click My Computer and click "Manage". In the left pane, click "Disk Management". In the right pane, right-click the volume, click "Change Drive Letter and Paths", click "Change", select the desired drive letter from the list box, and then click "OK" on each dialog box. You can now access the backup view using the specified drive letter.

*   Windows caching can affect the content of the backup view. If the content does not appear to be correct, restart your computer and check again.

*   You can view more than one backup simultaneously. Simply repeat steps 3 and 4.

*   If you open a backup view for a partition that cannot be explored (such as an EISA partition), the backup view is closed automatically.

- When a backup view is open, that backup will not be deleted to make room for new backups until it is closed or unless the storage system runs critically low on resources. If you view the oldest backup, and the maximum number of backups is reached, new backups cannot occur until the view of the oldest backup is closed (as described in the next step).

- When you close the DiskSafe Express application window, you will be prompted to close all open backup views. If you click "Yes", both the application window and all open views are closed. If you click "No", both the application window and all open views remain open.

6. When you have finished viewing or copying all the desired data, select the backup in the Backups list and click "Close View". The Windows Explorer window will close automatically, and the Backup View Open column for the selected backup will now display "No".

4.3.2   Recovering a Non-System Disk or Partition

You can recover a non-system disk or partition only as long as that disk or partition is not currently being backed up, and only as long as a more recent backup view is not open. For example, if you created backups on Monday and Tuesday, and Tuesday's backup view is open, you cannot recover Monday's backup until you close Tuesday's view.

In addition, if you recover a partition and other partitions of that same disk are also protected, protection for those other partitions temporarily stops until the selected partition is recovered.

> **Warning:** When you recover a disk or partition, you will lose any data that was written to the disk after the time of the selected backup, as well as any backups that were performed after the backup you're recovering. It is recommended that you copy any newer files that you want to keep to another disk before you recover the disk. To copy files from a backup, refer to Section 4.3.1.

In addition, if network errors occur or the storage system shuts down during recovery, your operating system might become unstable, and you will have to recover it using the recovery CD (or re-install the operating system if you did not protect your system disk). Be sure to recover your disks or partitions only when your environment is stable.

To recover a non-system disk or partition:

1. In the DiskSafe Express utility, click "Restore".

2. In the Protected disk list, select the disk or partition that you want to recover.

3. If a view of a more recent backup than the one that you want to recover is open (as

indicated by Yes in the Backup View Open column), select the open backup view and click "Close View".

4. In the Backups list, select the backup that you want to recover.

5. Click "Restore Disk".

6. When the confirmation message appears, click "Yes".

The disk or partition is recovered to exactly its state at the date and time of the selected backup.

To let you monitor the progress of this activity, the Status page appears automatically. The Current activity area displays the percentage of the recovery that has completed, and the speed at which the data is being sent over the network. The Progress bar graphically indicates how much of the recovery is complete.

> **Note:** You can cancel this operation at any time by clicking "Stop Current Activity". However, this will leave the local disk or partition in an incomplete state, and you will have to recover it again before you can use it.

7. When you are prompted to restart the computer, click "Yes".

You do not have to restart your computer immediately, but you cannot access the recovered disk or partition until you do.

As soon as you restart the computer, you must start DiskSafe Express and back up the recovered disk or partition manually (as described in Manually backing up your disk) to resume protection. In addition, if you recovered a partition and any other partitions on the same disk were protected, you must manually back up those partitions as well.

4.3.3   Recovering a System Disk or Partition

To recover a system disk or partition using the recovery CD:

1. Using the appropriate procedure for your system, configure the computer to boot from the CD-ROM drive.

2. Insert the recovery CD into the CD-ROM drive.

When responding to the prompts, use the arrow keys to highlight the desired item, use the space bar to select or clear options (an X appears in the brackets when the option is selected), and press "Enter" to make your selection. You can also tab between fields.

3. When the hardware list appears, select the network interface card (NIC) that you want to use when recovering the data, and then select "Next".

In most cases, there will be only one NIC, and you can simply select "Next".

This screen displays only the NICs on this system that are supported by DiskSafe Express. If no NICs appear on this screen, you might need to install an appropriate network driver. Select Load Driver, select the location from which you want to install the driver (Load From System for the local hard disk, Load From Floppy for a floppy disk drive, or Load From CDROM for a CD-ROM drive), insert the disk in the drive (if loading from a floppy disk or CDROM), and respond to the prompts. For information about obtaining the appropriate driver, contact your vendor.

To see a complete list of the detected hardware, select Rescan. When you are done viewing the list, select "OK".

4. Review the settings for your NIC and select "Next".

The recovery CD obtains the IP address to use from your DHCP server. If the displayed settings are not the ones you want to use, or if no IP address is displayed, select Config and specify the desired IP address or subnet mask. (If you make a mistake typing either the IP address or subnet mask, select "Disable" to clear the displayed information.) Then select "OK" and select "Next".

5. n the Client Name field, enter the full computer name of this computer. This name is always uppercase characters.

If you don't remember the full computer name, access the Manager and click "Backups" in the navigation bar. In the Protected disks list, the Computer Name column lists the computer name of each computer that has backed up disks to the storage system.

6. If your computer is a member of a Windows domain, enter the domain name in the Domain Name field. (If your computer is not a member of a Windows domain, leave this field blank.)

Initially, the recovery CD will attempt to connect to the storage system using only the computer name. If this fails, the domain name will be appended as well. This ensures that your computer can be properly authenticated.

7. In the Recovery Server field, enter the name or IP address of the storage system where the backups reside.

8. Make sure the selected authentication type is CHAP. DiskSafe Express supports only CHAP authentication.

9. In the Recovery Password field, enter the recovery CD password that you specified when you protected the disk or when you last changed the password.

If you don't remember your password, you can change it using the web interface and enter the new password here.

10. In the left column, select the backup that corresponds to the disk or partition that you want to recover.

    If you protected only one disk or partition, only one item will appear in this list.

    If you protected multiple disks or partitions, you can identify the right item by looking at the Attr and Size columns. The Attr column displays the attributes of each listed item (D for disk, P for partition, and S for system disk). For example, if you protected both a system disk and a data disk, the system disk will be labeled S, and the data disk will be labeled D. If you protected disks of different sizes, the Size column (which displays the number of megabytes) can also help you identify the right backup.

11. In the right column, select the date and time of the backup that you want to recover.

    In general, selecting Base Disk is the same as selecting the most recent backup. However, if your system crashed during the last backup, the base disk will be in an incomplete state. In that case, be sure to select one of the listed backup dates rather than Base Disk.

    If you select Base Disk, a backup of that disk image on the storage system is created, and this backup is recovered. As a result, if the maximum number of backups has already been performed, the oldest backup is deleted to make room for this backup.

12. Specify whether or not to delete all backups that occurred after the selected date by selecting or clearing Rollback the remote disk.

    Warning: This action is not reversible. If you select this option, you will not be able to subsequently recover from another later backup.

13. Specify whether or not to scan the differences between the backup and the disk to which you are recovering data by selecting or clearing Enable micro-scan.

    If you're simply overwriting corrupted data on the same disk that you protected previously, select this option. DiskSafe Express will scan both the backup and the disk, and copy only the data that differs between the two. This can minimize the impact to the network, although the scanning process takes some additional time.

    If you're recovering the backup to a brand new disk, clear this option. DiskSafe Express will copy all the data from the backup to the new disk without doing any scanning (there will be nothing to scan on the new disk).

14. Select "Next".

15. Select the disk where you want to recover the data, and select "Next".

> **Note:** If you are recovering a system disk, the system to which you are recovering the data must be identical to the original system. For example, if the original system had a particular type of network adapter, the system to which you are recovering the data must have the exact same type of network adapter. Otherwise, the recovered files will not operate properly.

16. If you selected the backup of a disk in step 10, go to step 18.

If you selected the backup of a partition in step In the left column, select the backup that corresponds to the disk or partition that you selected, select Restore to a partition to recover to an existing partition on the selected disk, or select Clear all partitions and create new to delete all the existing data on the selected disk and recover only the selected partition.

17. If you selected Restore to a partition in step If you selected the backup of a disk in step In the left column, select the backup that corresponds to the disk or partition that you selected, select the partition where you want to recover the data, and then select Next. (Otherwise, go to step Select .)

18. Select Yes to confirm the action.

> **Warning:** This overwrites any existing data on the selected disk. Although you can subsequently recover different data, you cannot recover the original data.

The status screen displays the progress of the recovery. You can cancel it at any time by selecting Abort. However, this leaves the disk or partition in an incomplete state (some of the data will have been recovered, but not all of it).

19. When the completion screen appears, review the results and do one of the following:

- To review information about any sectors that were not successfully recovered, select "Failed Sectors", review the displayed information, and select "Back".

- To recover another disk or partition, select "Continue".

- If you want to recover a different backup of the same computer from the same storage system, select "Yes" to retain the current configuration settings and return to step In the left column, select the backup that corresponds to the disk or partition that you selected.

- If you want to recover a different computer's backup, or if you want to recover a backup of the same computer from another storage system, select "No" to modify the current configuration settings and return to step 5.

- To restart the computer, select "Finish".

20. When the computer restarts, use the appropriate procedure for your system to configure the computer to boot from the local hard disk once more.

21. Start DiskSafe Express and remove protection from the recovered disk or partition (as described in the next section).

22. Restart the computer.

23. Protect the recovered disk once again, re-using the original backup

4.3.4   Removing Protection

If you no longer want to back up a particular disk or partition, you can remove protection as long as a recovery is not currently in progress for that disk or partition. (If a recovery is in progress, it must be cancelled it or completed before the protection can be removed.)

> **Note:** If you plan to delete a protected partition, be sure to remove protection before you delete that partition. Otherwise, you might not be able to protect other partitions on that disk.

When you remove protection, you will no longer be able to back up the selected disk or partition either automatically or manually, and you cannot recover data using DiskSafe Express. However, the backups that currently exist on the storage system are retained, and you can recover them using the recovery CD.

If you subsequently want to protect the same disk or partition again, you can re-use the space that was allocated for previous backups. You can also delete the existing backups on the storage system to free up space for backups of other disks or partitions, either for this computer or other computers.

To remove protection:

1. In the Protected disk list on any page, select the disk for which you want to remove protection.

2. From the Action menu, click "Remove Protection".

The disk disappears from the Protected disk list. If another disk is protected, that disk appears in the Protected disk list, and information about that disk now appears in the application window. If no other disk is protected, the Protected disk list and application window are blank.

Appendix A: Disk Configurations

Your storage system supports the following types of disk configurations:

- **Linear:** A linear configuration is similar to using multiple hard disks in a regular computer. Each disk is an independent entity, and the data on it is self-contained. You can add or remove the disks without affecting the other disks. All the available disk space is used for data.

  If your storage system has only one disk, you must use a linear configuration. However, you can use a linear configuration for two, three, or four disks as well.

- **RAID 0:** Instead of writing all the data to one disk in a linear fashion, some bytes are written to one disk, and other bytes are written to another. Performance is faster because reading and writing activities can occur on multiple disks simultaneously. All the available disk space is used for data.

  For RAID 0, your storage system must have at least two disks. However, you can use RAID 0 with three or four disks as well, and the disks can be any size.

- **RAID 1:** In this configuration, all the data written to one disk is duplicated on the other disk. This offers greater data protection since if one disk fails, all your data is still intact on the other disk. However, using RAID 1 means only half your available disk space is used for data; the other half is used for a duplicate (mirror) of that data.

  You can use RAID 1 only if your storage system has only two disks. If the disks are not the same size, the smaller of the two disks is used for data, and the larger of the two disks is used as the mirror.

  If one disk fails, the other disk continues to make its data available.

- **RAID 5:** Like RAID 0, RAID 5 offers increased performance by distributing the data across multiple disks. But unlike RAID 0, RAID 5 also offers data protection. If your storage system has three disks of equal size, two thirds of each disk are used for data, and the remaining third contains the parity information needed to reconstruct either of the other two. In this way, if any of the three disks fails, it can be reconstructed when a new disk is installed in the storage system.

  If your storage system has four disks of equal size, three fourths of each disk are used for data, and the remaining fourth contains the parity information needed to reconstruct either of the other three. If any of the four disks fails, it can be reconstructed when a new disk is installed.

You can use RAID 5 only if your storage system has at least three disks. If the disks are not the same size, the smallest of the disks determines how much disk space is available for data. For example, if one disk is 300 GB, one is 400 GB, and one is 500 GB, only 300 GB from each disk can be used. Two thirds of each disk (200 GB) is used for storage space, and the remaining third is used for parity information. As a result, for all three disks, only 600 GB of disk space would be available for data.

- **RAID 5 + spare:** In this configuration, three of the disks use RAID 5, and the fourth is empty. If any of the three disks fails, it is immediately rebuilt using the fourth spare disk. As a result, you can remove the failed disk and still have the ongoing fast performance and data protection offered by RAID 5. When the failed disk is repaired or replaced and re-installed into the storage system, it automatically becomes the spare for the other functioning three.

  You can use RAID 5 + spare only if your storage system has four disks. If the disks are not the same size, the smallest of the disks determines how much disk space is available for data, similar to RAID 5.

- **RAID 10:** RAID 10 is similar to RAID 1, but rather than having one disk mirror to one other disk, two disks mirror to the two other disks.

  You can use RAID 10 only if your storage system has four disks. The disks in the first two slots constitute the first pair, and the disks in the second two slots constitute the second pair. In each pair, the smaller of the two disks is used for data, and the larger of the two disks is used as the mirror.

  If one disk in the pair fails, the other disk continues to make its data available.

A.1 Adding Hard Disks

The effect of adding hard disks to your storage system varies, depending on the disk configuration you chose when you configured the system and the current state of the existing disks.

For example, in a linear configuration, you can add a new disk at any time, and data can be written to that disk as soon as it is added. Whether you previously removed a disk or one of the other disks failed makes no difference.

In a RAID configuration, the effect of adding a disk varies, depending on whether the RAID is in a normal or degraded state (as indicated on the Disks page). A normal state indicates that the RAID is functioning properly. A degraded state indicates that one or more disks have been removed or failed, but because of the data protection offered by the RAID, you can continue to

access all the data.

In a normal state, you cannot add a disk to a RAID 0 or RAID 1 configuration. Any disk that you install will not be used unless you subsequently reconfigure the storage system.

Warning: Reconfiguring your storage system disks deletes all the data on your storage system.

However, if you currently have three disks and a RAID 5 configuration, you can add a fourth disk as a spare (essentially changing from RAID 5 to RAID 5 + spare while retaining all your existing data).

In a degraded state, you can add a disk to a RAID at any time, and the new disk will be rebuilt to replace the disk that was removed or failed.

Warning: If the RAID has failed—that is, if so many disks have failed or been removed that the RAID can no longer function—you must either re-install the disks or reconfigure the entire storage system, deleting all the data on your system.

Adding hard disks to a linear or normal RAID configuration

To add a hard disk to a linear or normal RAID configuration:

1. Insert the hard disk into the storage system. You can do this whether the storage system is powered on or off.

2. Access the Manager or refresh the browser window to open the Disk Change Notification page (Figure B-1).

Disk Change Notification

One or more hard disks in the storage system have failed or been added or removed.

If you add or remove disks at this time, click Scan after each change to update the list of current disks. (If you add disks, please wait until the disk LED is green before you click Scan.) To power off the storage system, click Shut Down. The other available options vary, depending on the nature of the change.

Current state: Linear (NORMAL)

Previous disks

Slot	Model	Serial Number	Size	Disk Status
1	ST3250823AS	3ND05TJT	232.89 GB	Linear
2	ST3250823AS	3ND05EDM	232.89 GB	Linear
3	-	-	-	-
4	-	-	-	-

Current disks

Slot	Model	Serial Number	Size	Disk Status
1	ST3250823AS	3ND05TJT	232.89 GB	Linear
2	ST3250823AS	3ND05EDM	232.89 GB	Linear
3	ST3250823AS	3ND0551R	232.89 GB	New
4	-	-	-	-

| Scan | Shut Down | Add New Disk |

**

Figure B-1: Disk Change Notification Page

3. To add the disk to the storage system, click "Add New Disk". If the information on this page is not correct, click "Scan" to scan the storage system again and update the page. You can also click "Shut Down" to shut down the storage system, but you will be presented with this page again the next time you access the Manager. When you click "Add New Disk", the Add New Disk page appears (Figure B-2):

98
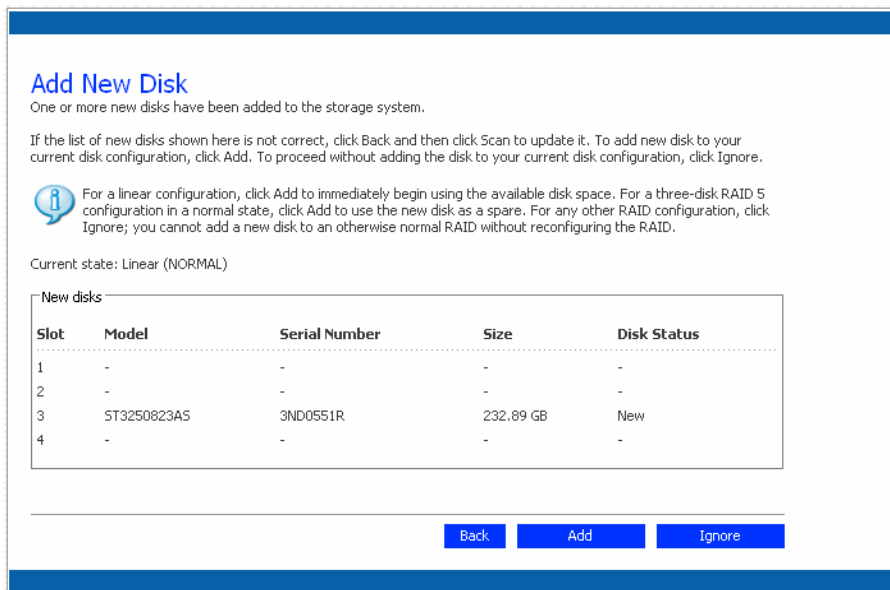
Figure B-2: Add New Disk Page

4. Take the desired action:

- **To add the disk to a linear configuration or use it as a spare for a normal three-disk RAID 5 configuration:** Click "Add" and the Disks page will indicate the current state of the disk configuration.

- **To add the disk to the storage system but not add it to the RAID at this time:** Click "Ignore" and the Disks page will list that the disk is part of the storage system, but its status is New, indicating that it is not being used. If you subsequently reconfigure the disks, you will be able to use this new disk.

- **To return to the previous page (for example, to re-scan the storage system):** Click "Back".

Adding hard disks to a degraded RAID configuration

To add a hard disk to a degraded RAID configuration:

1. Insert the hard disk into the storage system. You can do this whether the storage system is powered on or off.

2. Access the Manager or refresh the browser window. The Disk Change Notification page will appear (Figure B-3):

Disk Change Notification

One or more hard disks in the storage system have failed or been added or removed.

If you add or remove disks at this time, click Scan after each change to update the list of current disks. (If you add disks, please wait until the disk LED is green before you click Scan.) To power off the storage system, click Shut Down. The other available options vary, depending on the nature of the change.

Current state: RAID 5 (DEGRADED, Recovery : 2 %, Finish : 6 min, Speed : 5457K/sec)

Previous disks

Slot	Model	Serial Number	Size	Disk Status
1	ST3250823AS	3ND05TJT	232.89 GB	RAID 5
2	ST3250823AS	3ND05EDM	232.89 GB	RAID 5
3	-	-	-	-
4	-	-	-	-

Current disks

Slot	Model	Serial Number	Size	Disk Status
1	ST3250823AS	3ND05TJT	232.89 GB	RAID 5
2	ST3250823AS	3ND05EDM	232.89 GB	RAID 5
3	ST3250823AS	3ND0551R	232.89 GB	Rebuilding
4	-	-	-	-

Scan   Shut Down   Ignore

**

Figure B-3: Disk Change Notification Page – New Disk

3. Click "Ignore" to continue rebuilding the disk and return to the Manager.

The Disks page shows the progress of the rebuilding progress.

Alternatively, if the information on this page is not correct, click "Scan" to scan the storage system again and update the page.

You can also click "Shut Down" to shut down the storage system. When you restart the storage system, this page will re-appear.

A.2   Removing or Replacing Hard Disks

The effect of removing hard disks from your storage system or disk failure varies, depending on the disk configuration you chose when you configured the system and the current state of the existing disks.

For example, in a linear configuration, when you remove a disk or a disk fails, the data associated with that disk is no longer available, but the data on all the other disks remains available.

In a RAID configuration, the effect of disk removal/failure varies, depending on the RAID level

and whether the RAID is in a normal or degraded state. You can determine the effect of disk removal/failure by looking at the Hotplug Indicator on the Disks page. If this indicator is GREEN, disk removal/failure will have no effect on the RAID. If this indicator is YELLOW, disk removal/failure will cause RAID degradation, but you will still be able to access all the data. If the indicator is RED, disk removal/failure will cause the entire RAID to fail.

For example, in a RAID 5 configuration, all the disks are YELLOW. Removing any one of them will cause the RAID to be degraded, but all the data will still be available. However, after you remove one disk, all the other disks become RED, since removing any one of them at this point will cause the entire RAID to fail.

> **Note:** In a linear configuration, the Hotplug Indicator is RED for all the disks because removing any one of them will remove data from the storage system. However, this will not adversely affect any of the other disks.

In addition, while a disk is being rebuilt, all the other disks are RED, since removing any one of them at this point will cause the RAID to fail.

If you remove a viable disk and cause only RAID degradation, you can re-install the same disk and resume normal operation. (For information about adding a disk, refer to Adding hard disks.)

> **Note:** If you remove two or more disks, you must re-install them in the reverse order to help maintain data integrity. For example, if you remove disk A from slot 1 and then remove disk B from slot 2, you must re-install disk B first, then disk A. You can put the disks back into different slots, but they must be re-installed in the opposite order from which they were removed.

If you remove one or more viable disks and cause the entire RAID to fail, you can shut down the storage system, re-install the same disks, and then restart the storage system. As long as you re-install the original disks, the storage system should be able to resume proper operation, although the integrity of the data cannot be guaranteed. However, if you replace the removed disks with new disks, you must reconfigure your disks.

> **Warning:** Reconfiguring your disks will delete all the data on your storage system.

Responding to RAID degradation

When disk removal/failure causes RAID degradation, the Disk Change Notification page appears when you access the Manager or refresh the browser window (Figure B-4).

**
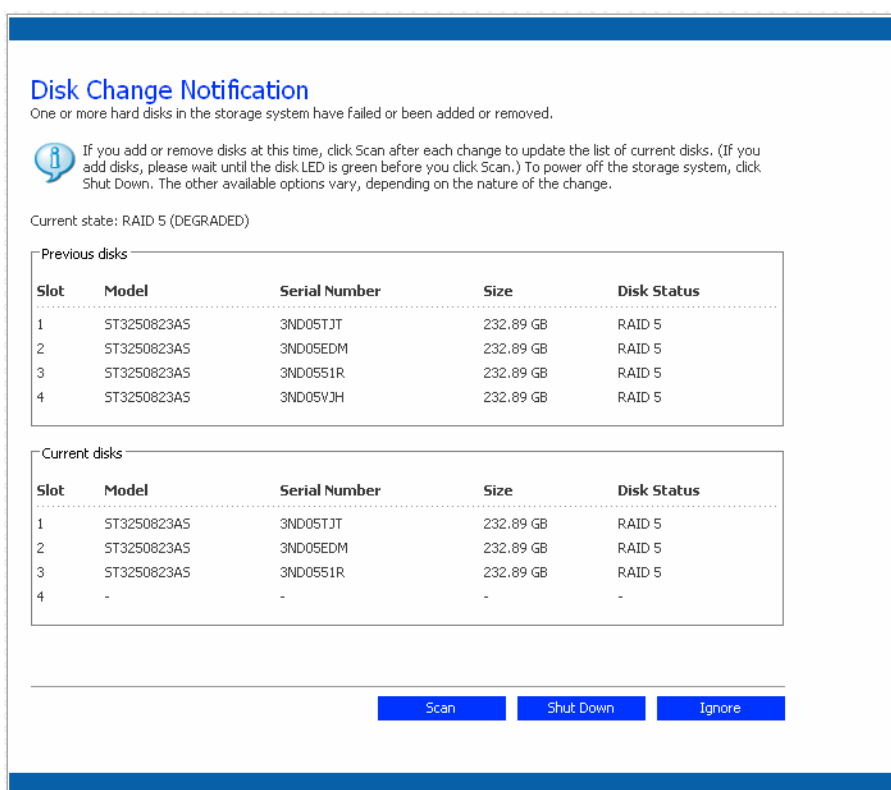
Figure B-4: Disk Change Notification Page – Degradation

Take the appropriate action:

- **To scan the storage system again and update the information on the page:** Click "Scan".

- **To re-install the same disk or install a new disk:** Click "Shut Down". After the storage system shuts down, install the disk and then restart the system.

    Note: If you are re-installing multiple disks, be sure to re-install them in the opposite order than you removed them.

- **To return to the web interface and continue to operate in a degraded mode:** Click "Ignore".

Responding to RAID failure

When disk removal/failure causes the entire RAID to fail, the Disk Change Notification page appears when you access the Manager or refresh the browser window (Figure B-5).

**

Figure B-5: Disk Change Notification Page – RAID Failure

Take the appropriate action:

- **Scan the storage system again and update the information on the page:** Click "Scan".

- **To re-install the same disk:** Click "Shut Down". After the storage system shuts down, re-install the same disk and then restart the system.

  Note: If you removed multiple disks, be sure to re-install them in the opposite order than you removed them.

- **To reconfigure the storage system using the available disks:** Click "Reconfigure Disks" and complete the system setup pages.

  Caution: Reconfiguring the storage system deletes all user information and all data on all the disks.

A.3 Swapping hard disks

If you are using RAID 5 + spare or RAID 10, you can move the hard disks from one slot to another whether or not the storage system is running. However, if you do this when the

storage system is running, you can swap only two disks, and you must restart the system after you swap the disks. If you swap the disks when the storage system is not running, you can swap all four disks, and the system will function as it previously did when you restart it.

> **Notes:** For RAID 5 + spare, if you swap the disks when the storage system is running, one of the swapped disks must be the spare. For RAID 10, the swapped disks must be in different pairs. For example, you can swap disks 1 and 3 or disks 2 and 4, but not disks 1 and 2, as those are members of the same pair.

If the storage system is running when you swap the disks, the Disk Change Notification page appears (as shown in the preceding section). Click "Shut Down" and then restart the system.

For all other disk configurations (linear, RAID 0, RAID 1, and RAID 5), you can swap the hard disks only when the storage system is powered off, and you can swap all four disks.

A.4 Transferring hard disks to a new storage system

If your storage system unit fails but the hard disks themselves are viable, you can transfer your existing hard disks to a new storage system, thereby preserving all your existing data.

To transfer hard disks to a new storage system:

1. Shut down both the old unit and the new unit.

    > **Warning:** If you do not shut down the new unit before you insert the hard disks, you will be prompted to re-initialize the disks. If you do this, all the data on your hard disks will be lost.

2. Transfer the hard disks to the new unit.

3. Connect the new unit to your network and power on the new unit.

4. Access the web interface for the new unit.

    As long as the new unit is in the same subnet as the old unit, you can access the Manager using the same procedure you used previously. However, if the new unit is in a different subnet, you might have to install the Storage System Console on a computer in the same subnet as the storage system and use the Storage System Console to access it.

5. If the firmware in the flash memory of the new unit differs from the firmware on the hard disks, a message appears, prompting you to update the flash memory on the storage system with the firmware from the hard disks. Click Update to proceed. If you don't want to upgrade the firmware at this time, click Shut Down to shut down the system.

Note: If the firmware on your new unit is newer than the firmware on your hard disks, you might want to contact your vendor about obtaining the latest firmware. Refer to "Upgrading the firmware" on page 62 for information about upgrading to newer firmware.

If no message appears, you can manage the unit as you did before.

Appendix B: Troubleshooting

Viewing the system log

The System Log page (Figure B-6) displays a list of events that have occurred on the storage system. Reviewing this list can help you identify and resolve any problems that you might encounter.

**
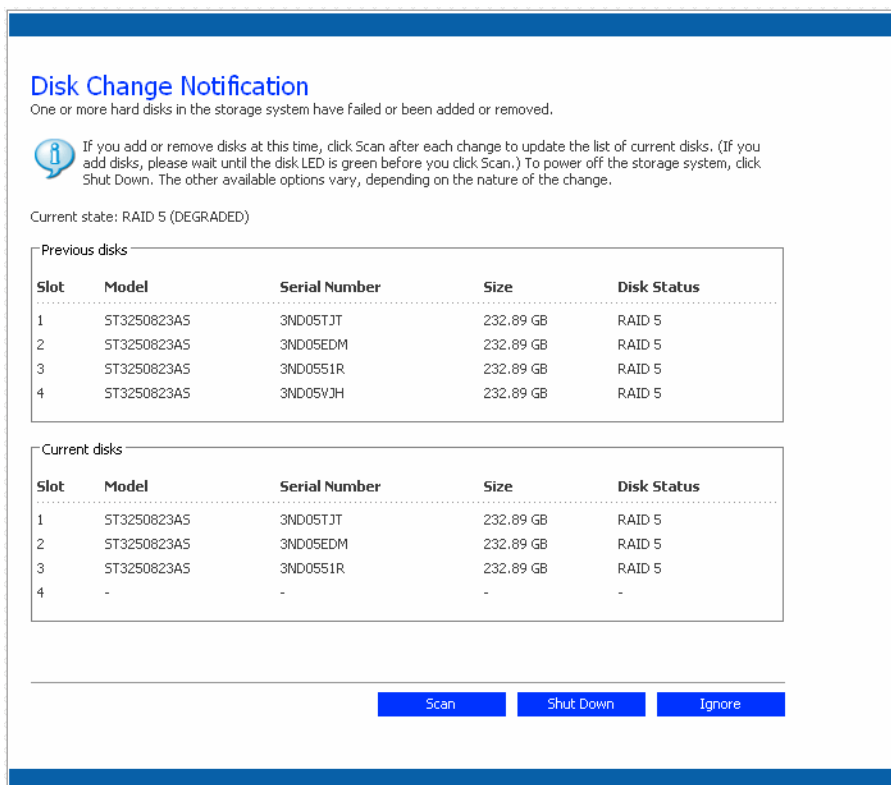
Figure B-6: System Log Page

To view event information:

1. In the navigation bar, click "Advanced".

2. In the left pane, click "System Log".

   The System Log page displays the date and time of the event, the type of event (I for informational, E for error, W for warning, and C for critical), and a brief description of the event.

3. If an event occurs while you're viewing this list, click "Refresh" to update it.

B.1   Disconnecting from Shared Folders

If you need to reconfigure the disks in your storage system or shut it down for any reason, all users should disconnect from the shared folders to ensure that the process proceeds smoothly. You might also want to have users disconnect from the shared folders if you want to change their access rights, since otherwise the change will not take effect until the user shuts down the computer.

The procedure for disconnecting from a shared folder varied, depending on the operating system used by the user.

Windows users

Windows users can disconnect from a shared folder using either My Computer or Windows Explorer, or the Storage System Console.

To disconnect from a shared folder using My Computer or Windows Explorer:

1. Close any files that you currently have open in the shared folder.

2. In My Computer or Windows Explorer, right-click the drive for the shared folder and then click Disconnect from the pop-up menu.

3. The shared folder should no longer appear in My Computer or Windows Explorer.

To disconnect from a shared folder using the Storage System Console:

1. Start the Storage System Console.

2.   In the left pane, double-click the name of the storage system that contains the shared folder from which you want to disconnect. The storage system name will expand to display all the available shared folders.

3. In the left pane, select the name of the shared folder from which you want to disconnect, and then click "Unmap Drive Letter".

Linux users

To disconnect from a shared folder using Linux, unmount the desired shared folder by entering the following command: "umount /my_directory" where my_directory is the name of the local directory. For example, if you mounted the shared folder using the following command: "mount 192.168.0.101:/nas/NASDisk-00002/public /my_directory" you would unmount it using the following command: "umount /my_directory". If you included a longer path when mounting the shared folder (such as "/mnt/my_directory"), use the same path wen unmounting it.

Mac users

The procedure for disconnecting from a shared folder on a Mac varies, depending on whether the Mac is running OS X or an older operating system.

To disconnect from a shared folder on a Mac running OS X:

1. On the desktop, select the shared folder from which you want to disconnect.

2. From the File menu, click "Eject".

Any open window to the shared folder closes, and the shared folder disappears from the desktop.

Other Mac operating systems, refer to the documentation included with the operating system for information about disconnecting from a shared folder.

B.2 Troubleshooting the Device

This section provides general information about common problems that you might have with your storage system and steps you can take to resolve them.

Problem: I can't access the Manager.

Resolution: If you are using the System Storage Console, make sure the computer where the Storage System Console is installed is in the same subnet as the storage system.

If you are using a Web browser, make sure the name or IP address of the storage system is correct. You can use the storage system name only if that name is registered with a DNS server in your network. In addition, if you configured the storage system to use a specific IP address, you might need to specify the IP address of the gateway in your network before you can successfully access the Manager using a Web browser. First access the Manager using the Storage System Console and then specify the gateway address and try to access it using a Web browser.

Problem: I forgot the password for logging in to the Manager.

Resolution: You can reset the storage system to use its original administrator user name (admin) and password (storage) by pressing the small, recessed reset button on the back of the storage system.

> Note: This also resets the storage system to its original network settings. If you previously configured the storage system to use a specific IP address, it will now obtain its IP address from the DHCP server (if any). If you don't have a DHCP server on the network, it will use its default IP address (192.168.0.101).

In addition, pressing this button restarts the storage system, which mightadversely affect user connections to shared folders. Be sure to do this only whenusers are not connected to shared folders or performing recovery.

Problem: The users can't access the shared folders.

Resolution:

- Make sure the storage system is powered on, connected to the network, and operating properly.

- Make sure the user configuration is correct.

  For Windows or OS X users, try changing the password and accessing the shared folder again.

  For Linux users, make sure the computer name or IP address is correct. If it's not, recreate the user by removing the existing user and adding it again.

- Make sure the users are using the proper procedure for accessing the shared folders, including the correct name or IP address of the storage system. (You can use the storage system name only if that name is registered with a DNS server on your network.)

  Windows users can't access shared folders using the Storage System Console unless their computers are on the same subnet as the storage system. If using the Storage System Console does not work, try accessing the shared folders using My Computer or Windows Explorer.

- Make sure the user's computer is connected to the network and can otherwise access the storage system.

  To check the network connection in a Windows environment, click Start --> Run and type cmd. At the command prompt, type the following: "ping IP_address" where IP_address is the IP address of the storage system. If you do not see "Reply from...", the problem is with your network.

Problem: The users can't create files in the shared folders.

Resolution: Check the access rights for the user. The user must have read/write rights to be able to create files in the shared folder.

Problem: The storage system is not distributing IP addresses.

Resolution: Make sure that Enable DHCP server is selected on the Network page, and that the starting and ending IP addresses are valid. The first three digit groups of both the starting

IP address and ending IP address must be the same.

If the network configuration is correct and it still doesn't work, the DHCP service might not be working properly. Restart the storage system.

Problem: The users cannot access the storage system using FTP.

Resolution: Make sure that Enable FTP server is selected on the Network page and that the users are using the correct address for accessing the storage system.

If the network configuration is correct and the users are using the proper address and it still doesn't work, the FTP service might not be working properly. Restart the storage system.

B.3 Troubleshooting DiskSafe Express

This section provides general information about common problems that you might have with DiskSafe Express and steps you can take to resolve them.

> **Note:** If you need help from Technical Support, you might be asked to create a diagnostic file. For information about this procedure, refer to Creating a diagnostic file.

Problem: The disk that I want to protect isn't listed.

Resolution: DiskSafe Express does not support dynamic disks. These types of disks are automatically filtered from the list of disks that you can protect.

Problem: Authentication errors occur when I try to protect a disk.

Resolution:

- When adding a storage system, make sure that you're using the correct name or IP address of the storage system. You can enter a storage system name only if that name is registered with a DNS server on your network.

- Make sure the computer is connected to the network and can otherwise access the storage system. To check the network connection, click Start → Run and type "cmd". At the command prompt, type the following: "ping IP_address" where IP_address is the IP address of the storage system. If you do not see "Reply from...", the problem is with your network.

- If the storage system already exists, select it in the list of backup locations and then click Remove. Then click Add to add it again. This resets the settings in the iSCSI initiator which might be causing the authentication problem.

Note: When authentication errors occur, invalid backups might be created on the storage system. To ensure that you don't use up disk space unnecessarily, be sure to delete any extraneous backups on the storage system. Compare the Backup disk ID on the Status page in DiskSafe Express with the Backup Disk ID on the Backups page in the Manager to determine which backup is actually being used.

Problem: The Status page indicates that the backup is offline.

Resolution:

- Make sure the storage system is powered on.

- Check the network connection to the storage system.

  To do this, click Start → Run and type "cmd". At the command prompt, type the following: "ping IP_address" where IP_address is the IP address of the storage system. If you do not see "Reply from...", the problem is with your network.

- Make sure that the backup has not been deleted on the storage system by checking the Backups page.

  If it has been deleted, remove protection and protect the disk again.

- If you changed the name of your computer, the storage system will not recognize it any longer. Remove protection for all your disks or partitions, delete the old computer name from the storage system, and then protect your disks again.

Problem: A backup did not occur at its regularly scheduled time.

Resolution:

- Check the schedule to confirm that it is correctly configured.

- Make sure the computer is powered on during the scheduled backup time.

- Make sure the storage system is powered on during the scheduled backup time.

- On the Status page, make sure that the Status is Normal. If protection is stopped (for example, if you recovered the disk or recovered a different partition on the same disk), backups will not occur until you resume protection by clicking Back Up Now.

- If you changed the name of your computer, the storage system will not recognize it any longer. Remove protection for all your disks or partitions, delete the old computer name from the storage system, and then protect your disks again.

- If the IP address of the storage system changed (for example, if the storage system obtains its IP address from a DHCP server and acquired a new one after you added the storage system to the list of backup locations), you must start DiskSafe Express so that it can retrieve the new IP address. You must do this each time the IP address on the storage system changes.

Problem: I can't change my backup schedule.

Resolution: On the Status page, make sure that the Status is Normal. If protection is stopped (for example, if you recovered the disk or recovered a different partition on the same disk), you cannot change the schedule until you resume protection by clicking "Back Up Now".

Problem: I forgot my recovery CD password.

Resolution: Reset the password using the storage system. Once you reset it on the storage system, you can use the new password with the recovery CD.

B.4 Creating a Diagnostic File

In some cases, you might need assistance from Technical Support to solve problems that you might have with DiskSafe Express, When you contact the Technical Support team, they might ask you to create a diagnostic file to help them better understand your environment and configuration settings.

You can create a diagnostic file using either the DiskSafe Express application or, in the event of a system failure, using the recovery CD. To create a diagnostic file using the recovery CD, the computer must have a floppy disk drive or a directly connected USB disk.

> **Note:** This diagnostic file does not include the log files associated with the Intelligent Management Agent (IMA). You might be asked to send those files (iscmlib.log and iscmservice.log) separately.

Using DiskSafe Express

To create a diagnostic file using DiskSafe Express:

1. Run DiskSafe Express.

2. From the Action menu, click Create Diagnostic File.

3. Click Save to save the file using the default file name, or type the desired file name in the File name text box and then click Save.

If desired, you can save the file in a different location.

Once the file has been created, you can send it to Technical Support.

Using the recovery CD

To create a diagnostic file using the recovery CD:

1. Insert the recovery CD into the computer's CD-ROM drive and press Alt+F2.

2. At the command line, enter the following command and then press Enter: "xray"

3. When prompted, insert a formatted floppy disk into the computer's floppy disk drive or attach a USB disk and press Enter.

4. Select the media where you want to save the diagnostic file and press Enter. The screen indicates whether the process succeeded or failed. Once the file has been created, you can copy it from the floppy disk or USB disk to another operational computer and send it to Technical Support.

5. To return to the recovery CD menu, press Alt+F1.

Appendix C: Glossary

Client – Any desktop, notebook or laptop that is connected to the freeStor 4020.

DHCP (Dynamic Host Configuration Protocol) – A protocol that allows computers to be automatically assigned an IP address from a DHCP server.

DNS Server Address (Domain Name System) – The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate between domain names and IP addresses, and to control email delivery.

DSE (DiskSafe EXpress) – A software solution that allows users to back up their data and operating system information. Once the system has been backed up, it can be easily and completely recovered in the event of a hard drive failure. Additionally, if the system becomes corrupted (e.g. a virus infection) but the hard drive is still operational, the user can restore only the affected files.

Ethernet – Ethernet networks are connected by cables and hubs, and move electronic data between computers. The term Ethernet refers to the family of local-area network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol.

IEEE (The Institute of Electrical and Electronics Engineers) – Among its responsibilities, the IEEE sets standards of networking, including Ethernet LANs. IEEE standards ensure interoperability between systems of the same type. The IEEE promotes the engineering process of creating, developing, integrating, sharing, and applying knowledge about electronic and information technologies and sciences.

IP Address (Internet Protocol) – An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number must be between 0 and 255. For example, 1.160.10.240 could be an IP address.

LAN (Local Area Network) – A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). A home network is considered a LAN.

MAC Address (Media Access Control) – A MAC address is a hardware address that uniquely identifies each node of a network. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

SATA (serial advanced technology attachment) – SATA is a successor to the older Parallel ATA or IDE technology allowing for faster data transfer speeds.

Subnet Mask – A mask used to determine what subnet an IP address belongs to. Subnets enable the network administrator to further divide the host part of the address into two or more subnets.

RAID (redundant array of independent disks) – RAID technology allows multiple hard drives to be grouped together to provide performance enhancements and/or data redundancy.

TCP/IP (Transmission Control Protocol/Internet Protocol) – Short for Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet.