USRobotics®

Serial ATA 4-Drive NAS

User Guide

R46.1702.00
rev 0.8 04/07

U.S. Robotics Corporation
935 National Parkway
Schaumburg, Illinois
60173-5157
USA

Contents

Safety Instructions

Introducing Your Storage System

Getting Started

Managing Your Storage System

Accessing the Storage System through FTP and SSH

Protecting Local Disks

Disk Configurations

Troubleshooting

Support Information

Regulatory Information

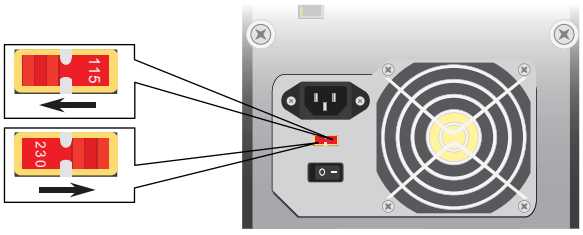
U.S. Robotics Corporation Two (2) Year Limited Warranty

Safety Instructions

Use the following safety guidelines to help ensure your own personal safety and to help protect your storage system and working environment from potential damage.

General

- Do not attempt to service the storage system yourself unless you are a trained service technician. Always follow installation instructions closely.
- To help prevent electric shock, plug the unit and device power cables into properly grounded electrical outlets. These cables are equipped with 3-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- In order to prevent electric shock, disconnect power to the unit by removing the power cord from the electrical outlet.
- To help avoid the potential hazard of electric shock, do not use, connect or disconnect any cables or perform maintenance or reconfiguration of this product during an electrical storm.
- To help avoid possible damage to the system board, wait 5 seconds after turning off the computer before disconnecting a device from the storage system.
- To avoid shorting out your computer when disconnecting a network cable, first unplug the cable from the network adapter on the back of your computer, and then from the network jack. When reconnecting a network cable to your computer, first plug the cable into the network jack, and then into the network adapter.
- Ensure that nothing rests on your storage system's cables and that the cables are not located where they can be stepped on or tripped over. Keep your unit away from radiators and heat sources. Also, do not block cooling vents. Avoid placing loose papers underneath your storage system; and do not place it in a closed-in wall unit or on a bed, sofa, or rug.
- Do not spill food or liquids on your storage system
- Do not push any objects into the openings of this product. Doing so can cause fire or electric shock by shorting out interior components.
- Your storage system is equipped with a manual voltage selection switch — The voltage selection switch on the back panel must be manually set to operate at the correct operating voltage. To avoid damaging the product, be sure that the voltage selection switch is set to match the AC power available at your location:
    - 115 V/60 Hz in most of North America.
    - 230 V/50 Hz in most of Europe.



Introducing Your Storage System

The Serial ATA 4-Drive NAS is an intelligent network storage solution for small and medium-sized offices and home network environments. It provides up to 2.0 TB of hard disk space for both shared files and backups of your computer hard disks, offering an ideal way to distribute and protect important data.

To make it easy to back up your computer hard disks, this solution includes DiskSafe Express, a software application that provides reliable data protection and rapid data recovery in the event of a system crash or disk failure. With DiskSafe Express, you can recover your local disks or partitions without having to reinstall or reconfigure the operating system or applications, dramatically shortening recovery time.

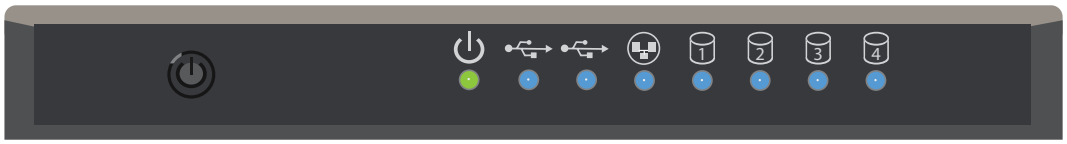
Package Contents

- USR8700 Serial ATA 4-Drive NAS
- Power Cord
- Ethernet Cable
- Installation CD-ROM
- Quick Installation Guide
- DiskSafe Express recovery CD

Physical Features

Front

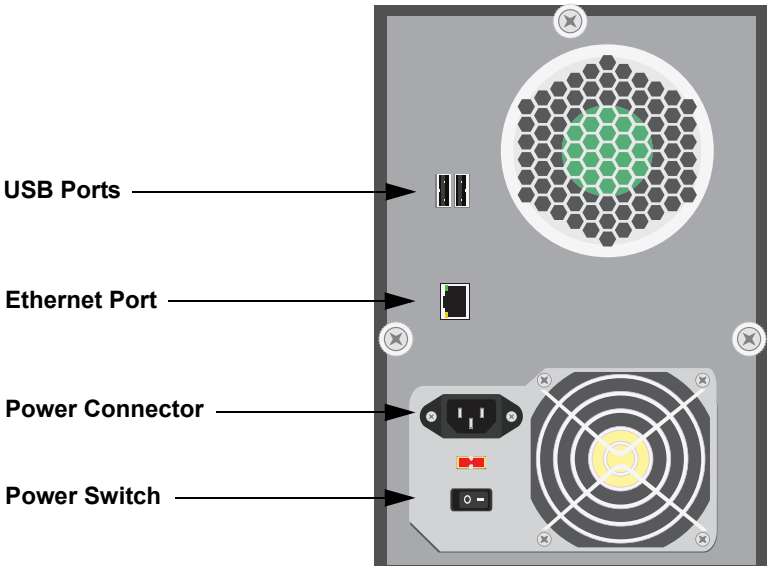
The Serial ATA 4-Drive NAS system has the following status LEDs:



Symbol	Name	State	Condition
⏻	Power	Off	Not receiving power
		Solid	Receiving power: normal operation
		Flashing	Booting or shutting down by power button
⇄	USB 2.0	Off	USB device not available
		On	USB device available
🖧	LAN (10/100/1000 Mbps)	Off	Not connected to network
		Solid	Connected to network
		Flashing	Transmitting or receiving network data

Symbol	Name	State	Condition
	Disk (1–4)	Off	Drive not available
		On	Drive available
		Flashing	Drive activity

Back



System Requirements

- Microsoft Windows Vista; Microsoft Windows XP; Microsoft Windows Server 2003; or Microsoft Windows 2000 Professional, Server, or Advanced Server with Service Pack 4
- Web Browser with JavaScript enabled - Internet Explorer 6.0 or Firefox 1.06 or newer

Key Features and Benefits

- **Flexible storage capacity**—The storage system supports up to four 3.5" SATA-I hard disks, with a capacity of 80–500 GB each. You can start with just one and add more as your needs grow.
- **Built-in data protection**—In addition to a linear disk configuration in which all the disks are treated as independent entities, the storage system supports several different types of RAIDs (redundant arrays of independent disks). This means that you can take advantage of the build-in data protection and data duplication offered by advanced RAID levels. If your storage system has multiple hard disks and one fails, you won't lose important data. For more information, refer to "Disk Configurations," beginning on page 125.
- **Simple administration**—You can run the browser-based management interface from any computer in

your network, and its informative wizards and configuration pages will help you accomplish your tasks quickly and easily.

- **Status at a glance**—The **Home** page of the management interface lets you quickly determine how much space is being used and who's currently connected.
- **Support for multiple platforms**—Whether the computers in your network run Windows, Mac OS X or other Mac operating systems, or Linux, you can set up file sharing for each of them.
- **Security**—Only authorized users can access the shared folders on your storage system. You can also control whether the user can only view the information in the shared folders or also add, modify, or delete files there.
- **Fast performance**—With its gigabit Ethernet support, the storage system provides fast access to the data you need, when you need it.
- **Printer support**—You can attach up to two pass-through printers to the storage system's USB sockets, and all users can access them.

Hardware Specification

Processor	Intel IOP80219 400 MHz
Memory	DDR 256 MB
Flash	32 MB NOR Flash
Hard Disks	Up to four 3.5" SATA-I hard disks (80–500 GB each) **Note:** The total amount of storage space cannot exceed 2 TB.
Maximum Capacity	2 TB
Network	Intel gigabit LAN port interface
SATA Controller	Intel SATA Controller
USB	Two Type A USB 2.0 sockets
EMI Safety	CE/FCC Class B
System Power	200 W PSU
Operating Temperature	0º C to 85º C (32º F to 185º F)
Operating Humidity	10–90% relative humidity
Storage Temperature	-20º C to 70º C (-4º F to 158º F)
Storage Humidity	5–90% non-condensing humidity

Note: If the temperature of the entire unit reaches or exceeds 85º C (185º F) or if the temperature if any of the disks reaches or exceeds 55º C (131º F), the storage system shuts down automatically.

If the temperature of any of the disks reaches or exceeds 42º C (107.6º F), the fan will run at full speed. If the temperature of any of the disks reaches or falls below 37º C (98.6º F), the fan will slow down.

Software Specification

Operating System	Linux Kernel 2.6.10
Network Service	DHCP client/server (default IP address is 192.168.0.101)
Supported Web Browsers	• Microsoft Internet Explorer 6.0 or newer • Mozilla Firefox 1.06 or newer
RAID	• Standard RAID 0 • RAID 1 • RAID 5 • RAID 5 + spare • RAID 10
File-Sharing Protocols	• CIFS/SMB • NFS
Access Control	• Users have read-only or read/write access to shared folders • 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 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.

Getting Started

Getting started with your storage system involves the following general steps:

1. Install your storage system.

   This process involves installing both the hardware and software components of your storage system and specifying the initial configuration.

   For step-by-step instructions for this process, see “Installing Your Storage System” on page 11.

2. After installation is complete and the storage system restarts, start the Web User Interface and log in.

   For more information about this step, see “Accessing the Web User Interface” on page 25.

3. Add users.

   This is necessary only if you are using local authentication mode and want to control access to the shared folders, or if some users in your network use Linux or Macs other than those running OS X.

   For more information about this step, see “Adding Users” on page 31.

4. Create shared folders.

   By default, the storage system includes a shared folder named **public**, which all Windows and Mac OS X users can access. However, you might want to create other shared folders as well. For example, in an office environment, you might want to create a shared folder for company policies that everyone can view, and separate folders for confidential business documents that only selected individuals can view or change. In a home environment, you might want to set up separate folders for different types of files, like photos, videos, or music.

   For more information about this step, see “Creating Shared Folders” on page 34.

5. Access the shared folders.

   For information about this step, see “Accessing Shared Folders” on page 37.

6. Protect your computer hard disks.

   This process involves installing DiskSafe Express on each computer that you want to protect and specifying which hard disks or partitions to back up and how often backups should occur.

   For more information about this step, see "Protecting Local Disks," beginning on page 89.

Installing Your Storage System

1. Determine your Configuration.

   Before you set up your system, you need to decide which configuration you will use. For configuration

considerations, see “Step One: Determine Your Configuration” on page 12.

2. Set up your storage system.

   This involves installing the hard disks, attaching any optional USB devices, attaching the storage system to your network, and powering up the system.

   For information about this step, see “Step Two: Set up Your storage system” on page 13.

3. Install the Storage System Console.

   You will need the Storage System Console to initialize your hard disks in step 4.

   For information about this step, see “Step Three: Install the Storage System Console” on page 16

4. Initialize the Hard Disks.

   This step loads firmware from the storage unit’s memory to each disk. “Step Four: Initialize the Hard Disks” on page 17.

5. Configure your storage system.

   Before you can use your storage system, you need to perform some initial configuration tasks, like setting the date and time, and specifying how much space to use for file sharing and how much to use for backups. The System Setup wizard guides you through this process.

   For information about this step, see “Step Five: Configure your Storage System” on page 20.

If you bought your Serial ATA 4-Drive NAS with the disks already installed and configured, and you do not want to change your disk configuration, skip step one and proceed with “Attaching USB Devices” in step two on page 15.

Step One: Determine Your Configuration

Before you start the physical installation of your storage system, decide which configuration is best suited to your needs. The configuration that you choose may affect the order in which you load the disks into your storage system, and you will need to specify your configuration choice when you reach “Step Five: Configure your Storage System” on page 20.

Each supported configuration has a different balance of desirable characteristics, as shown in the table below. The configurations available to you depend on the number of disks installed in your storage system. Use this table to select your configuration based on the number of disks you intend to use and the characteristics that are of the highest priority to you.

Number of Disks	Configuration	Methods Used	Configuration Characteristics		
			Available Capacity*	Data Redundancy	Performance
1	Linear	Independent disks	500 GB	No	Good
2	Linear	Independent disks	1.0 TB	No	Good
	RAID 0	Striping	1.0 TB	No	High
	RAID 1	Mirroring	500 GB	Yes	Good

Number of Disks	Configuration	Methods Used	Configuration Characteristics		
			Available Capacity*	Data Redundancy	Performance
3	Linear	Independent disks	1.5 TB	No	Good
	RAID 0	Striping	1.5 TB	No	High
	RAID 5	Striping with parity	1.0 TB	Yes	Good
4	Linear	Independent disks	2.0 TB	No	Good
	RAID 0	Striping	2.0 TB	No	High
	RAID 5	Striping with parity	1.5 TB	Yes	Good
	RAID 5 with Spare	Striping with parity; spare drive automatically rebuilds a failed drive	1.0 TB	Yes	Good
	RAID 10	Striping, Mirroring	1.0 TB	Yes	Good

* Available capacity based on 500-GB drives

For more information about configurations, see the "Disk Configurations" on page 125.

Step Two: Set up Your storage system

Setting up your storage system consists of the following steps:

Installing the Hard Disks

Attaching USB Devices

Connecting the Storage System to the Network

Powering Up the Storage System

Installing the Hard Disks

If you have fewer than four hard disks in your storage system, you might want to add more at this time. You can add disks later, but changing your disk configuration once the disks contain data might cause data loss.

Note: The storage system must have at least one SATA hard disk with a capacity of at least 80 GB.

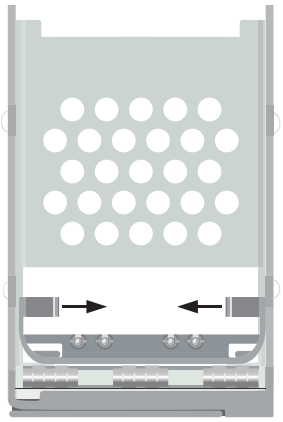
USRobotics strongly recommends that you install all the hard disks that you want to use in the storage system at this time in order to avoid data loss.

USRobotics also recommends that you use 4 disks of the same size for optimum performance.

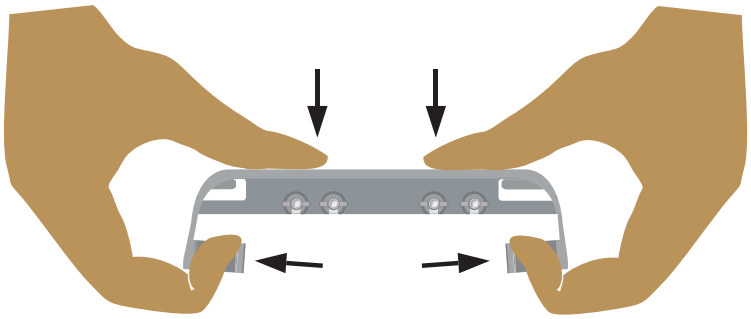
To install the hard disks, you need a Phillips head screwdriver.

1. Remove the top hard disk tray from the storage system:

2. Near the front of the tray is a spacer containing four screws. Squeeze the tabs toward each other to remove the spacer from the tray.

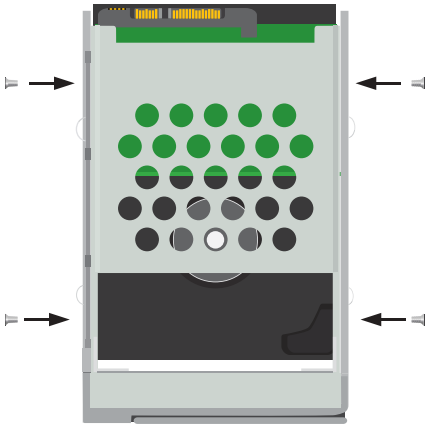


3. With the flat edge of the spacer up and the screws facing a flat surface (such as a table or desk top), flex the sides of the spacer apart from each other to release the screws.



4. Make sure that the hard disk is a SATA disk. It should have a SATA connector similar to the following:

5. Slide the new hard disk into the tray (connector end down and toward the back of the tray), and fasten the screws on the sides of the tray:



6. Slide the hard disk and tray back into the storage system until it snaps into place.

If you have fewer than four disks, load the bottom trays first and leave the top tray or trays empty.

If you have four disks that are not the same size and you intend to use RAID 10, USRobotics recommends that you load the disks in ascending order of disk capacity, starting with the smallest disk in the bottom slot (slot 1),

Notes:

- If you install a hard disk that was previously part of a RAID, it will rebuild automatically.
- If you later replace all of the disks with higher-capacity disks, you must format those disks.

For more information about disk configurations, see the "Disk Configurations" on page 125.

7. Repeat steps 1 through 6 for each disk that you will use in your storage system.

Attaching USB Devices

If you have USB storage devices or printers, you can attach them to the USB ports on the back of the storage system.

Note: USB hubs are not supported. In addition, any USB disk must be formatted before you use it with the storage system, and only the first partition of a FAT or FAT32 file system will be recognized. Do not attach the storage system directly to a USB port on a computer.

Connecting the Storage System to the Network

To connect your storage system to your network, insert one end of the supplied RJ-45 Ethernet cable into the Ethernet port on the back of the storage system. Then insert the other end into a network port.

Powering Up the Storage System

To power up the storage system, insert the power cable into the power connector on the back of the storage system and plug the other end into a power outlet.

Note: USRobotics recommends that you plug the storage system into a surge protector or uninterruptible power supply to prevent damage to the system from power surges.

Once you have connected the power cable, make sure that the power switch on the back of the storage system is set to the on position. Then press and release the power button on the front of the storage system.

The power and Disk LEDs flash while the storage system is booting. Once the system has finished booting, the Disk LEDs stop flashing.

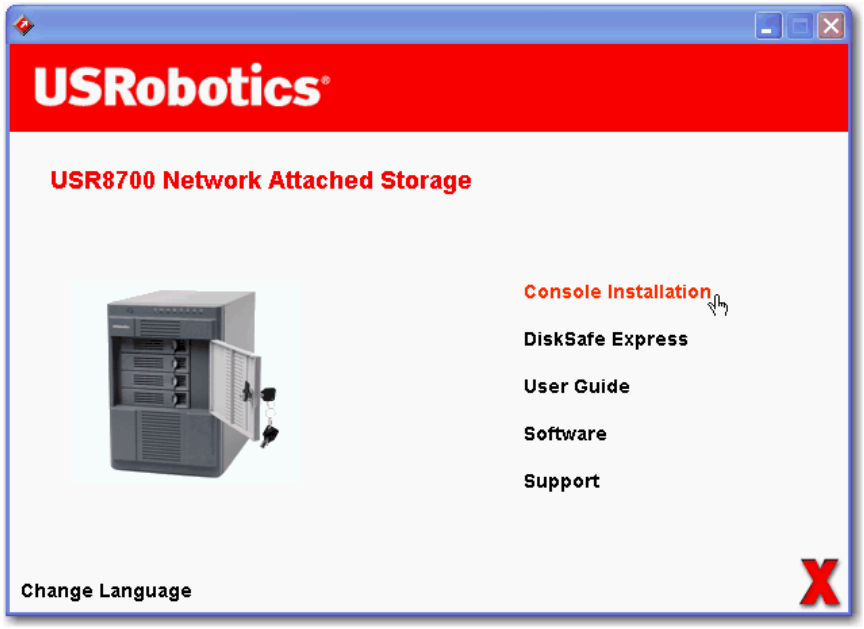
If the hard disk installation was successful, the Disk LED is blue. If there is a problem, the Disk LED is off. If this occurs, shut down the system, remove and inspect the hard disk for any installation problem, and reinstall it. To shut down the system, press and hold the power button for approximately five seconds until the Disk LEDs start flashing. Then release the power button; the storage system will shut down after a short period.

Step Three: Install the Storage System Console

Install the Storage System Console on a computer on the same network as the Serial ATA 4-Drive NAS:

1. Insert the USRobotics Installation CD-ROM into your CD-ROM drive.
2. If prompted, select your preferred language, then review the License Agreement and click **Yes**.

   The installation CD prompts you to make a choice:

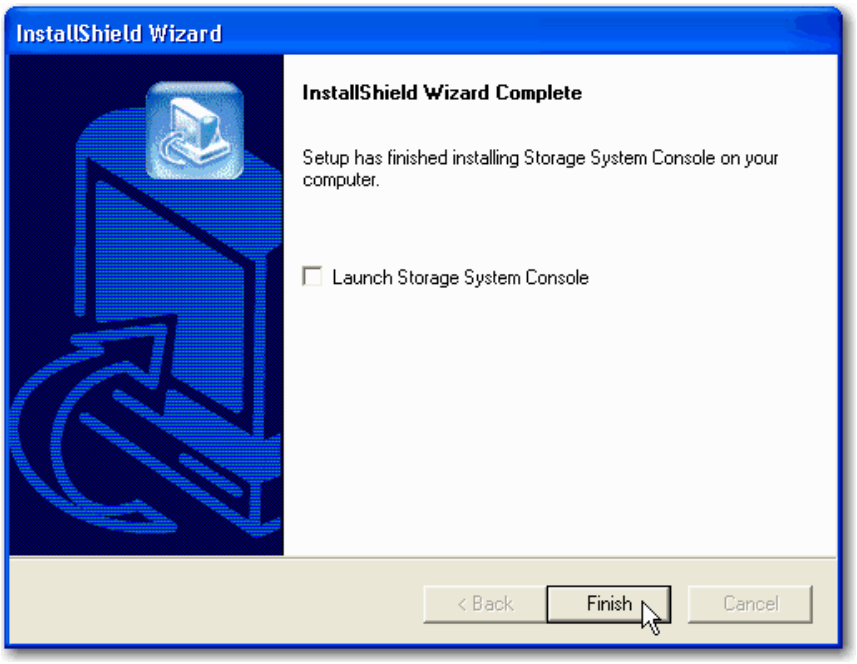


3. Select **Console Installation**.

   The installation wizard appears.

4. Follow the on-screen prompts to install the Storage System Console. When installation is complete,

the following window appears:



5. Click **Finish**.

Step Four: Initialize the Hard Disks

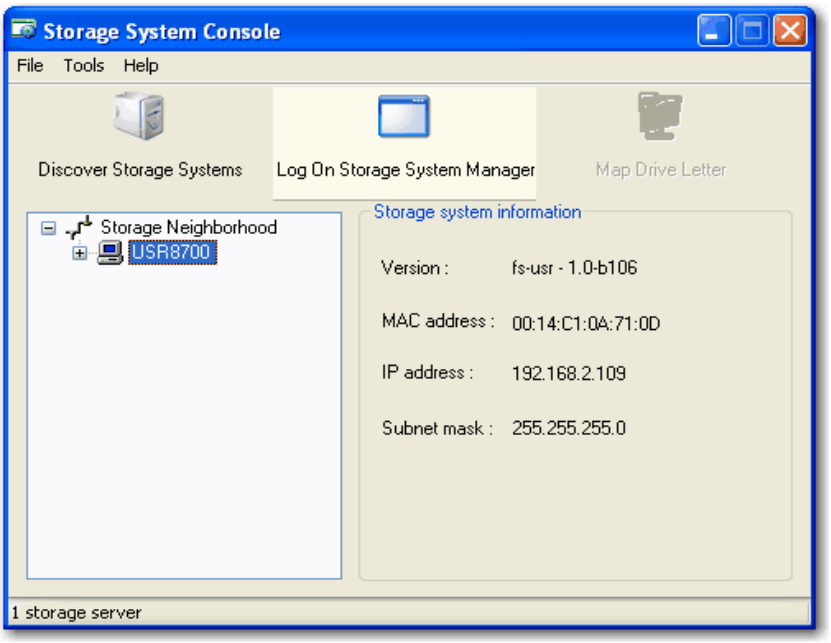
To initialize the hard disks, follow these steps:

1. Start the Storage System Console as follows:

   Windows Vista or XP: click **Start > All Programs > Storage System Console**.

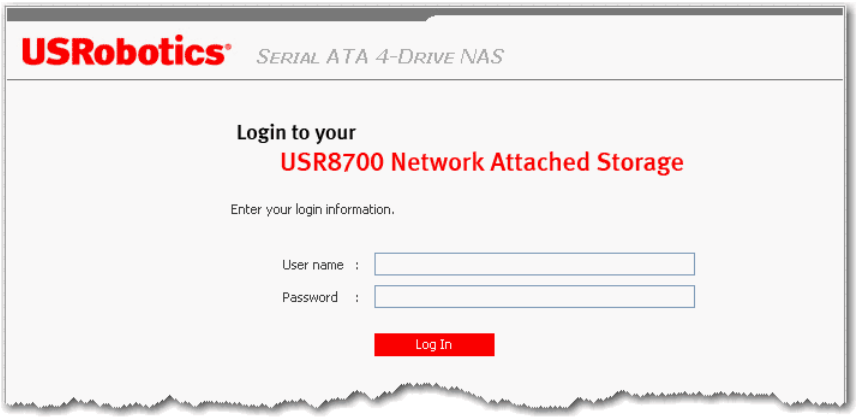
   Other Windows operating systems: click **Start > Programs > Storage System Console**.

The **Storage System Console** appears:



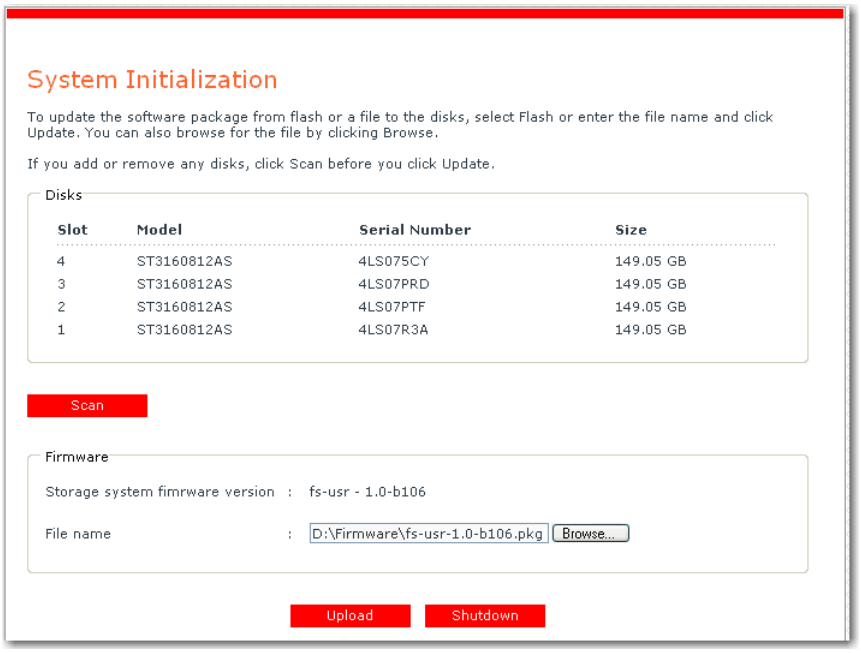
2. In the left pane, click the name of the storage system. Then click **Log On Storage System Manager**.

   If you see the **Login** page,



   your storage system was initialized and configured before you bought it. You are finished with the installation procedure and can begin using your Serial ATA 4-Drive NAS system, or you can reconfigure your disks if you choose to do so. Skip the remaining installation steps and proceed with “Accessing the Web User Interface” on page 25.

If the **System Initialization** page appears, you need to initialize your disks:



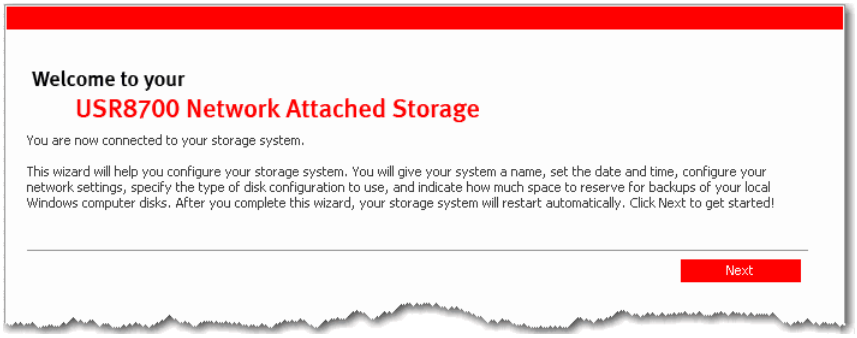
If not all the hard disks have been detected, or if you want to add, remove, or reorder the disks at this time, insert or remove the disks one at a time and click **Scan** after each action. If you are adding disks, be sure to wait until the Disk LED is blue before you click **Scan**.

Note: USRobotics strongly recommends that you install all the hard disks that you want to use in the storage system at this time, since changing the number of hard disks later can require disk reconfiguration and possible data loss.

3. Click **Browse** and locate the USRobotics Installation CD-ROM.
4. Open **`Firmware\fs-usr-1.2-b609.pkg`**.
5. On the **System Initialization** page, click **Upload**.

   The firmware on the storage system's internal flash memory is uploaded to the hard disks.

When this process is complete, the storage system restarts and displays the welcome page:



Step Five: Configure your Storage System

Once initial setup has been completed, follow these steps to run the System Setup wizard and perform the necessary initial configuration:

1. On the welcome page, click **Next**.

   The **End User Software License Agreement** page appears.

2. If you agree to the terms, select I accept the license agreement and click **Next**.

   The **Host Name** page appears.

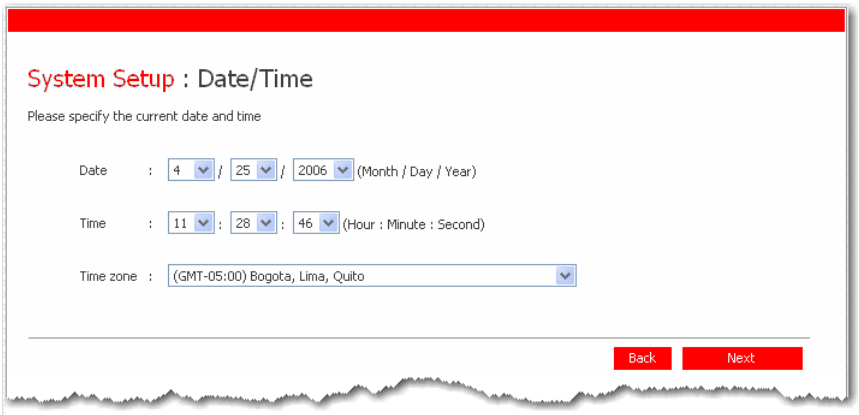
3. Click **Next** to accept the default storage system name (USR8700)

   OR

   Enter the name that you prefer and then click **Next**.

   The storage system name can be up to 15 characters long and can include letters, numbers, and hyphens.

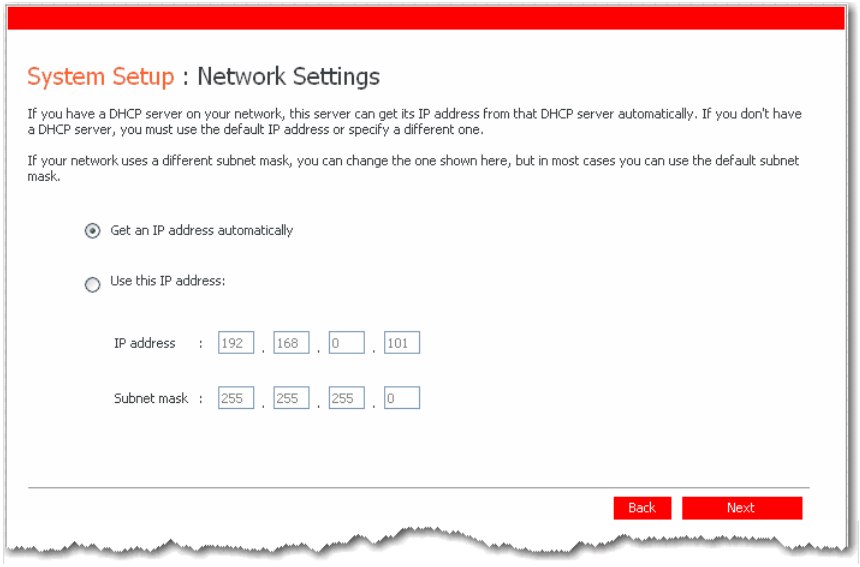
   When you click **Next,** the **Date/Time** page appears:



Specify the current date, time, and time zone, and then click **Next**.

Specify the time using the 24-hour format. For example, enter 2:00 P.M. as 14:00:00.

When you click **Next**, the Network Settings page appears:

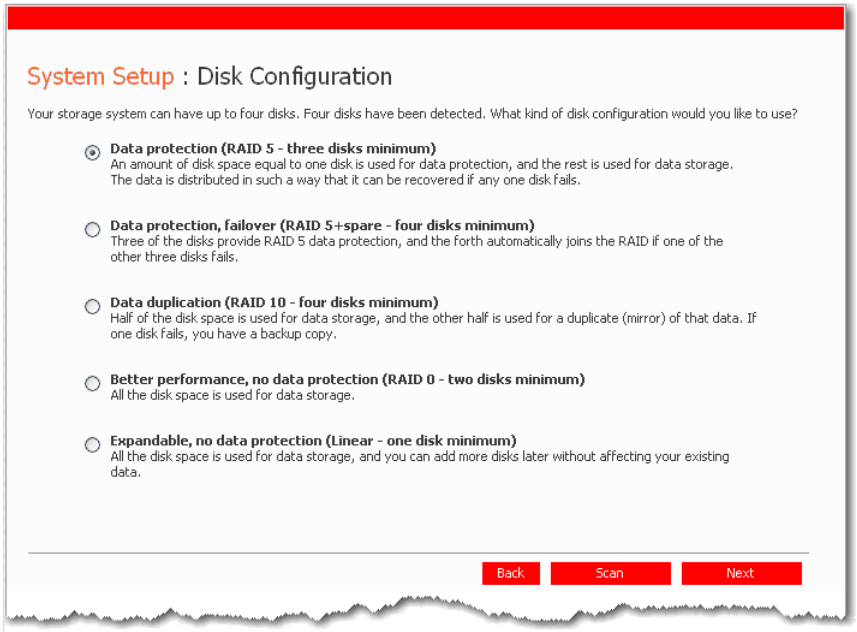


4. By default, if your network has a DHCP server, the storage system obtains an IP address automatically from that server.

   If your network does not have a DHCP server, the default IP address and subnet mask are used. (The default IP address is 192.168.0.101, and the default subnet mask is 255.255.255.0).

   To accept the default settings, click **Next**. Otherwise, specify the desired settings and then click **Next**.

   The **Disk Configuration** page appears. The options that appear on this page vary depending on the number of hard disks that are currently installed in the system.



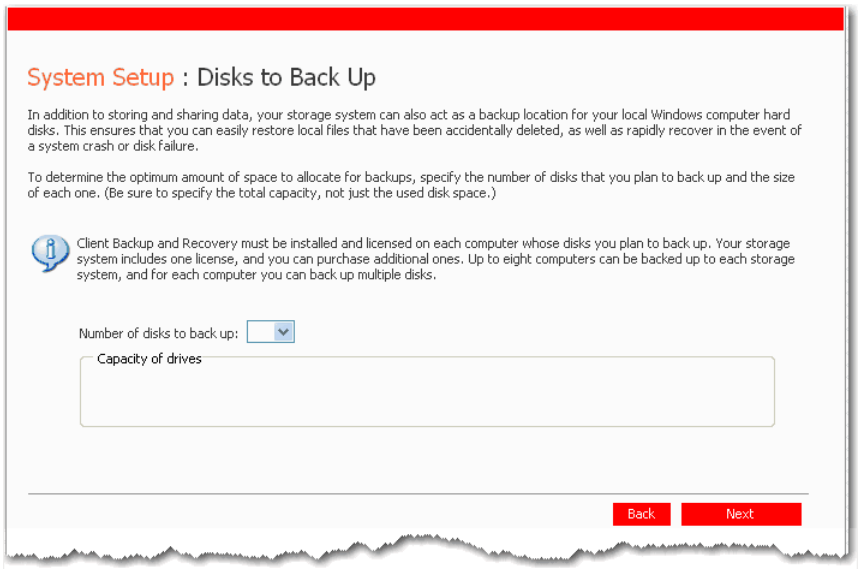
5. Select the configuration that you chose from the table on page 12 and click **Next**.

   By default, the storage system selects the configuration that provides the best level of data protection available: for a single disk, a linear configuration; for two disks, RAID 1; and for three or four disks, RAID 5.

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

   If you want to add or remove hard disks, do so one at a time. For each disk, wait until the Disk LED is blue and click **Scan**. When you are finished adding disks, select your configuration and click **Next**.

   When you click **Next**, the **Disks to Back Up** screen appears:



6. In **Number of disks to back up**, select the total number of disks that you plan to back up to this storage system. The maximum number of disks you can back up is 25.

   If you do not plan to back up any disks, select 0, click **Next**, and go to step 9.

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

   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 should select 10.

   When you select a number, a corresponding number of text boxes (Disk 1, Disk 2, etc.) appear in

Capacity of drives:

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

   To determine the size of a computer's disk, on that computer:

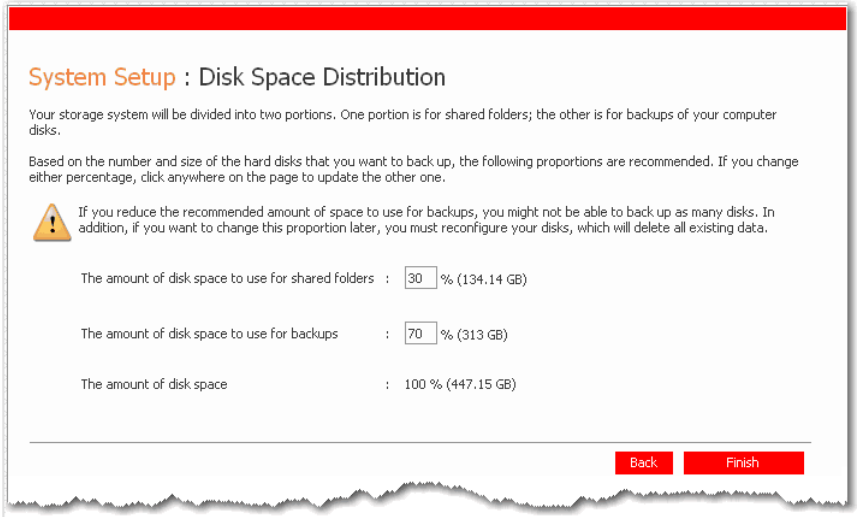
   - Windows Vista: click **Start > Computer**, right-click the disk, and select **Properties**.
   - Windows 2000: on the desktop, double-click **My computer**, right-click the disk, and select **Properties.**
   - Other Windows operating systems: click **Start > My Computer**, right-click the disk, and select **Properties**.

   Be sure to enter the entire capacity of each disk, not just the amount of used disk space.

   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.

When you click **Next**, the **Disk Space Distribution** page appears:



8. To accept the suggested percentages for file sharing and backup, click **Finish**.

   To change these proportions, enter a new percentage in either text box. (When you click anywhere on the page, the other text box updates automatically so that both percentages add up to 100%.) Then click **Finish**.

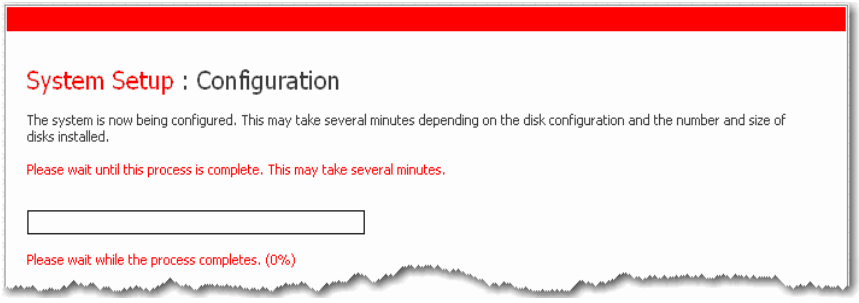
Caution: If you reduce the recommended amount of space to use for backups, you might not be able to back up as many disks or use the maximum allowed number of backup versions. The recommended amount of space is greater than the total size of all your disks to accommodate multiple backup versions.

If you change these proportions after you finish the wizard, you will lose all data in your shared folders and all existing backups.

Backup of computer disks is provided through a separate backup and recovery utility. You can install DiskSafe Express from the USRobotics Installation CD-ROM for this purpose. For more information about DiskSafe Express, see the “Protecting Local Disks” on page 89.

9. in the confirmation window, click **OK**.

   The **Configuration** page appears and the system is configured according to the settings you specified. Once the configuration is complete, the system restarts



Congratulations. You have successfully completed the installation procedure. Please register your Serial ATA 4-Drive NAS at www.usr.com/productreg/.

Accessing the Web User Interface

Once you have completed the initial configuration of your storage system, you can access the Web User Interface to add users, create shared folders, and perform other tasks related to managing your storage system.

There are two ways to access the Web User Interface:

- Using a Web browser with JavaScript enabled (Microsoft Internet Explorer 6.0 or Mozilla Firefox 1.06 or newer)
- Using the Storage System Console (a Windows application that must be installed on each computer where you want to use it)

Using a Web browser, you can access the Web User Interface from any computer in your network, but you must know the name or IP address of the storage system. 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 Web User Interface using a Web browser. First access the Web User Interface using the Storage System Console and then specify the gateway address (as described in "Changing the Network Settings" on page 72) and try to access it using a Web browser.

Using the Storage System Console, you can access the Web User Interface only from a computer in the same subnet as the storage system, but you do not need to know the name or IP address of the storage system or otherwise modify the network settings.

Note: The Storage System Console launches a Web browser, so the computer where you install the Storage System Console must have Microsoft Internet Explorer 6.0 or Mozilla Firefox 1.06 or newer installed and set as the default browser with JavaScript enabled.

If Internet Explorer 7.0 or Firefox 2.0 indicate a certificate error, continue to the website.

Accessing the Web User Interface Using a Web browser

To access the Web User Interface using a Web browser:

1. From any computer in your network, run Microsoft Internet Explorer 6.0 or Mozilla Firefox 1.06 or newer, enter the following in the address bar, and then press Enter:

   `http://`*`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.

   When the login page appears, you can bookmark it so that you can quickly and easily access it the next time.

2. Log in to the Web User Interface (as described in "Logging In to the Web User Interface" on page 27).

Accessing the Web User Interface Using the Storage System Console

If you want to access the Web User Interface using the Storage System Console, you must install the Storage System Console on each computer from which you plan to manage the storage system. You can install the Storage System Console on any computer that runs one of the following operating systems:

- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows XP
- Microsoft Windows 2000 Professional, Server, or Advanced Server with Service Pack 2 or newer

To install the Storage System Console, follow the instructions in “Step Three: Install the Storage System Console” on page 16.

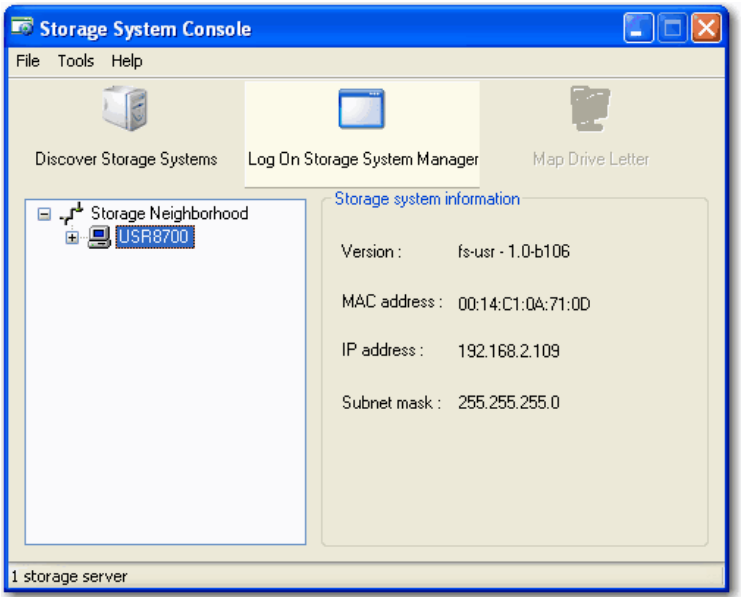
Running the Storage System Console

Once you have installed the Storage System Console, you can run it and access the Web User Interface:

1. Start the Storage System Console as follows:

   - Windows Vista or XP: click **Start** > **All Programs** > **Storage System Console**.
   - Other Windows operating systems: click **Start** > **Programs** > **Storage System Console**.

   As soon as you start the Storage System Console, it automatically scans the network for storage system servers. This might take a few minutes. As soon as the scan is complete, the left pane displays a tree view of all storage system servers discovered by the scan:



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.

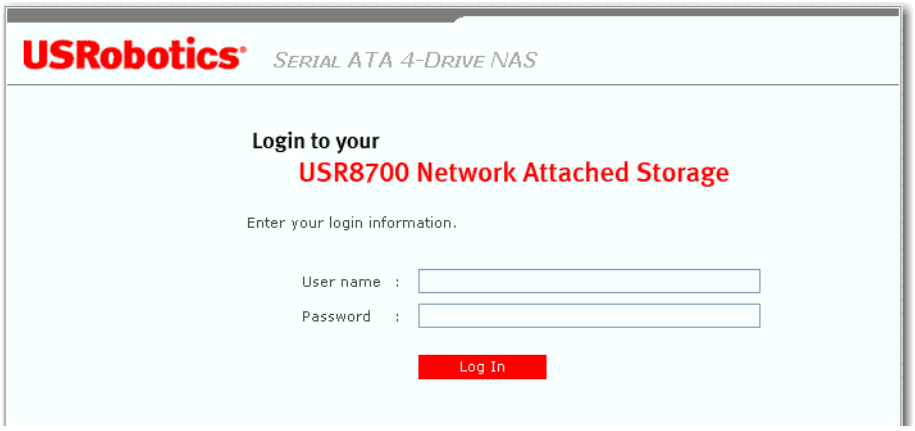
2. In the left pane, select the name of the storage system that you want to manage (for example, **Storage**), and then click **Log On Storage System Manager**.

3. If a certificate error is indicated, click **Continue to this website**.

4. Log in to the Web User Interface (as described in "Logging In to the Web User Interface" on page 27).

Logging In to the Web User Interface

Whether you access the Web User Interface using a Web browser or the Storage System Console, the login page appears. This ensures that only authorized individuals can change the storage system settings.



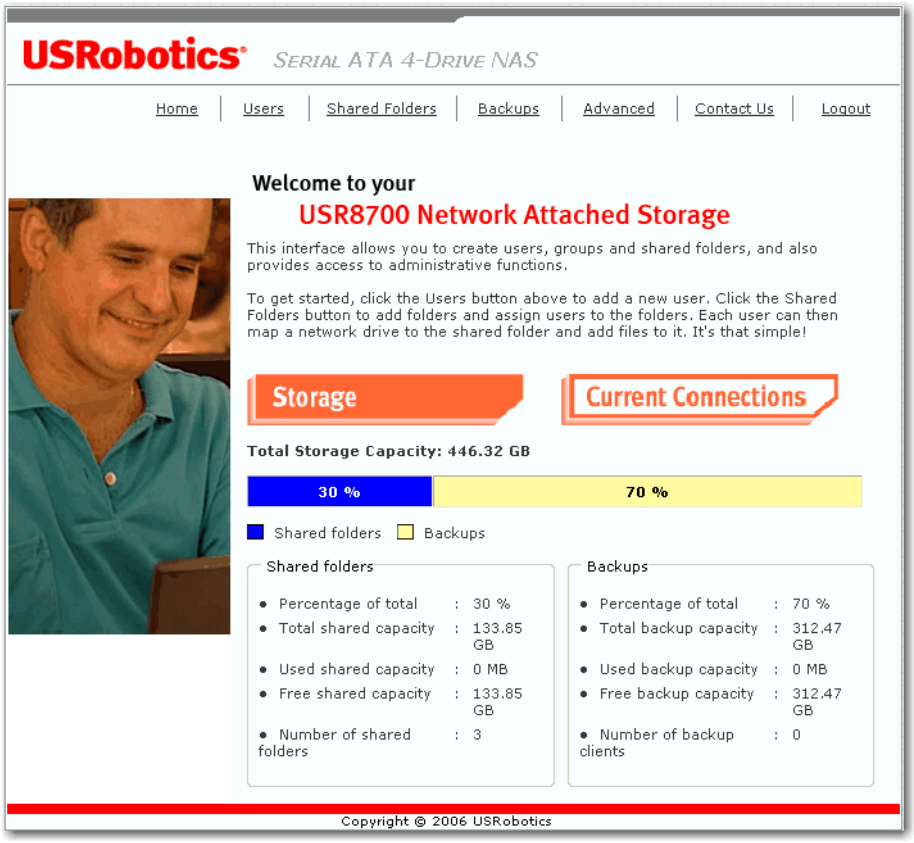
To log in, enter the administrator user name and password, and then click **Log In**.

The default administrator user name is **admin**, and the default password is **storage**. (These are case-sensitive.) However, you can change the name and password at any time. For more information, see "Changing the System Settings" on page 69.

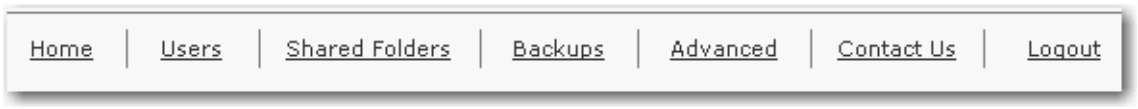
You can also change the language to use for the Web User Interface by clicking the desired language button.

Navigating the Web User Interface

Once you log in to the Web User Interface, the **Home** page appears:



The top of the **Home** page (and every page in the Web User Interface) displays a navigation bar that lets you access all the features of the storage system:



Note: Do not use the navigation bar while in the process of making changes to user, group, shared folder and system settings. Using the navigation bar before completion would cancel the process and lose the entries made in the course of that change.

- **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. (Initially, there is no used space.) This page also displays total number of shared folders and the number of networked computers (backup clients) that have backed up one or more disks on the stor-

age system.

Note: The total storage capacity will be less than the total size of all your 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.

On the **Home** page, you can also click **Current Connections**:

This displays information about Windows and Mac OS X users who are currently connected to shared folders, including which shared folder they are accessing and when they logged on.

Notes:

- If anyone accessed a shared folder using the **guest** user name (which is described in more detail in “Adding Users” on page 31), **guest** appears in the **Users** column, followed in parentheses by the computer name.
- Due to the nature of the NFS protocol, Linux and other 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.

- **Users**—Displays a list of all currently configured users. If you are using local authentication mode, you can add, modify and remove all types of users and groups of Windows and Mac OS X users. If you are using Active Directory authentication mode, you can add, modify, and remove Linux users and other Mac users. You can also use this page to change the authentication mode.

  For more information, see “Adding Users” on page 31 and “Managing Users” on page 45.

- **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.

  For more information, see “Creating Shared Folders” on page 34 and “Managing Shared Folders” on page 58.

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

  For more information, see “Managing Backups” on page 61 and Chapter , "Protecting Local Disks," beginning on page 89.

- **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.

For more information, see Chapter , "Managing Your Storage System," beginning on page 45.

- **Contact Us**—Provides information about USRobotics and the other products and services it offers.
- **Log Out**—Logs you out of the Web User Interface.

Browser-Based Web User Interface Navigation

There are various browser features that make navigation of the Web User Interface easier and faster than simply using the links provided by the interface's current page.

Note: Do not use browser-based navigation while in the process of making changes to user, group, shared folder and system settings. The effect would be the same as selecting a link in the page's navigation bar before completing the change: cancelation of the process and loss of all entries made in the course of that change.

History

Browsers maintain a history of web sites and pages visited, including the pages of the Web User Interface site. History makes navigation of the Web User Interface quick and easy. It is accessed by both Internet Explorer and Firefox with the CTRL+H key combination. A sidebar appears on the left side of the browser window, listing the browsing history by date. Select Today or a previous day. Then select the site matching what currently appears in the browser's Address bar following:

```
https://
```

If the storage system has a name registered with a DNS server on your network and that name appears in the Address bar, select the storage system's name in the history sidebar. Otherwise, select the IP address that matches what is currently displayed in the Address bar.

The history of the chosen item expands upon selection, revealing a list of pages previously visited in that site. Depending on the browser used, either the pages' titles or addresses are displayed. Selecting the appropriate title or address opens that specific page.

Back and Forward Buttons

Browsers that access the Web User Interface have Back and Forward buttons in their toolbars. These toolbar buttons are located in the upper left corner of the browser window and appear as left or right arrows. These buttons allow quick navigation between pages recently visited; earlier in history (Back button or left arrow) or after the current page's place in history (Forward button or right arrow).

For example, Alice accessed the **System Status** page and then selected the navigation bar's **Home** link. If she wanted to return to the previous page using the pages' links, she would select the navigation bar's **Advanced** link and then the **System Status** link appearing at left. Using the browser toolbar's Back and Forward buttons, she could flip back and forth between the **System Status** and **Home** pages. Even handier is remembering the key combinations of ALT+LEFT ARROW for Back and ALT+RIGHT ARROW for Forward.

Favorites or Bookmarks

If the storage system has a name registered with a DNS server on your network or uses a static IP address, Favorites (Internet Explorer) or Bookmarks (Firefox) are another browser feature you can use to naviagate between the pages of the Web User Interface. Internet Explorer and Firefox both use CTRL-D to add Favorites or Bookmarks. Refer to your browser's Help for more information.

Adding Users

Note: By default the storage system uses local authentication mode. If your site uses Active Directory, you might want to use Active Directory authentication mode instead. Since all user data and all shared folder assignments are deleted when you switch from one mode to another, it is recommended that you decide which mode you want to use before proceeding. For more information, refer to "Changing the Authentication Mode" on page 53.

In the default local authentication mode, the storage system includes a user named **guest** that has a password of **guest** (active directory authentication does not include **guest**). Windows and Mac OS X users can access all shared folders that **guest** is authorized to access. However, you might want to add other users as well. For example, if you want 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 your network provides maximum flexibility and security, enabling you to control exactly who can access what information.

In addition, only Windows and Mac OS X users can use the **guest** user name. If there are Linux users or Mac users who aren't using OS X in your network, you must add users to allow those individuals to access any shared folders. (In Active Directory authentication mode, you can add only Linux/other Mac users.)

When you add a Windows or Mac 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.)

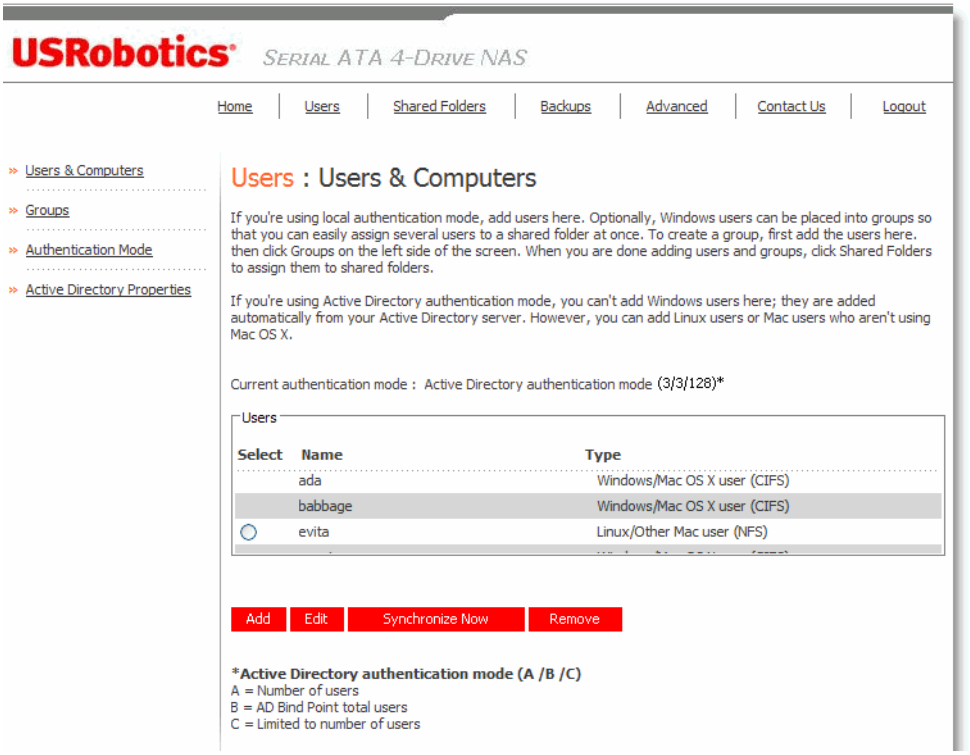
You can add up to 128 Windows or Mac OS X users, and up to 128 Linux or other Mac users (for a total of up to 256 users).

Note: Since each Linux/other Mac user can represent multiple users, the number of actual users can be higher.

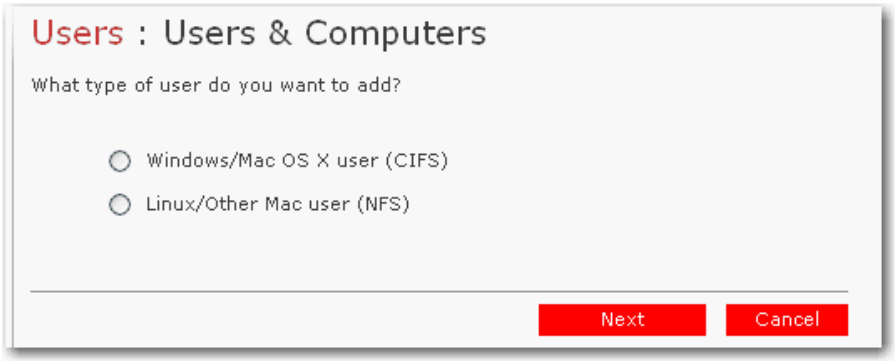
To add a user:

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

The **Users & Computers** page appears:



2. Click **Add**.



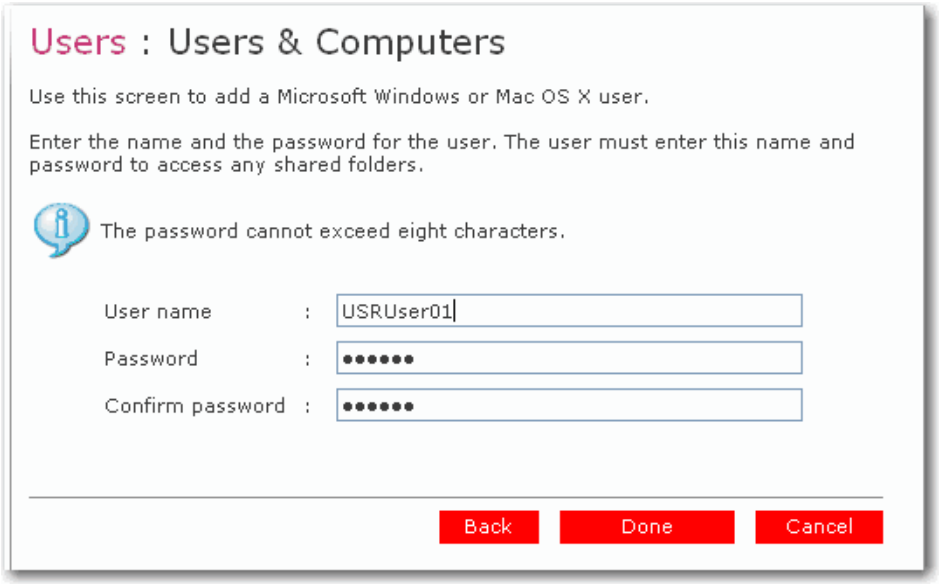
3. Select the type of user that you want to add, and then click **Next**.

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

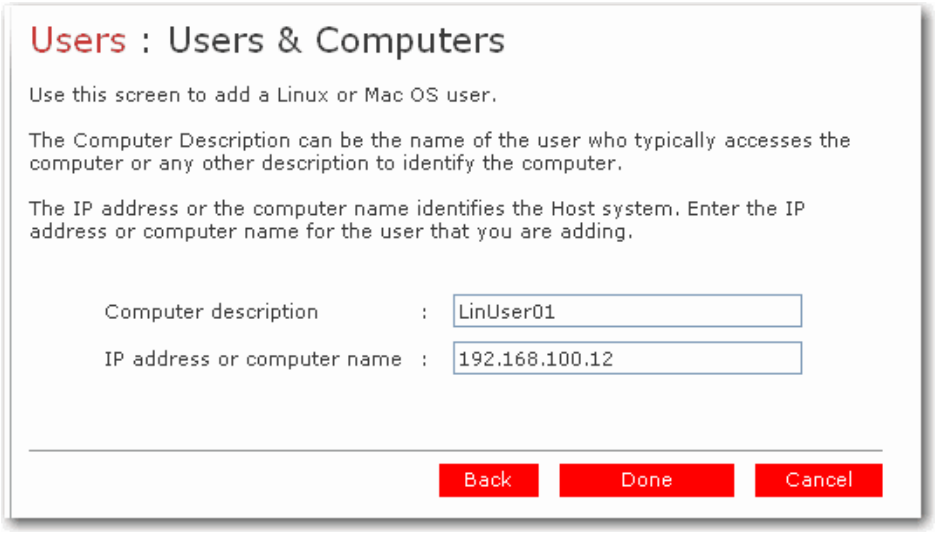
Note: Linux users and Mac users who are not using OS X access shared folders using the Network File System (NFS). In this environment, access to shared folders is given to entire computers, not to individual users of those computers. However, in Windows and Mac OS X environments, each computer user can have individual access to a shared folder.

The page that appears next varies, depending on the user type you selected.

- **Windows/Mac OS X user (CIFS)**



- **Linux/Other Mac user (NFS)**



4. Enter the requested user information and click **Done**:

For this type of user	Do this
Windows/Mac OS X user (CIFS)	Enter the user name and password for accessing the shared folders. (You must enter the password a second time to confirm it.) The user name can be up to 20 characters long and can include letters and numbers. **Note:** If the user name and password that you specify 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.
Linux/Other Mac user (NFS)	Enter a computer description and the IP address or computer name of the person's computer. The **Computer description** can be the name of the person who typically uses the computer, or any other description that you want to provide to identify the computer in **Users**. This description can be up to 15 characters long. The **IP address or computer name** is the IP address or the actual computer name in the computer's system configuration. **Note:** Note: You can create a single user that actually represents multiple computers. In **IP address or computer name**, you can use the wildcard characters * and ? to indicate a range of names. For example, `client*` or `client?` would include all computers in the subnet whose name begins with `client`. `*.company.com` would include all computers in the domain company.com. However, these wildcards cannot be used with IP addresses.

   The specified user name and type appears in the list on the **Users & Computers** page.

5. Repeat steps 2 through 4 until you have added all the users that you want to add at this time. (You can always add more users later.)

   To put Windows or Mac OS X users into groups, see "Working with Groups" on page 49.

Creating Shared Folders

In the default local authentication mode, the storage system includes a shared folder named **public**. All Windows and Mac OS X users can access it to create, modify or delete files there, unless you change the list of authorized users or their access rights (as described in "Changing User Access to Shared Folders" on page 59). In Active Directory authentication mode, you must manually assign users to this folder in order to provide them with access.

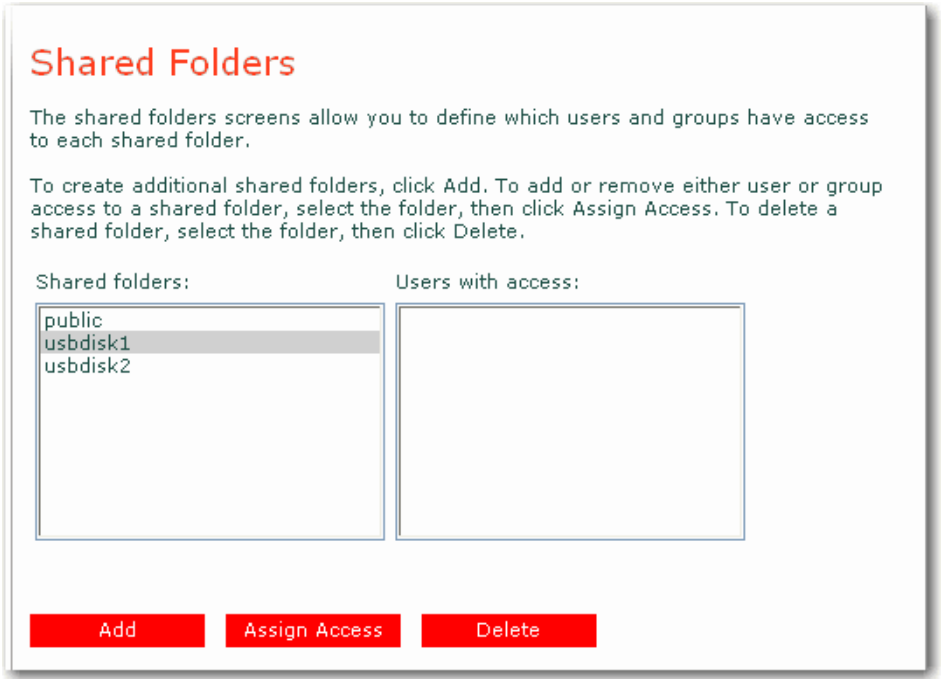
However, you might want to create other shared folders as well. For example, in an office environment, you might want to create a shared folder for company policies that everyone can only view, and separate shared folders for confidential business files that only selected individuals or departments can view or 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 Mac OS X users can access the **public** folder, you would need to create shared folders if your network includes Linux or other Mac users.

You can create up to 128 shared folders. Users who can access and write to these shared folders can create additional sub-folders for organizing the files they store there.

To create a shared folder:

1. In the navigation bar, click **Shared Folders**.

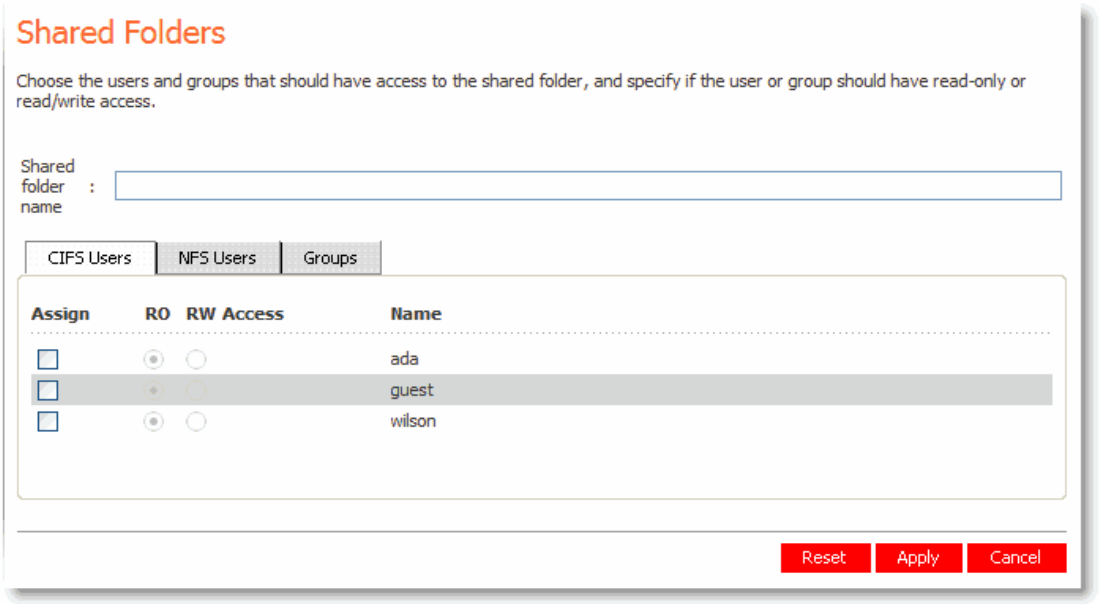
   The **Shared Folders** page appears:



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

In addition, shared folders created as the result of adding a Windows/Mac OS X user do not appear in the **Shared folders** list.

2. Click **Add**.



3. In **Shared folder name**, enter a unique name for the shared folder.

   This name can be up to 64 characters long and can contain letters, numbers, hyphens, underlines, and spaces. It cannot begin with a period or contain a double period or the following characters: **/ \ [ ] : ; | = , + * ? < > @ " ' # ~ ` % $**..

   Note: Each shared folder name must be unique. For example, if you create a shared folder named *Photos* for Windows/Mac OS X users, you cannot subsequently create a shared folder named *Photos* for Linux/other Mac users.

   In addition, the shared folder name cannot be the same as any Windows Mac OS X user name.

4. Select either **CIFS**, **NFS** or **GROUP**, assign users and select **RO** (read only) or **RW** (read/write) access for each user.

   For any shared folder or USB disk, you can specify which users can access it and what level of access they have.

5. To allow users access to the shared folder or USB disk, select those users and their access.

   Users with **RO** (read only) access can only view the files in the shared resource; users with **RW** (read/write) access can also add, modify, and delete folders and files in the shared resource.

   To cancel a user's selection, clear their check box.

   For any shared folder or USB disk, you can specify which users can access it and what level of access they have.

   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, 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).

Note: Linux users and Mac users who are not using OS X 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 Mac OS X environments, each computer user can have individual access to a shared folder.

If you created groups (as described in "Adding a Group" on page 49), you can perform this step with the **Group** tab.

The **Group** tab displays all groups. For example, if you created a group named Group1, and added User2 and User3 to that group, by default, none of them are assigned access to the shared folder.

Select Group1 and click **RO** (Read-Only). User2 and User3 are not assigned the access. This allows you to specify unique access rights for those users. You could select User3 and click **RW** (Read/Write). This would mean that everyone in Group1 would have read-only access to the shared folder except User3, who would have read/write access to it.

6. When finished, click **Apply**.

Note: You can also click **Cancel** to negate the shared folder assignments or **Reset** the current shared folder.

Accessing Shared Folders

Once you have added users and created shared folders (as described in "Adding Users" on page 31 and "Creating Shared Folders" on page 34), the users need to perform some simple steps to be able to access those folders. The procedure for doing this varies, depending on the user's operating system. Each user can access only those shared folders that the user is authorized to access.

Note: If the storage system uses Active Directory authentication mode, and the clocks of the storage system and the Active Directory server differ by more than five minutes, errors will occur when users try to access the shared folders. You must adjust the system settings of the storage system for time, time zone, or both to ensure that they match (as described in "Changing the System Settings" on page 69).

If you change the IP address of the storage system, users who accessed the shared folders using the previous IP address will be disconnected and need to repeat the procedures described below using the new IP address.

Windows Users

If you are using Windows, you have two options for accessing shared folders: you can use Windows 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.

Using the Storage System Console, you do not need to remember the server name of the storage system or its shared folders; the Storage System Console displays them automatically. However, the computer

where you install the Storage System Console must be on the same network as the storage system.

> **Note:** If your storage system uses Active Directory authentication mode (as described in "Changing the Authentication Mode" on page 53), only the **public** folder is accessible via the Storage System Console. To access all other shared folders, you must use Windows Explorer.

Using Windows

To access a shared folder using Windows:

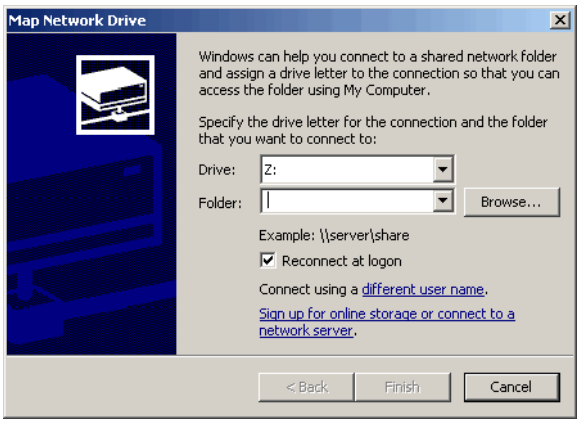
1. Windows Vista: click **Start > Computer**.

   Windows 2000: on the desktop, double-click **My Computer**.

   Other Windows operating systems: click **Start > My Computer**.

2. From the **Tools** menu, click **Map Network Drive**.

   The **Map Network Drive** dialog box appears:



   The exact appearance of this dialog box varies, depending on your operating system.

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

4. In **Folder**, 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
```

Note: You can use the storage system name if:

- Your computer is in the same subnet as the storage system.
- You added the IP address and name of the storage system to your local **hosts** file.
- You manually registered the name with a DNS server in your network.

Alternatively, you can click **Browse** and select the shared folder from the **Microsoft Windows Network**.

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

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

6. Click **Finish**.

7. 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 are not 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 Windows Explorer.

Using the Storage System Console

To access a shared folder using the Storage System Console:

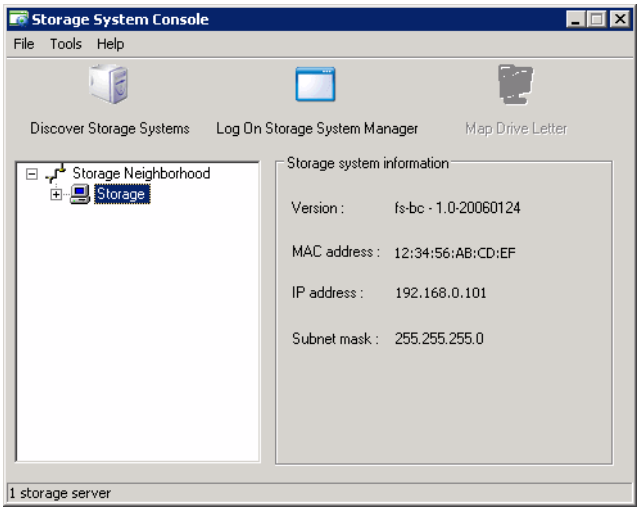
1. Install the Storage System Console (as described in “Step Three: Install the Storage System Console” on page 16).

2. Windows Vista or XP: click **Start** > **All Programs** > **Storage System Console**.

   Other Windows operating systems: click **Start** > **Programs** > **Storage System Console**.

   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 system servers it found:

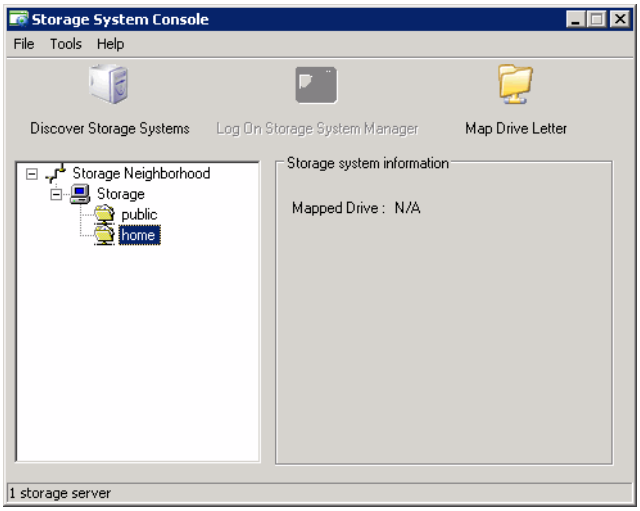


Note: If you connect a storage system to the network after the Storage System Console has already scanned it, or if you change the IP address of the storage system, you must click **Discover Storage Systems** to scan the network again and update the tree in the left pane.

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

   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:



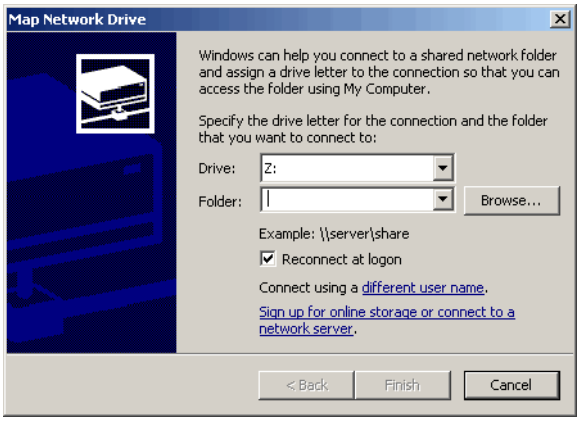
Note: All shared folders appear in the left pane. However, you can access only the ones that you are authorized to use.

If your storage system uses Active Directory authentication mode, you must manually create a **guest** user account in order to use and create shared folders.

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

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

The **Map Network Drive** dialog box appears:



The exact appearance of this dialog box varies, depending on your operating system.

5. In **Drive**, select the drive letter that you want to assign to the shared folder.

6. To automatically connect to this shared folder each time you log on to Windows, select **Reconnect at**

logon.

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 are not 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 Windows Explorer.

Linux Users

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.

Mac Users

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.)

Mac OS X

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

1. From the **Go** menu, click **Connect to Server**.
2. In **Address**, 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 server name if:

   - Your computer is in the same subnet as the storage system.
   - You added the IP address and name of the storage system to your local **hosts** file.
   - You manually registered the name with a DNS server in your network.

3. In **Select a share**, 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.

Managing Your Storage System

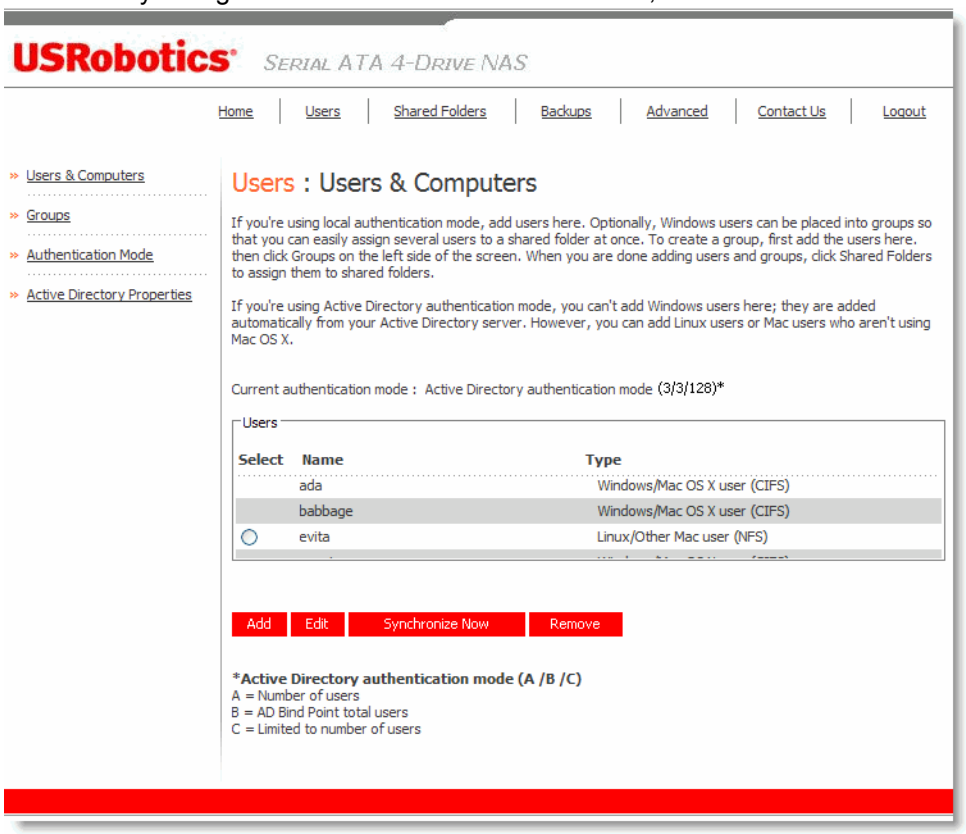
The Web User Interface lets you perform a number of tasks to help you get the most from your storage system:

- Managing Users—Add, modify or remove users, or put users into groups.
- Managing Shared Folders—Create shared folders, rename existing shared folders, change which users can access existing shared folders or their access rights, and delete shared folders that you no longer need to keep.
- Managing Backups—View which computer disks are backed up, change the password for recovering a backup, or delete a backup.
- Setting Up E-mail Alerts—Specify whether or not e-mail notifications should be sent when a problem occurs, and who should receive them.
- Upgrading the Firmware—Upgrade your storage system firmware to the latest version.
- Disconnecting USB Devices—If you are using optional USB devices, you must disconnect them using the Web User Interface before you physically unplug them.
- Changing the System Settings—Change the storage system name or time and date settings, as well as the administrator name or password for logging in to the Web User Interface.
- Changing the Network Settings—Change the workgroup name, the storage system server's IP address, the gateway or DNS server settings, or the settings that allow the storage system to act as a DHCP or FTP server.
- Reconfiguring Your Storage System Disks—Change the proportions of your storage system that are allocated to shared folders and backups, or change your disk configuration.
- Viewing System Status Information—See details about CPU and memory usage, how long the storage system has been running, disk temperatures, etc.
- Logging Out of the Web User Interface—Log out of the Web User Interface so that no one else can use your computer to make changes to the storage system.
- Shutting Down the Storage System—Shut down the storage system using the Web User Interface rather than pushing the power button on the storage system manually.

Managing Users

When you click **Users** in the navigation bar, the **Users & Computers** page appears. This page displays a

list of all currently configured Windows and Mac OS X users, as well as all Linux and other Mac computers.



Only the individuals or computers that appear on this page can access the shared folders or back up their local hard disks on the storage system. (In this guide, the term *user* refers to both individuals and computers.) You can add, modify, or remove users at any time.

The storage system uses local authentication mode by default, which means that you can add, modify, or remove all types of users at any time. If you are using Active Directory authentication mode, you can add, modify, or remove Linux or other Mac users, but not Windows and Mac OS X users. These users are controlled entirely by the Active Directory server while in Active Directory authentication mode. For that reason, there is only one editable user shown above. For more information about authentication modes, refer to “Changing the Authentication Mode” on page 53.

If you are using local authentication mode, you can also put Windows and Mac OS X users into groups. This makes it easier to give several users access to the same shared folder at once. For example, in an office environment, you might create one group for all users and give that group read-only access to a shared folder with corporate policies. You might then create separate groups for each department (such as Sales or HR) and give those groups read/write access to shared folders with information specifically for those groups (such as expense reports or company benefits). Each user can be a member of multiple groups.

If you are using Active Directory authentication mode, you cannot create groups using the Web User Interface. All groups are controlled entirely by the Active Directory server.

Adding Users

To add a user, refer to “Adding Users” on page 31.

Modifying Users

In local authentication mode, for Windows and Mac OS X users you can change the password used to access the shared folders, but not the user name. This change will not affect current connections, but will take effect the next time the person tries to connect to a shared folder. (In Active Directory authentication mode, you cannot modify Windows and Mac OS X users, only Linux and other Mac users.)

For Linux and other Mac users, you can change the IP address or computer name, but not the computer description. Changing this information immediately disconnects that computer from the shared folders.

Note: To change the user name or computer description, you must remove the existing user as described in "Removing Users" on page 48, and then add a new user with the desired name or description as described in "Adding Users" on page 31.

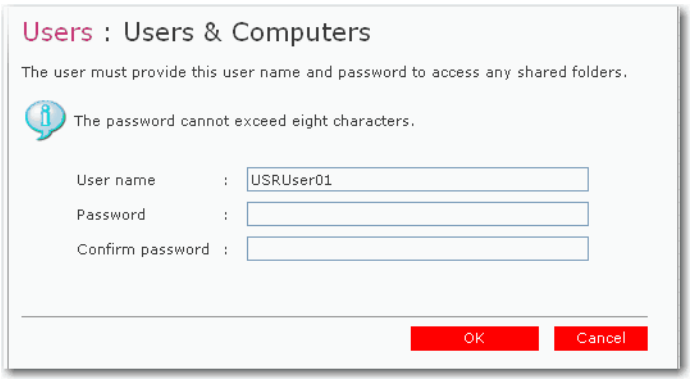
To modify a user:

1. In the navigation bar, click **Users**.
2. Select the user that you need to modify.
3. Click **Edit**.

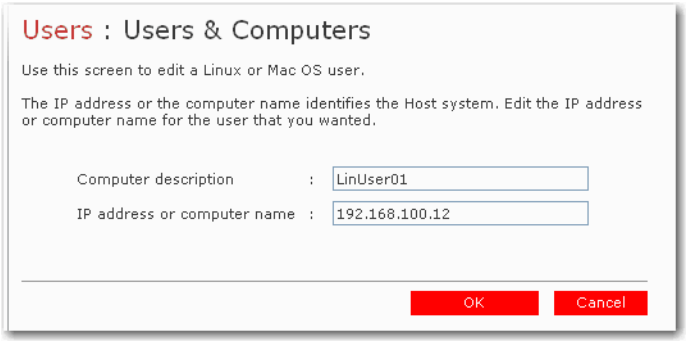
Note: If the storage system uses Active Directory authentication mode and you select a Windows or Mac OS X user, this button is dimmed.

The page that appears next varies, depending on the type of user you selected:

- **Windows/Mac OS X user (CIFS)**



- **Linux/Other Mac user (NFS)**



4. Make the desired change and click **OK**:

For this type of user	Do this
Windows/Mac OS X user (CIFS)	Enter the password for accessing the shared folders. (You must enter the password a second time to confirm it.) **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 folders.
Linux/Other Mac user (NFS)	Enter the computer's IP address or the actual computer name in the computer's system configuration. A single user can actually represent multiple computers. In **IP address or computer name**, you can use the wildcard characters * and ? to indicate a range of names. For example, `client*` or `client?` would include all computers in the subnet whose name begins with `client`. `*.company.com` would include all computers in the domain company.com. However, these wildcards cannot be used with IP addresses. **Note:** If the user is currently connected to a shared folder, changing this information will disconnect the user.

Removing Users

In local authentication mode, you can remove any user except the **guest** user. In Active Directory authentication mode, you can remove a Linux user or a Mac user not running Mac OS X, but you cannot remove Windows or Mac OS X users. Windows or Mac OS X users can be removed only on the Active Directory server.

If you remove a user who is currently connected to the storage system, that user remains connected until the user disconnects from the shared folder or shuts down the computer.

Caution: When you remove a Windows or Mac OS X user, the folder whose name matches that user name is automatically deleted. If you are removing the user simply to change the person's user name, first have the user copy any data from this folder to another location to ensure that it is not lost.

To remove a user:

1. In the navigation bar, click **Users**.
2. Select the user that you need to remove.
3. Click **Remove**.

Note: If the storage system uses Active Directory authentication mode and you select a Windows or Mac OS X user, this button is dimmed.

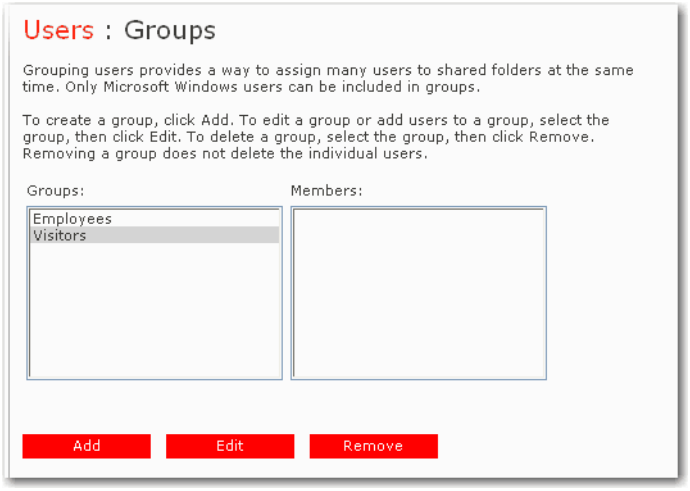
4. When prompted to confirm the removal, click **OK**.

   The user no longer appears in the list on the **Users** page.

Working with Groups

Windows and Mac 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 navigation bar and click **Groups** in the left pane, the page displays a list of all currently configured groups. When you select a group in the **Groups** list, the members of that group appear in the adjacent **Members** list.



If you are using local authentication mode, you can add a group, modify the group membership, or remove groups at any time. If you are using Active Directory authentication mode, you can view group membership but not add, modify or remove groups. Those actions can be done only on the Active Directory server.

Adding a Group

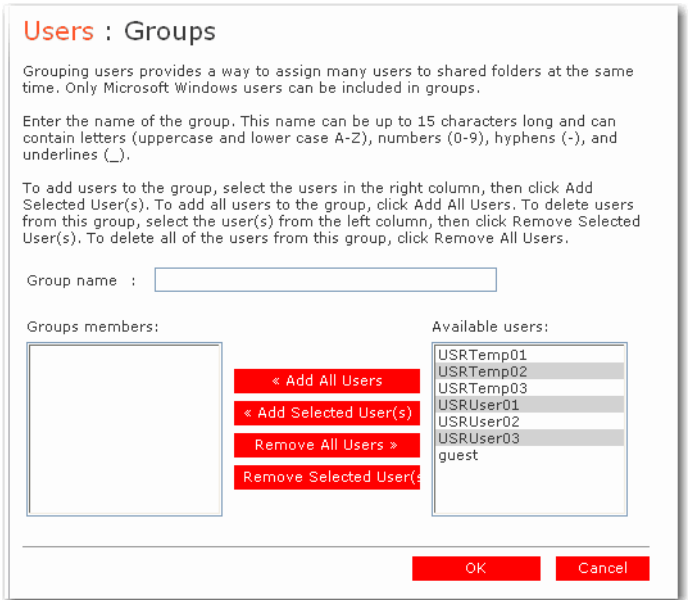
In local authentication mode, when you create a group, you typically specify which users should be members of that group, although you can create an empty group and add users later. (You must add users as described in “Adding Users” on page 31 before you can add those users to a group.)

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.

You can create up to 128 groups.

To add a group:

1. In the navigation bar, click **Users**.
2. In the left pane, click **Groups**.
3. Click **Add**.



Note: If the storage system uses Active Directory authentication mode and you select a Windows or Mac OS X user, this button is dimmed.

4. In **Group name**, enter a unique name for the group.

   This name can be up to 15 characters long and can include letters, numbers, hyphens, and underlines. It cannot begin with a period, contain spaces or a double period, or contain the following characters: / \ [ ] : ; | = , + * ? < > @ " ' # ~ ` % $

5. Specify which users should belong to this group, and then click **OK**:

To do this	Do this
Add all users to the group	Click **Add All Users**. All users move from **Available users** to **Group members**.
Add selected users to the group	In **Available users**, select the user(s) that you need to add and then click **Add Selected User(s)**.[a]
Remove all users from the group	Click **Remove All Users**. All users move from **Group members** to **Available users**.
Remove selected users from the group	In **Group members**, select the user(s) that you need to remove from the group and then click **Remove Selected User(s)**.*

a 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.

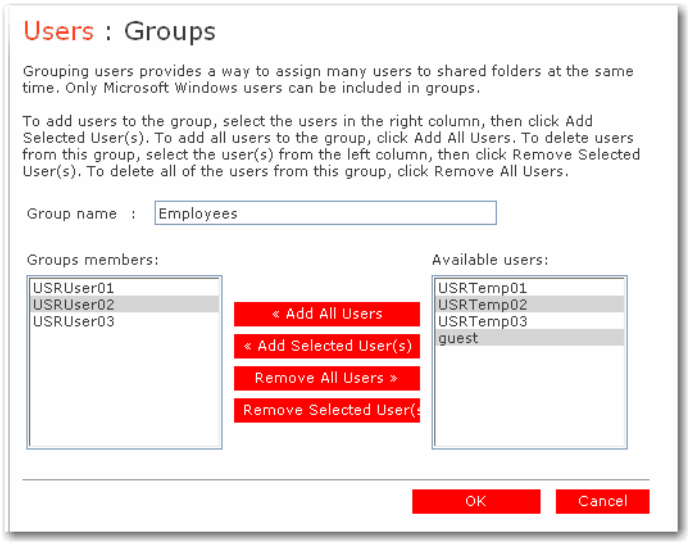
Changing the Group Membership

In local authentication mode, 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 change the group membership:

1. In the navigation bar, click **Users**.
2. In the left pane, click **Groups**.
3. In **Groups**, select the group whose membership you need to change.
4. Click **Edit**.



Note: If the storage system uses Active Directory authentication mode and you select a Windows or Mac OS X user, this button is dimmed.

5. Specify which users should belong to this group, and then click **OK**:

To do this	Do this
Add all users to the group	Click **Add All Users**.
Add selected users to the group	In **Available users**, select the user(s) that you need to add and then click **Add Selected User(s)**.[a]
Remove all users from the group	Click **Remove All Users**.
Remove selected users from the group	In **Group members**, select the user(s) that you need to remove from the group and then click **Remove Selected User(s)**.*

a 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.

The selected users move from one list to the other.

On the **Groups** page, when you select this group in the **Groups** list, the adjacent **Members** list immediately reflects the changes you just made.

Removing a 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 **Groups**, select the group that you need to remove.
4. Click **Remove**.
5. When prompted to confirm the removal, click **OK**.

The group no longer appears in **Groups**.

Changing the Authentication Mode

Your storage system can operate in one of two modes:

- Local authentication mode
- Active Directory authentication mode

In local authentication mode, the storage system authenticates all users who try to connect to shared folders, and you can add, modify, or remove all types of users. By default, the storage system uses local authentication mode.

In Active Directory authentication mode, the Active Directory server authenticates all Windows and Mac OS X users who try to connect to shared folders. You can use the Web User Interface to add, modify, or remove Linux or other Mac users, but not Windows or Mac OS X users. In addition, you cannot create groups. You must add Windows and Mac OS X users to your Active Directory server in order to provide those users with access to shared folders on the storage system. All Windows and Mac OS X users and groups are controlled entirely by the Active Directory server.

If you use Active Directory authentication mode, the **User must change password at next logon** check box must be cleared in the properties for each user on the Active Directory server who will be accessing shared folders on the storage system. In addition, each user's password can be no longer than 24 characters.

Active Directory authentication mode does not automatically include a guest user account. However, the Active Directory administrator can create one on the Active Directory server.

With Active Directory authentication mode, the clocks of the storage system and the Active Directory server must not differ by more than five minutes. Errors will occur whenever the storage system tries to connect to the Active Directory server (such as when you set the authentication mode, when synchronization between the two systems occurs, and when users access shared folders). The time settings of the storage system must match the Active Directory server, as described in "Changing the System Settings" on page 69.

Even if the storage system and Active Directory server are in the same time zone and have the same time, errors might still occur if the Active Directory server adjusts for daylight saving time. In this case, you must change both the time zone and time on the storage system. For example, if the Active Directory server time is 2:00 P.M. in the Central Time zone (GMT-06:00), you would set the storage system time zone to Eastern Time (GMT-05:00) and then set the time to match the Active Directory server (14:00). If you do this, do not synchronize the storage system with an NTP server, as the time is readjusted based on the time zone.

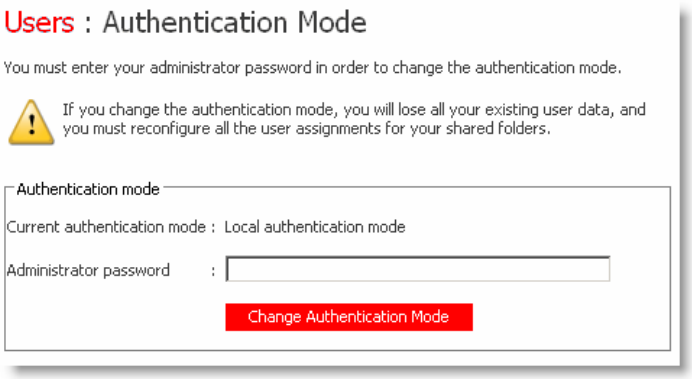
You can change the authentication mode at any time, but you must provide the administrator password of the storage system to do so.

Caution: Changing the authentication mode deletes all your existing user data and shared folder assignments. However, if any users are currently accessing shared folders, they will remain connected until they disconnect from the shared folders or shut down their computer.

To change the authentication mode:

1. In the navigation bar, click **Users**.
2. In the left pane, click **Authentication Mode**.

   The **Authentication Mode** page displays the current authentication mode.



3. In **Administrator password**, enter the password for accessing the storage system.
4. Click **Change Authentication Mode**.

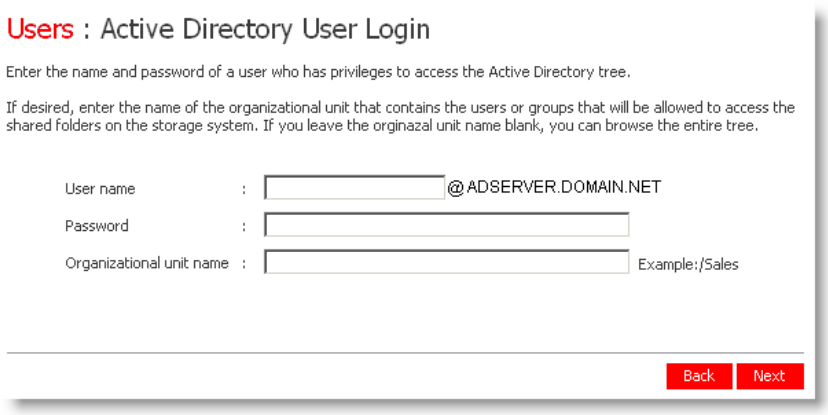
   If you are currently using local authentication mode, the **Active Directory Server** page appears.

5. In **Primary server IP address**, enter the IP address of your primary Active Directory server.
6. If desired, enter the IP address of a secondary Active Directory server in **Secondary server IP address**. This server is used if the primary Active Directory server is not available.

   The secondary server must be in the same domain as the primary server.

7. Click **Next**.

The **Active Directory User Login** page appears.



8. In **User name**, enter the name of a user who has privileges to access the Active Directory tree.

   When accessing the Active Directory server, this name is appended to the fully qualified domain name shown on this page.

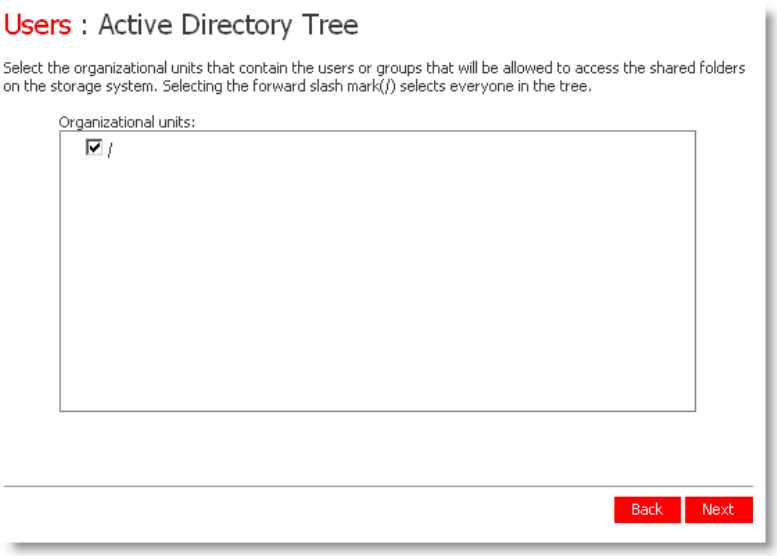
9. In **Password**, enter the password associated with the specified user name.

10. If you need to specify the name of the organizational unit that contains the users and groups that will be able to access shared folders on the storage system, enter the name in **Organizational unit name** (up to 256 characters). The unit must not have more than 100 subunits, and the name must be preceded by a slash (as in **/Sales**).

Note: The name of the organizational unit itself cannot contain a slash. For example, if the name is **Sales/Marketing**, you must specify a different organizational unit name, leave the name blank, or change the name of the organizational unit on the Active Directory server.

If you omit an organizational unit name, you can browse the **Active Directory tree** on the next page. However, if the tree has more than 100 subunits, you must specify an organizational unit name.

When you click **Next**, the **Active Directory Tree** page appears.



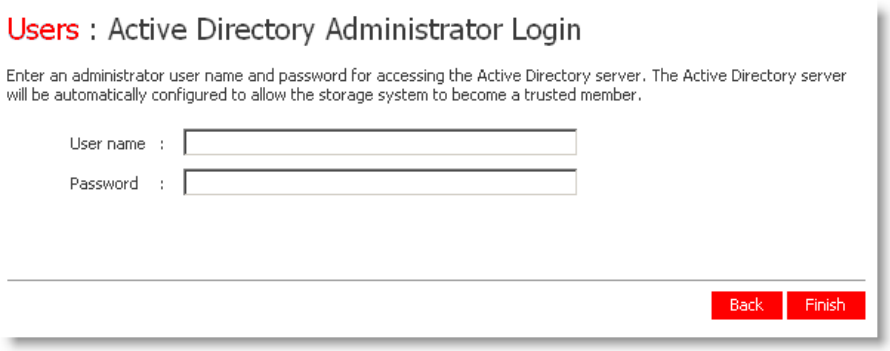
Note: If the storage system time and Active Directory server time differ by more than five minutes, an error message appears. You must adjust the storage system time, time zone, or both to ensure that they match (as described in "Changing the System Settings" on page 69).

11. Select the organizational units that contain the users or groups that will be allowed to access the shared folders on the storage system, and then click **Next**.

    You must select at least one organizational unit. Selecting the slash (/) selects everyone in the tree.

Note: Your storage system supports up to 128 users and 128 groups. If the selected organizational unit exceeds these maximums, the excess users or groups will not be added to the storage system.

The **Active Directory Administrator Login** page appears.



12. In **User name**, enter an administrator user name for accessing the Active Directory server.

    This account is used to automatically configure the Active Directory server to allow the storage system to become a trusted member and communicate directly with that server. It is used only when setting up this relationship.

13. In **Password**, enter the password associated with the specified user name, and then click **Finish**.

    All users and groups associated with the selected organizational unit are imported into the storage system and appear on the **Users & Computers** and **Groups** pages. At this point, you can assign these users and groups to shared folders (as described in "Changing User Access to Shared Folders" on page 59).

Modifying the Active Directory Properties

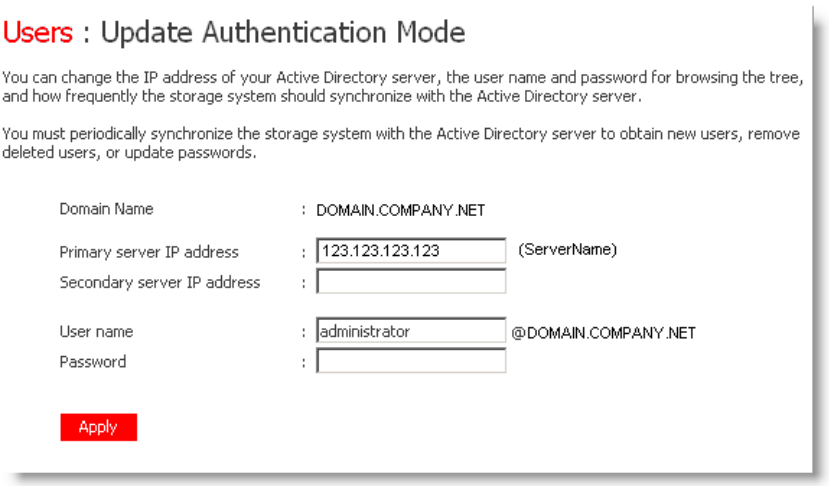
If the storage system is using Active Directory authentication mode, **Active Directory Properties** appears in the left pane when you click **Users** in the navigation bar. With **Active Directory Properties**, you can change the IP address of your primary or secondary Active Directory server, and the user name or password for browsing the Active Directory tree.

To modify the Active Directory properties:

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

2. In the left pane, click **Active Directory Properties**.

   The **Update Authentication Mode** page appears.



3. Make the desired changes, and click **Apply**.

To change this	Do this
The IP address of the primary Active Directory server	In **Primary server IP address**, enter the IP address of your primary Active Directory server. **Note:** The new server must reside in the same domain as the original server. To change domains, you must switch back to local authentication mode and then switch to Active Directory authentication mode again (as described in "Changing the Authentication Mode" on page 53).
The IP address of the secondary Active Directory server	In **Secondary server IP address**, enter the IP address of your secondary Active Directory server. (You cannot use the server's name.) **Note:** The secondary server must reside in the same domain as the primary server.

To change this	Do this
The user name or password for browsing the Active Directory tree	In **User name**, enter the name of a user who has privileges to access the Active Directory tree. In **Password**, enter the password associated with that user name. This user name and password is used to obtain new user and group information from the Active Directory server at every synchronization.

Synchronizing the Storage System and Active Directory server

By default, the storage system obtains information about users and groups from the Active Directory server every 30 minutes, and you can change this value (as described in "Modifying the Active Directory Properties" on page 57).

If you add a new user or group to the Active Directory server and do not need to wait until the next synchronization before assigning that user or group to a shared folder, you can synchronize the storage system and Active Directory server immediately. You should also do this if a user's password is changed on the Active Directory server and the user can no longer access shared folders on the storage system.

To synchronize the storage system and Active Directory server:

1. In the navigation bar, click **Users**.
2. In the left pane, select either **Users & Computers** or **Groups**.
3. Click **Synchronize**.

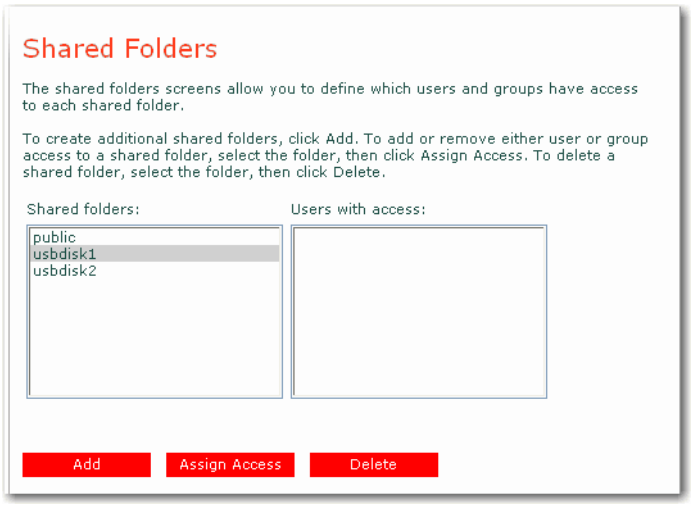
   The page displays the progress of the synchronization.

Note: If the clocks of the storage system and the Active Directory server differ by more than five minutes, errors will occur when the two systems synchronize. You must adjust the storage system time, time zone, or both to ensure that they match (as described in "Changing the System Settings" on page 69).

Managing Shared Folders

When you click **Shared Folders** in the navigation bar, the page displays a list of shared resources, including both shared folders and USB devices. When you select an item in the **Shared folders** list, the users and groups that can access that item appear in **Users with access**. (For groups, the group name is

preceded by an @ symbol.)



By default, the storage system includes a shared folder named **public**. In local authentication mode, all users are automatically assigned to this folder and can create, modify, or delete files there (unless you change the list of authorized users or their access rights as described in “Changing User Access to Shared Folders” on page 59). In Active Directory authentication mode, you must manually assign users to this folder in order to provide them with access.

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

You can create additional shared folders and delete them at any time. For both shared folders and USB disks, you can change which users have access and what they can do there.

Adding Shared Resources

To create a shared folder, refer to “Creating Shared Folders” on page 34.

Changing User Access to Shared Folders

For any shared folder that appears in **Shared folders** or any USB disk, you can change which users can access it and what level of access they have.

Note: By default, all users have read/write access to the **public** folder, but you can change their individual assignments or access rights for the **public** folder at any time.

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:

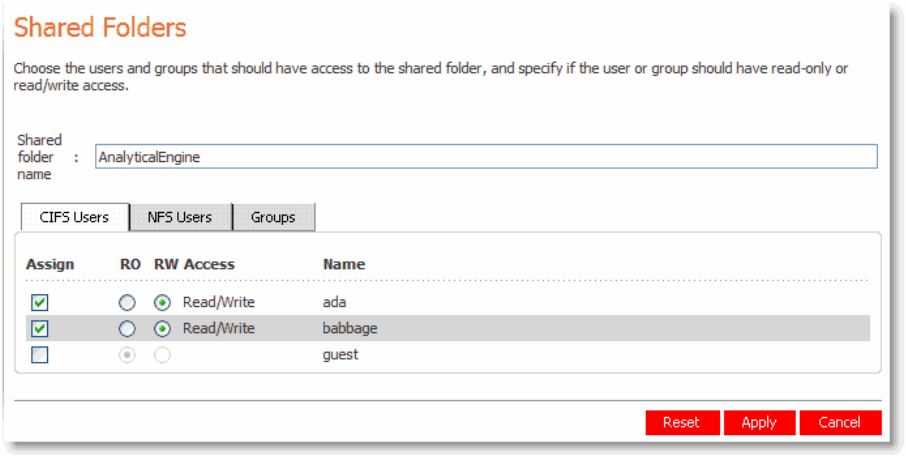
1. In the navigation bar, click **Shared Folders**.
2. In **Shared folders**, select the shared folder or USB disk whose user access you need to change.
3. Click **Assign Access**.
4. Select the tab for the type of user that you need to assign, change, or remove.

   Chose the appropriate tab based upon the user's operating system—**CIFS Users** for Windows/Mac OS X users or **NFS Users** for Linux/Other Mac users. You can assign both types of users to the same shared folder.

   Note: Linux users and Mac users who are not using OS X 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 Mac OS X environments, each computer user can have individual access to a shared folder.

   If you created groups (as described in "Adding a Group" on page 49), you can perform this step with groups as well.

5. Select the desired access settings for each user and then click **Apply**.



Deleting a 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.

Caution: Deleting a shared folder deletes *all* the subfolders and files in that shared folder. If you need to delete only selected subfolders or files, access the shared folder (as described in "Accessing Shared Folders" on page 37) and delete the desired items.

Notes:

- You cannot delete the **public** folder.
- You cannot delete the contents of a USB disk using the **Shared Folders** page. To delete its contents, you must give yourself read/write access to that disk (as described in “Changing User Access to Shared Folders” on page 59), access the disk (as described in “Accessing Shared Folders” on page 37), and then delete the desired folders and files.

  To remove the USB disk from the storage system, use the Web User Interface to disconnect it (as described in “Disconnecting USB Devices” on page 68). Then physically unplug the USB disk from the storage system.

  Even after you physically unplug the USB disk, it remains in the **Shared folders** list. This ensures that you do not need to re-assign users if you later reconnect the USB disk.

To delete a shared folder:

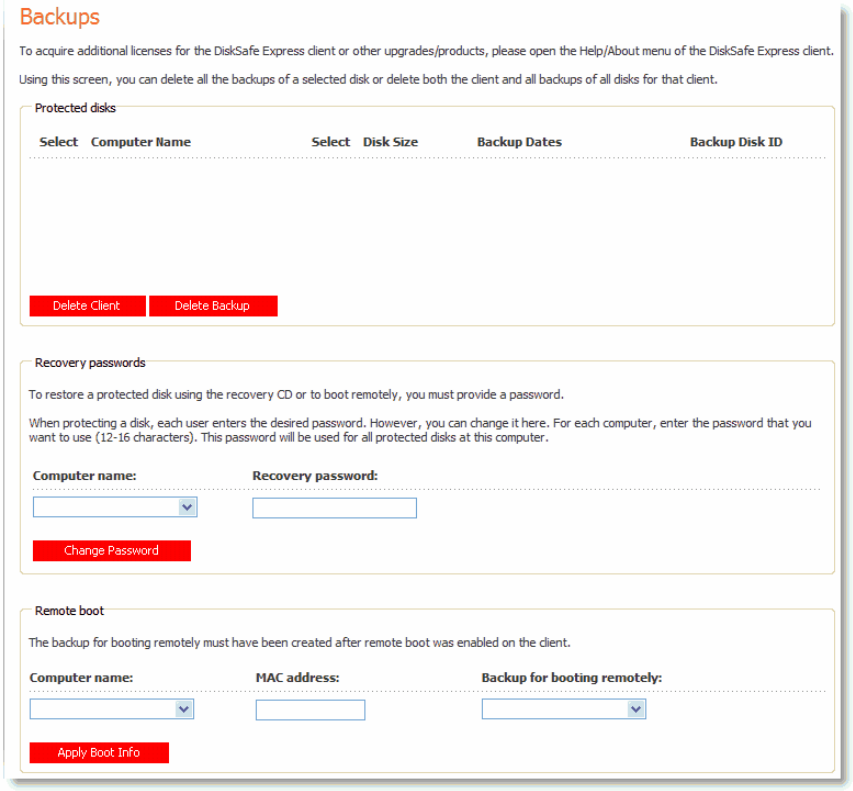
1. In the navigation bar, click **Shared Folders**.
2. In the **Shared folders** list, select the shared folder that you need to delete.
3. Click **Delete**.
4. When prompted to confirm the deletion, click **OK**.

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

Managing Backups

Once the users have used DiskSafe Express to back up their computer hard disks to the storage system (as described in "Protecting Local Disks," beginning on page 89), the **Backups** page displays a list of those users’ computers, 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).



If a user needs to recover a disk using the recovery CD or remotely boot from a backup on the storage system, the user will be prompted for a password. The user provided this password when protecting the disk. If the user forgets it, you can reset the password using the Web User Interface. (For information about recovering a disk using the recovery CD, refer to “Recovering a System Disk or Partition” on page 116. For information about booting remotely, refer to “Recovering a System Disk While Booting Remotely” on page 119.)

For booting remotely, you can also specify the MAC address to use (if you need to remotely boot a computer using a different computer’s backup) and the backup to boot from.

In addition, 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 you can delete those backups manually using the Web User Interface.

Changing the Recovery Password

To change the recovery password:

1. In the navigation bar, click **Backups**.

2. In **Computer name** within **Recovery passwords**, select the name of the computer whose recovery password you need to change.

3. In **Recovery password**, type the password to use.

   This password must be 12–16 characters long. It cannot contain multi-byte words. This means that you

can only enter ASCII characters whose code values are less than 128.

4. Click **Change Password**.

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

   The user must provide this password when recovering a disk from this storage system using the recovery CD or when remotely booting from a backup on the storage system.

Configuring Remote Boot

Normally, when you enable remote boot for a client computer (as described in "Enabling Remote Boot" on page 110), no additional action is necessary on the storage system. However, if you need to remotely boot one computer from another computer's backup, you must change the MAC address associated with the other computer's backup to that computer's MAC address. For example, if Computer1 has been infected by a virus, and all of its backups are also infected, you might need to boot Computer1 from one of Computer2's backups and recover that disk to Computer1. To do this, you must change the MAC address associated with Computer2 to Computer1's MAC address.

Note: If you try to recover one computer from another computer's backup, both computers must have identical hardware. Otherwise, the recovered files will not operate properly.

You can remotely boot only from backups that were created after remote boot was enabled on the client computer.

You can also specify which backup to remotely boot from. By default, you always boot from the latest backup. (You can boot from an earlier backup, but no matter which backup you boot from, you can recover only the latest backup.)

To configure remote boot:

1. In the navigation bar, click **Backups**.

2. In **Computer name** within **Remote boot**, select the name of the computer whose backup you need to remotely boot from.

3. If you are remotely booting the computer from its own backup, do not change the **MAC address**. However, if you are booting a different computer from the selected computer's backup, enter the MAC address of the NIC of the computer that you need to remotely boot in **MAC address**.

4. From **Backup for booting remotely**, select the time and date of the backup that you need to remotely boot from.

   To always boot from the most recent backup, select **Latest backup**.

   An asterisk (*) identifies the backup that will be used for booting remotely.

Note: If the selected backup is deleted to make room for newer backups, the most recent backup will be used for booting remotely if created after remote boot was enabled on the client computer.

5. Click **Apply Boot Info**.

6. When the confirmation message appears, click **OK**.

   If you changed the backup for booting remotely, an asterisk appears next to the selected backup.

Deleting a Backup

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 need 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. In the navigation bar, click **Backups**.

2. Select the disk whose backups you need to delete (in the second **Select** column).

3. Click **Delete Backup**.

4. When prompted to confirm the deletion, click **OK**.

   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. For more information, refer to "Removing Protection" on page 122 and "Protecting Your Disks" on page 98.

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.

To delete a client:

1. In the navigation bar, click **Backups**.

2. Select the computer whose backups and computer name you need to delete from the storage system (in the first **Select** column).

3. Click **Delete Client**.

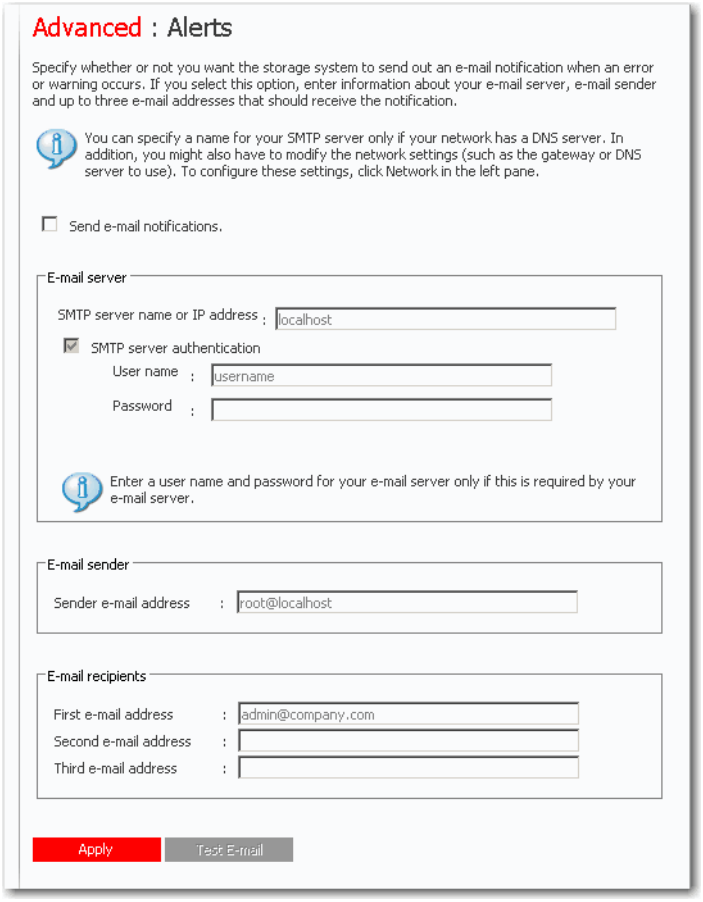
4. When prompted to confirm the deletion, click **OK**.

   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. For more information, refer to "Removing Protection" on page 122 and "Protecting Your Disks" on page 98.

Setting Up E-mail Alerts

The **Alerts** page allows you to set up the storage system to notify up to three people via e-mail 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.

To set up e-mail alerts:

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

2. Specify whether or not the storage system should send e-mail notifications when a problem occurs by selecting or clearing **Send e-mail notifications**.

   If you select this option, you must provide the fully qualified domain name or IP address of your e-mail server and at least one e-mail address.

   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 e-mail notifications later. If you clear this option, you do not need to complete the rest of this procedure; simply click **Apply**.

3. In **SMTP server name or IP address**, enter the fully qualified domain name or IP address of your e-mail server.

4. Specify whether or not your e-mail server requires authentication by selecting or clearing **SMTP server authentication**.

   If you select this option, you must enter a user name and password for logging into that server in **User name** and **Password**.

   If you clear this option, no authentication will be performed.

5. If your e-mail server cannot use the default sender e-mail address (root@localhost), or if you need the individuals who receive e-mail notifications to be able to reply to the alert, enter the address that you need to appear as the return address in **Sender e-mail address**.

   For example, you could enter your own e-mail address (such as MyName@MyCompany.com).

6. In **First e-mail address**, enter the e-mail address of an individual who should receive e-mail notifications when a problem occurs.

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

7. If you need e-mail notifications to be sent to other individuals as well, enter the appropriate e-mail addresses in **Second e-mail address** and **Third e-mail address**.

8. Click **Apply**.

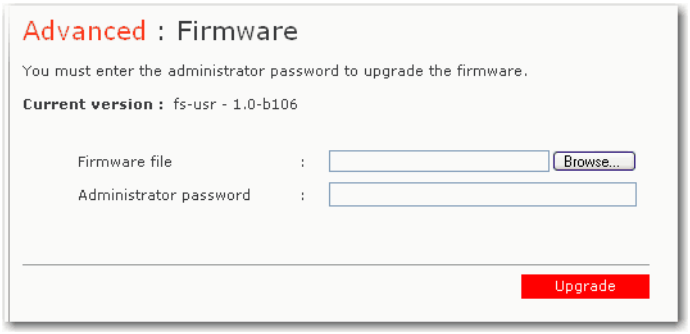
9. When the confirmation message appears, click **OK**.

10. To confirm that the configuration is correct, click **Test E-mail**, and click **OK** on the confirmation message.

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 need to modify the network settings (such as the gateway to use). For information about changing the network settings, refer to "Changing the Network Settings" on page 72.

Upgrading the Firmware

The **Firmware** page displays the current version of the firmware that is installed on your storage system. It also allows you to upgrade whenever newer firmware becomes available.



For additional security, you must enter your administrator password in order to upgrade the firmware.

Caution: When you upgrade the firmware, the storage system restarts, and access to the Web User Interface is temporarily interrupted. In addition, 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 system 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 need 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 recovery is not occurring.

If you upgrade from version 1.0, the personal folders (the **home** folders) that were automatically created for each Windows or Mac OS X user will be deleted. To retain the data in those folders, you must copy it to another location before upgrading the firmware.

To upgrade the firmware:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Firmware**.
3. In **Firmware file**, enter the path and file name for the firmware package (such as **`D:\fs-usr-1.2-b609.pkg`**), or click **Browse** to find and select the file from the displayed list.
4. In **Administrator password**, enter the password that you use for logging in to the Web User Interface.

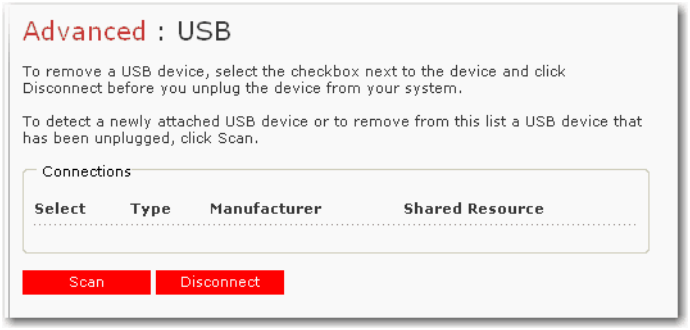
5. Click **Upgrade**.

6. If you are upgrading from version 1.0 or 1.1, click **Continue** to delete all **home** folders and proceed with the upgrade.

7. When the confirmation message appears, click **OK**.

Disconnecting USB Devices

The **USB** page 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.)



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

To disconnect a USB device:

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

2. In the left pane, click **USB**.

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

4. Click **Disconnect**.

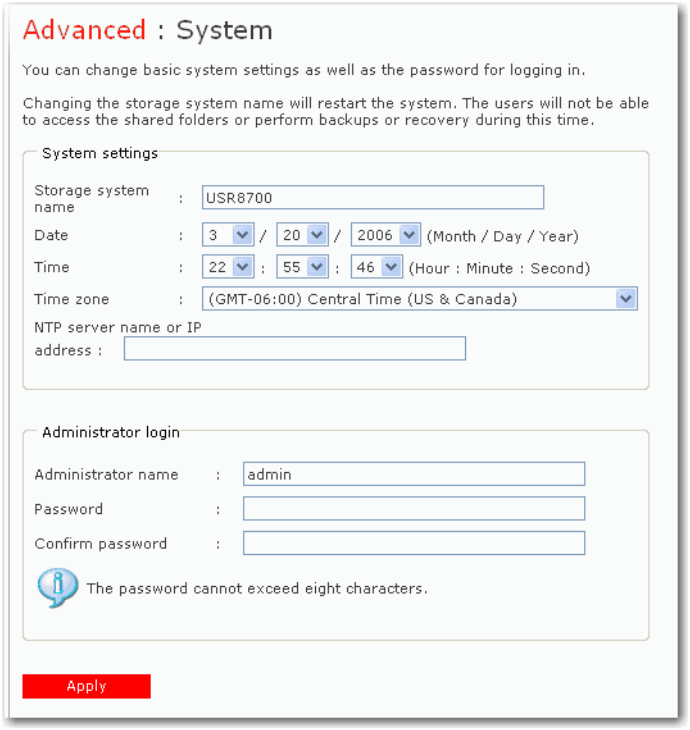
5. When the confirmation message appears, click **OK**.

   You can now unplug the USB device.

> **Note:** If you inadvertently disconnect a USB device that you need 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.

Changing the System Settings

The **System** page 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. You can also change the administrator name and password used for logging into the Web User Interface.



In local authentication mode, you can change any of these settings at any time. In Active Directory

authentication mode, you cannot change the storage system name.

Note: If you change the name of the storage system, be sure to also change that name in any local hosts files or on the DNS server in your network. The storage system does not register its name with your DNS server automatically.

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 (as described in "Disconnecting from Shared Folders" on page 136) and then access the shared folders again using the new name (as described in "Accessing Shared Folders" on page 37).

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 (as described in "Removing Protection" on page 122) and protect their disks again (as described in "Protecting Your Disks" on page 98), using the new name.

Using the **System** page, you can also change the administrator password to use for logging in to the Web User Interface.

To change any of the system settings:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **System**.
3. Make the desired changes:

To change this	Do this
The storage system name	In **Storage system name**, enter the new name to use for the storage system. This name can be up to 15 characters long and can include letters, numbers, and hyphens. **Note:** If you change the name of the storage system, be sure to also change that name in any local hosts files or on the DNS server in your network. The storage system does not register its name with your DNS server automatically. In Active Directory authentication mode, you cannot change the storage system name.

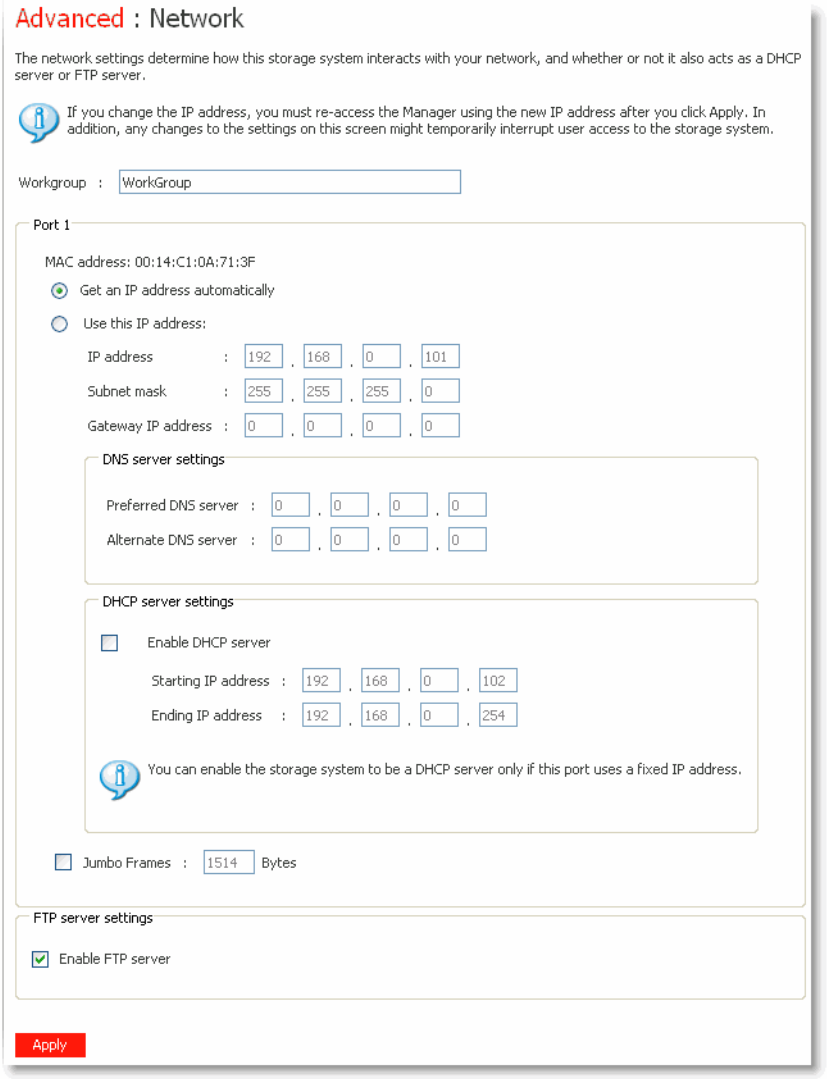
To change this	Do this
The system date, time, or time zone	In **Date**, enter or select the desired month, date, and year. In **Time**, enter or select the desired hour, minute, and second. In **Time zone**, select the desired time zone. **Note:** The storage system time does not automatically change to reflect daylight saving time. Even if the storage system and Active Directory server are in the same time zone and have the same time, errors might occur if the Active Directory server adjusts for daylight saving time. In this case, you must change both the time zone and time on the storage system. For example, if the Active Directory server time is 2:00 P.M. in the Central Time zone (GMT-06:00), you would set the storage system time zone to Eastern Time (GMT-05:00) and then set the time to match the Active Directory server (14:00). If you do this, do not synchronize the storage system with an NTP server, as the time is readjusted based on the time zone.
NTP server name or IP address	In **NTP server name or IP address**, enter the name or IP address of the Network Time Protocol server from which the storage system should set its time. You can use a name only if it is resolvable. The storage system will synchronize its time with the NTP server every hour.
The administrator name or password	In **Administrator name**, enter the user name to use for logging in to the Web User Interface. In **Password** and **Confirm password**, enter the password to use for logging in to the Web User Interface. It cannot contain multi-byte words. This means that you can only enter ASCII characters whose code values are less than 128. The user name and password are case-sensitive. To reset the password to its factory default: 1. If the storage system is running, shut it down by pressing the power button unit for approximately 5 seconds. 2. After the storage unit has shut down, press and hold the power button until the power LED comes on, and then release the button. 3. As soon as the LEDs for all of your disks have come on, press and hold the power button for 2 seconds, and then release the button. The default login administrator name is **admin**. The defalut login password is **`storage`**.

4. Click **Apply**.

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

Changing the Network Settings

The **Network** page displays the network settings that were set when you initially configured the storage system.



You can change these settings at any time.

Note: Changing the IP address or subnet mask can have several effects:

- Access to the Web User Interface will be temporarily disrupted. If you access the Web User Interface using the Storage System Console or using the IP address of the storage system, you will need to access it again using the new IP address. In addition, if previously you added the IP address of the storage system to a local **hosts** file or DNS server, you must update the IP address in those resources.
- Users who accessed the shared folders using the previous IP address will be disconnected and must access them again using the new IP address (as described in "Accessing Shared Folders" on page 37).
- Users who backed up their disks to the storage system using the previous IP address must remove protection for all affected disks (as described in "Removing Protection" on page 122) and protect their disks again (as described in "Protecting Your Disks" on page 98), 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 need 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.

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 or Mac OS X users to 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 (as described in "Adding Users" on page 31). For more information, refer to "Accessing the Storage System through FTP and SSH" on page 85.

To change any of the network settings:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Network**.
3. Make the desired changes:

To change this	Do this
The workgroup to which the storage system belongs	In **Workgroup name**, enter the name of the workgroup. This name can be up to 15 characters long.
The IP address used by the storage system	In the **Port 1** group box, either select **Get an IP address automatically** to obtain the IP address from your DHCP server, or select **Use this IP address** and enter the IP address and subnet mask in the subsequent text boxes. If you select **Get an IP address automatically** and your network does not have a DHCP server, or if the storage system is directly attached to your computer, the default IP address and subnet mask are used. (The default IP address is 192.168.0.101, and the default subnet mask is 255.255.255.0).

To change this	Do this
The IP address of the gateway	If your network includes a gateway, and if the storage system uses a specified IP address rather than obtaining one from the DHCP server, enter the IP address of the default router in **Gateway IP address**. If your network does not include a gateway, leave these text boxes blank. (If the storage system obtains its IP address from a DHCP server, the gateway will obtain its IP address from the DHCP server as well.)
The DNS server to use	If your network includes a DNS server, and the storage system uses a specified IP address rather than obtaining one from the DHCP server, enter the primary IP address in **Preferred DNS server** and the secondary IP address in **Alternate DNS server**. If your network does not include a DNS server, or if the storage system obtains its IP address from the DHCP server, leave these text boxes blank. (If the storage system obtains its IP address from a DHCP server, the DNS server IP address is obtained from the DHCP server as well.)
The DHCP settings	If you need to use the storage system as a DHCP server, in the **Port 1** group box, select **Use this IP address** and enter the IP address and subnet mask in the subsequent text boxes. Then select **Enable DHCP server**, enter the beginning IP address in **Starting IP address**, and enter the last IP address in **Ending IP address**. For example, if the **Starting IP address** is 192.168.0.103 and the **Ending IP address** is 192.168.0.107, the storage system will allocate the IP addresses 192.168.0.103, 192.168.0.104, 192.168.0.105, 192.168.0.106, and 192.168.0.107 to the first five computers that try to obtain their IP addresses from the storage system. As soon as one of those computers shuts down or otherwise loses its network connection, that IP address will be assigned to the next computer that tries to obtain its IP address from the storage system. If you do not need to use the storage system as a DHCP server, clear the **Enable DHCP server** check box. (If **Get an IP address automatically** is selected, you cannot use the storage system as a DHCP server.)
The packet size for transferring data	Specify whether or not to transfer larger data packets between the storage system and the computers in your network by selecting or clearing **Jumbo Frames**. If you clear **Jumbo Frames**, the storage system will use ordinary 1514-byte packets. If you select **Jumbo Frames**, you can specify a larger packet size (from 1514 up to 9014 bytes). **Note:** Using **Jumbo Frames** allows you to transfer data more quickly. However, you can select this option only if your network, Ethernet switch, and the network interface cards (NICs) on the computers in your network support the specified packet size. To determine whether you can use jumbo frames, refer to the documentation for those components.

To change this	Do this
The FTP settings	If you need to use the storage system as an FTP server, select the **Enable FTP server** check box. If you do not need to use the storage system as an FTP server, clear this option. For information about accessing the storage system using FTP, refer to "Accessing the Storage System through FTP and SSH" on page 85.

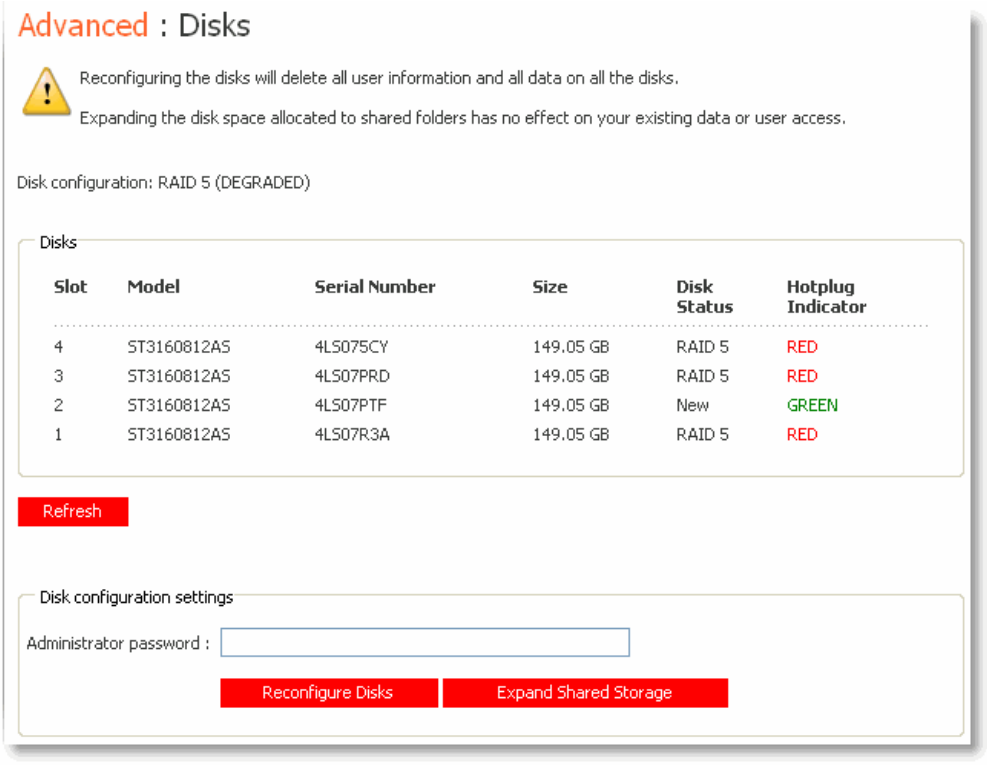
4. Click **Apply**.

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

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

Reconfiguring Your Storage System Disks

The **Disks** page displays information about all the hard disks that are currently installed in your storage system:



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:
  - **Normal**—All the disks are working properly.
  - **Degraded**—One or more disks have failed but all the data is still available.
  - **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:
  - **RAID *n***—The disk is working properly as part of the specified RAID level.
  - **New**—The disk has been added to the storage system but is not part of a RAID.
  - **Spare**—The disk is acting as a spare disk for the RAID.
  - **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:

Caution: If the hotplug indicator for a disk is red or yellow, removing the disk will result in a loss of data. To avoid such loss, remove a disk only if its hotplug indicator is green

  - **RED**—Removing the disk will cause the RAID to fail.
  - **YELLOW**—Removing the disk will cause RAID degradation.
  - **GREEN**—Removing the disk will not affect the RAID.

Note: Whenever you add or remove a disk from the storage system, you must click **Refresh** to update this page.

For detailed information about RAIDs and how adding, removing, or swapping disks affects the storage system, refer to "Disk Configurations," beginning on page 125.

Expanding the shared storage

The disk space on your storage system is divided into two portions. One portion is for shared folders; the other is for backups of your computer disks. The **Storage Status** view on the **Home** page shows how much disk space is currently allocated for shared folders, how much is used by backups, and how much is available for either.

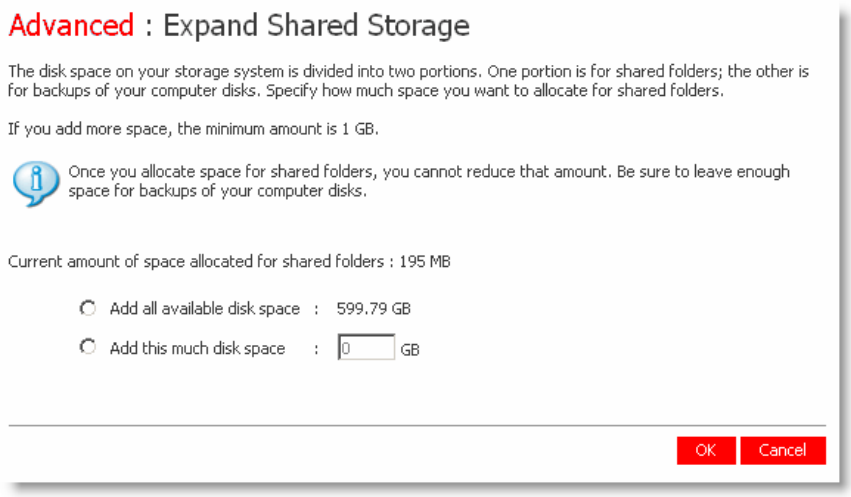
You can expand the amount of disk space allocated for shared folders (as long as free disk space is available), but you cannot reduce it without reconfiguring your disks and losing all of your data. Therefore, allocate the least amount of space for shared folders until all the computer disks that you plan to protect

have been backed up to the storage system.

To expand the amount of disk space allocated for shared folders:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Disks**.
3. In **Administrator password**, enter your password for logging in to the Web User Interface.
4. Click **Expand Shared Storage**.

   The **Expand Shared Storage** page appears:



5. Specify how much disk space to add to the space that is currently allocated for shared folders.

   To allocate all available disk space, select **Add all available disk space**.

   To allocate a specific amount, select **Add this much disk space** and enter the desired number of gigabytes. The minimum is 1 GB, and the maximum is the total amount of space currently available. You can specify only whole numbers.

6. Click **OK**.
7. When the confirmation message appears, click **OK**.

Reconfiguring the Disks

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.

Caution: Changing the disk configuration or percentage to allocate for shared folders will delete all user information and all data on all the disks.

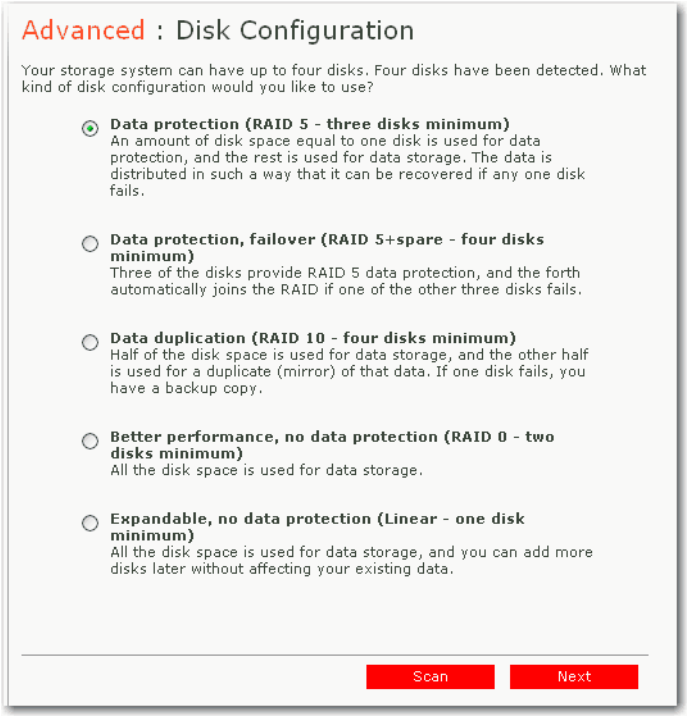
Before you change these settings, have all the users disconnect from all shared folders (as described in "Disconnecting from Shared Folders" on page 136) and remove protection from all disks (as described in "Removing Protection" on page 122).

When you are done, you must re-add all users (as described in "Adding Users" on page 31), create new shared folders (as described in "Creating Shared Folders" on page 34), and have all users once again access the shared folders (as described in "Accessing Shared Folders" on page 37) and protect their disks (as described in "Protecting Your Disks" on page 98).

To change the disk configuration or storage space allocation:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Disks**.
3. In **Administrator password**, enter your password for logging in to the Web User Interface.
4. Click **Reconfigure Disks**.
5. When the confirmation message appears, click **OK**.

   The **Disk Configuration** page appears. The options that appear on this page vary, depending on the number of hard disks that are currently installed in the system.



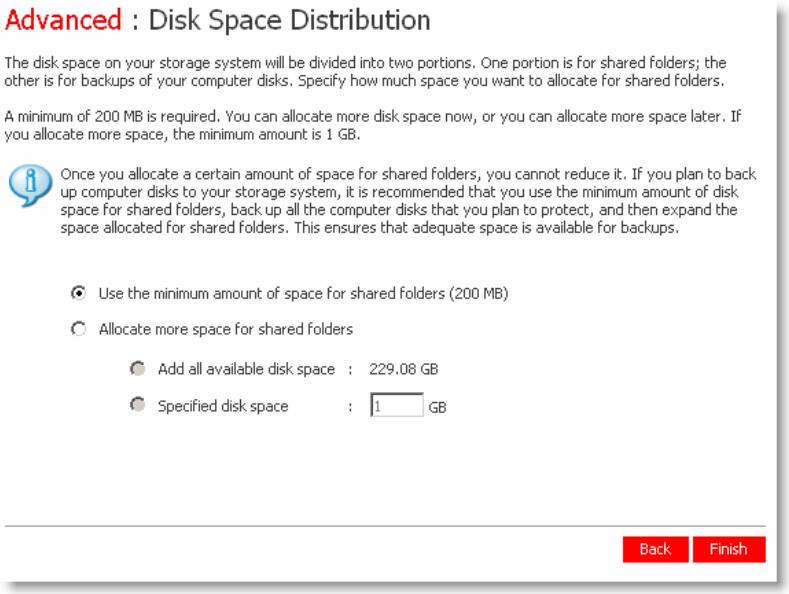
6. If you need to add or remove hard disks, do so one at a time and click **Scan** after each action. If you

are adding disks, wait until the disk LED is blue before you click **Scan**.

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.

If you need to change the disk configuration, select the desired RAID level and then click **Next**. (For detailed information about the different RAID levels, refer to "Disk Configurations," beginning on page 125.)

The **Disk Space Distribution** page appears:



7. To accept how the disk space will be proportioned for shared folders and backups (only 200 MB will be allocated for shared folders), click **Finish**.

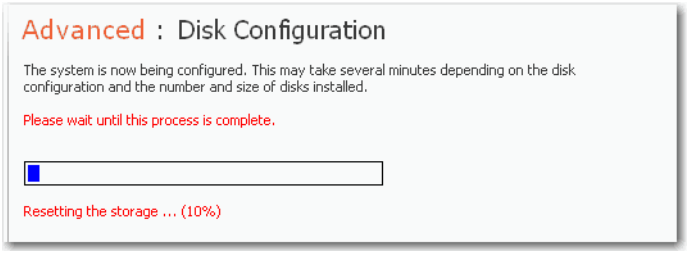
   To allocate more space for shared folders, select **Allocate more space for shared folders** and then specify how much space to allocate (either **All available disk space** or **Specified disk space**). If you select **Specified disk space**, enter the number of gigabytes to allocate for shared folders (the minimum is 1 GB). Then click **Finish**.

   Note: You can expand the amount of disk space allocated for shared folders later (as long as free disk space is available), but you cannot reduce it without reconfiguring your disks and losing all of your data.

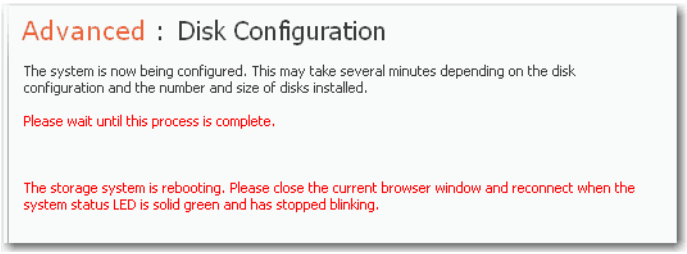
   If you plan to back up computer disks to your storage system, it is recommended that you use the minimum amount of space for shared folders, back up all the computer disks that you plan to protect, and then expand the space allocated for shared folders. This ensures that adequate space is available for backups.

8. When the confirmation message appears, click **OK**.

The screen displays the progress of the process:



When this process is complete, the storage system restarts.



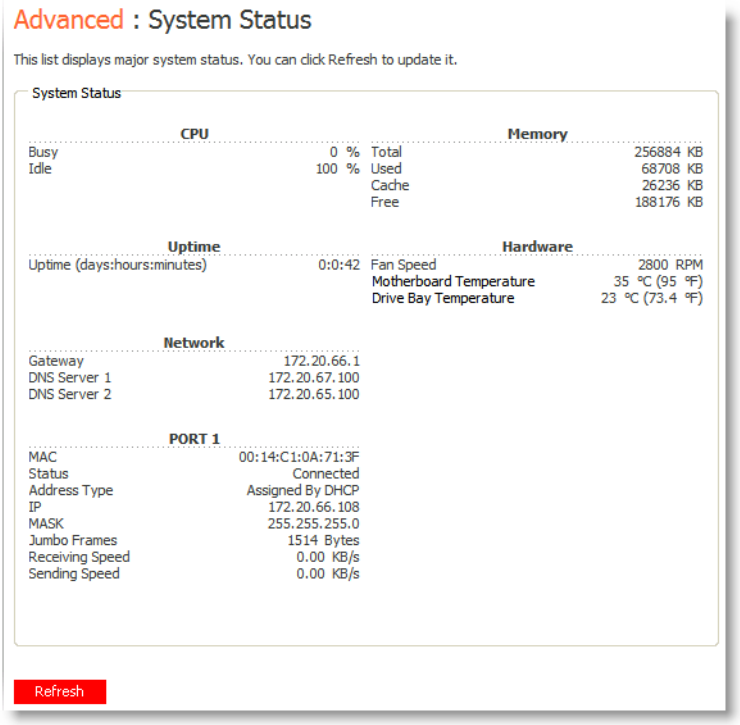
9. Close the browser window.

   After the system has restarted, you can access the Web User Interface and re-create your users and shared folders (as described in "Adding Users" on page 31 and "Creating Shared Folders" on page 34).

Viewing System Status Information

When you click **Advanced** in the navigation bar and click **System Status** in the left pane, you can view many of the operational parameters of your storage system, including CPU usage, memory usage, the amount of time that the storage system has been running, the current fan speed, the temperatures of the CPU and disks, the IP address of the gateway (which you can change as described in "Changing the Network Settings" on page 72), the IP address(es) of the DNS servers in your network, the network settings of your ports (several of which you can change as described in "Changing the Network Settings" on page 72), the MAC addresses of your ports, and the speed at which data is being sent and received.

To update the information on this page, click **Refresh**.



Note: The fan speed changes depending on the temperature of the unit. If the temperature of the motherboard reaches or exceeds 85° C (185° F), or if the temperature of the drive bay reaches or exceeds 55° C (131° F), the storage system shuts down automatically.

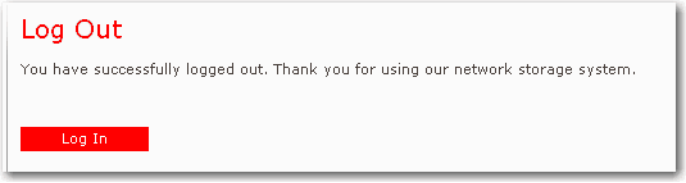
Logging Out of the Web User Interface

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

To log out:

1. In the navigation bar, click **Log Out**.
2. When the confirmation message appears, click **OK**.

   The **Log Out** page appears:



3. To log back in to the Web User Interface later, click **Log In**.

Shutting Down the Storage System

To shut down the storage system, you use the power button on the unit itself, or you can shut the system down remotely using the Web User Interface.

Shutdown by Using the Power Button

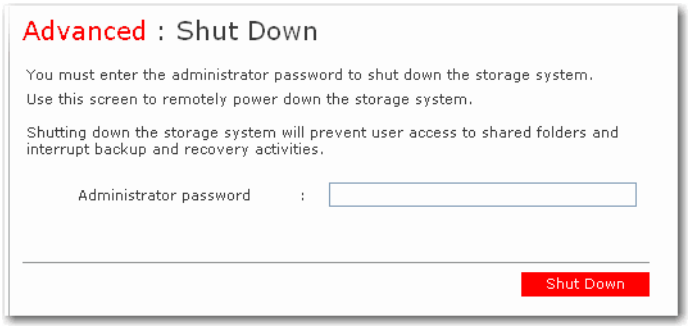
For a gradual shutdown (recommended), press and release the power button quickly.

For an immediate shutdown (not recommended), press and hold the power button until the LEDs turn off. This takes about four or five seconds.

Caution: An immediate shutdown can damage either the hard drive or the hard drive's file structure.

Shutdown through the Web User Interface

To ensure that you do not shut down the system accidentally, you must enter your administrator password to do this.



Caution: 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 system 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 need 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 Web User Interface:

1. In the navigation bar, click **Advanced**.
2. In the left pane, click **Shut Down**.
3. In **Administrator password**, enter the password for logging in to the Web User Interface.
4. 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 Web User Interface, an error message will appear, since the storage system will no longer be running.

Accessing the Storage System through FTP and SSH

FTP

If you enabled the storage system to act as an FTP server, all Windows or Mac OS X users can use a Web browser to access the **public** folder and their personal folders. For information about enabling the storage system to act as an FTP server, see "Changing the Network Settings" on page 72

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 Mac 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).

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

   You can use **guest** as the user name, but you will be able to access only the **public** folder.

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.

   Even if you browse to other websites, you 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: FTP can not transfer files larger than 2 GB.

SSH

SSH provides an extra layer of secure communication between the storage system and its administrator. It

has no effect on file transfers between the users and the storage system in any way.

To enable SSH support:

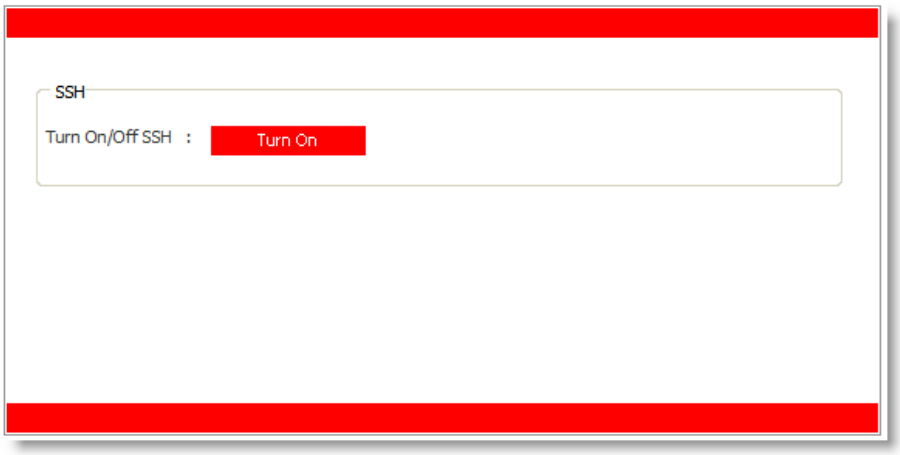
1. Enter this URL in the browser's address bar, and then press Enter:

   `http://storage_system/ssh_controlF.cgi`

   where *storage_system* is the name or IP address of the storage system.

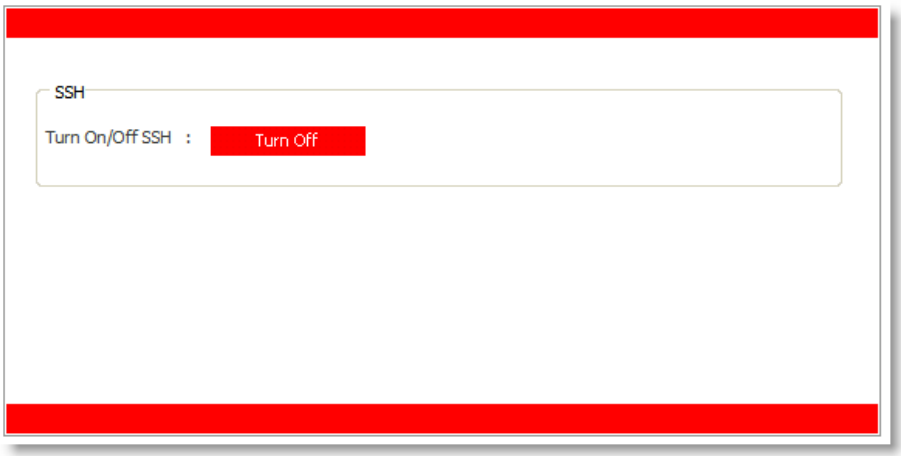
   Note: You can use the storage system name only if that name is registered with a DNS server on your network.

   The **SSH** page appears. This is a hidden web page that is not accessable from the Web User Interface.



2. Click **Turn On**.

   When SSH becomes active, the **SSH** page changes to allow the administrator the option of later disabling SSH.



   To return to the Web User Interface, click the browser's **Back** button until the Web User Interface reappears, or enter this URL in the browser's address bar, and then press Enter:

`http://storage_system/home_mainF.cgi`

where *storage_system* is the name or IP address of the storage system. This URL returns to the **Home** page of the Web User Interface.

To disable SSH support:

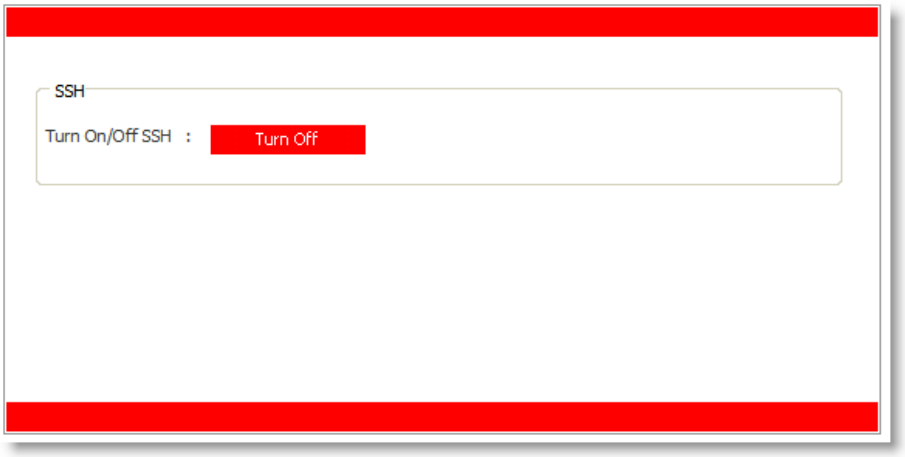
1. Enter this URL in the browser's address bar, and then press Enter:

   `http://storage_system/ssh_controlF.cgi`

   where *storage_system* is the name or IP address of the storage system.

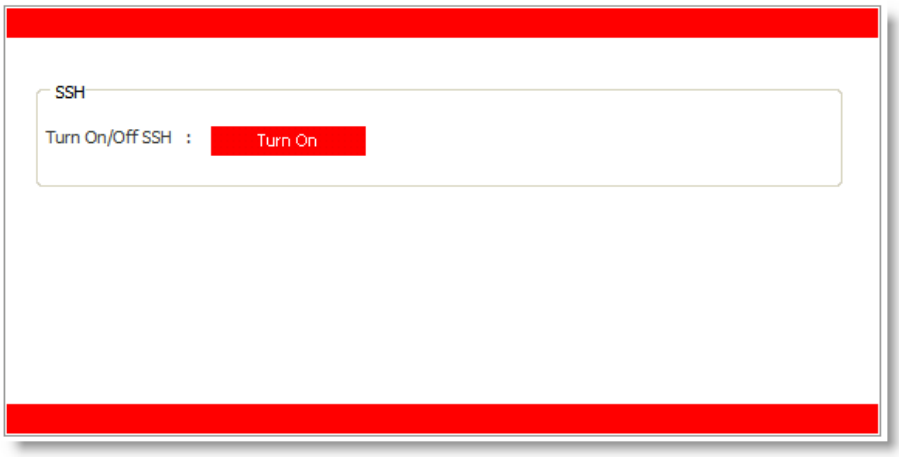
   Note: You can use the storage system name only if that name is registered with a DNS server on your network.

   The **SSH** page appears.



2. Click **Turn Off**.

   When SSH becomes inactive, the **SSH** page changes to allow the administrator the option of later enabling SSH.



To return to the Web User Interface, click the browser's **Back** button until the Web User Interface reappears, or enter this URL in the browser's address bar, and then press Enter:

`http://`*`storage_system/home_mainF.cgi`*

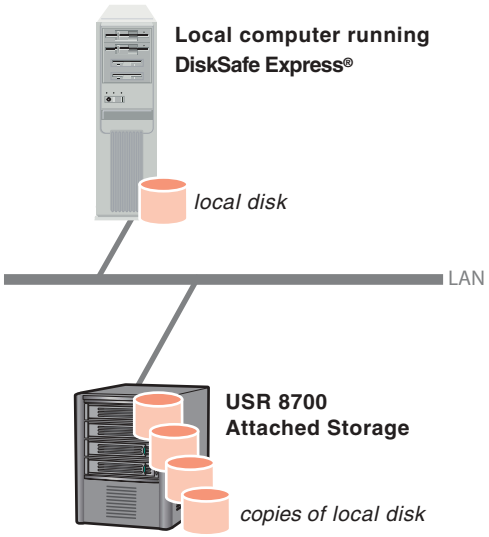
where *storage_system* is the name or IP address of the storage system. This URL returns to the **Home** page of the Web User Interface.

Protecting Local Disks

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, whichever you prefer. (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. Once the maximum of supported backups are saved on the storage system, the oldest backup is automatically deleted upon every subsequent backup.



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.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 need 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. (Alternatively, if your computer does not support the recovery CD but does support the PXE protocol, you can boot your computer from a backup on the storage system and recover your system disk.) Recovering the whole disk makes it contain exactly the same data that it contained at the time the backup was performed—you do not need to reinstall or reconfigure the

operating system or applications.

Getting Started

System Requirements

Each computer where DiskSafe Express is installed must have the following:

- One of the following operating systems:
  - Microsoft Windows XP Home Edition or Professional with Service Pack 2 or newer
  - Microsoft Windows Server 2003
  - Microsoft Windows 2000 Professional, Server, or Advanced Server with Service Pack 4
- Microsoft iSCSI Initiator 2.0

  Note: For information about downloading and installing this item, refer to the next section, "Installing the Microsoft iSCSI Initiator."

- 20 MB free hard disk space

  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 you are using a firewall on the computer that you plant to protect, open TCP port 11762 on the firewall. This ensures that DiskSafe Express can communicate with the storage system.

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-befd1319f825&DisplayLang=en

2. Scroll down to the **Files in This Download** section and download the item that ends with **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**.

   The installation wizard starts.

5. On the first page of the installation wizard, click **Next**.

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 need 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**.

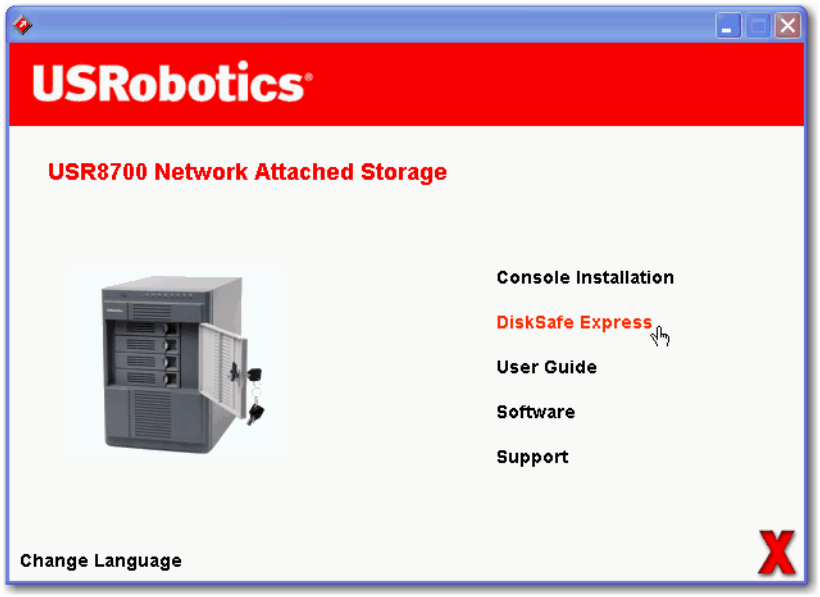
   After your computer restarts, you can install DiskSafe Express.

Installing DiskSafe Express

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

To install DiskSafe Express:

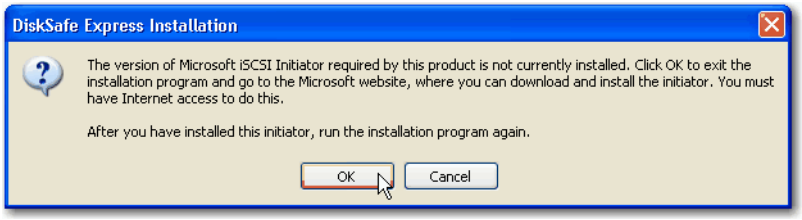
1. Insert the USRobotics Installation CD into a CD-ROM drive. The startup program prompts you to make a choice:



2. Select **DiskSafe Express**.

3. If the Microsoft iSCSI Initiator 2.0 is already installed, go to step 4.

   If this component is not currently installed, the following prompt appears:



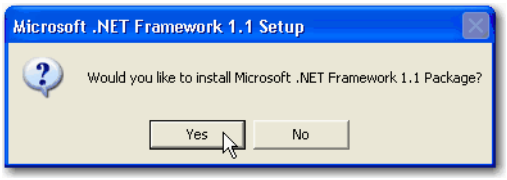
   Click **OK** to go to the Microsoft website, click **iSCSI Software Initiator v2.0**, and follow the instructions in "Installing the Microsoft iSCSI Initiator" on page 90.

   You must install the Microsoft iSCSI Initiator 2.0 before you can install DiskSafe Express.

   When you have finished installing the iSCSI initiator, re-start the installation of DiskSafe Express.

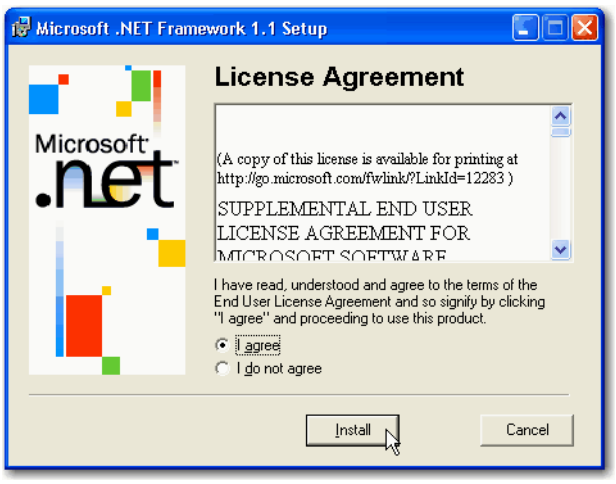
4. If Microsoft .NET Framework 1.1 is already installed, go to step 7.

   If this component is not currently installed, the following prompt appears:



   Click **Yes** to install this component. (You cannot install DiskSafe Express without first installing Microsoft .NET Framework 1.1.)

   When you click **Yes**, the setup utility for Microsoft .NET Framework 1.1 starts:



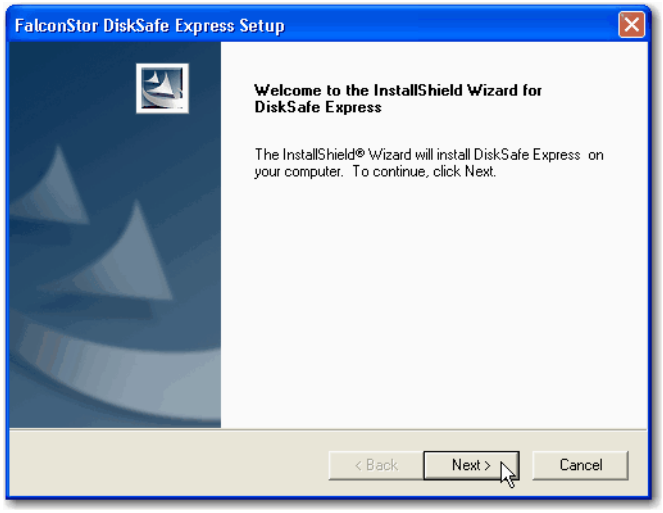
5. If you agree to the terms of the license agreement, select **I agree** and then click **Install**.

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

Note: The remaining time might be reported as 0 but the configuration is continuing in the background.

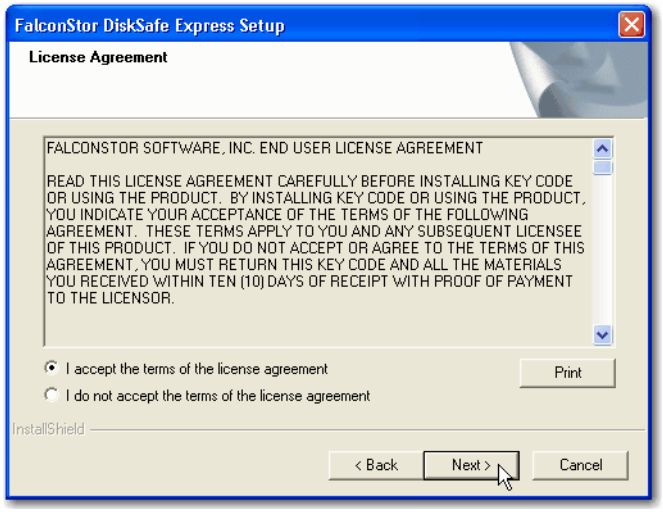
6. When a message appears, indicating that the installation of Microsoft .NET Framework 1.1 is complete, click **OK**.

   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:



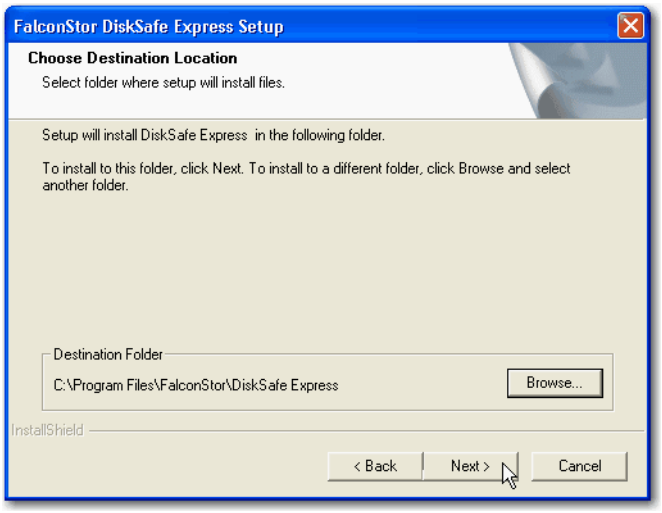
7. On the welcome page, click **Next**.

   The license agreement appears:



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

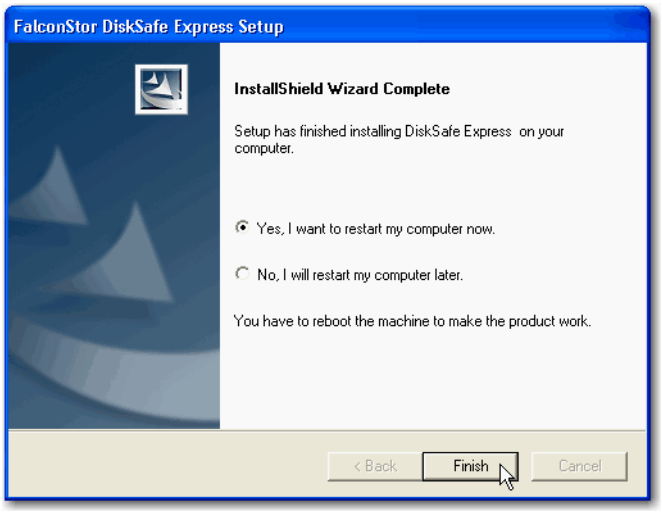
9. Click **Next** to install DiskSafe Express in the displayed location.



Alternatively, you can click **Browse**, select or enter a different location, click **OK**, and then click **Next**.

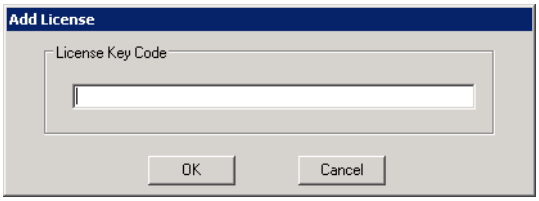
Note: You must install DiskSafe Express on the drive that you boot from (that is, where Windows is installed, typically C:).

10. To complete the installation and restart your computer, click **Finish**.



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 need to restart the computer immediately after installation, but you do need to restart it before running DiskSafe Express.

After you restart the computer, the **Add License** dialog box appears:



11. Type the key code for licensing the product and click **OK**.

    The license key is on the back of the recovery CD envelope.

    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 “Activating Your license” on page 96.

    If your computer has an Internet connection, the license is activated automatically. Click **OK** on the confirmation message, and the Protect a Disk wizard starts. For information about this wizard, refer to “Protecting Your Disks” on page 98.

    If your Internet connection is temporarily down, or if your 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 “Activating Your license” on page 96.

Starting DiskSafe Express

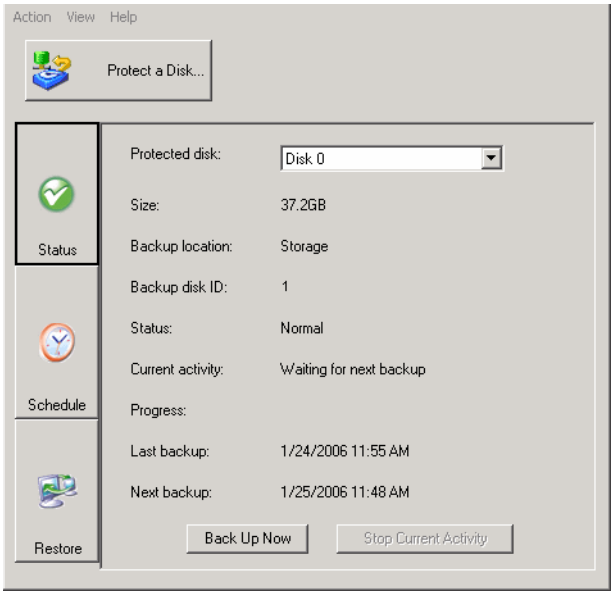
To start DiskSafe Express:

Windows Vista or XP: click **Start** > **All Programs** > **USRobotics** > **DiskSafe Express.**

Other Windows operating systems: click **Start** > **Programs** > **USRobotics** > **DiskSafe Express.**

If you did not protect a disk after installing DiskSafe Express and restarting your computer, you are prompted to do so the first time you run this application. For information about this wizard, refer to “Protecting Your Disks” on page 98.

If you already protected a disk, the application window appears:



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 recovery. For more information, refer to “Activating Your license” on page 96.

Activating Your license

When you install DiskSafe Express and restart your computer, you are 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 was not activated. You must activate your license within 30 days of installing DiskSafe Express; otherwise, you will not be able to perform backups or recovery.

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: Activation is tied to your computer's hardware. Once you have activated a particular license, if your computer hardware changes, or if you subsequently install DiskSafe Express on a different computer using the same key code, an error message appears. You must export your current license data (**Action** > **License** > **Offline Activation** > **Export License Data**) and e-mail the license file to Activate.Keycode@falconstor.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.

If you need assistance with this procedure, contact Technical Support.

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**.

   The **Offline Activation** dialog box appears.

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.

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

   `Activate.Keycode@falconstor.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.

8. From the **Action** menu, click **License** > **Offline Activation**.

9. Click **Import Activation Code**.

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

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

    The license is now activated and you can continue to backup up and recover your data.

12. 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**.

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

2. In **License key code**, enter the new key code.

3. Click **OK**.

4. 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.)

Protecting Your Disks

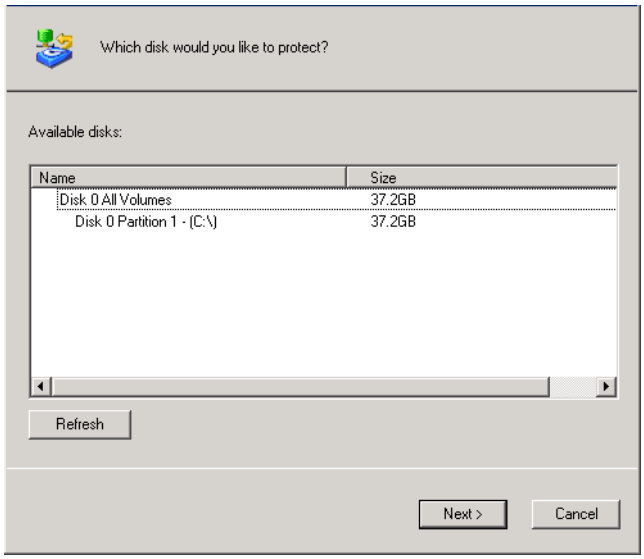
After you install DiskSafe Express and restart your computer, the Protect a Disk wizard runs automatically. Using this wizard, you can specify which disk or partition you need to back up, where the backups should be stored, when automatic backups (if any) should occur, and what password you need to use 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**.

   The Protect a Disk wizard runs.

2. In the **Available disks** list, select the disk or partition that you need to protect.



Even if your computer has only one hard disk, two items appear 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 entire 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 must 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.

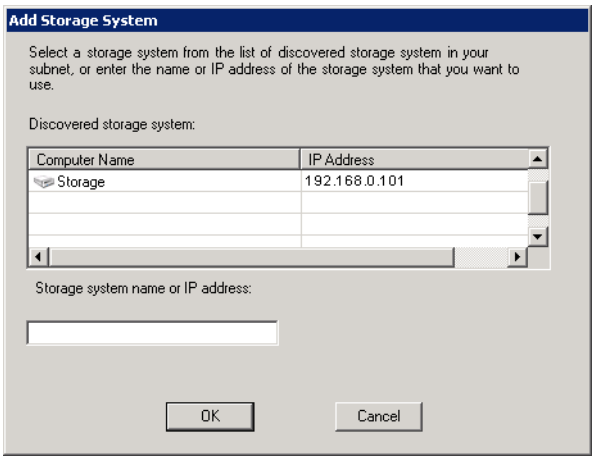
Note:

- 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.

What to do next:

In this case	Go to this step
You never previously completed the Protect a Disk wizard	3
You previously completed the Protect a Disk wizard and connected to a storage system	4
You previously protected this disk and removed protection (as described in "Removing Protection" on page 122)	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. (It might take a few seconds to complete the scan. You can cancel it at any time by clicking **Cancel** on the scanning message box.)



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

If no storage systems are automatically discovered, or if you need to back up your disk to a different storage system, enter the name or IP address of the desired storage system in **Storage system name or IP address**.

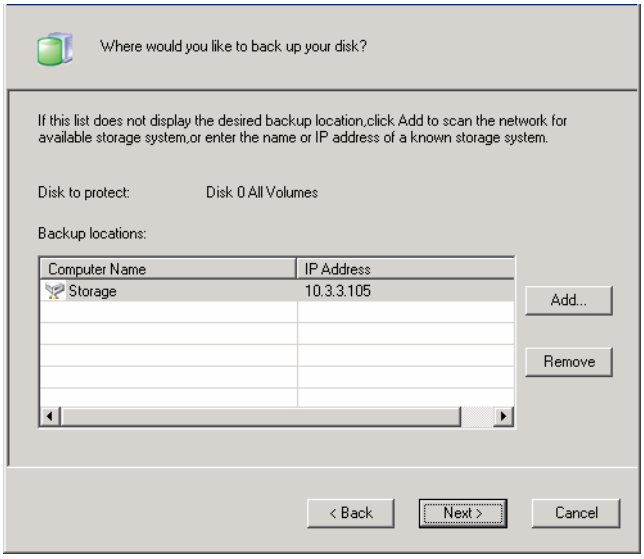
Note: You can enter a storage system name only if that name is registered with a DNS server on your network.

Then 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 **Backup locations**, select the storage system to use for backups of this disk or partition. (The

first backup location in the list is selected by default.)

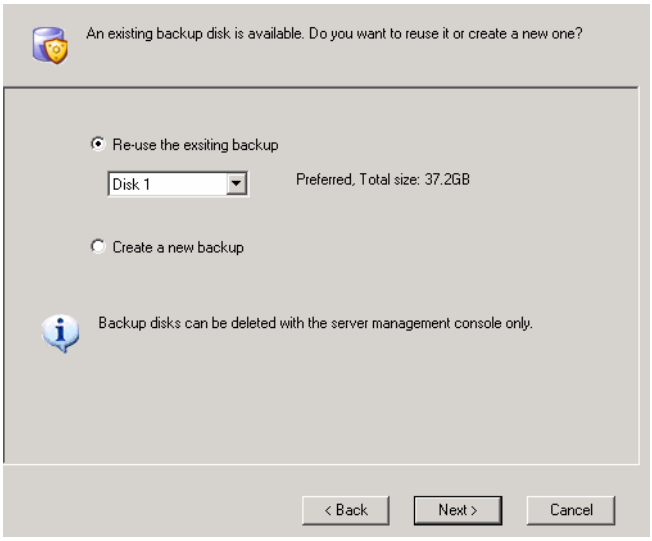


If you need to scan the network for new storage systems, or add a new one manually, click **Add** and repeat step 3.

If you need 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:

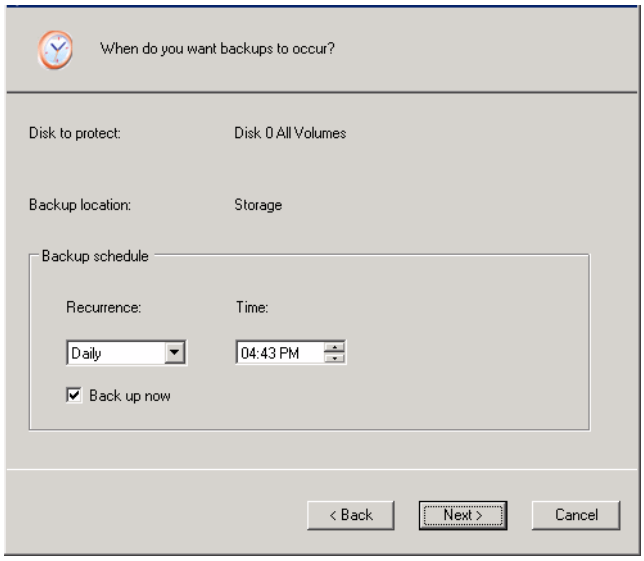


If you select **Re-use the existing backup**, you must select which backup to re-use from the list. The disk ID and size also appear to help you identify exactly which backup to use. Then click **Next** and go

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 need backups to occur.



For example, if you need 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 do not need 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" on page 104).

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 are protecting multiple disks or partitions, it is recommended that you schedule each backup to occur at a different time.

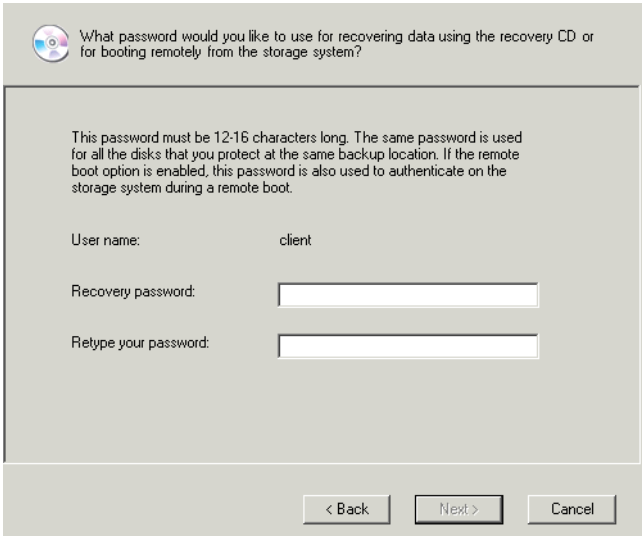
- Once you complete this wizard, if a backup does not occur at its scheduled time for any reason, a message will appear, advising you of this and giving you the option to perform the backup immediately or wait until the next scheduled backup.

---

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.

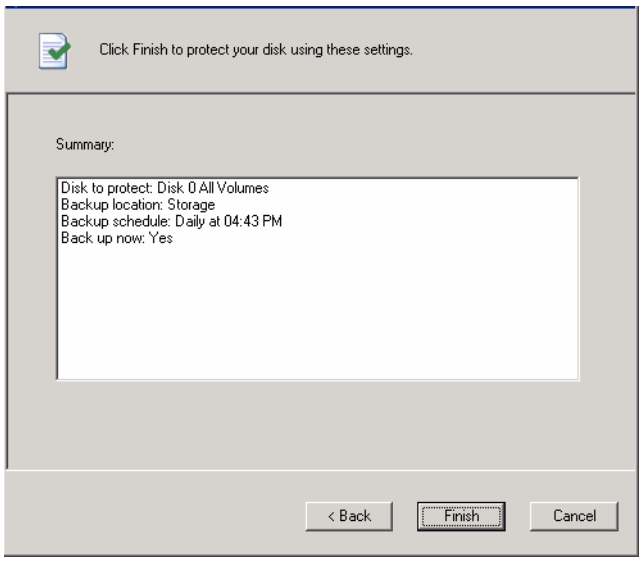
8. If you ever need to recover your disk using the recovery CD, you'll be prompted for a password. In **Recovery password**, enter the password that you'd like to use, enter it again in **Retype your password**, and then click **Next**.



Notes:

- The recovery password must be 12–16 characters long. It cannot contain multi-byte words. This means that you can only enter ASCII characters whose code values are less than 128.
- 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 (as described in "Changing the Recovery Password" on page 107).

9. Review all your selections and click **Finish**.



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

10. If you need 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.

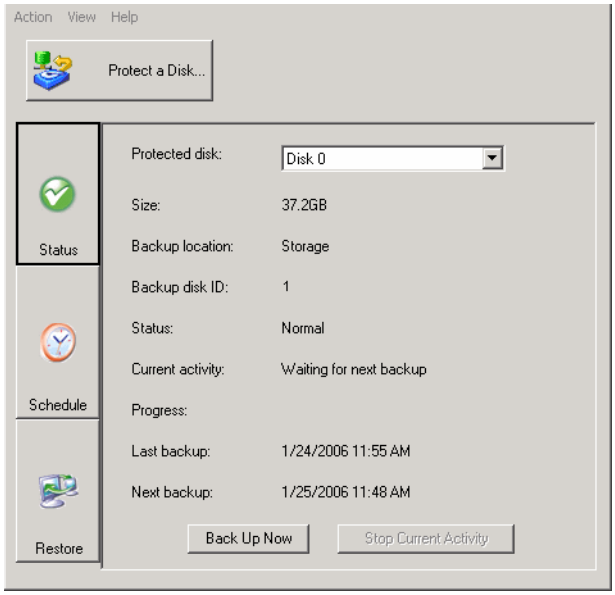
Manually Backing Up Your Disk

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 are 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. Click **Status**.



2. In the **Protected disk** list, select the disk that you need 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**.

Stopping a Backup or Recovery in Progress

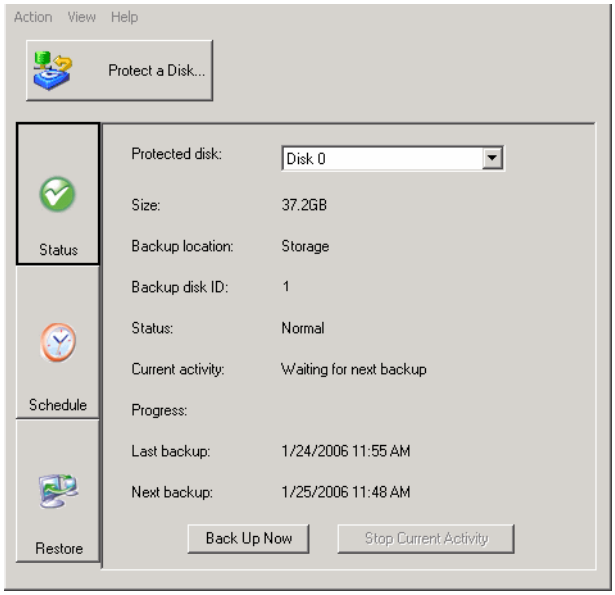
Once a backup or recovery starts, you can stop it at any time—for example, if you notice that your system is not responding as quickly as you'd like, and you want to free up processing bandwidth for other tasks.

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. Click **Status**.



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

3. Click **Stop Current Activity**.

   If you are stopping a backup, the backup stops immediately.

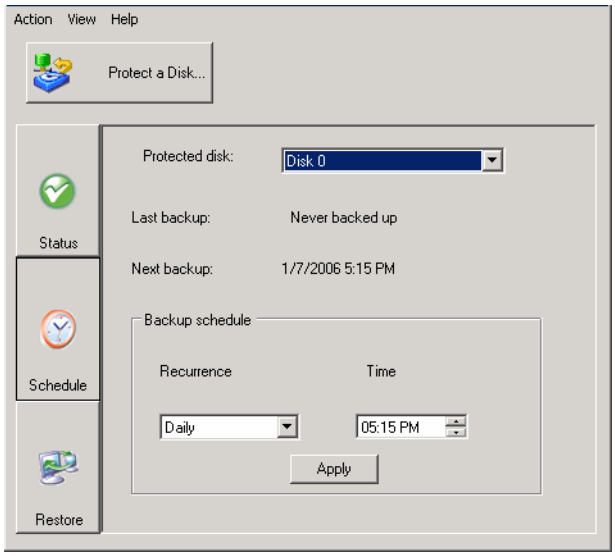
   If you are stopping a recovery, a confirmation message appears. Click **OK** to stop the recovery now, or click **Cancel** to proceed with it.

Changing the Backup Schedule

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

To change the backup schedule:

1. Click **Schedule**.



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

3. Specify when you need backups to occur.

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

   If you do not need 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" on page 104).

4. Click **Apply**.

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

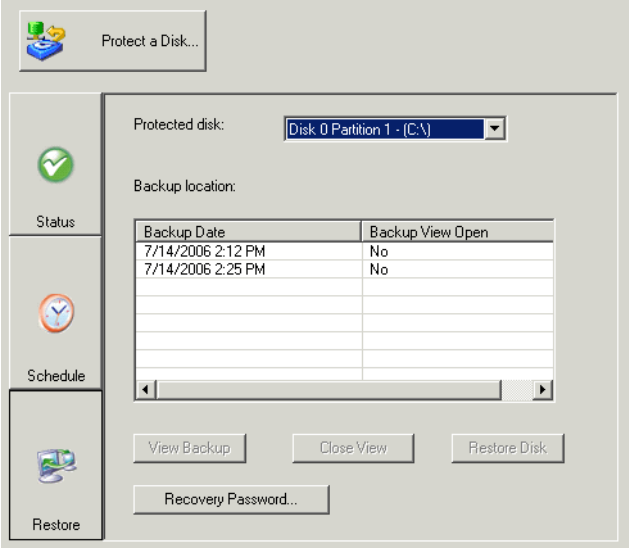
Changing the Recovery Password

When you protect a disk, you specify what password to use for recovering the disk using the recovery CD or when you remotely boot from a backup on the storage system. You can change this password at any time as long as the **Status** of the backup is **Normal**. (This ensures that the change is also made on the storage system.)

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 password.

To change the recovery password:

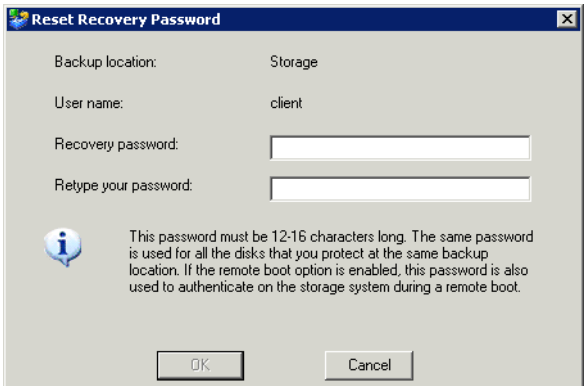
1. Click **Restore**.



2. In **Protected disk**, select a disk whose backup resides on the storage system whose recovery password you need 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 Password**.



4. In **Recovery password**, enter the desired password.

   This password must be 12–16 characters long. It cannot contain multi-byte words. This means that you can only enter ASCII characters whose code values are less than 128.

5. In **Retype your password**, enter the password again.

6. Click **OK**.

Enabling or Disabling Remote Boot

If you need to recover your system disk or partition, using the recovery CD is recommended (as described in "Recovering a System Disk or Partition" on page 116). However, if your computer does not support the recovery CD but does support the PXE protocol, you can remotely boot your computer from a backup on the storage system and then recover your system disk. (If you are not sure whether your computer supports the PXE protocol, try to enable remote boot. If your computer does not support the PXE protocol, an error message will appear during this process.)

Caution: You must determine whether or not your computer supports the recovery CD before a system failure occurs. To do this, perform steps 1 through 3 in "Recovering a System Disk or Partition" on page 116 and use **Diagnostic Mode** to confirm that at least one network interface card is supported.

If your computer does not support the recovery CD, enable remote boot before a system failure occurs. Once your system has failed, you cannot enable remote boot.

If your computer does not support either the recovery CD or the PXE protocol, gather your hardware information (as described in step 3 in "Recovering a System Disk or Partition" on page 116) and send it to your vendor. You might be able to obtain an updated recovery CD or a new driver that will make your computer compatible with your existing recovery CD.

You can enable remote boot only if the following criteria have been met:

- Windows was installed on the first partition of the first disk in your computer.
- DiskSafe Express was installed on that system disk.
- You protected your system disk or partition.
- You are accessing the computer directly rather than using Remote Desktop.

Note: If DiskSafe Express was installed on the same disk but on a different partition than Windows, the entire system disk must be protected rather than each individual partition. If you protected each partition individually, remove protection for those partitions (as described in "Removing Protection" on page 122) and protect the entire disk (as described in "Protecting Your Disks" on page 98).

You must wait until the initial backup of your system disk or partition has completed before you enable remote boot.

When you enable remote boot, your network connection will be temporarily interrupted. It is recommended that you enable remote boot when this will not adversely affect any network applications that you might be running.

If remote boot is successfully enabled, a new backup is created automatically.

Once you have enabled remote boot, if you subsequently need to boot remotely using a different network interface card (NIC), you must first disable remote boot and then enable it again, specifying the other NIC. In addition, after you recover a disk while booting remotely, you must disable and re-enable remote boot.

Enabling Remote Boot

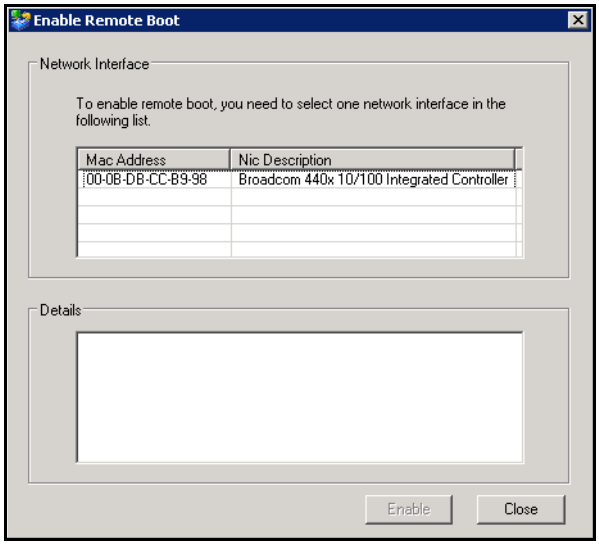
To enable remote boot:

1. In the **Protected disk** list on any page, select your system disk or partition.

   If you protected multiple system disks or partitions, select the first system disk or partition on your computer (typically Disk 0).

2. From the **Action** menu, click **Enable Remote Boot**.

   The **Enable Remote Boot** dialog box displays a list of all the NICs on your computer.



3. Select the NIC that you need to use when remotely booting from the storage system.

4. Click **Enable**.

   A message appears, advising you that your network connection will be temporarily interrupted.

5. Click **Yes** to allow the temporary network interruption. Your network connection will be restored immediately after this process is complete.

   On the **Enable Remote Boot** dialog box, the **Details** area shows the progress of the enabling process. If any problems are encountered—for example, if the selected disk or partition was not your system disk—that portion of the process is marked as **Failed**. You can click the plus sign next to the process description to expand it and display an error message that explains exactly what happened.

6. When a message advises you that drivers will be installed, click **OK**.

7. If a window appears warning that the software has not passed Windows testing, continue with the installation. USRobotics has thoroughly tested the operation of the software with Windows to ensure its safe operation.

   For Windows XP, click **Continue Anyway**.

For Windows 2000, click **Yes**.

For Windows XP only:

If the Found New Hardware Wizard asks to connect to the Windows update Web site to search for software, select **No, not this time** and click **Next**.

With **Install the software automatically (Recommended)** selected, click **Next**.

If remote boot was successfully enabled (as indicated in the **Details** area), a new backup is created automatically.

Note: If remote boot was successfully enabled but the new backup was not created (as indicated in the **Details** area), you must perform a manual backup (as described in "Manually Backing Up Your Disk" on page 104). You can remotely boot only from backups that were performed after remote boot was enabled.

8. Click **Close**.

   If no problems were encountered, you can now remotely boot from the storage system (as described in "Recovering a System Disk While Booting Remotely" on page 119).

   If any problems were encountered, take corrective action. For example, if you did not previously protect a system disk or partition, do so now (as described in "Protecting Your Disks" on page 98). Then repeat this procedure for enabling remote boot until all parts of the process complete successfully.

Disabling Remote Boot

Disabling remote boot restarts your computer automatically. Save and close any open files on your system before doing this.

To disable remote boot:

1. From the **Action** menu, click **Disable Remote Boot**.
2. When the confirmation message appears, click **OK**.

   Your computer restarts automatically.

Recovering Data

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

- **Recover selected folders, files, or sections of files**—If you accidentally permanently deleted a folder or file that you need 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 for-

mat of the data in a file—without adversely affecting the data on your local disk. For more information, refer to “Recovering Files from a Backup” on page 113.

- **Recover 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.

  Caution: When you do this, 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 are recovering. You might want to copy any newer files that you need to keep to another disk before you recover the disk. To copy files from a backup, refer to “Recovering Files from a Backup” on page 113.

  In addition, in rare cases (for example, if your data disk contains applications like anti-virus programs that interact with the operating system), if network errors occur or the storage system shuts down during recovery, your operating system might become unstable, and you will need 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 are recovering. For more information, refer to “Recovering a Non-system Disk or Partition” on page 115.

- **Recover 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 need 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 “Recovering a System Disk or Partition” on page 116.

  If your computer does not support the recovery CD but does support the PXE protocol, you can boot your computer from a backup on the storage system and then recover your system disk. For more information, refer to “Recovering a System Disk While Booting Remotely” on page 119.

  Caution: It is strongly recommended that you determine whether or not your computer supports the recovery CD before a system failure occurs. To do this, perform steps 1 through 3 in “Recovering a System Disk or Partition” on page 116 and use **Diagnostic Mode** to confirm that at least one network interface card is supported.

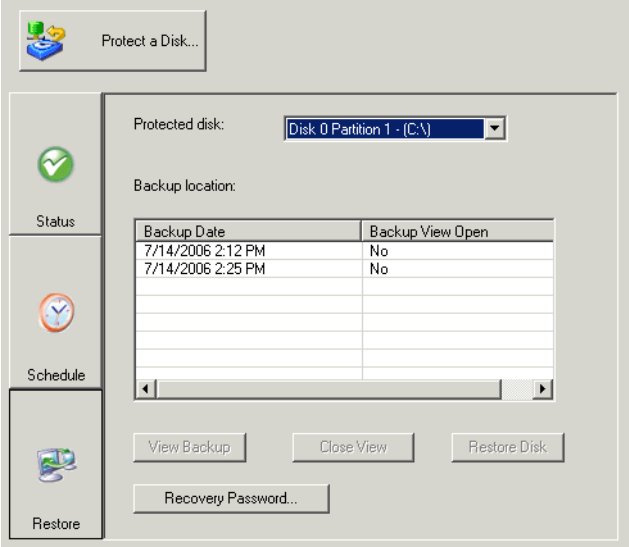
  If your computer does not support the recovery CD, you must enable remote boot (as described in “Enabling Remote Boot” on page 110) before a system failure occurs. Once your system has failed, you cannot enable remote boot.

  If your computer does not support either the recovery CD or the PXE protocol, gather your hardware information (as described in step 3 in “Recovering a System Disk or Partition” on page 116) and send it to your vendor. You might be able to obtain an updated recovery CD or a new driver that will make your computer compatible with your existing recovery CD.

Recovering Files from a Backup

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

1. Click **Restore**.



2. In the **Protected disk** list, select the disk that contains the folders or files that you need 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 need, and copy any of the data to your local disk.

Caution: You can open and change the files in the backup view, and even create new folders or files there. 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,

  1. Windows Vista: click **Start**, right-click **Computer** and select **Manage**.

     Windows 2000: on the desktop, right-click **My Computer** and select **Manage**.

     Other Windows operating systems: click **Start**, right-click **My Computer** and click **Manage**.

  2. In the left pane, click **Disk Management**.

  3. 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 under “Recovering Files from a Backup” on page 113 for each backup that you need to view.

- 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 are 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.

4. When you have finished viewing or copying all the desired data, select the backup in **Backups** and click **Close View**.

   The Windows Explorer window closes automatically, and the **Backup View Open** column for the selected backup now displays **No**.

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.

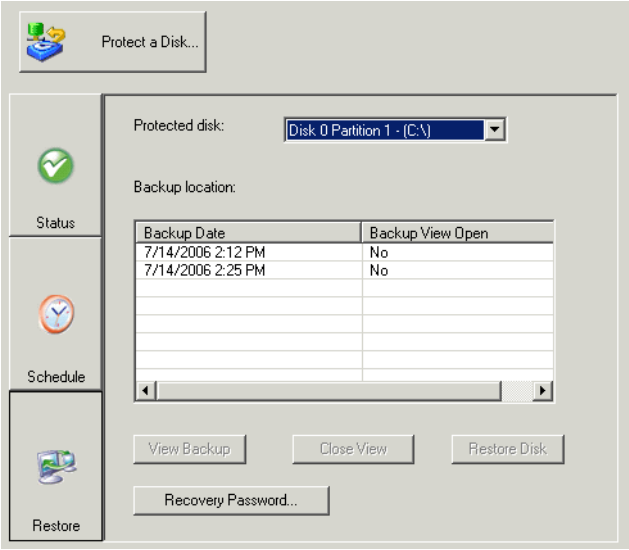
In addition, if you recover a partition and other partitions of that same disk are also protected, protection for those other partitions temporarily stops until the selected partition is recovered.

Caution: 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 are recovering. You might want to copy any newer files that you need to keep to another disk before you recover the disk. To copy files from a backup, refer to "Recovering Files from a Backup" on page 113.

In addition, if network errors occur or the storage system shuts down during recovery, your operating system might become unstable, and you will need 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. Click **Restore**.



2. In the **Protected disk** list, select the disk or partition that you need 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 need 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 need to recover it again before you can use it.

7. When you are prompted to restart the computer, click **OK**.

   You do not need 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" on page 104) 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.

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 need 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 need 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 CD-ROM), 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 need 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. In the **Client Name** field, enter the full computer name of this computer.

   This name is always in upper case.

   If you do not remember the full computer name, access the Web User Interface (as described in "Accessing the Web User Interface" on page 25) 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.

   Note: You can use the storage system name only if your network has a DNS server.

8. Make sure the selected authentication type is **CHAP**.

   DiskSafe Express supports only **CHAP** authentication.

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

   If you do not remember your password, you can change it on the storage system (as described in "Changing the Recovery Password" on page 62) and enter the new password here.

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

    If you protected only one disk or partition, only one item appears 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 have 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**.

> **Caution:** 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 are 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 are 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 10, 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 16, select the partition where you want to recover the data, and then select **Next**. (Otherwise, go to step 18.)

18. Select **Yes** to confirm the action.

> **Caution:** 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 do this	Do this
Review information about any sectors that were not successfully recovered	Select **Failed Sectors**, review the displayed information, and select **Back**.
Recover another disk or partition	Select **Continue**. If you need 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 10. If you want to recover a different computer's backup, or if you need 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.
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 "Removing Protection" on page 122).

    Since the computer is disconnected from the network, you might see messages about the backup being offline. This is normal.

22. Restart the computer.

23. Protect the recovered disk once again (as described in "Protecting Your Disks" on page 98).

Recovering a System Disk While Booting Remotely

If your computer meets the prerequisites, you can remotely boot it from a backup on your storage system and recover your system disk or partition. You can recover only your most recent backup.

Note: If you replaced the original hard disk, the new disk must be at least as large as the original 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.

Prerequisites

Before you can recover a disk while booting remotely, the following criteria must be met:

- The computer that you are remotely booting must be in the same subnet as the storage system.
- Remote boot must be enabled for that computer (as described in "Enabling Remote Boot" on page 110).

- At least one backup must have been performed after remote boot was enabled.
- The network must have a DHCP server, or your storage system must be configured to act as a DHCP server (as described in “Changing the Network Settings” on page 72).
- If you plan to remotely boot your computer from a different computer’s backup, you or your administrator must enter the MAC address of your computer’s network interface card (NIC) on the storage system. For more information, refer to “Configuring Remote Boot” on page 63.
- If you need to remotely boot from any backup other than the most recent one, you or your administrator must select the desired backup on the storage system. For more information, refer to “Configuring Remote Boot” on page 63.

Recovering the disk

To recover a system disk or partition while booting remotely:

1. Start your computer.
2. Use the appropriate procedure to configure your computer to boot from the NIC.

   For example, you might press F12 when the boot menu appears. For more information, refer to the documentation for your computer.

   When the computer restarts, allow it to boot from the NIC. (You might be prompted to press F1 to continue.)
3. When prompted, press F8.
4. Using the arrow keys, select **Remote Boot (Windows)** and then press Enter.
5. When prompted, enter the password that you specified when you protected the system disk or when you last changed the password for that disk.

   If you do not remember your password, ask your system administrator to change it on the storage system (as described in “Changing the Recovery Password” on page 62) and enter the new password.
6. If any error messages appear, click **OK**.
7. Log in as you normally do.

   The message **Network Boot Mode** appears on the screen to confirm that you are working from the storage system.

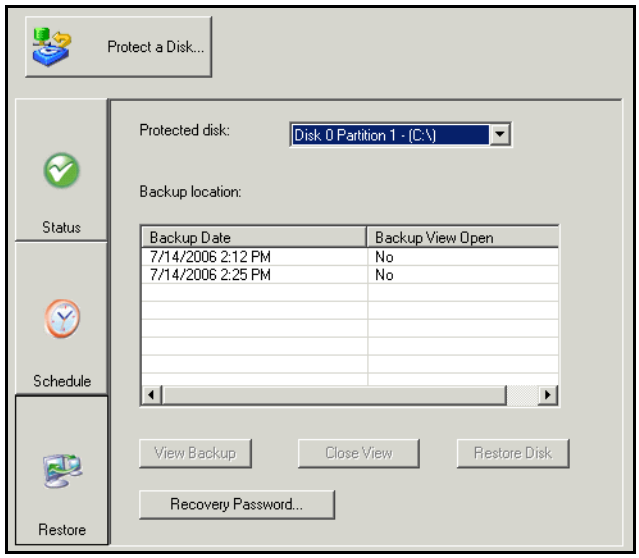
Caution: You can open or change files, and create new files or folders while remotely booting. However, only the data that existed at the time of the selected backup will be recovered. If you need to save any new data, you must copy the files or folders to a different location, such as a network server.

8. Start DiskSafe Express.

Caution: While booting remotely, do not try to use DiskSafe Express for any operation other than recovering the system disk.

9. When a message advises you that the computer name has changed, click **OK**.

10. Click **Restore**.



The **Protected disk** list displays the disk or partition that you are currently booting from.

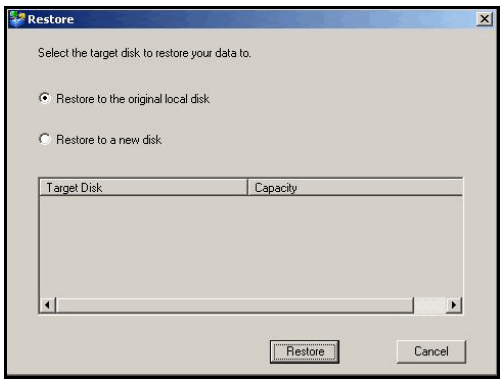
11. In **Backups**, select the most recent backup.

You cannot recover any backup except the most recent one.

Note: If no backups appear in this list, the backup that you booted from is not using the same recovery password as the storage system. This can occur if you changed the recovery password on the storage system before booting remotely, or if you changed it between backups in DiskSafe Express and booted from an earlier backup. To resolve this issue, you must reset the password in the Microsoft iSCSI Initiator (as described in "Resetting the Recovery Password in the Microsoft iSCSI Initiator" on page 145). Then restart DiskSafe Express.

12. Click **Restore Disk**.

The **Restore** dialog box appears.



13. Specify whether you are restoring to the original disk or a new disk.

    If you are recovering to a new disk, select the desired disk from the list. Then click **Restore**.

14. When the confirmation message appears, click **Yes**.

    The backup is recovered to your local disk, and the progress of this process is displayed. You can cancel the recovery at any time by clicking **Stop** in the progress dialog box.

Note: Do not shut down your computer, disconnect from the network, or perform any other tasks until this process is complete.

15. After the recovery is complete, click **OK** to restart your computer.

16. Use the appropriate procedure to configure your computer to boot from the local disk once more.

17. If you changed the recovery password, reset it in the Microsoft iSCSI Initiator after your computer restarts (as described in “Resetting the Recovery Password in the Microsoft iSCSI Initiator” on page 145).

18. Start DiskSafe Express and remove protection from all your disks and partitions (as described in “Removing Protection” on page 122). This disables remote boot and restarts your computer. Then protect your disks again (as described in “Protecting Your Disks” on page 98), reusing the existing backups.

    If you need to recover any other data disks or partitions, you can do so (as described in “Recovering a Non-system Disk or Partition” on page 115). However, be sure to do this after you have removed protection and then reprotected the disks.

19. Enable remote boot again (as described in “Enabling Remote Boot” on page 110).

Removing Protection

If you no longer need 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, you must cancel it or wait until it completes before you can remove protection.)

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 (as described in “Recovering Files from a Backup” on page 113 and “Recovering a Non-system Disk or Partition” on page 115). However, the backups that currently exist on the storage system are retained, and you can recover them using the recovery CD (as described in “Recovering a System Disk or Partition” on page 116).

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. For more information, refer to “Configuring Remote Boot” on page 63.

To remove protection:

1. In **Protected disk**, select the disk for which you want to remove protection.

2. From the **Action** menu, select **Remove Protection**.

3. When the confirmation message appears, click **Yes**.

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

4. If remote boot was enabled, it is disabled. When prompted, click **OK** to restart your computer.

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 any 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.

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 (as described in “Reconfiguring Your Storage System Disks” on page 75).

Caution: 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.

Caution: 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

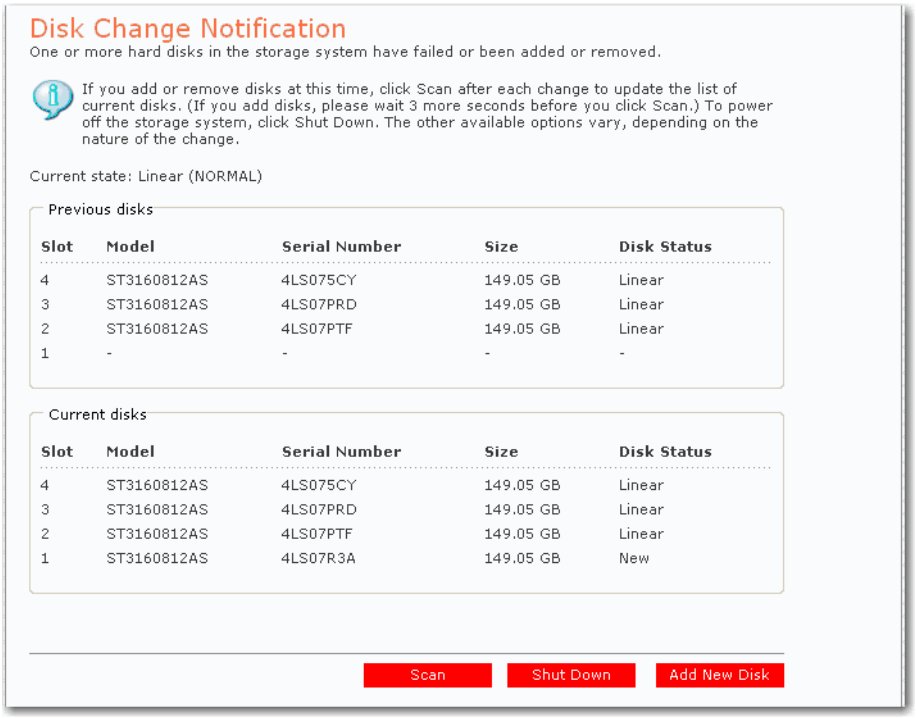
To add a hard disk to a linear or normal RAID configuration:

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 Web User Interface or refresh the browser window.

The **Disk Change Notification** page appears:

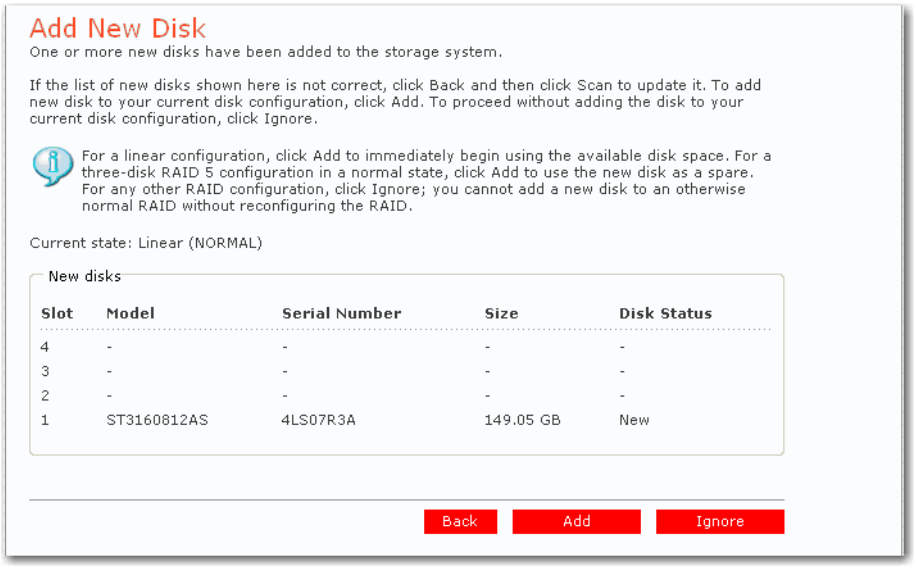


3. To add the disk to the storage system, click **Add New Disk**.

   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 Web User Interface.

   When you click **Add New Disk**, the following page appears:



4. Take the desired action:

To do this	Do this
Add the disk to a linear configuration or use it as a spare for a normal three-disk RAID 5 configuration	Click **Add**. The **Disks** page indicates the current state of the disk configuration.
Add the disk to the storage system but not add it to the RAID at this time	Click **Ignore**. The **Disks** page lists 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 (as described in "Reconfiguring Your Storage System Disks" on page 75), you will be able to use this new disk.
Return to the previous page (for example, to re-scan the storage system)	Click **Back**.

Adding Hard Disks to a Degraded RAID Configuration

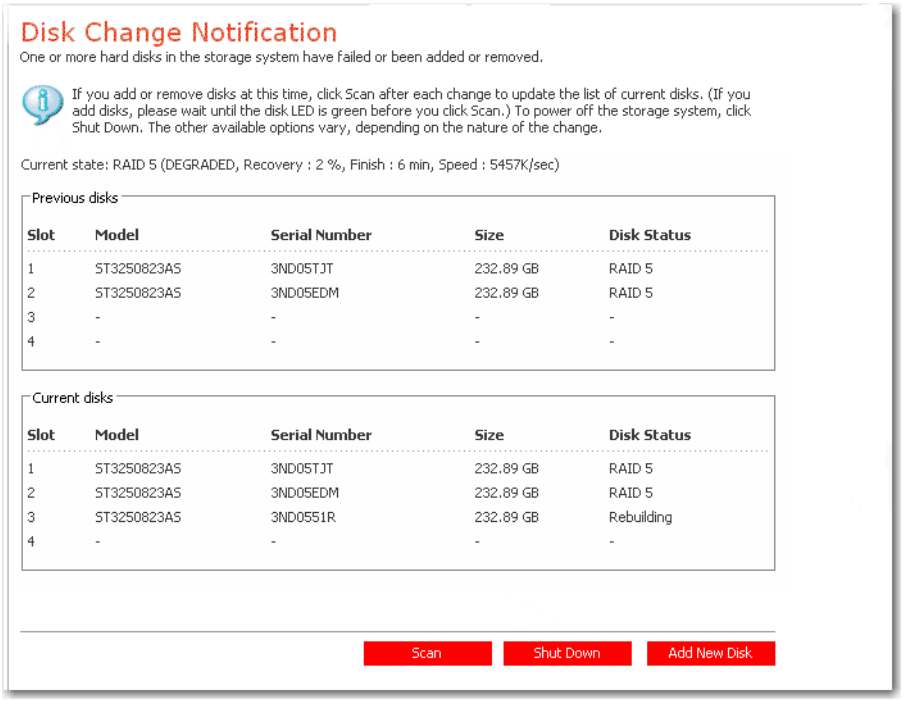
To add a hard disk to a degraded RAID configuration:

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 Web User Interface or refresh the browser window.

   The **Disk Change Notification** page appears:



3. Click **Ignore** to continue rebuilding the disk and return to the Web User Interface.

   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 re-appears.

Removing Hard Disks or Responding to Disk Failure

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. While this will not adversely affect the data on any of the other disks, it will affect the integrity of any file that resides partially on the removed disk and partially on a remaining disk.

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” on page 126.)

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.

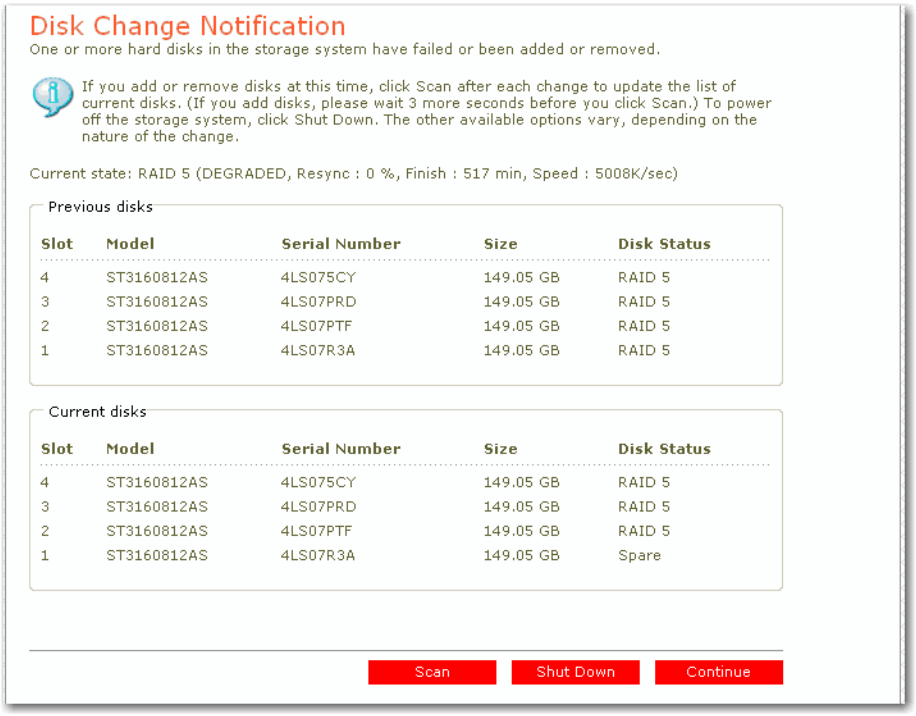
If you remove one or more viable disks and cause the entire RAID to fail, you can shut down the storage system, re-install the same disks, and then restart the storage system. As long as you re-install the original disks, the storage system should be able to resume proper operation, although the integrity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

your disks (as described in “Reconfiguring Your Storage System Disks” on page 75).

Caution: 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 Web User Interface or refresh the browser window:

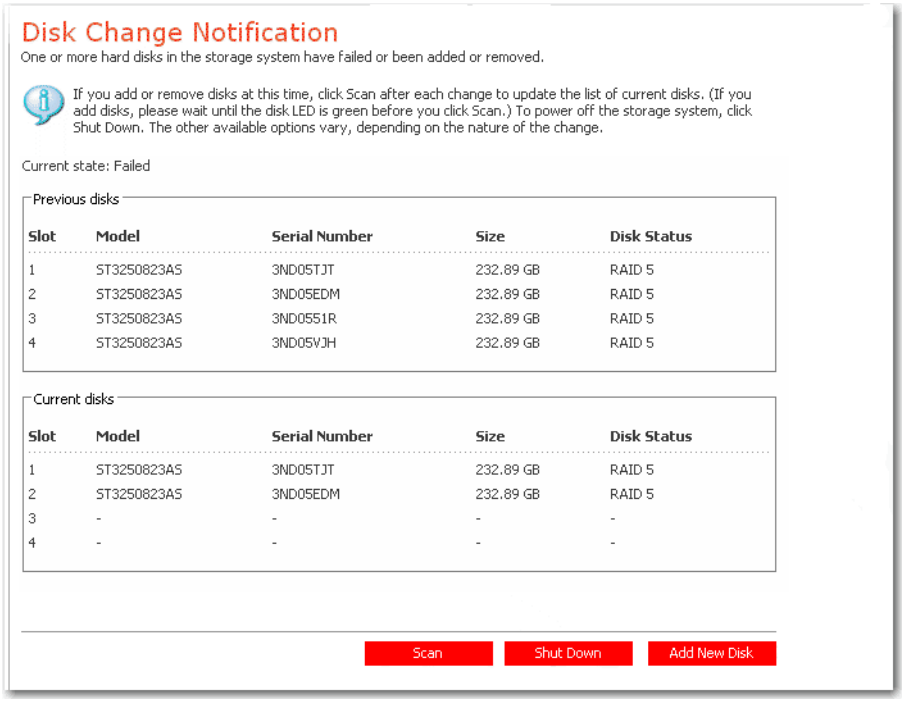


Take the appropriate action:

To do this	Do this
Scan the storage system again and update the information on the page	Click **Scan**.
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.
Return to the Web User Interface and continue to operate in a degraded mode	Click **Continue**.

Responding to RAID Failure

When disk removal/failure causes the entire RAID to fail, the **Disk Change Notification** page appears when you access the Web User Interface or refresh the browser window:



Take the appropriate action:

To do this	Do this
Scan the storage system again and update the information on the page	Click **Scan**.
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.
Reconfigure the storage system using the available disks	Click **Reconfigure Disks** and complete the system setup pages (as described in "Step Five: Configure your Storage System" on page 20). **Caution:** Reconfiguring the storage system deletes all user information and all data on all the disks.

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.

Caution: If the hotplug indicator for a disk is red or yellow, removing the disk will result in a loss of data. To avoid such loss, remove a disk only if its hotplug indicator is green

Note: 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.

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.

   Caution: 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 User Interface for the new unit (see “Accessing the Web User Interface” on page 25).

   As long as the new unit is in the same subnet as the old unit, you can access the Web User Interface using the same procedure you used previously. However, if the new unit is in a different subnet, you might need 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 do not 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 that on your hard disks, you can obtain the latest firmware from www.USR.com. To apply it, see “Upgrading the Firmware” on page 67

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

Troubleshooting

Resetting the Web User Interface Password

To reset the password to its factory default:

1. If the storage system is running, shut it down by pressing the power button unit for approximately 5 seconds.

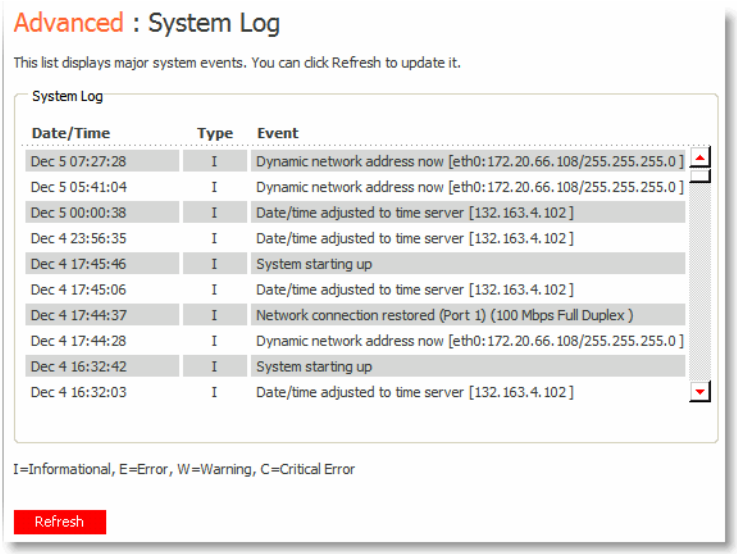
2. After the storage unit has shut down, press and hold the power button until the power LED comes on, and then release the button.

3. As soon as the LEDs for all of your disks have come on, press and hold the power button for 2 seconds, and then release the button.

The default password is **`storage`**. The default login user name is **`admin`**.

Viewing the System Log

The **System Log** page 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.



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 are viewing this list, click **Refresh** to update it.

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 Windows or the Storage System Console.

Disconnecting Using Windows

To disconnect from a shared folder using Windows:

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

2. Windows Vista: click **Start > Computer**,

   Windows 2000: on the desktop, double-click **My Computer**.

   Other Windows operating systems: click **Start > My Computer**.

3. Right-click the drive for the shared folder, and select **Disconnect**.

   The shared folder no longer appears in Windows Explorer.

Disconnecting Using the Storage System Console

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

1. Run the Storage System Console (as described in “Running the Storage System Console” on page 26).

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 expands 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.

Mac OS X

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

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

Troubleshooting the Storage System

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

I cannot access the Web User Interface.

If you are using the Storage System 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 Web User Interface using a Web browser. First access the Web User Interface using the Storage System Console (as described in "Accessing the Web User Interface Using the Storage System Console" on page 26) and then specify the gateway address (as described in "Changing the Network Settings" on page 72.) and try to access it using a Web browser.

The users cannot access the shared folders.

- Make sure the storage system is powered on, connected to the network, and operating properly.
- If the storage system uses local authentication mode, make sure the user configuration is correct.

  For Windows or Mac OS X users, try changing the password (as described in "Modifying Users" on page 47) 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 (as described in "Removing Users" on page 48) and adding it again (as described in "Adding Users" on page 31).
- If the storage system uses Active Directory authentication mode, check the user configuration on the Active Directory server.
- If the domain administrator has set user accounts with **User must change password at next logon**, the user may encounter problems in mapping to the share before the password is changed. To change the password:

  1. Press ALT+CTRL+DEL
  2. Select **Change Password**.
  3. Change **User name** to the name you want.
  4. Change **Log on to:** to the domain containing the user in step 3.
  5. Set the password to the desired password.
  6. Map to the share again.
- If the storage system uses Active Directory authentication mode, make sure the clocks of the storage system and the Active Directory server do not differ by more than five minutes. If they do, adjust the storage system time, time zone, or both to ensure that they match (as described in "Changing the System Settings" on page 69).
- Even when the storage system and Active Directory server are in the same time zone and have the same time, errors might occur if the Active Directory server adjusts for daylight saving time. In this

case, you must change both the time zone and time on the storage system. For example, if the Active Directory server time is 2:00 P.M. in the Central Time zone (GMT-06:00), you would set the storage system time zone to Eastern Time (GMT-05:00) and then set the time to match the Active Directory server (14:00). If you do this, do not synchronize the storage system with an NTP server, as the time will be readjusted based on the time zone.

- Make sure that users are using the proper procedure for accessing the shared folders (as described in "Accessing Shared Folders" on page 37), including the correct name or IP address of the storage system. (Windows and Mac OS X users can use the storage system name only if their computers are in the same subnet as the storage system, if they added the storage system's IP address and name to their local hosts file, or if the storage system name was manually registered with a DNS server in your network. Linux users must use the IP address.)

  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 Windows Explorer (as described in "Using Windows" on page 38).

- Make sure that 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 text and press Enter:

  `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 you are using Active Directory authentication mode, make sure that **User must change password at next logon** is cleared in the properties for each user on the Active Directory server who will be accessing shared folders on the storage system. Each user's password can be no longer than 24 characters.

The users cannot create files in the shared folders.

- Check the access for the user (as described in "Changing User Access to Shared Folders" on page 59). The user must have read/write access to be able to create files in the shared folder.

- There might not be enough space allocated to the shared folders. Expand the amount of available disk space (as described in "Expanding the shared storage" on page 76).

I am having trouble switching to Active Directory authentication mode.

- Make sure you identified the Active Directory server by its IP address rather than its name.

- If you are using a secondary Active Directory server, make sure that you identified it by its IP address rather than its name, that its IP address is different than the IP address of the primary server, and that it resides in the same domain as the primary server.

- Make sure the specified user name and password have sufficient privileges for browsing the Active Directory tree.

- If you specified an organizational unit name, make sure that it exists on the Active Directory tree, that

the unit name is no longer than 256 characters and does not contain a slash (/), that the unit contains no more than 100 subunits, and that you preceded the unit name with a slash (such as /Sales).

- Make sure the storage system time and Active Directory server time do not differ by more than five minutes. If they do, you must adjust the storage system time, time zone, or both to ensure that they match (as described in “Changing the System Settings” on page 69).

- Even if the storage system and Active Directory server are in the same time zone and have the same time, errors might still occur if the Active Directory server adjusts for daylight saving time. In this case, you must change both the time zone and time on the storage system. For example, if the Active Directory server time is 2:00 P.M. in the Central Time zone (GMT-06:00), you would set the storage system time zone to Eastern Time (GMT-05:00) and then set the time to match the Active Directory server (14:00). If you do this, do not synchronize the storage system with an NTP server, as the time will be readjusted based on the time zone.

- Make sure the administrator user name and password for accessing the Active Directory server are valid and have sufficient privileges for adding the storage system to the Active Directory tree.

Not all of my Active Directory users or groups were added to the storage system.

The storage system can accommodate a maximum of 128 users and 128 groups. If the selected organizational unit on the Active Directory server has more than that, the excess users or groups will not be added to the storage system.

To better control which users or groups are added to the storage system, you might want to create a new organizational unit that contains the appropriate number of entities, switch back to local authentication mode (as described in “Changing the Authentication Mode” on page 53), and then switch to Active Directory authentication mode again, specifying the new organizational unit.

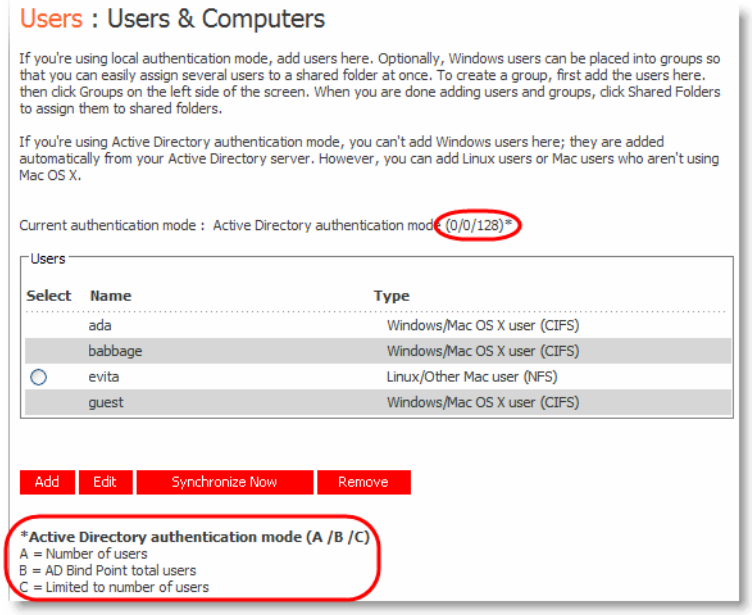
The user names that appear on the storage system do not match the names that appear in the Active Directory tree.

The storage system displays the **User logon name** that appears on the **Account** tab in the **Properties** dialog box on the Active Directory server. This name might differ from the name that appears in the Active Directory tree. To ensure that the names are the same, you can either change the **User logon name** to match the name displayed in the tree, or change the name in the tree to match the **User logon name**.

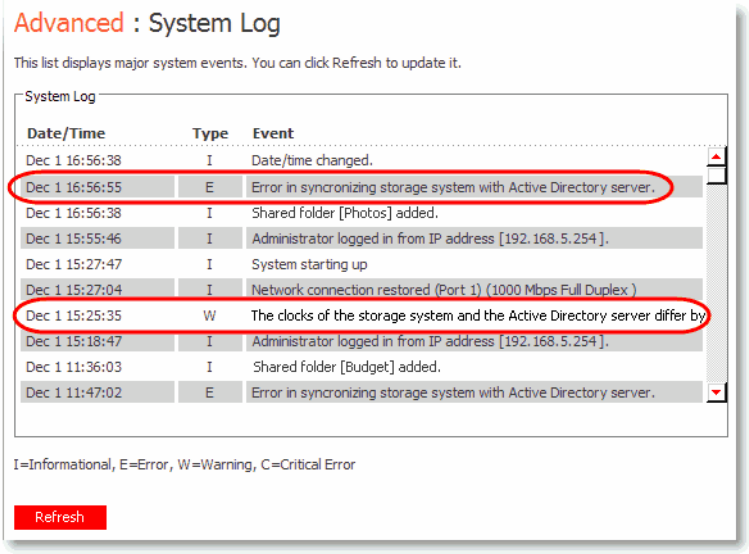
The storage system stopped synchronizing with the Active Directory server.

When you click **Users** in the navigation bar, the **Users & Computers** page appears. This page indicates the current authentication mode above the list of users. For Active Directory authentication mode it also

displays in parentheses the number of users, AD Bind Point total users, and the limit for number of users.



If the numbers within the parentheses indicate zero users and zero AD Bind Point users (0/0/128), navigate to the **Advanced : System Log** page and look for synchronization or clock errors.



If synchronization or clock errors are indicated, navigate to the **Advanced : System** page and compare the system time settings with the Active Directory server's time. If they are not within five minutes of each other, change the time for the storage system (as described in "Changing the System Settings" on page 69) so that their times match. Return to the **Users : Users & Computers** page and click **Synchronize Now**.

The storage system is not distributing IP addresses.

Make sure that **Enable DHCP server** is selected on the **Network** page (as described in "Changing the Network Settings" on page 72), 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.

The users cannot access the storage system using FTP.

Make sure that **Enable FTP server** is selected on the **Network** page (as described in "Changing the Network Settings" on page 72) and that the users are using the correct address for accessing the storage system (as described in "Accessing the Storage System through FTP and SSH" on page 85).

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.

A package size error displays when I upgrade the firmware.

- If you downloaded the firmware from a website or copied it from a CD, compare the original size of the package file with the size of the package file that you are using. If they differ, download or copy the file again to ensure that it is not corrupted.
- Restart the storage system and try again. This ensures that any temporary files on the storage system are deleted before the firmware is upgraded.

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" on page 144.

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

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

Authentication errors occur when I try to protect a disk.

- When adding a storage system, make sure that you are 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 text and press Enter:

  `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 do not use up disk space unnecessarily, be sure to delete any extraneous backups on the storage system (as described in "Configuring Remote Boot" on page 63). Compare the **Backup disk ID** on the **Status** page in DiskSafe Express with the **Backup Disk ID** on the **Backups** page in the Web User Interface to determine which backup is actually being used.

The Status page indicates that the backup is offline.

- 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 text and press Enter:

  `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 (as described in "Managing Backups" on page 61).

  If it has been deleted, remove protection (as described in "Removing Protection" on page 122) and protect the disk again (as described in "Protecting Your Disks" on page 98).

- 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 (as described in "Removing Protection" on page 122), delete the old computer name from the storage system (as described in "Deleting a Client" on page 64), and then protect your disks again (as described in "Protecting Your Disks" on page 98).

A backup did not occur at its regularly scheduled time.

- Check the schedule (as described in "Changing the Backup Schedule" on page 106) 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 the **Status** is **Offline**, review the troubleshooting procedures in the preceding section.

- 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 (as described in "Removing Protection" on page 122), delete the old computer name from the storage system (as described in "Deleting a Client" on page 64), and then protect your disks again (as described in "Protecting Your Disks" on page 98).

- 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.

I can't change my backup schedule.

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**.

I forgot my recovery password.

Reset the password using the storage system (as described in "Managing Backups" on page 61). Once you reset it on the storage system, you can use the new password with the recovery CD or for booting remotely from the storage system.

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 (as described in "Starting DiskSafe Express" on page 95).

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 **File name** 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, enter your e-mail address and press Enter.

   This ensures that your e-mail address is saved as part of the diagnostic file in case Technical Support needs to contact you.

4. When prompted, insert a formatted floppy disk into the computer's floppy disk drive or attach a USB disk and press Enter.
5. 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.

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

   For information about using the recovery CD to restore data, refer to "Recovering a System Disk or Partition" on page 116.

Resetting the Recovery Password in the Microsoft iSCSI Initiator

The recovery password used by the recovery CD and for booting remotely is actually the Microsoft iSCSI Initiator CHAP secret. When you protect a disk or change the recovery password using DiskSafe Express, the Microsoft iSCSI Initiator is configured automatically.

If you forget this password, you can reset it on the storage system. However, if you do this when your system is down (that is, while you are booting from the recovery CD or booting remotely), the recovery password in your Microsoft iSCSI Initiator will not match the recovery password on the storage system. As a result, when you recover your system disk using the recovery CD and then boot from the local disk, you will not be able to connect to the storage system. Likewise, when you boot remotely, you will not be able to recover your disks at all.

You will not be able to recover your disks if you change the recovery password between backups using DiskSafe Express and then remotely boot from one of the earlier backups. The recovery password in the

Microsoft iSCSI Initiator will not match the recovery password on the storage system.

To address this issue, you must reconfigure the Microsoft iSCSI Initiator to use the password that you specified on the storage system. If you are using the recovery CD, you must do this after you recover your system disk. If you are booting remotely, you must do this while in Network Boot Mode (before you recover your system disk) and again after you recover your disk and boot locally.

To reset the recovery password in the MIcrosoft iSCSI initiator:

1. Windows Vista or XP: click **Start > All Programs > Microsoft iSCSI Initiator** > **Microsoft iSCSI Initiator**.

   Other Windows operating Systems: click **Start > Programs > Microsoft iSCSI Initiator** --> **Microsoft iSCSI Initiator**.

2. Click the **Targets** tab.

3. If more than one target appears in **Targets**, select the one that contains the name of the storage system.

   The **Status** should be **Disconnected**.

4. Click **Log On**.

5. Click **Advanced**.

6. Select **CHAP logon information**.

7. In **User name**, type your computer name in all capital letters.

8. In **Target secret**, type the recovery password that you specified on the storage system.

9. Click **OK** on the **Advanced Settings** and then the **Log On to Target** dialog boxes.

   The **Status** of the target should now be **Connected**.

10. Click **OK** on the **iSCSI Initiator Properties** dialog box.

Support Information

If you are having trouble with the configuration or operation of your Storage System:

1. Refer to "Troubleshooting," beginning on page 135 in this guide.

2. Go to the Support section of the USRobotics Web site at www.usr.com/support/. Many of the most common difficulties that users experience have been addressed in the FAQ and Troubleshooting Web pages for your product. The product number of the USR8700 Network Attached Storage is 8700. You may need to know this to obtain information on the USRobotics Web site.

3. Submit your technical support question using an online form at www.usr.com/emailsupport/.

4. Contact the USRobotics Technical Support Department. To receive assistance, you need your serial number.

Country	Webmail	Voice
United States	www.usr.com/emailsupport	(888) 216-2850
Canada	www.usr.com/emailsupport	(888) 216-2850
Austria / Österreich / Ausztria	www.usr.com/emailsupport/de	07110 900 116
Belgium / België	www.usr.com/emailsupport/nl	070 23 35 45
Belgium/ Belgique	www.usr.com/emailsupport/be	070 23 35 46
Czech Republic / Česká republika	www.usr.com/emailsupport/cz	
Denmark	www.usr.com/emailsupport/ea	38323011
Finland	www.usr.com/emailsupport/ea	08 0091 3100
France	www.usr.com/emailsupport/fr	0825 070 693
Germany / Deutschland	www.usr.com/emailsupport/de	0180 567 1548
Greece / Ελλάδα	www.usr.com/emailsupport/gr	
Hungary / Magyarország	www.usr.com/emailsupport/hu	0180 567 1548
Ireland	www.usr.com/emailsupport/uk	1890 252 130
Italy / Italia	www.usr.com/emailsupport/it	39 02 69 43 03 39
Luxembourg / Luxemburg	www.usr.com/emailsupport/be	342 080 8318
Middle East/Africa	www.usr.com/emailsupport/me	+ 44 870 844 4546
Netherlands / Nederland	www.usr.com/emailsupport/nl	0900 202 5857
Norway	www.usr.com/emailsupport/ea	23 16 22 37
Poland / Polska	www.usr.com/emailsupport/pl	
Portugal	www.usr.com/emailsupport/pt	21 415 4034
Russia / Россия	www.usr.com/emailsupport/ru	8 800 200 20 01
Spain / España	www.usr.com/emailsupport/es	902 117964
Sweden / Sverige	www.usr.com/emailsupport/se	08 5016 3205
Switzerland / Schweiz / Suisse /Svizzera	www.usr.com/emailsupport/de	0848 840 200

Country	Webmail	Voice
Turkey / Türkiye	www.usr.com/emailsupport/tk	0212 444 4 877
United Arab Emirates	www.usr.com/emailsupport/me	0800 877 63
United Kingdom	www.usr.com/emailsupport/uk	0870 844 4546

For current support contact information, go to www.usr.com/support.

Regulatory Information

Manufacturer's Declaration of Conformity

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL 60173
U.S.A.

declares that this product conforms to the FCC's specifications:
Part 15, Class B

Operation of this device is subject to the following conditions:

1. this device may not cause harmful electromagnetic interference, and

2. this device must accept any interference received including interference that may cause undesired operations.

This equipment complies with FCC Part 15 for Home and Office use.

Caution to the User: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Radio and Television Interference:

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

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

UL Listing/CUL Listing:

This information technology equipment is UL Listed and C-UL Listed for both the US and Canadian markets respectively for the uses described in the User Guide. Use this product only with UL Listed Information Technology Equipment (ITE).

For Canadian Users

Industry Canada (IC)

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled Digital Apparatus, ICES-003 of Industry Canada.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

CE

CE Compliance

Declaration of Conformity

We, U.S. Robotics Corporation of 935 National Parkway, Schaumburg, Illinois, 60173-5157 USA, declare under our sole responsibility that the product, U.S. Robotics Serial ATA 4-Drive NAS, Model 8700, to which this declaration relates, is in conformity with the following standards and/or other normative documents.

EN60950-1
EN55022
EN55024
EN61000-3-2
EN61000-3-3

We hereby declare that the above named product is in conformity with the essential requirements and other relevant provisions of Directives 89/336/EC and 73/23/EC

An electronic copy of the original CE Declaration of Conformity is available at U.S. Robotics website: www.usr.com

U.S. Robotics Corporation Two (2) Year Limited Warranty

1.0 GENERAL TERMS:

1.1 This Limited Warranty is extended only to the original end-user purchaser (CUSTOMER) and is not transferable.

1.2 No agent, reseller, or business partner of U.S. Robotics Corporation (U.S. ROBOTICS) is authorised to modify the terms of this Limited Warranty on behalf of U.S. ROBOTICS.

1.3 This Limited Warranty expressly excludes any product that has not been purchased as new from U.S. ROBOTICS or its authorised reseller.

1.4 This Limited Warranty is only applicable in the country or territory where the product is intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

1.5 U.S. ROBOTICS warrants to the CUSTOMER that this product will be free from defects in workmanship and materials, under normal use and service, for TWO (2) YEARS from the date of purchase from U.S. ROBOTICS or its authorised reseller.

1.6 U.S. ROBOTICS sole obligation under this warranty shall be, at U.S. ROBOTICS sole discretion, to repair the defective product or part with new or reconditioned parts; or to exchange the defective product or part with a new or reconditioned product or part that is the same or similar; or if neither of the two foregoing options is reasonably available, U.S. ROBOTICS may, at its sole discretion, provide a refund to the CUSTOMER not to exceed the latest published U.S. ROBOTICS recommended retail purchase price of the product, less any applicable service fees. All products or parts that are exchanged for replacement will become the property of U.S. ROBOTICS.

1.7 U.S. ROBOTICS warrants any replacement product or part for NINETY (90) DAYS from the date the product or part is shipped to Customer.

1.8 U.S. ROBOTICS makes no warranty or representation that this product will meet CUSTOMER requirements or work in combination with any hardware or software products provided by third parties.

1.9 U.S. ROBOTICS makes no warranty or representation that the operation of the software products provided with this product will be uninterrupted or error free, or that all defects in software products will be corrected.

1.10 U.S. ROBOTICS shall not be responsible for any software or other CUSTOMER data or information contained in or stored on this product.

2.0 CUSTOMER OBLIGATIONS:

2.1 CUSTOMER assumes full responsibility that this product meets CUSTOMER specifications and requirements.

2.2 CUSTOMER is specifically advised to make a backup copy of all software provided with this product.

2.3 CUSTOMER assumes full responsibility to properly install and configure this product and to ensure proper installation, configuration, operation and compatibility with the operating environment in which this product is to function.

2.4 CUSTOMER must furnish U.S. ROBOTICS a dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) for any warranty claims to be authorised.

3.0 OBTAINING WARRANTY SERVICE:

3.1 CUSTOMER must contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre within the applicable warranty period to obtain warranty service authorisation.

3.2 Customer must provide Product Model Number, Product Serial Number and dated Proof of Purchase (copy of original purchase receipt from U.S. ROBOTICS or its authorised reseller) to obtain warranty service authorisation.

3.3 For information on how to contact U.S. ROBOTICS Technical Support or an authorised U.S. ROBOTICS Service Centre, please see the U.S. ROBOTICS corporate Web site at: www.usr.com

3.4 CUSTOMER should have the following information / items readily available when contacting U.S. ROBOTICS Technical Support:

- Product Model Number
- Product Serial Number
- Dated Proof of Purchase
- CUSTOMER contact name & telephone number
- CUSTOMER Computer Operating System version
- U.S. ROBOTICS Installation CD-ROM
- U.S. ROBOTICS Installation Guide

4.0 WARRANTY REPLACEMENT:

4.1 In the event U.S. ROBOTICS Technical Support or its authorised U.S. ROBOTICS Service Centre determines the product or part has a malfunction or failure attributable directly to faulty workmanship and/or materials; and the product is within the TWO (2) YEAR warranty term; and the CUSTOMER will include a copy of the dated Proof of Purchase (original purchase receipt from U.S. ROBOTICS or its authorised reseller) with the product or part with the returned product or part, then U.S. ROBOTICS will issue CUSTOMER a Return Material Authorisation (RMA) and instructions for the return of the product to the authorised U.S. ROBOTICS Drop Zone.

4.2 Any product or part returned to U.S. ROBOTICS without an RMA issued by U.S. ROBOTICS or its authorised U.S. ROBOTICS Service Centre will be returned.

4.3 CUSTOMER agrees to pay shipping charges to return the product or part to the authorised U.S. ROBOTICS Return Centre; to insure the product or assume the risk of loss or damage which may occur in transit; and to use a shipping container equivalent to the original packaging.

4.4 Responsibility for loss or damage does not transfer to U.S. ROBOTICS until the returned product or part is received as an authorised return at an authorised U.S. ROBOTICS Return Centre.

4.5 Authorised CUSTOMER returns will be unpacked, visually inspected, and matched to the Product Model Number and Product Serial Number for which the RMA was authorised. The enclosed Proof of Purchase will be inspected for date of purchase and place of purchase. U.S. ROBOTICS may deny warranty service if visual inspection of the returned product or part does not match the CUSTOMER supplied information for which the RMA was issued.

4.6 Once a CUSTOMER return has been unpacked, visually inspected, and tested U.S. ROBOTICS will, at its sole discretion, repair or replace, using new or reconditioned product or parts, to whatever extent it deems necessary to restore the product or part to operating condition.

4.7 U.S. ROBOTICS will make reasonable effort to ship repaired or replaced product or part to CUSTOMER, at U.S. ROBOTICS expense, not later than TWENTY ONE (21) DAYS after U.S. ROBOTICS receives the authorised CUSTOMER return at an authorised U.S. ROBOTICS Return Centre.

4.8 U.S. ROBOTICS shall not be liable for any damages caused by delay in delivering or furnishing repaired or replaced product or part.

5.0 LIMITATIONS:

5.1 THIRD-PARTY SOFTWARE: This U.S. ROBOTICS product may include or be bundled with third-party software, the use of which is governed by separate end-user license agreements provided by third-party software vendors. This U.S. ROBOTICS Limited Warranty does not apply to such third-party software. For the applicable warranty refer to the end-user license agreement governing the use of such software.

5.2 DAMAGE DUE TO MISUSE, NEGLECT, NON-COMPLIANCE, IMPROPER INSTALLATION, AND/OR ENVIRONMENTAL FACTORS: To the extent permitted by applicable law, this U.S. ROBOTICS Limited Warranty does not apply to normal wear and tear; damage or loss of data due to interoperability with current and/or future versions of operating system or other current and/or future software and hardware; alterations (by persons other than U.S. ROBOTICS or authorised U.S. ROBOTICS Service Centres); damage caused by operator error or non-compliance with instructions as set out in the user documentation or other accompanying documentation; damage caused by acts of nature such as lightning, storms, floods, fires, and earthquakes, etc. Products evidencing the product serial number has been tampered with or removed; misuse, neglect, and improper handling; damage caused by undue physical, temperature, or electrical stress; counterfeit products; damage or loss of data caused by a computer virus, worm, Trojan horse, or memory content corruption; failures of the product which result from accident, abuse, misuse (including but not limited to improper installation, connection to incorrect voltages, and power points); failures caused by products not supplied by U.S. ROBOTICS; damage cause by moisture, corrosive environments, high voltage surges, shipping, abnormal working conditions; or the use of the product outside the borders of the country or territory intended for use (As indicated by the Product Model Number and any local telecommunication approval stickers affixed to the product).

5.3 TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. U.S. ROBOTICS NEITHER ASSUMES NOR AUTHORISES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, WARRANTY, OR USE OF ITS PRODUCTS.

5.4 LIMITATION OF LIABILITY. TO THE FULL EXTENT ALLOWED BY LAW, U.S. ROBOTICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF U.S. ROBOTICS OR ITS AUTHORISED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT U.S. ROBOTICS OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

6.0 DISCLAIMER:

Some countries, states, territories or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to CUSTOMER. When the implied warranties are not allowed by law to be excluded in their entirety, they will be limited to the TWO (2) YEAR duration of this written warranty. This warranty gives CUSTOMER specific legal rights, which may vary depending on local law.

7.0 GOVERNING LAW:

This Limited Warranty shall be governed by the laws of the State of Illinois, U.S.A. excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

U.S. Robotics Corporation
935 National Parkway
Schaumburg, IL, 60173
U.S.A.