Altos easyStore

User's Manual

acer

ALTOS EASYSTORE

User's Manual
Version 1.2

Appendix A: Software Specifications

Appendix B: Configurations

Appendix C: Hardware Specifications

Technical Assistance

Glossary

Preface

This guide provides you with the following information:

l   An overview of the Altos easyStore and instructions for setting it up to provide shared storage space to users in your network

l   Information about advanced features for configuring your storage system

l   Instructions for installing and using DiskSafe^{TM} Express to back up your networked computer disks to the storage system and recover that data as needed

l   Reference material about product specifications and troubleshooting

Documentation conventions

l   **Bold** is used to indicate menu items, buttons, labels, and file and folder names.

l   Instructions to click a series of menu items are indicated with an arrow (-->).

For example, the instructions to click the **Start** menu, click **Programs**, and then click **Storage System Console** are presented as **Start** --> **Programs** --> **Storage System Console**.

l   When you see two keys joined by a plus sign (+), press and hold down the first key, and then press the second key. For example, Alt+F2 indicates that you should press and hold down the Alt key and then press F2.

l   Significant information or exceptions are indicated with the note icon shown at the left.

l   The potential for data loss or corruption is indicated with the caution icon shown at the left.

l   The term *Windows* refers to any supported Microsoft® Windows® operating system.

Related documentation

In addition to this guide, you can find information about DiskSafe Express in the online help. To access the online help, click **Help** --> **Help Topics** in the DiskSafe Express application window.

Introducing Your Storage System

<div align="right">

1

</div>

ALTOS EASYSTORE is an intelligent network storage solution for small and medium-sized offices and home network environments. It provides up to 2 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.

What your package includes

Before you begin using your storage system, please make sure that your package includes the following items:

- The Altos easyStore unit

- One power cord

- One RJ-45 Ethernet cable

- Installation CD (for the Storage System Console and DiskSafe Express)

- DiskSafe Express recovery CD

If any of these items are missing, please contact the reseller or retailer from which you purchased this product.

Additional accessories

The storage system supports up to two USB disks, which can be purchased separately.

Notes:

l   Only USB disks are supported. USB hubs and other USB devices are not supported.

l   Any USB disk must be formatted before you can use it with the storage system, and only the first partition of a FAT or FAT32 file system will be recognized.

l   Do not use a USB cable to attach the storage system directly to a USB port on a computer.

Key features and benefits

l   **Flexible storage capacity**—The storage system supports up to four 3.5" SATA-I hard disks, with a capacity of 250–500 GB each.

l   **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 Appendix B, "Disk Configurations."

l   **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.

l   **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.

l   **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.

l   **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.

l   **Fast performance**—With its gigabit Ethernet support, the storage system provides fast access to the data you need, when you need it.

Getting Started 2

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

1. Set up your storage system.

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

2. Install the Storage System Console on a computer in the same subnet as your storage system and initialize the hard disks on your storage system.

   Initializing the hard disks involves installing the operating system and other software from a file on your installation CD to each of the hard disks in your storage system. (Altos easyStore comes already configured)

   For information about this step, refer to "Initializing your storage system."

3. Access the Web-based management interface (the Manager) and log in.

   For information about this step, refer to "Accessing the Manager" and "Logging in to the Manager."

4. Add users.

   This is necessary only if you're 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 information about this step, refer to "Adding users."

5. Create shared folders.

   By default, the storage system includes a shared folder named **public**.
   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 information about this step, refer to "Creating shared folders."

6.   Access the shared folders.

For information about this step, refer to "Accessing shared folders."

7.   Protect your computer hard disks.

This 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 information about this step, refer to Chapter 5, "Protecting Local Disks."

Initializing your storage system

Altos easyStore comes with four hard disks drive, they are already initialized. You must install the Storage System Console on a computer in the same subnet as your storage system and use that application to connect to the storage system.

Installing the Console

You can install the Console on any computer that runs one of the following operating systems:

l   Microsoft Windows Server 2003

l   Microsoft Windows XP

l   Microsoft Windows 2000 Professional, Server, or Advanced Server with Service Pack 2 or newer

> **Note:**   To access the storage system, the Console launches a Web browser, so the computer where you install the Console must have Microsoft Internet Explorer 6.0 or Firefox 1.06 or newer installed as well. In addition, one of those browsers must be your default browser. If you're not sure how to configure the default browser, refer to the documentation for your browser.

To install the Console:

1.   At a computer in the same subnet as your storage system, insert the installation CD into a CD-ROM drive.

2.   Start the setup utility for the Console.

3. On the welcome page, click **Next**.
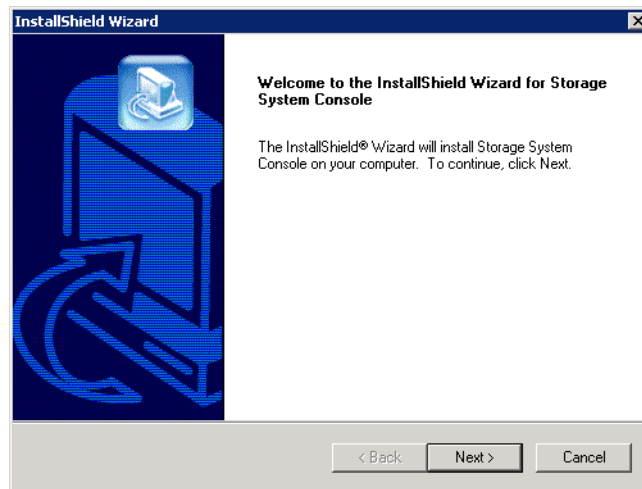
4. If you agree to the terms of the license agreement, click **Yes**.

5. Enter your name and company name and then click **Next**.

6. Click **Next** to install the Console in the displayed location, or click **Browse** to select or specify a different location and then click **Next**.
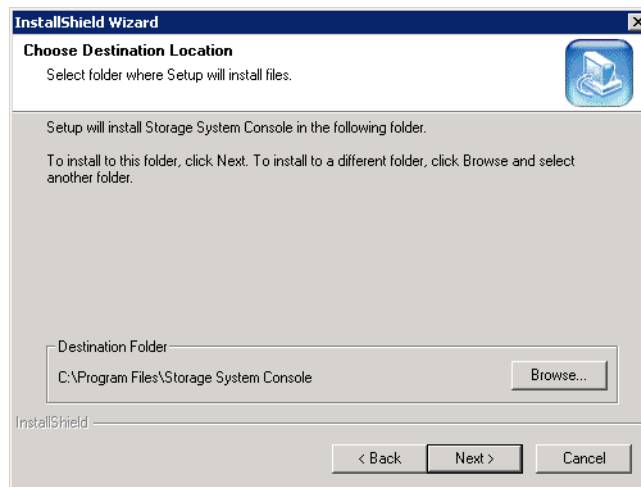
7. Review your selections and click **Next**.
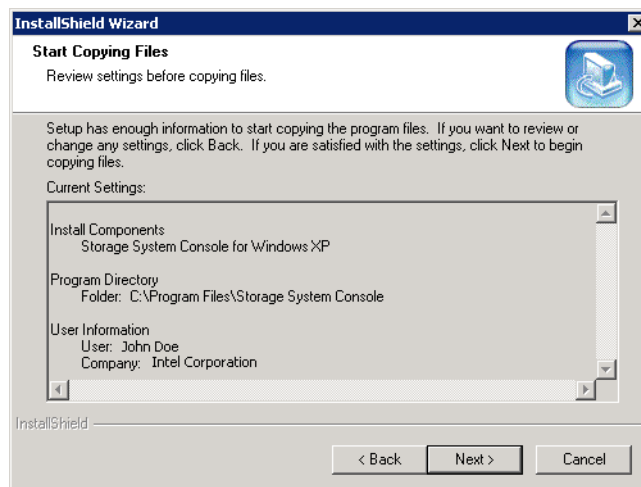
8.   To install the Console, click **Finish**.
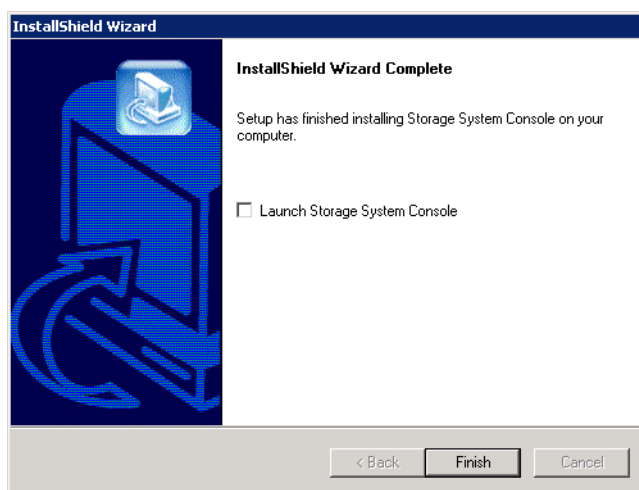
If you want to start the Console immediately after it is installed, select the **Launch Storage System Console** check box before you click **Finish**.

Starting the Console

Once you have installed the Console (as described in "Installing the Console"), you can use the following procedure to start it.

> **Note:**   If the storage system is not directly connected to your computer and your network does not have a DHCP server, you must change the IP address of your computer to use the same subnet as the storage system. (You can change it back after you have configured the storage system.)
>
> To do this, access your local area network properties. (For example, you might right-click **My Network Places** and click **Properties**, and then right-click your network connection and click **Properties**.) In the list, select **Internet Protocol (TCP/IP)** and click **Properties**. The IP address can be any address beginning with 192.168.0 except 192.168.0.101, since that's the IP address used by the storage system. The subnet mask must be 192.168.0.1. Then click **OK** to close each open dialog box.
>
> When you configure the storage system (as described in "Configuring your storage system"), you can specify whatever IP address you would like the storage system to use. If the IP address of the storage system is in a different subnet than your computer, you must also specify the gateway to use (as described in "Changing the network settings"). This ensures that you can manage the storage system from any computer using a Web browser (as described in "Accessing the Manager using a Web browser"). Then you can change your computer's IP address back to its original setting.

To start the Console:

1.   Click **Start** --> **Programs** --> **Storage System Console**.

     As soon as you start the Console, it automatically scans the network for storage systems. This might take a few minutes. As soon as the scan is complete, the left pane displays a tree view of all the storage systems it found.

![Storage System Console]

Note icon
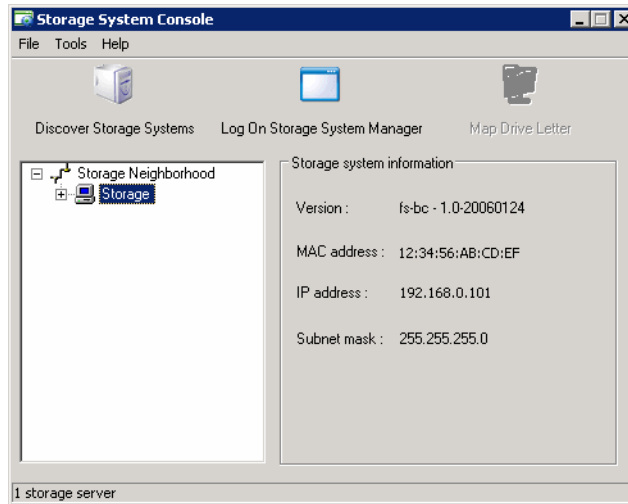
> **Note:** If you connect a storage system to the network after the Console has already scanned it, or if you subsequently change the IP address of the storage system, you must click **Discover Storage Systems** to scan the network again and update the tree in the left pane.
>
> If no storage system displays in the left pane, your computer might not be in the same subnet as the storage system. Be sure to install the Console on a computer in the same subnet as the storage system and try again.

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

   If your storage system uses both available ports to connect to the network, you can select either item.

3. If your storage system has not yet been initialized, the **System Initialization** page displays. For more information, refer to the next section, "Initializing the disks."

   If your storage system been initialized but not yet configured, the welcome page for the System Setup Wizard displays. For more information, refer to "Configuring your storage system".

   If your storage system has been initialized and configured, the login page for the Manager displays. For more information, refer to "Logging in to the Manager".

Initializing the disks

Once you have installed the Console (as described in "Installing the Console"), started it, and connected to the storage system (as described in "Starting the Console"), the **System Initialization** page displays:
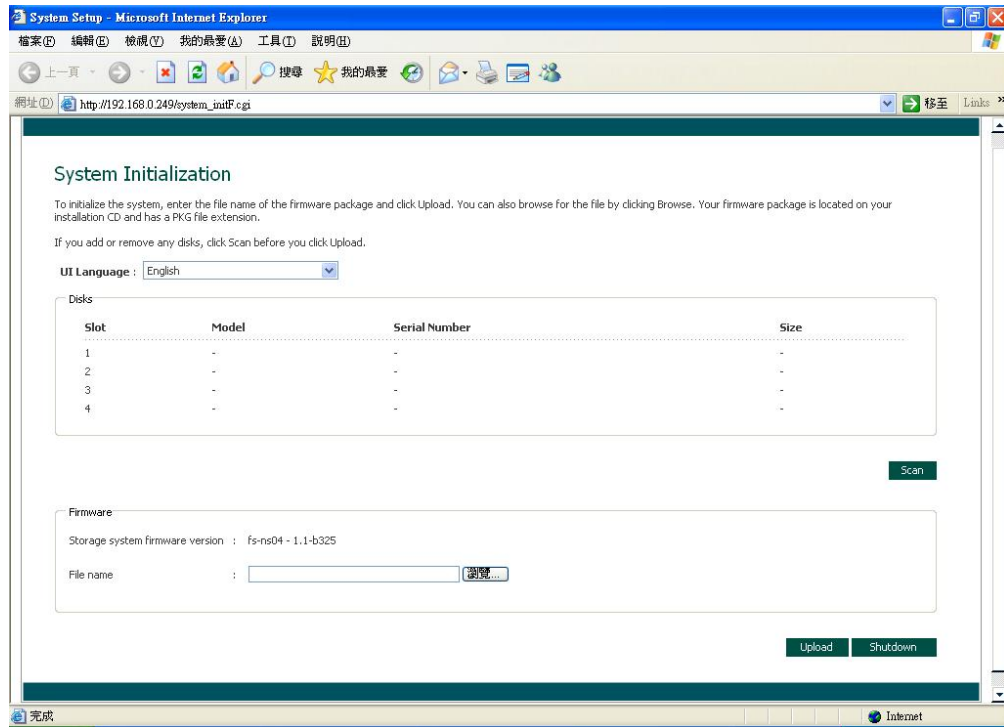
If all the hard disks have not been detected, or if you want to add, remove, or re-order the disks at this time, insert or remove the disks one at a time and click **Scan** after each action.

1.   Insert the installation CD into your computer's CD-ROM drive, type the path to the firmware package in the **File name** text box, and click **Upload**.

Alternatively, you can click **Browse** and browse the CD for the firmware package. The firmware package is the file on the CD that ends in the PKG file extension.

The firmware is uploaded to the hard disks. When this process is complete, the storage system restarts.

> **Note:** The operating system and storage system software are installed on each disk in your storage system to ensure that the failure or removal of any one disk will not cause the entire storage system to fail.

2. If the welcome screen does not appear immediately after the storage system restarts, close the browser window and log in again using the Console.

You can now perform initial configuration (as described in "Configuring your storage system")

Configuring your storage system

Once your storage system has been initialized (as described in "Initializing your storage system"), follow these steps to run the System Setup wizard and perform the necessary initial configuration:

1. If you have not already installed the Storage System Console, install it (as described in "Installing the Console") and start it (as described in "Starting the Console").

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

    The welcome page displays:
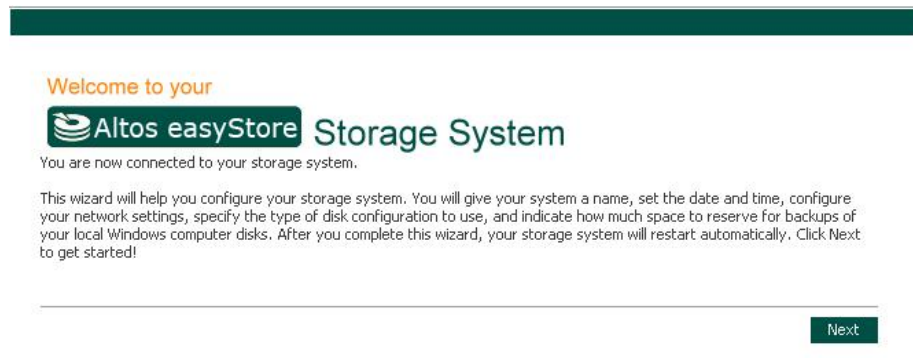
2. On the welcome page, click **Next**.

The **End User Software License Agreement** page displays:

3. If you agree to the terms, select the **I accept the license agreement** check box and then click **Next**.

The **Host Name** page displays:

4. Click **Next** to accept the default storage system name (**Storage**), or enter whatever name 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 displays:

System Setup : Date/Time

Please specify the current date and time

Date   : 10 ▾ / 11 ▾ / 2006 ▾ (Month / Day / Year)

Time   : 17 ▾ : 40 ▾ : 36 ▾ (Hour : Minute : Second)

Time zone : (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London ▾

[Back] [Next]

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

The time should be expressed in 24-hour format. For example, 2:00 P.M. would be entered as 14:00:00.

> **Note:**   The storage system time does not automatically change to reflect daylight savings time. To accommodate this, you can manually adjust the time as needed. For more information, refer to "Changing the system settings."

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

System Setup : Network Settings

If you have a DHCP server on your network, this server can get its IP address from that DHCP server automatically. If you don't have a DHCP server, you must use the default IP address or specify a different one.

If your network uses a different subnet mask, you can change the one shown here, but in most cases you can use the default subnet mask.

◉ Get an IP address automatically

◯ Use this IP address:

IP address   : 192 . 168 . 0 . 101

Subnet mask : 255 . 255 . 255 . 0

[Back] [Next]

6.   By default, if your network has a DHCP server, the storage system obtains its IP address from that server.

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

When you click **Next**, the **Disk Configuration** page displays. (The options that appear on this page vary, depending on the number of hard disks that are currently installed in the system.)
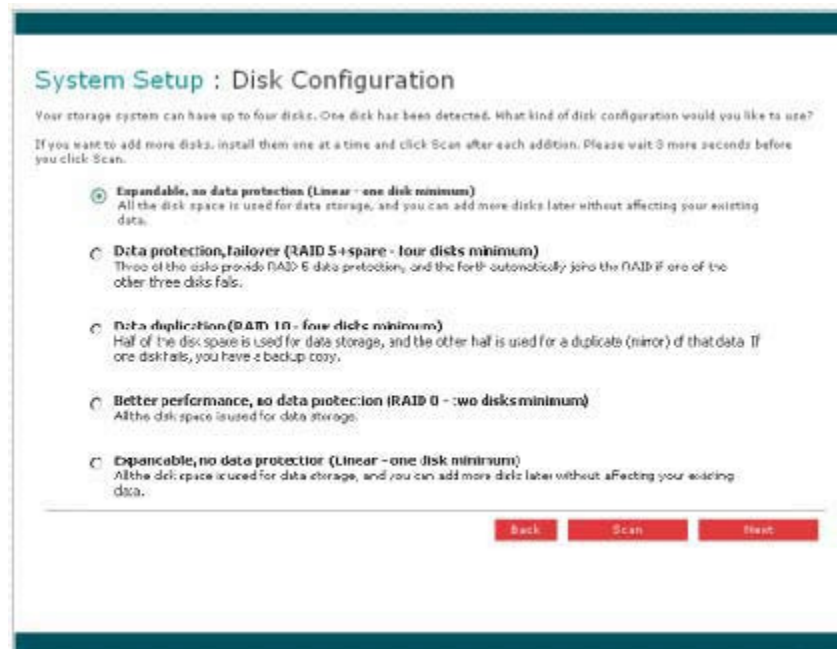
7.   If you want to add or remove hard disks, do so one at a time and click **Scan** after each action.

Note: It is strongly recommended 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.

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 want to change the disk configuration, select the desired RAID level and then click **Next**. (For detailed information about the different RAID levels, refer to Appendix B, "Disk Configurations.")

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

8. 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**.

    If you want 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 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.

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

    The **Configuration** page displays and the system is configured according to the settings you specified. Once the configuration is complete, the system restarts.
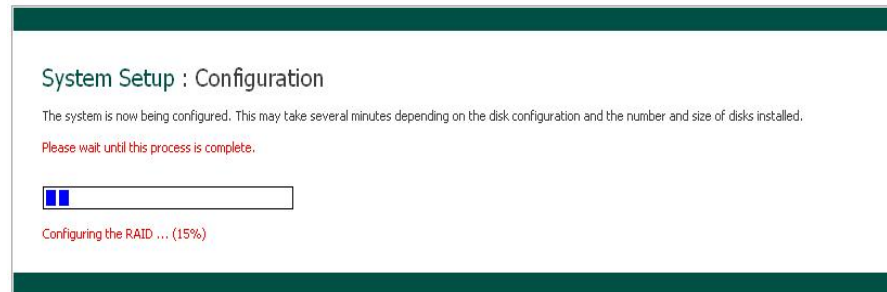
10. After the storage system restarts, you can access the Manager, add users, and create shared folders.

    For more information, refer to "Accessing the Manager", "Logging in to the Manager", "Adding users", and "Creating shared folders."

Accessing the Manager

Once you have initialized and configured your storage system (as described in "Initializing your storage system" and "Configuring your storage system"
), you can access the Manager to add users, create shared folders, and perform other tasks related to managing your storage system.

There are two ways to access the Manager:

l   Using the Console

l   Using a Web browser (Microsoft Internet Explorer 6.0 or Firefox 1.06 or newer)

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

Using a Web browser, you can access the Manager 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 Manager using a Web browser. First access the Manager using the Console and then specify the gateway address (as described in "Changing the network settings".) and try to access it using a Web browser.

Accessing the Manager using the Console

To access the Manager using the Console:

1.   If you have not already done so, install the Console on each computer from which you plan to manage the storage system (as described in "Installing the Console")

2.   Start the Console and connect to the storage system (as described in "Starting the Console").

3.   Log in to the Manager (as described in "Logging in to the Manager").

Accessing the Manager using a Web browser

To access the Manager using a Web browser:

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

   `https://`*`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 your computer is in the same subnet as the storage system, if you added the storage system's IP address and name to your local **hosts** file, or if you manually registered the name with a DNS server in your network.

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

2. Log in to the Manager (as described in "Logging in to the Manager").
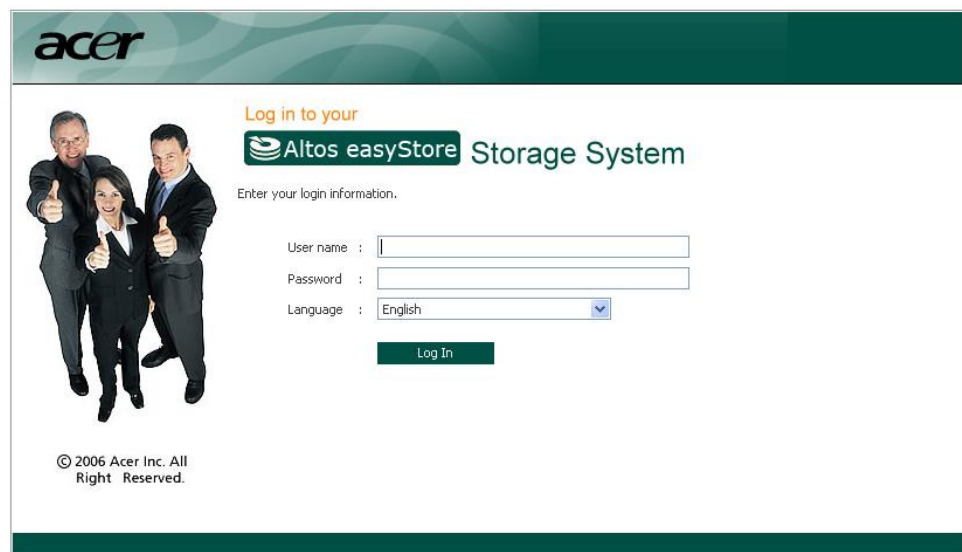
Logging in to the Manager

To ensure that your connection to the storage system is secure, the HTTPS protocol is used, and only individuals who know the administrator user name and password can view or change any of the storage system settings.

To log in to the Manager:

1. When the security alert displays, click **Yes**.

    The login page displays.

2. Enter the administrator user name and password.

    The default user name is **admin**, and the default password is **storage**. (These are case-sensitive.) Once you have logged in, you can change both the administrator user name and password at any time. For more information, refer to "Changing the system settings".

3. Click **Log In**.

Navigating the Manager

Once you log in to the Manager, the **Home** page displays:
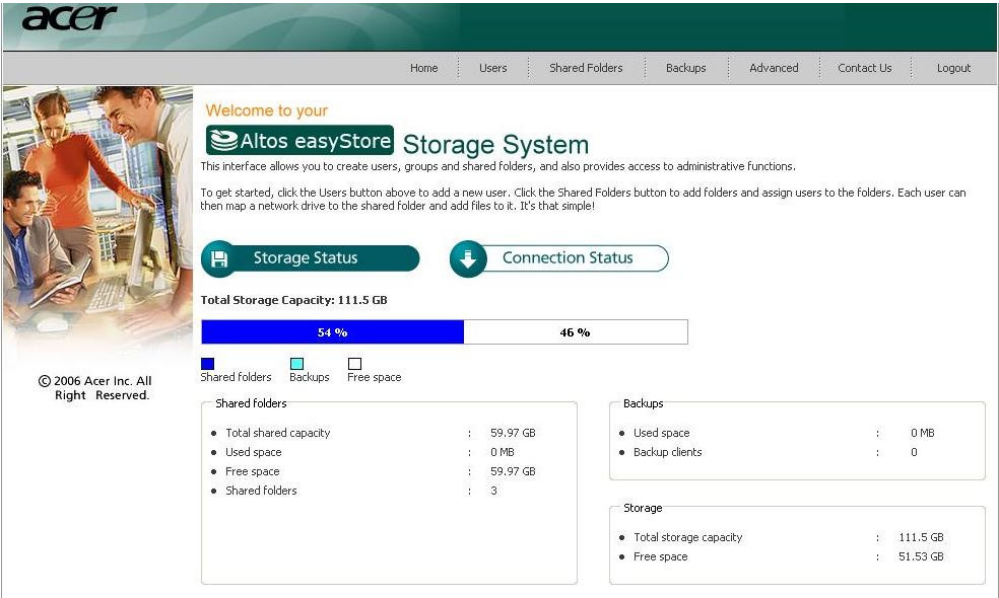
The top of the **Home** page (and every page in the Manager) displays a navigation bar that lets you access all the features of the storage system:

Home	Users	Shared Folders	Backups	Advanced	Contact Us	Logout
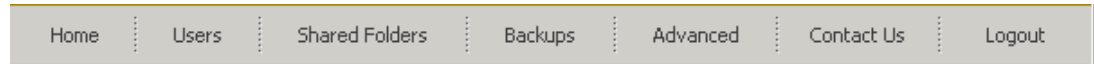
l   **Home**—Displays information about your storage system, including how the storage space is being used and which users are connected. For more information, refer to "Viewing information about your storage system"

l   **Users**—Displays a list of all currently configured users. If you're using local authentication mode, you can add, modify, and remove all types of users, and add, modify, and remove groups of Windows and Mac OS X users. If you're 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, refer to "Adding users", "Managing users", and "Changing the authentication mode".

l   **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, refer to "Creating shared folders" and "Managing shared folders".

l   **Backups**—Displays a list of all computer disk backups that currently exist and lets you change the recovery password, delete backups or a backup client, and change information related to booting remotely.

For more information, refer to "Managing backups" and Chapter 5, "Protecting Local Disks."

l   **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 the system status or system events; and shutting down the system remotely.

For more information, refer to Chapter 3, "Managing Your Storage System,"

l   **Contact Us**—Provides information about FalconStor and the other products and services it offers.

l   **Log Out**—Logs you out of the Manager.

Viewing information about your storage system

The **Home** page can display two different views: **Storage Status** and **Connection Status**. You can switch from one view to the other by clicking the desired button on the **Home** page.

l   **Storage Status**—Displays information about the total storage capacity on the storage system, how much disk space is allocated for shared folders, how much is currently used by backups, and how much is available for either. (Initially, there is no used backup space. The information on this page changes as each computer backs up its hard disks to the storage system. You might have to refresh the browser window to reflect these changes.)

This page also indicates how much of the storage space allocated for shared folders is actually used, the total number of shared folders, and the number of networked computers (backup clients) that have backed up one or more disks on the storage system.
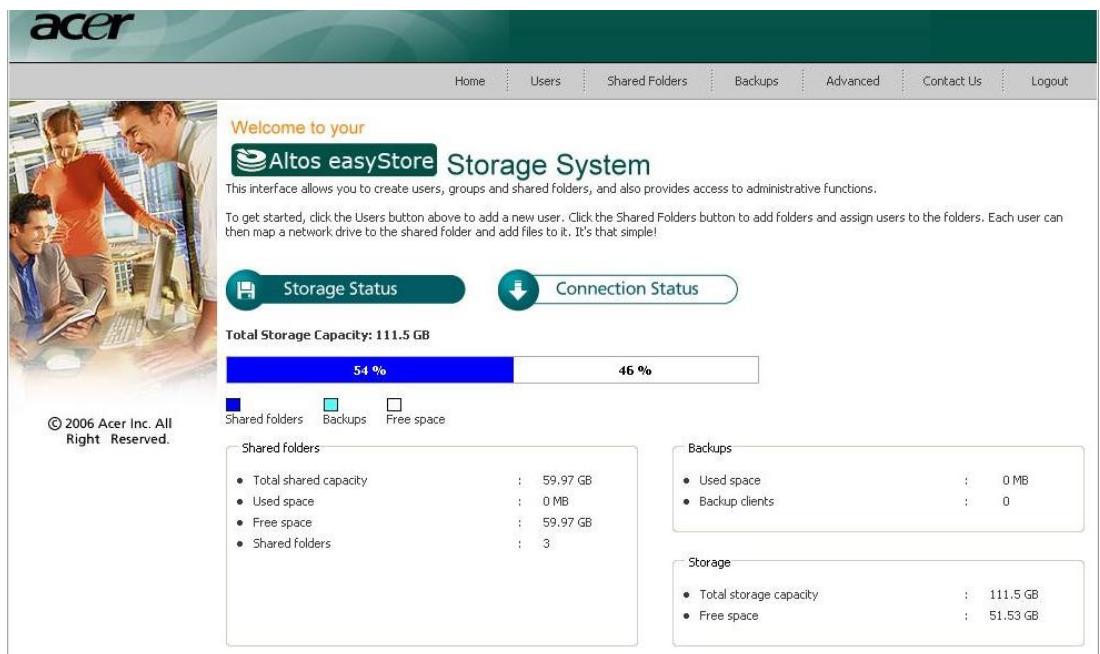
Note: The total storage capacity will be less than the total size of all your hard disks because some of the disk space is needed for the operating system and management software.

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.

l **Connection Status**—Displays a list of the 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.
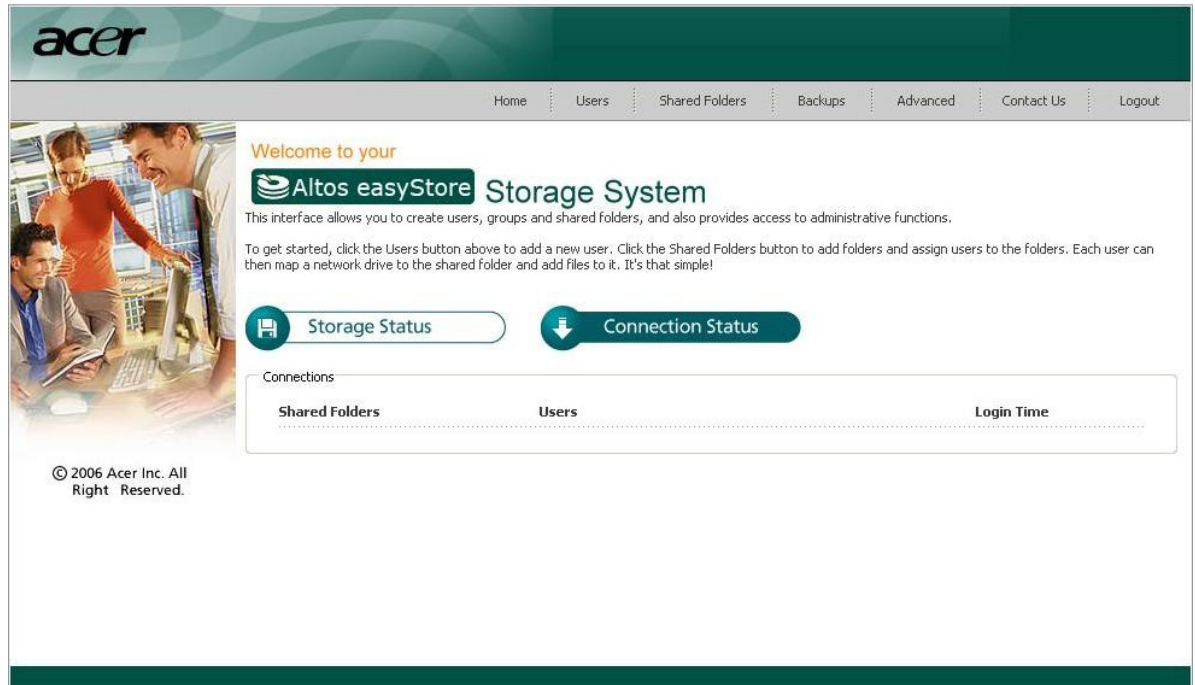
Notes:

l If anyone accessed a shared folder using the **guest** user name (which is described in more detail in "Adding users"), **guest** displays in the **Users** column, followed in parentheses by the computer name.

l Due to the nature of the NFS protocol, Linux and other Mac users are not listed on this page.

l Ongoing backup or recovery activities do not appear on this page.

l 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 there.

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"

In local authentication mode, by default the storage system includes a user named **guest** that has a password of **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.)

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 displays:

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)**.

    Notes:

    l   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.

    l   If your storage system uses Active Directory authentication mode, you can add only Linux/other Mac users.

The page that displays 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. It cannot begin with a period, contain spaces or a double period, or contain the following characters: **/ \ [ ] : ; | = , + * ? < > @ " ' # ~ ` % $**
	The password can be up to 24 characters long.
	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 the **Users** list. This description can be up to 15 characters long. It cannot contain the following characters: **/ \ [ ] : ; | = , + * ? < > @ " '**
	The **IP address or computer name** is the IP address or the actual computer name in the computer's system configuration. The computer name cannot contain spaces or the following characters: **Λ [ ] : ; | = , + * ? < > @ "**
	Note: You can create a single user that actually represents multiple computers. In the **IP address or computer name** text box, 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 displays 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.)

If you'd like to put Windows/Mac OS X users into groups, refer to "Working with groups."

Creating shared folders

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 "Assigning users to shared folders" on page 55). In Active Directory authentication mode, you must manually assign users to this folder in order to provide them with access.

You can 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.

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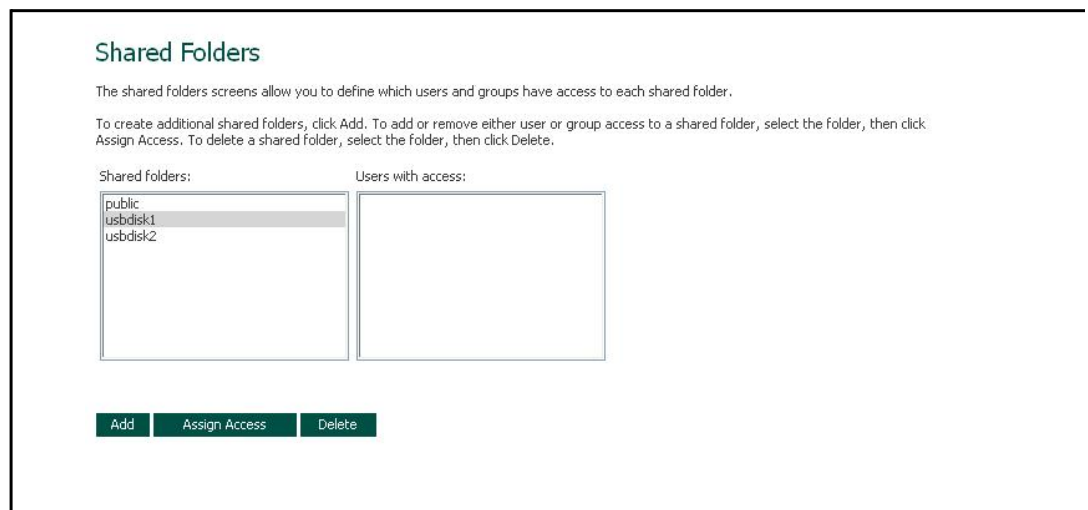
> **Note:** The **Shared folders** list includes **usbdisk1** and **usbdisk2**, whether or not any USB disks have been connected to the storage system.

2. Click **Add**.

3. In the **Shared folder name** text box, enter a unique name for the shared folder, and then click **Next**.

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

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

4. Select either the **CIFS**, **NFS** or **GROUP** tabs, check the **Assign** box for the user and select the radio button for either **RO** (read only) or **RW** (read/write) access.

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

.

To do this	Do this
Allow selected users to access to the shared folder or USB disk	Click the check box next to the user(s) name and change their access,
	Users with read-only access can only view the files in the shared resource; users with read/write access can view, add, modify, and delete folders and files in the shared resource.
	If you wish to cancel the selection, click the check box again to remove the check.

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 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).

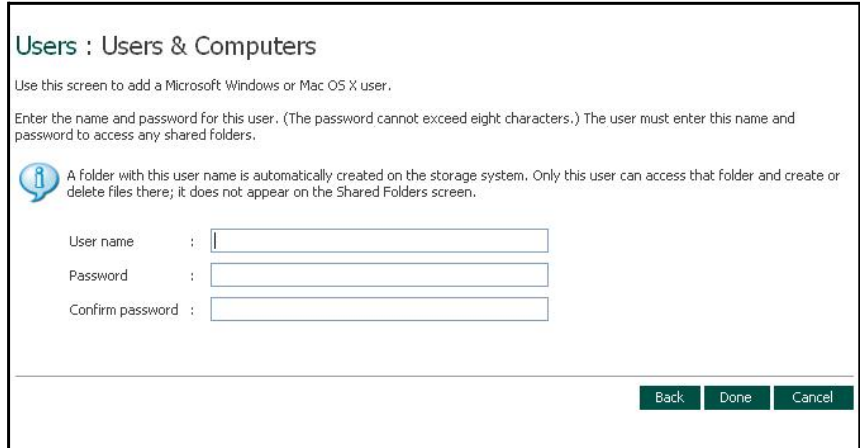> **Note:** Linux users and Mac users who are not using OS X access shared folders using NFS. In this environment, access to shared folders is given to entire computers, not to individual users of those computers. However, in Windows and Mac OS X environments, each computer user can have individual access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

> **Note:** If you created groups (as described in "Adding a group"), you can perform this step with the **Group Tab**.

> This tab will display all groups. For example, if you created a group named Group1, and added User2 and User3 to that group, by default, none of them will be assigned the 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.

5. When finished, click **Apply**.

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

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 display in the **Users with access** list. (For groups, the group name is preceded by an **@** symbol.)

Shared Folders

The shared folders screens allow you to define which users and groups have access to each shared folder.

To create additional shared folders, click Add. To add or remove either user or group access to a shared folder, select the folder, then click Assign Access. To delete a shared folder, select the folder, then click Delete.

Shared folders: Users with access:

```
public
usbdisk1
usbdisk2
```

```
Add     Assign Access     Delete
```

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. (You change the list of authorized users or their access rights). 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 can access them and what they can do with the subfolders and files there.

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 want to delete only selected subfolders or files, access the shared folder (as described in "Accessing shared folders") and delete the desired items.

Notes:

l   You cannot delete the **public** folder.

l   You cannot delete the contents of a USB disk using the **Shared Folders** page.

To remove the USB disk from the storage system, use the Manager to disconnect it.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 don't have 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 want to delete.

3. Click **Delete**.

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

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

Assigning users to shared folders

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

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

3. Click **Assign Access,** select the user that you want to assign and change the access level.

Although you can choose only one user type at a time, you can assign both types of users to the same shared folder.:

4. When finished, click **Apply** then **OK**.

5. To assign users of a different type, repeat this procedure, selecting the other user type in step 3.

Managing Your Storage System

<div style="text-align: right">3</div>

The Web-based storage system Manager enables you perform a number of tasks to help you get the most from your storage system:

l   Managing users—Add, modify, or remove users; put users into groups; or change the authentication mode.

l   Managing shared folders—Create shared folders, rename existing shared folders, change which users can access existing shared folders or their access rights, or delete shared folders that you no longer want to keep.

l   Managing backups—View which computer disks are backed up, change the password for recovering a backup, specify which backup to remotely boot from, or delete a backup or backup client.

l   Setting up e-mail alerts—Specify whether or not e-mail notifications should be sent when a problem occurs, and who should receive the notifications.

l   Upgrading the firmware—Upgrade your storage system firmware to the latest version.

l   Disconnecting USB devices—If you're using optional USB devices, you must disconnect them using the Manager before you physically unplug them.

l   Changing the system settings—Change the storage system name or time and date settings, as well as the user name or password for logging in to the Manager.

l   Changing the network settings—Change the workgroup name, the storage system's IP address, the gateway or DNS server settings, or the settings that allow the storage system to act as a DHCP server or FTP server.

l   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.

l   Viewing system status information—See details about CPU and memory usage, how long the storage system has been running, disk temperatures, etc.

l   Logging out of the Manager—Log out of the Manager so that no one else can use your computer to make changes to the storage system.

l   Shutting down the storage system—Shut down the storage system using the Manager 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 displays. This page displays a list of all currently configured Windows and Mac OS X users, as well as all Linux and other Mac computers. (In this guide, the term *user* refers to both individuals and computers.)
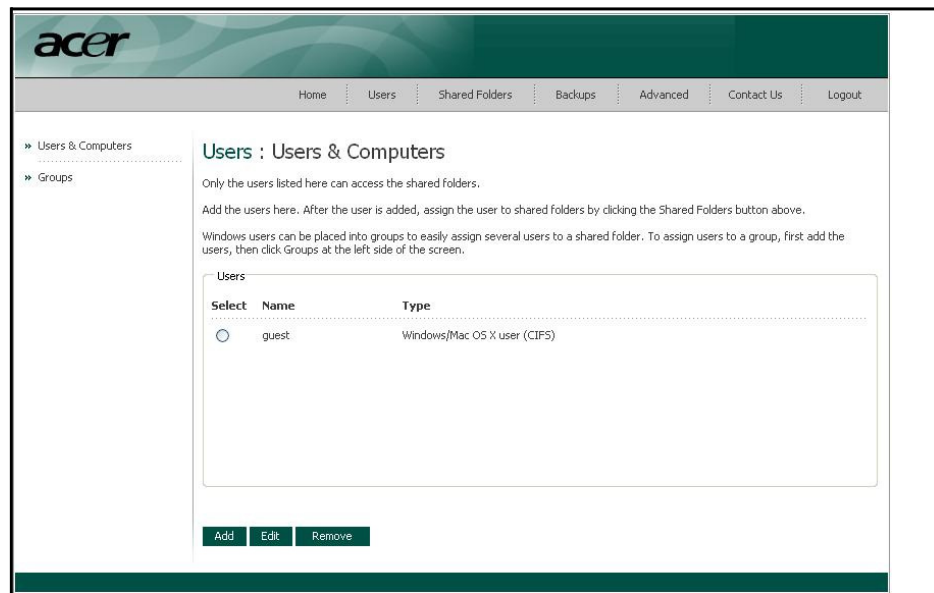
By default, the storage server uses local authentication mode, which means that you can add, modify, or remove all types of users at any time. If you're using Active Directory authentication mode, you can add, modify, or remove Linux or other Mac users, but not Windows users. All Windows users are controlled entirely by the Active Directory server. (For more information about authentication modes, refer to "Changing the authentication mode.")

If you're 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're using Active Directory authentication mode, you cannot create groups using the Manager. All groups are controlled entirely by the Active Directory server.)

Adding users

To add a user, refer to "Adding users".

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/Mac OS X users, only Linux/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", and then add a new user with the desired name or description as described in "Adding users"

To modify a user:

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

2. Select the radio button next to the user that you want to modify.

3. Click **Edit**.

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

The page that displays 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 the **IP address or computer name** text box, 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 an remove any Linux user or any Mac user not running Mac OS X, but you cannot remove any Windows/Mac OS X user. Those 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.

To remove a user:

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

2.   Select the radio button next to the user that you want to remove.

3.   Click **Remove**.

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

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

The user no longer displays 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.
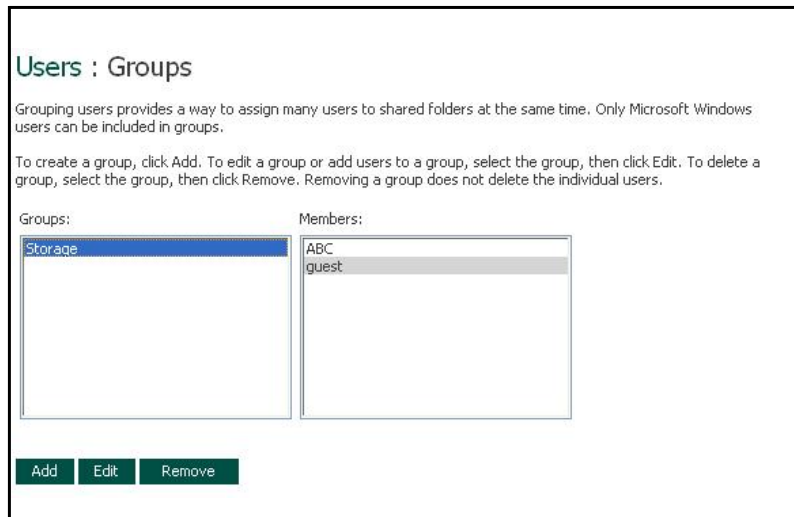
If you're using local authentication mode, you can add a group, modify the group membership, or remove groups at any time. If you're using Active Directory authentication mode, you can view the group membership but not add, modify, or remove groups. Those actions can be done only on the Active Directory 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" 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**.

![Users : Groups dialog box]

Users : Groups

Grouping users provides a way to assign many users to shared folders at the same time. Only Microsoft Windows users can be included in groups.

Enter the name of the group. This name can be up to 15 characters long and can contain letters (uppercase and lower case A-Z), numbers (0-9), hyphens (-), and underlines (_).

To add users to the group, select the users in the right column, then click Add Selected User(s). To add all users to the group, click Add All Users. To delete users from this group, select the user(s) from the left column, then click Remove Selected User(s). To delete all of the users from this group, click Remove All Users.

Group name   :

Groups members: Available users:
                                                         ABC
                                                         guest
                            « Add All Users
                          « Add Selected User(s)
                          Remove All Users »
                        Remove Selected User(s) »

                                                              OK   Cancel

Note: If the storage system uses Active Directory authentication mode, this button displays dimmed.

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

    This name can be up to 15 characters long and can include letters, numbers, hyphens, and 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 the **Available users** list to the **Group members** list.
Add selected users to the group	In the **Available users** list, select the user(s) that you want to add and then click **Add Selected User(s)**.[a]
Remove all users from the group	Click **Remove All Users**. All users move from the **Group members** list to the **Available users** list.
Remove selected users from the group	In the **Group members** list, select the user(s) that you want to remove from the group and then click **Remove Selected User(s)**.[a]

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.

1. 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 the **Groups** list, select the group whose membership you want to change.

4. Click **Edit**.

![Users : Groups dialog]

Users : Groups

If you're using local authentication mode, grouping users provides a way to assign many users to shared folders at the same time

If you're using Active Directory authentication mode, you can't add groups here; they are added automatically from your Active D

Current authentication mode : Local authentication mode

Groups: Members:

Acer   guest

Add   Edit   Remove

> **Note:**   If the storage system uses Active Directory authentication mode, this button displays 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 the **Available users** list, select the user(s) that you want 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 the **Group members** list, select the user(s) that you want to remove from the group and then click **Remove Selected User(s)**.[a]

[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

In local authentication mode, 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. (In Active Directory authentication mode, you cannot remove a group on the storage system. That can be done only on the Active Directory server.)

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

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

On the other hand, if the Executives group had read/write access to the Budget shared folder, but Alice had read-only access, when you remove the group, Bob and Carlos will no longer have access to the Budget shared folder (since their access rights were determined by their group membership), but Alice will continue to have read-only access, since that access right was granted to her on a user level.

To remove a group:

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

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

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

4.   Click **Remove**.

> **Note:**   If the storage system uses Active Directory authentication mode, this button displays dimmed.

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

The group no longer displays in the **Groups** list.

Changing the authentication mode

Your storage system can operate in one of two modes:

l   Local authentication mode

l   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 (both Windows/Mac OS X and Linux/other Mac users). By default, the storage system uses local authentication mode.

In Active Directory authentication mode, the Active Directory server authenticates all Windows users who try to connect to shared folders. You can add, modify, or remove Linux /other Mac users, but not Windows users. In addition, you cannot create groups. All Windows users and groups are controlled entirely by the Active Directory server.

✎   **Notes:**

l   The authentication mode has no effect on backups performed using DiskSafe Express.

l   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.

l   If you use Active Directory authentication mode, you must add any Mac OS X users to your Active Directory server in order to provide those users with access to shared folders on the storage system.

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

l   If you use 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 whenever the storage system tries to connect to the Active Directory server (that is, when you set the authentication mode, when synchronization between the two systems occurs, and when users access shared folders). You must adjust the storage system time, time zone, or both to ensure that they match (as described in "Changing the system settings").

   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 savings 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.

You can change the authentication mode at any time, but you must provide the administrator password 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 the **Administrator password** text box, enter the password for accessing the storage system.

4.   Click **Change Authentication Mode**.

     The **Authentication Mode** page displays.

5. If you're currently using Active Directory authentication mode, **Local authentication mode** is selected by automatically, and **Active Directory authentication mode** displays dimmed. Click **Finish**. All your existing user data and user assignments are deleted, and you can add new users (as described in "Adding users") and assign them to shared folders (as described in "Assigning users to shared folders").

    If you're currently using local authentication mode, **Active Directory authentication mode** is selected automatically, and **Local authentication mode** displays dimmed. Click **Next**. The **Active Directory Server** page displays.

    Users : Active Directory Server

    Enter the IP address of your primary Active Directory server. If desired, you can also enter the IP address of the secondary Active Directory server to use if the primary Active Directory server is not available.

    Primary server IP address   :
    Secondary server IP address :

    Next

6. In the **Primary server IP address** text box, enter the IP address of your primary Active Directory server. (You cannot use the server's name.)

7. If desired, enter the IP address of a secondary Active Directory server in the **Secondary server IP address** text box. (You cannot use the server's name.) This server will be used if the primary Active Directory server is not available.

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

8. Click **Next**.

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

    Users : Active Directory User Login

    Enter the name and password of a user who has privileges to access the Active Directory tree.

    If desired, enter the name of the organizational unit that contains the users or groups that will be allowed to access the shared folders on the storage system. If you leave the organizational unit name blank, you can browse the entire tree.

    User name   :   @FFF.COM
    Password   :
    Organizational unit name :   Example:/Sales

    Back   Next

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

    When accessing the Active Directory server, this name will be appended with the fully qualified domain name shown on this page.

10. In the **Password** text box, enter the password associated with the specified user name.

11. If you want 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 the **Organizational unit name** text box (up to 256 characters). This unit must not have more than 100 subunits, and the name must be preceded by a forward 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 either 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 here, 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 displays.

Users : Active Directory Tree

Select the organizational units that contain the users or groups that will be allowed to access the shared folders on the storage system. Selecting the forward slash mark(/) selects everyone in the tree.

Organizational units:

☐ /Users

[Back] [Next]

> **Note:**   If the storage system time and Active Directory server time differ by more than five minutes, an error message displays. You must adjust the storage system time, time zone, or both to ensure that they match (as described in "Changing the system settings").
>
> 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 savings 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.

12. 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 forward slash mark (/) selects everyone in the tree.

> **Note:**   Your storage system supports only 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 displays.

Users : Active Directory Administrator Login

Enter an administrator user name and password for accessing the Active Directory server. The Active Directory server will be automatically configured to allow the storage system to become a trusted member.

User name : administrator
Password   : ••••

Back   Finish

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

    This account will be 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.

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

All the current 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 "Assigning users to shared folders").

Modifying the Active Directory properties

If your storage system is currently using Active Directory authentication mode, an item called **Active Directory Properties** displays in the left pane when you click **Users** in the navigation bar. When you click this item, you can change the IP address of your primary or secondary Active Directory server, the user name or password for browsing the Active Directory tree, and how frequently the storage system should synchronize with the Active Directory server.

To modify the Active Directory properties:

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

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

    This item displays only if you are currently using Active Directory authentication mode. To determine which mode you're currently using, click **Authentication Mode** in the left pane and observe the mode specified in the right pane.

    When you click **Authentication Directory Properties**, the **Update Authentication Mode** page displays.

3. Make the desired changes, if any, and click **Apply**:

To change this	Do this
The IP address of the primary Active Directory server	In the **Primary server IP address** text box, enter the IP address of your primary Active Directory server. (You cannot use the server's name.) **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").
The IP address of the secondary Active Directory server	In the **Secondary server IP address** text box, 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.
The user name or password for browsing the Active Directory tree	In the **User name** text box, enter the name of a user who has privileges to access the Active Directory tree. In the **Password** text box, enter the password associated with that user name. This user name and password will be used to obtain new user and group information from the Active Directory server at every synchronization.
The number of minutes between synchronizations	In the **Synchronization interval (minutes)** text box, enter the number of minutes that should elapse between synchronizations. If this interval is too short, network traffic might be adversely affected. If this interval is too long, users whose passwords have changed might experience problems accessing shared folders.

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").

If you add a new user or group to the Active Directory server and don't want 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 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, click either **Users & Computers** or **Groups**.

3. Click **Synchronize**.

    The page displays the progress of the synchronization.

    Notes:

    l   Your storage system supports only 128 users and 128 groups. If the selected organizational unit on your Active Directory server currently exceeds these maximums, the excess users or groups will not be added to the storage system.

    l   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").

    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 savings 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.

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 the **Users with access** list. (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. (You change the list of authorized users or their access rights). 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 can access them and what they can do with the subfolders and files there.

Creating shared folders

To create a shared folder, refer to "Creating shared folders"

Assigning users to shared folders

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

3. Click **Assign Access**.

4. Select the type of user that you want to assign, change the access level for, or remove, 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 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.

    Although you can choose only user type at a time, you can assign both types of users to the same shared folder.

The page that displays next varies, depending on which type of user you selected.

Windows/Mac OS X user (CIFS)

Linux/Other Mac user (NFS)

5.   Specify which users should be able to access this shared folder or USB disk, and then click **OK**:

To do this	Do this
Allow selected users to access to the shared folder or USB disk	In the **Unauthorized users** list, select the user(s) who should be able to access the shared resource and then click **Add (Read-Only)** or **Add (Read/Write)**.[a]
	Users with read-only access can only view the files in the shared resource; users with read/write access can view, add, modify, and delete folders and files in the shared resource.
Prevent selected users from accessing the shared folder or USB disk	In the **Authorized users** list, select the user(s) who should not be able to access the shared resource and then click **Remove**.[a]

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.

Notes:

l   To change the access level for a user, select the user in the **Authorized users** list and click **Remove**. Then select that user in the **Unauthorized users** list and click either **Add (Read-Only)** or **Add (Read/Write)**, depending on the access level you now want the user to have.

l   If you created groups (as described in "Adding a group"), you can perform this step with groups as well.

This page shows all groups and all users. For example, if you created a group named Group1, and added User2 and User3 to that group, the **Unauthorized groups** list includes Group1, and the **Unauthorized users** list includes User2 and User3. If you select Group1 and click **Add (Read-Only)**, Group1 moves to the **Authorized groups** list, but User2 and User3 do not move to the **Authorized users** list. This allows you to specify unique access rights for those users. For example, you could select User3 and click **Add (Read/Write)**. This 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.   To assign users of a different type, repeat this procedure, selecting the other user type in step 4.

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 want to delete only selected subfolders or files, access the shared folder (as described in "Accessing shared folders") and delete the desired items.

Notes:

l   You cannot delete the **public** folder.

l   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 "Assigning users to shared folders"), access the disk (as described in "Accessing shared folders"), and then delete the desired folders and files.

To remove the USB disk from the storage system, use the Manager to disconnect it (as described in "Disconnecting USB devices"). 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 don't have 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 want to delete.

3. Click **Delete**.

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

   The shared folder no longer displays in the **Shared folders** list, 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 Chapter 5, "Protecting Local Disks,"
), the **Backups** page displays a list of each computer that has done this, the size of each protected disk, the date and time of all available
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 ever has 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 to do so. The user had to provide this password when protecting the disk. However, if the user forgets it, you can reset the password using the Manager. (For information about recovering a disk using the recovery CD, refer to "Recovering a system disk using the recovery CD". For information about booting remotely, refer to "Recovering a system disk while booting remotely".)

For booting remotely, you can also specify the MAC address to use (if you want 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 Manager.

Changing the recovery password

To change the recovery password:

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

2. In **Computer name** list in the **Recovery passwords** group box, select the name of the computer whose recovery password you want to change.

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

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

4. Click **Change Password**.

5. When the confirmation message displays, 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"), no additional action is necessary on the storage system. However, if you want to remotely boot one computer from another computer's backup, you must change the MAC address. For example, if Computer1 has been infected by a virus, and all of its backups are also infected, you might want 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.

> **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 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 the **Computer name** list in the **Remote boot** group box, select the name of the computer whose backup you want to remotely boot from.

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

    Remote boot must have been previously enabled on that computer.

4. From the **Backup for booting remotely** list, select the time and date of the backup that you want 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.

Notes:

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

l   If the selected backup is deleted to make room for newer backups, the most recent backup will be used for booting remotely.

---

5. Click **Apply Boot Info**.

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

    If you changed the backup for booting remotely, an asterisk now displays 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 displays on the **Backups** page. However, that computer name remains in the storage system and counts toward the total number of computers that are allowed to back up to the storage system. If you want to delete all backups of all disks and the computer name, refer to the next section, "Deleting a client."

To delete all backups of a disk:

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

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

3. Click **Delete Backup**.

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

    The disk no longer displays on the **Backups** page, and all backup versions are deleted. If only one disk was protected, the computer name disdisplays 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" and "Protecting your disks".

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

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" and "Protecting your disks".

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 five minutes of the event. In addition, if the problem is fixed within that time frame—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 the **Send e-mail notifications** check box.

    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 have to complete the rest of this procedure; simply click **Apply**.

3. In the **SMTP server name or IP address** text box, 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 the **SMTP server authentication** check box.

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

    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 want the individuals who receive e-mail notifications to be able to reply to the alert, enter the address that you want to appear as the return address in the **Sender e-mail address** text box.

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

6. In the **First e-mail address** text box, 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 want e-mail notifications to be sent to other individuals as well, enter the appropriate e-mail addresses in the **Second e-mail address** and **Third e-mail address** text boxes.

8. Click **Apply**.
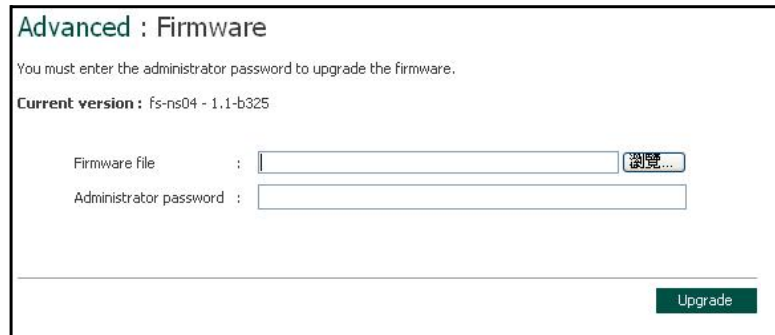
9. When the confirmation message displays, click **OK**.

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 have to modify the network settings (such as the gateway to use). For information about changing the network settings, refer to "Changing the network settings"

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 it if newer firmware becomes available.

Advanced : Firmware

You must enter the administrator password to upgrade the firmware.

Current version : fs-ns04 - 1.1-b325

Firmware file   :   [   ]   [瀏覽...]
Administrator password   :   [   ]

[Upgrade]

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

⚠️ **Caution:**

l   When you upgrade the firmware, the storage system restarts. Access to the Manager is temporarily interrupted, and users will not be able to access the shared folders during this process. If users have files open on the storage system, data might be lost. Be sure to have all users save their changes and close any open files before you upgrade the firmware.

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

l   If you upgrade from version 1.0 or 1.1, the personal folders (that is, the **home** folders) that were automatically created for each Windows or Mac OS X user will be deleted. If you want 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 the **Firmware file** text box, enter the path and file name for the firmware package (such as **D:\fs-bc - 1.2-b507.pkg**), or click **Browse** and select the file from the displayed list.

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

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

To disconnect a USB device:

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

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

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

4. Click **Disconnect**.

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

    You can now unplug the USB device.

    Note: If you inadvertently disconnect a USB device that you want to retain, unplug it from the storage system, plug it back in, and then click **Scan**. This reactivates the USB device.

    Since the USB device always remains on the **Shared Folders** page, any user assignments are always retained.

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.

In local authentication mode, you can change any of these settings at any time. In Active Directory authentication mode, you can change any of these settings except the storage system name. You can also change the administrator name and password to use for logging in to the Manager.

To change any of the system settings:

1. 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 the **Storage system name** text box, 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.
The system date, time, or time zone	In the **Date** fields, enter or select the desired month, date, and year.
	In the **Time** field, enter or select the desired hour, minute, and second.
	In the **Time zone** list, select the desired time zone.
	Note: The storage system time does not automatically change to reflect daylight savings time. To accommodate this, you can manually adjust the time and/or time zone as needed.
Network Time Protocol (NTP) server name or IP address	In the **NTP server name or IP address** text box, enter the name or IP address of the NTP 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 the **Administrator name** text box, enter the user name to use for logging in to the Manager.
	In the **Password** and **Confirm password** text boxes, enter the password to use for logging in to the Manager. It cannot contain multi-byte words. This means you can only enter ASCII character whose code value is less than 128.
	The user name and password are case-sensitive.

4. Click **Apply**.

5. When the confirmation message displays, 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:
>
> l   Access to the Manager will be temporarily disrupted. If you access the Manager using a Web browser and an IP address, you will need to use the new IP address. In addition, if you added the storage system's IP address to a local **hosts** file or DNS server, you must update the IP address in those resources.
>
> l   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")
>
> l   Users running DiskSafe Express must restart that application. If a backup or recovery was in progress and did not complete successfully, perform the action again.

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 and Mac OS X users to use a Web browser to access the **public** folder. For more information, refer to "Accessing shared folders using FTP".

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 the **Workgroup name** text box, enter the name of the workgroup. This name can be up to 15 characters long.
The IP address(es) 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 port on 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 the **Gateway IP address** text boxes. (This is typically the same IP address as the port, with the last number being 1.)
	If your network does not include a gateway, or if the port obtains its IP address from the DHCP server, leave these text boxes blank. (If the port 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 if the port on the storage system uses a specified IP address rather than obtaining one from the DHCP server, enter the primary IP address in the **Preferred DNS server** text boxes and the secondary IP address in the **Alternate DNS server** text boxes.
	If your network does not include a DNS server, or if the port obtains its IP address from the DHCP server, leave these text boxes blank. (If the port obtains its IP address from a DHCP server, the DNS server IP address will be obtained from the DHCP server as well.)
The DHCP settings	If you want 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 the **Enable DHCP server** check box, enter the beginning IP address in the **Starting IP address** text boxes, and enter the last IP address in the **Ending IP address** text boxes.
	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 want 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.)

To change this	Do this
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 the **Jumbo Frames** check box.
	If you clear this option, the storage system will use 1514-byte packets.
	If you select this option, you can specify a larger packet size (from 1514 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.
The FTP settings	If you want to use the storage system as an FTP server, select the **Enable FTP server** check box.
	If you do not want to use the storage system as an FTP server, clear this option.
	For information about accessing the storage system using FTP, refer to "Accessing shared folders using FTP".

4.   Click **Apply**.

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

> **Note:**   If you changed the IP address of the storage system, you must now access the Manager 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:

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

l   The overall status of the disks:

n   **Normal**—All the disks are working properly.

n   **Degraded**—One or more disks have failed but all the data is still available.

n   **Failed**—The storage system has stopped working properly.

l   The slot where each hard disk resides

l   The model number, serial number, and size of each hard disk

l   The current status of each disk:

   n   **Linear** or **RAID** *n*—The disk is working properly as part of the specified configuration.

   n   **New**—The disk has been added to the storage system but is not currently being used.

   n   **Spare**—The disk is acting as a spare disk for the RAID.

   n   **Rebuilding**—The disk is being rebuilt (for example, when a failed disk is replaced)

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

l   The hotplug indicator:

   n   **RED**—Removing the disk will cause the RAID to fail.

   n   **YELLOW**—Removing the disk will cause RAID degradation.

   n   **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 Appendix B, "Disk Configurations," beginning.

You can change the disk configuration or amount of 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.

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 your data. Therefore, it is recommended that you 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 the **Administrator password** text box, enter your password for logging in to the Manager.

4.   Click **Expand Shared Storage**.

The **Expand Shared Storage** page displays:

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 displays, click **OK**.

Reconfiguring the disks

⚠️   **Caution:**   Changing the disk configuration will delete all user information and all data on all the disks.

Before you do this, have all the users disconnect from all shared folders (as described in "Disconnecting from shared folders") and remove protection from all disks (as described in "Removing protection").

When you are done, you must re-add all users, create new shared folders, and have users once again protect their disks.

To change the disk configuration:

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

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

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

4. Click **Reconfigure Disks**.

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

    The **Disk Configuration** page displays. (The options that appear on this page vary, depending on the number of hard disks that are currently installed in the system.)
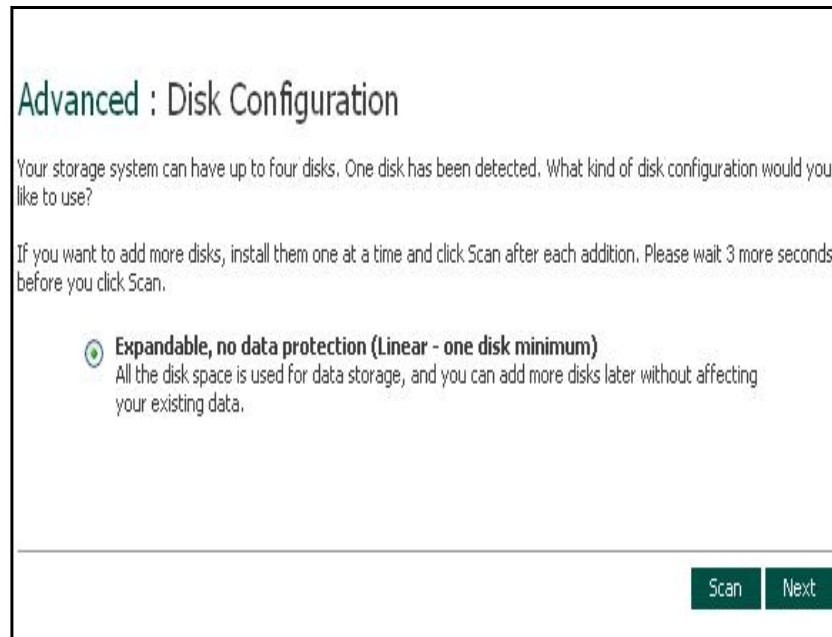
6. If you want to add or remove hard disks, do so one at a time and click **Scan** after each action.

    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 want to change the disk configuration, select the desired RAID level and then click **Next**. (For detailed information about the different RAID levels, refer to Appendix B, "Disk Configurations.")

The **Disk Space Distribution** page displays:

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**.

    If you want 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 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 displays, click **OK**.

The screen displays the progress of the process:
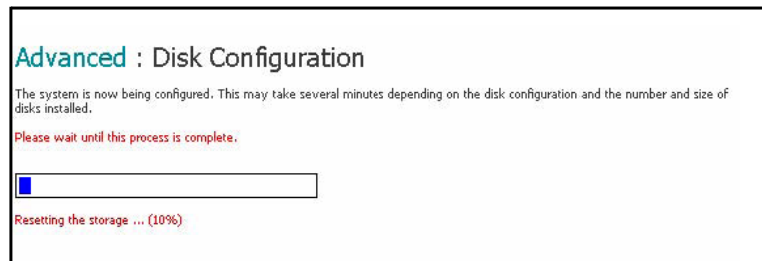
When this process is complete, the storage system restarts.
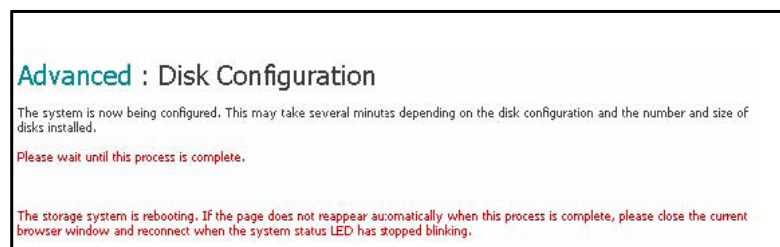
9. Close the browser window.

    After the system has restarted, you can access the Manager and re-create your users and shared folders (as described in "Adding users" and "Creating shared folders").

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"), the IP address(es) of the DNS servers in your network, the network settings of your port (several of which you can change as described in "Changing the network settings"), the MAC addresses of your port, and the speed at which data is being sent and received.

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

Advanced : System Status

This list displays major system status. You can click Refresh to update it.

System Status

CPU		Memory	
Busy	0 %	Total	256940 KB
Idle	100 %	Used	67236 KB
		Cache	26156 KB
		Free	189704 KB

Uptime		Hardware	
Uptime (days:hours:minutes)	0:1:19	Fan Speed	1824 RPM
		CPU Temp	39 °C
		Disk 1 and 2 Temp	25 °C
		Disk 3 and 4 Temp	26 °C

Network	
Gateway	---
DNS Server 1	0.0.0.0
DNS Server 2	---

PORT 1		PORT 2	
MAC	00:90:0B:08:C4:66	MAC	00:90:0B:08:C4:67
IP	192.168.0.249	IP	192.168.1.101
MASK	255.255.255.0	MASK	255.255.255.0
Jumbo Frames	1514 Bytes	Jumbo Frames	1514 Bytes
Receiving Speed	0.00 KB/s	Receiving Speed	0.00 KB/s
Sending Speed	0.00 KB/s	Sending Speed	0.00 KB/s

Refresh

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

Logging out of the Manager

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

To log out:

1. In the navigation bar, click **Log Out**.

2. When the confirmation message displays, click **OK**.
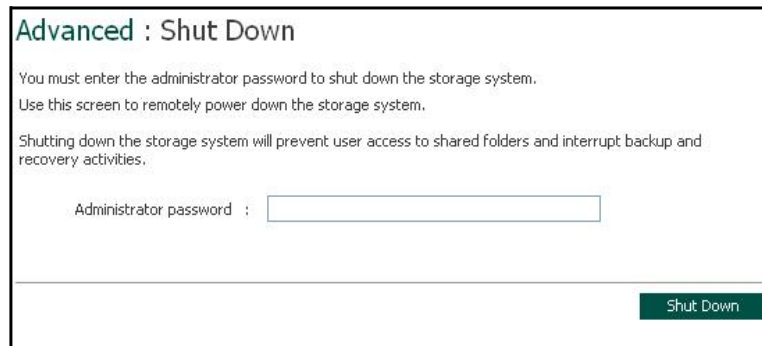
    The **Log Out** page displays:

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

Shutting down the storage system

To shut down the storage system, you can press the power button on the unit itself, or you can shut the system down remotely using the Manager. To ensure that you don't shut down the system accidentally, you must enter your administrator password to do this.

Advanced : Shut Down

You must enter the administrator password to shut down the storage system.
Use this screen to remotely power down the storage system.

Shutting down the storage system will prevent user access to shared folders and interrupt backup and recovery activities.

Administrator password :

Shut Down

⚠️ **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 server is powered on again. However, shutting down the storage system when a disk is being recovered can potentially corrupt the user's operating system, and the user will have to recover the system disk using the recovery CD (or, if the system disk was not protected, re-install the operating system).

To shut down the storage system using the Manager:

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

2.   In the left pane, click **Shut Down**.

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

4.   Click **Shut Down**.

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

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

Working with Shared Folders

4

Accessing shared folders

Once you have added users and created shared folders (as described in "Adding users" and "Creating shared folders"), 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.

Notes:

l   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 storage system time, time zone, or both to ensure that they match (as described in "Changing the system settings").

l   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 must repeat the procedures described here using the new IP address.

Windows users

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

Note: If your storage system uses Active Directory authentication mode (as described in "Changing the authentication mode"), only the **public** folder is accessible via the Console. To access all other shared folders, you must use My Computer/Windows Explorer.

Using My Computer/Windows Explorer

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

1. Open My Computer/Windows Explorer.

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

    The Map Network Drive dialog box displays:
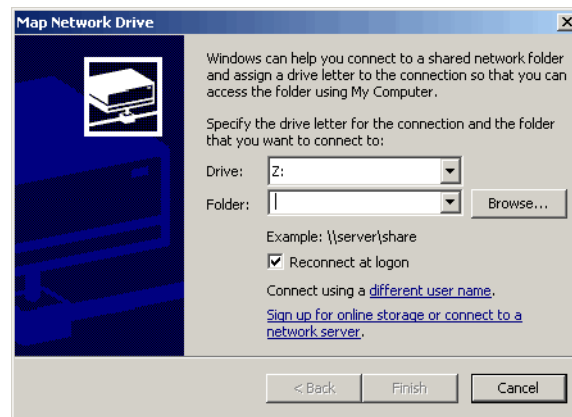
    The exact appearance of this dialog box varies, depending on your operating system.

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

4. In the **Folder** text box, enter the following:

    `\\`*`storage_system`*`\`*`shared_folder`*

    where *storage_system* is the name or IP address of the storage system, and *shared_folder* is the name of the shared folder. For example, if your storage system's IP address is 192.168.0.101 and the shared folder name is **Photos**, you would enter the following:

    `\\192.168.0.101\Photos`

    Note: You can use the storage system name only if your computer is in the same subnet as the storage system, if you added the storage system's IP address and name to your local **hosts** file, or if 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 storage system uses local authentication mode and the **guest** user has access to this shared folder, you can use **guest** as both the user name and password.

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

Using the Console

To access a shared folder using the Console:

1.   Install the Console (as described in "Installing the Console").

1.   Click **Start** --> **Programs** -->**Storage System Console**.

As soon as you start the Console, it automatically scans the network for storage systems. This might take a few minutes. As soon as the scan is complete, the left pane displays a tree view of all the storage systems it found:
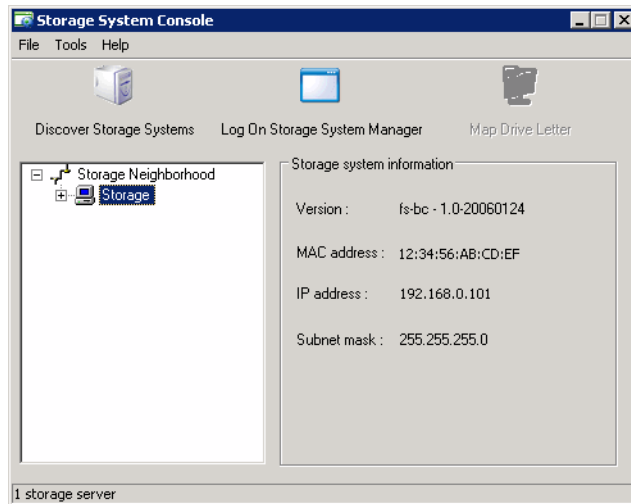
Note: If you connect a storage system to the network after the Console has already scanned it, or if you change the IP address of the storage system, you must click **Discover Storage Systems** to scan the network again and update the tree in the left pane.

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

If your storage system uses both available ports to connect to the network, you can double-click either name.

The storage system name expands to display all the available shared folders:
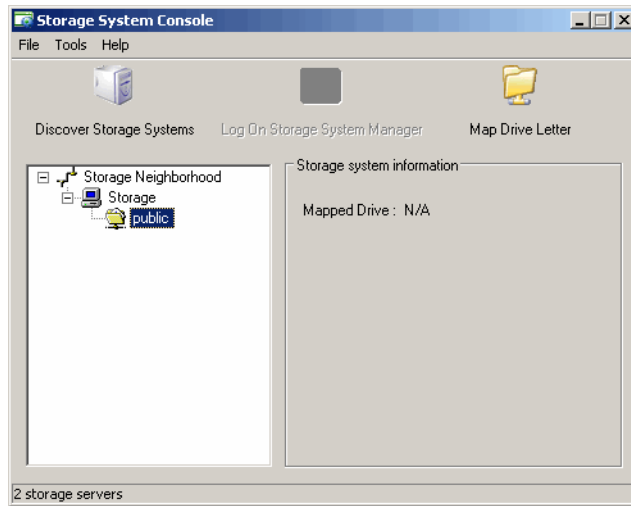
✎   **Notes:**

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

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

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

The Map Network Drive dialog box displays:
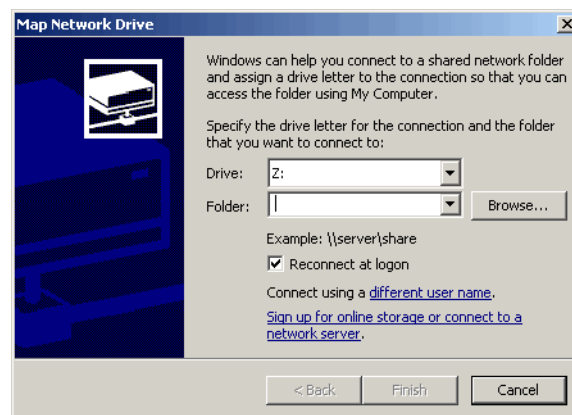
The exact appearance of this dialog box varies, depending on your operating system.

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

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 My Computer/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 IP address of the storage system.

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 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 the **Address** text box, enter the following and click **Connect**:

    `smb://`*`storage_system`*

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

    > **Note:**   You can use the storage system name only if your computer is in the same subnet as the storage system, if you added the storage system's IP address and name to your local **hosts** file, or if you manually registered the name with a DNS server in your network.

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

4. Enter the user name and password for accessing this shared folder, and then click **OK**.

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

   An icon with the name of the shared folder is created on the desktop.

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

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

Other Mac operating systems

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

Accessing shared folders using FTP

If you enabled the storage system to act as an FTP server (as described in "Changing the network settings"), all Windows and Mac OS X users can use a Web browser to access the **public** folder.

> **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 Windows and Mac OS X users have full read/write access to the **public** folder when accessing it via FTP.

To access shared folders using FTP:

1. At a computer running Windows or Mac OS X, 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 your computer is in the same subnet as the storage system, if you added the storage system's IP address and name to your local **hosts** file, or if you manually registered the name with a DNS server in your network.

   You can also use **guest** as the user name.

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 the **public** folder and you can create new ones.

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

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. (Users who connected to shared folders using FTP can disconnect simply by closing the browser window.)

Windows users

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

Disconnecting using My Computer/Windows Explorer

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

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

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

    The shared folder no longer displays in My Computer/Windows Explorer.

Disconnecting using the Console

To disconnect from a shared folder using the Console:

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

2. Start the Console (as described in "Starting the Console").

3. In the left pane, double-click the name of the storage system that contains the shared folder from which you want to disconnect.

    If your storage system uses both available ports to connect to the network, you can double-click either name.

    The storage system name expands to display all the available shared folders.

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

    The shared folder no longer displays in My Computer/Windows Explorer.

Linux users

To disconnect from a shared folder using LInux:

l   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 disdisplays 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.

Protecting Local Disks 5

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. Alternatively, you can disable automatic backups and just perform backups manually at a time of your choosing. Once the maximum number of supported backups are saved on the storage system, the oldest backup is automatically deleted each time a new backup is performed.
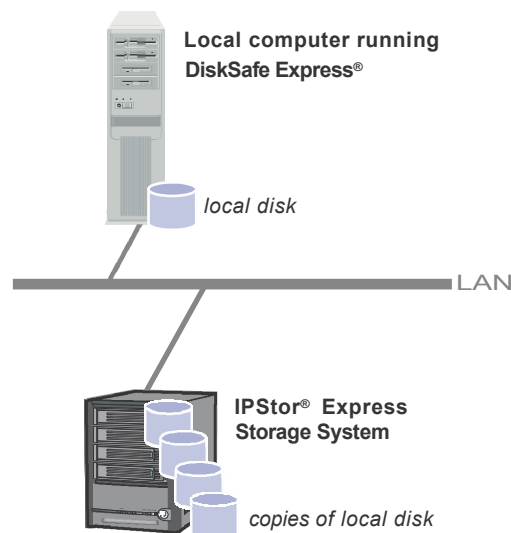
To ensure that valuable storage space isn't used up by duplicate data, when DiskSafe Express performs each subsequent backup, it copies only the data that has changed since the last time a backup was performed. This also minimizes the impact on your network. Yet through unique technology on the storage system, each backup is a complete point-in-time image. You can view or recover the entire disk or partition exactly as it existed at a particular date and time.

Whenever you want to recover data from the storage system, you can do so quickly and easily. If you need to recover just a few files or folders, you can access the desired backup and copy what you need back to your local disk. If you need to recover an entire data disk or partition (that is, a disk or partition that does not contain any of the files needed to run the operating system), you can do so using DiskSafe Express. And if you need to recover your whole system 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.) When you recover a disk, it contains exactly the same data that it contained at the time the backup was performed—you don't have to reinstall or reconfigure the operating system or applications.

Getting started

System requirements

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

l   One of the following operating systems:

   n   Microsoft Windows XP Home Edition or Professional (Service Pack 2)

   n   Microsoft Windows Server 2003 (SP1)

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

l   An enabled network interface card

l   A CD-ROM drive (for installation and using the recovery CD)

> **Note:**   A CD-ROM drive is not required for installation if an image of the CD is accessible via a network server.

l   Microsoft iSCSI Initiator 2.*x*

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

l   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.

Additional prerequisites

In addition to the system requirements, the following criteria must be met:

l   You must be logged on as an administrator to install DiskSafe Express and run it for the first time. However, after you have run the application once as an administrator, you can subsequently run it when logged on as a user.

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

> **Note:**   Previous releases allowed the use of underscores (_) in the computer name. If your computer name included this character and you protected a
> disk, you must remove protection from all disks (as described in "Removing protection"), delete the client from the storage system (as described in "Deleting a client"), and protect the disks again (as described in "Protecting your disks"). In addition, when you
> protect your disks again, you must remove the storage system from the list of backup locations and add it again (as described in step 4 in "Protecting your disks".)

---

l   If you're 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. In addition, make sure that your firewall does not block incoming network communication to the Microsoft iSCSI Initiator.

Installing the Microsoft iSCSI Initiator

Before you can install DiskSafe Express, you must download and install the Microsoft iSCSI Initiator 2.*x*.

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 in **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 displays, 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 displays telling you to configure the settings in the Control Panel, click **OK**.

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

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

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

     After your computer restarts, you can install DiskSafe Express.

Installing DiskSafe Express

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

To install DiskSafe Express:

1.   Log on as an administrator and insert the installation CD into a CD-ROM drive.

2.   Start the setup utility for 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 displays:
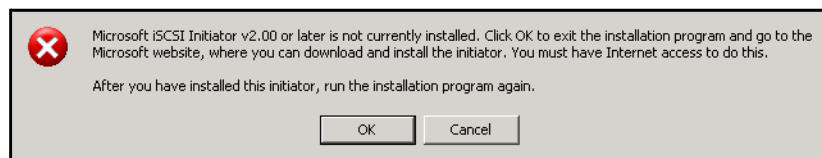
     Click **OK** to go to the Microsoft website and then click **OK** to cancel the installation of DiskSafe Express.

     On the Microsoft website, click **iSCSI Software Initiator v2.0**, and follow the instructions in "Installing the Microsoft iSCSI Initiator".

     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, 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 and it might appear that no progress is occurring. However, configuration is occurring in the background.

6.   When a message displays, 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 displays:
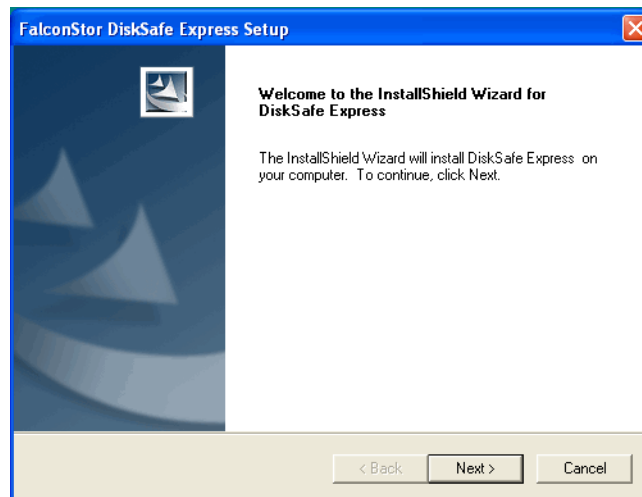
7.   On the welcome page, click **Next**.

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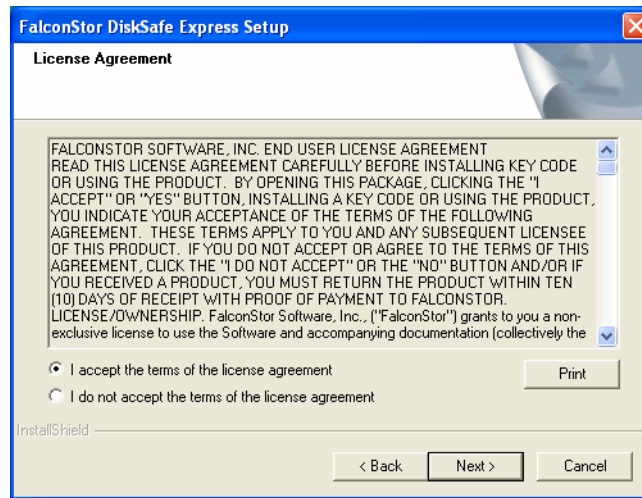
8. If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and then click **Next**.

9. Click **Next** to install DiskSafe Express in the displayed location.
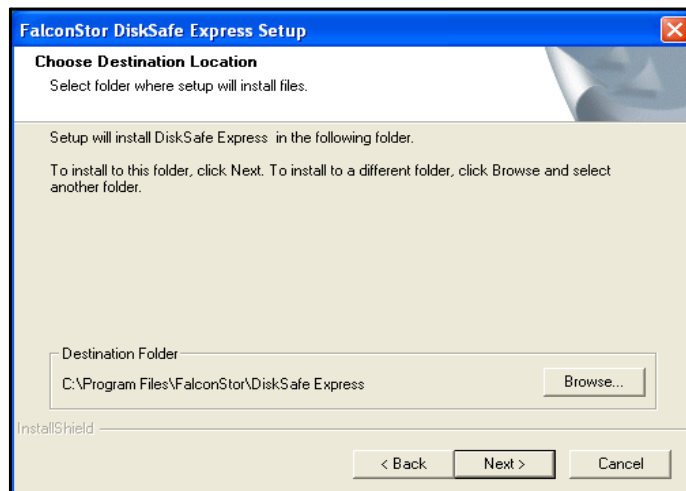
Alternatively, you can click **Browse**, select or enter a different location, click **OK**, and then click **Next**.

> **Note:** It is strongly recommended that you install DiskSafe Express on the partition that you boot from (that is, where Windows is installed, typically C:).
>
> If you install it on a non-system partition of your system disk, you will not be able to recover that partition using the DiskSafe Express application window. In addition, if you plan to remotely boot from a backup on the storage system, you must protect the entire disk rather than just the system partition.
>
> If you install DiskSafe Express on a different disk than your system disk, you will not be able to remotely boot at all.

10. To complete the installation and restart your computer, click **Finish**.
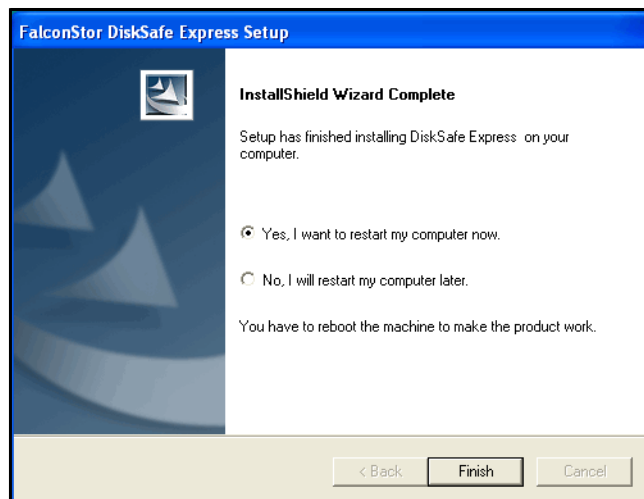
If you do not want to restart your computer at this time, select **No, I will restart my computer later** and then click **Finish**. When the confirmation message displays, click **OK**. You do not have to restart the computer immediately after installation, but you do have to restart it before running DiskSafe Express.

> **Note:** If you do not restart your computer and you subsequently reinstall DiskSafe Express, serious problems can occur with your installation. It is strongly recommended that you restart your computer at your earliest convenience.

11. After you restart your computer, click **OK** on the welcome message.

The Add License dialog box displays:
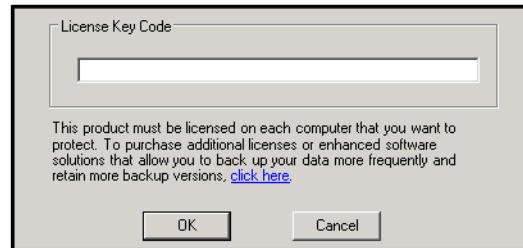
12. Enter the key code for licensing the product and click **OK**.

If your computer has an Internet connection, the license is activated automatically. When you click **OK** on the confirmation message, the Protect a Disk wizard starts. For information about this wizard, refer to "Protecting your disks".

> **Note:** If you previously used this key code on a different computer, an error message displays, and you must re-activate your license. For more information, refer to "Activating your license".

If your Internet connection is temporarily down, or if this computer doesn't have an Internet connection, click **OK** on the warning message. The Protect a Disk wizard still starts, but after 30 days you will no longer be able to perform backups or recovery until you activate the license. For more information, refer to "Activating your license".

Starting DiskSafe Express

To start DiskSafe Express, do either of the following:

l   Click **Start** --> **Programs** --> **DiskSafe Express**.

l   If the DiskSafe Express Agent is running (as indicated by the presence of the Agent icon ( ) in the system tray), double-click this icon.

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".

If you already protected a disk, the application window displays:
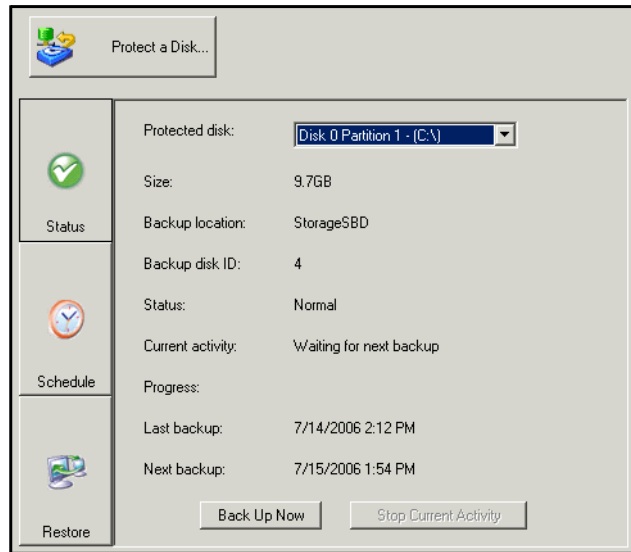
The **Status** page displays the name of the disk that you protected and related information, such as the size of the disk, the name of the storage system where the backup resides (**Backup location**), the number used to identify the backup disk on the storage system (**Backup disk ID**), the current backup status, a progress bar that displays 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 displays, 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".

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).

If your computer had no network interface card (NIC) when you installed DiskSafe Express, or your NIC was disabled, and you subsequently add or enable a NIC, you must add the license again (as described in "Replacing your existing license") in order to activate it.

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 displays. Contact Technical Support for further assistance.

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 displays.

2. Click **Export License Data**.

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

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

    n A floppy disk

    n 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 where the returned license file exists and double-click it.

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

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

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 the **License key code** text box, enter the new key code.

3. Click **OK**.

4. When the confirmation message displays, 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 want to back up, where the backups should be stored, when automatic backups (if any) should occur, and what password you want to use with the recovery CD or booting remotely. If you cancel this wizard, you can start it again at any time using the following procedure.

Before you protect a disk, it is recommended that you confirm that sufficient space is available on the storage system. At least an additional 20% of the disk size is required for changed data. For example, if the disk that you want to protect is 15 GB, at least 18 GB of space must be available on the storage system. The **Home** page in the Manager (described in "Navigating the Manager") displays the amount of available space.

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 want to protect.
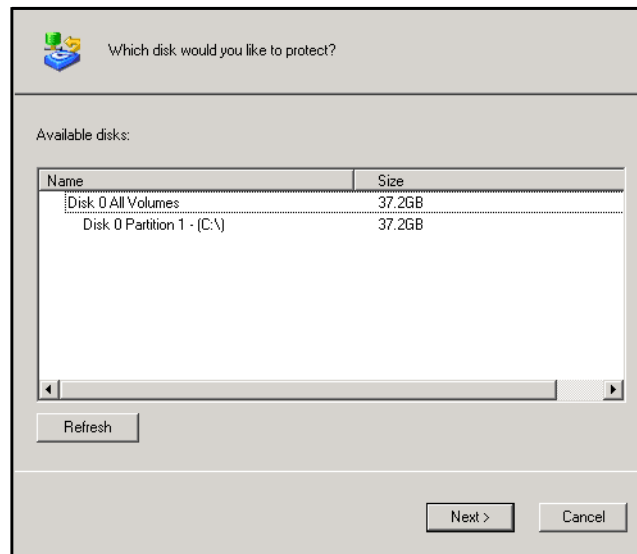
Even if your computer has only one hard disk, two items appear in this list. The first item represents the entire hard disk, and the second item represents the partition on that disk. (If there's only one partition on the disk, the partition is the same as the entire disk.)

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 have to recover the entire disk. If you select just a partition, you can subsequently recover just that partition.

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

> **Recommendations:**
>
> l   If your computer has only one disk with one partition, select the entire disk.
>
> l   If any partition (such as an EISA partition) precedes your system partition, select the entire disk. This ensures that you can remotely boot from and recover the disk.
>
> l   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.
>
>   However, if DiskSafe Express was installed on the data partition, protect the entire disk rather than the individual partitions. This ensures that you can remotely boot from that disk.

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, or an allocation error occurred the first time you tried to protect the disk	5

3. When the Add Storage System dialog box displays, DiskSafe Express automatically scans your subnet for storage systems. Any storage systems that are detected appear in the **Discovered storage systems** list.
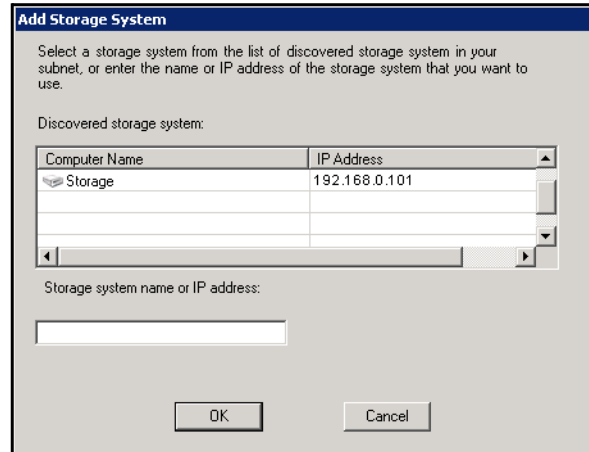
From the **Discovered storage systems** list, select the storage system where you want to back up the selected disk. The name of the storage system automatically displays in the **Storage system name or IP address** text box.

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

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 the **Backup locations** list, select the storage system to use for backups of this disk or partition. (The first backup location in the list is selected by default.)
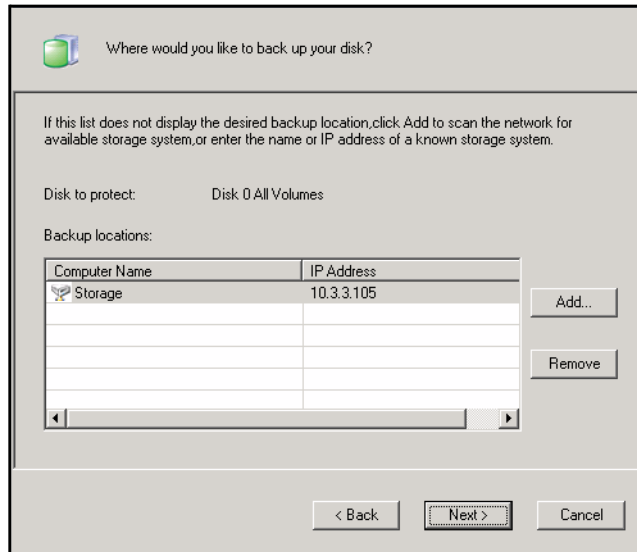
If you want to scan the network for new storage systems, or add a new one manually, click **Add** and repeat step 3.

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

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

5. If you previously protected this disk and removed protection, specify whether or not you want to re-use the existing backup or create a new one.
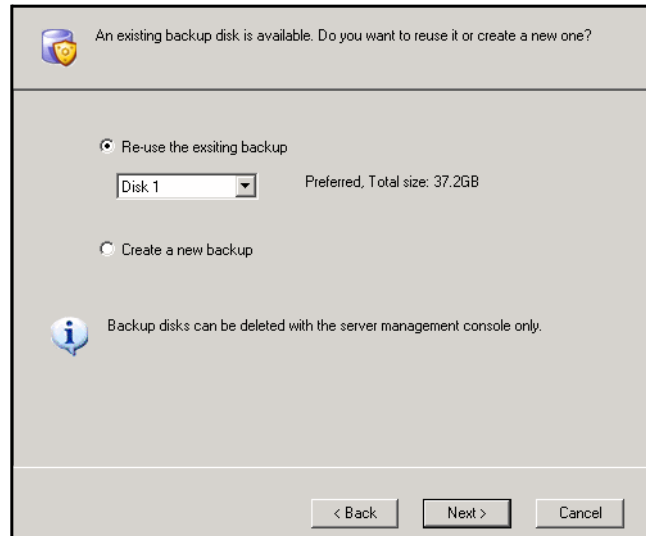
If you select **Re-use the existing backup**, you must select which backup to re-use from the list. When you select an item from the list, the size also displays to help you identify exactly which backup to use. The word **Preferred** displays for the backup that best matches the disk that you're currently protecting. Once you have selected the desired backup, click **Next** and go to the next step.
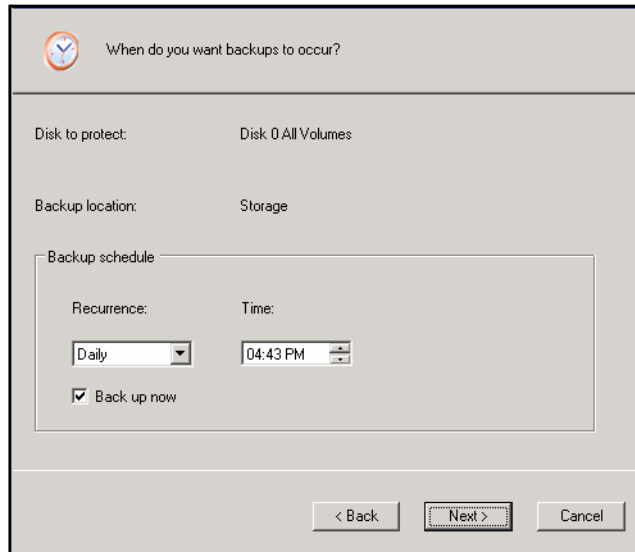
> **Note:**   If the list does not display the expected information, you might need to click **Cancel**, click **Action** --> **Repair Connection**, and then try to protect the
> disk again. Repairing the network connection refreshes the information about the backups that exist on the storage system.

> **Caution:**   If you select any disk other than the preferred one, all the data associated with the selected disk will be overwritten with the data associated with the disk that you're protecting, and you will not be able to recover any previous backups associated with the selected disk.

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

6. Specify when you want backups to occur.

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

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

Notes:

l   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.

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

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.

> **Note:** Be sure to back up your disk or partition before you try to recover it using the recovery CD (as described in "Recovering a system disk using the recovery CD").

8. If you ever need to recover your disk using the recovery CD or remotely boot from a backup on the storage system, you'll be prompted for a password. In the **Recovery password** text box, enter the password that you'd like to use, enter it again in the **Retype your password** text box, and then click **Next**.

> **Notes:**
>
> l   The recovery password must be 12–16 characters long. It cannot contain multi-byte words. This means you can only enter ASCII character whose code value is less than 128.
>
> l   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.
>
> l   You can change this password later using DiskSafe Express (as described in "Changing the recovery password" and using the storage system (as described in "Changing the recovery password").

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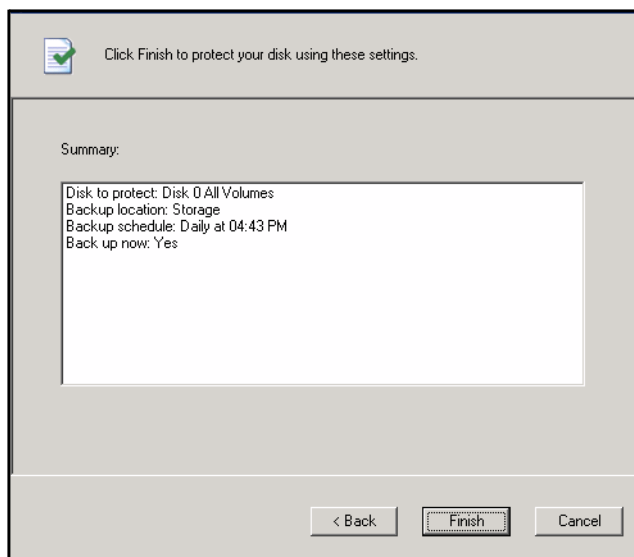
If you selected the **Back up now** check box, the backup will begin as soon as you click **Finish**, and you can review its progress on the **Status** page in DiskSafe Express.

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

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

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). You can also back up a disk manually as long as a backup or recovery is not currently occurring. For example, if you're about to install a new application, you might want to back up your disk right before you do that so that if any problems occur, you can recover your disk to the state it was in immediately before you installed the application.

To manually back up a disk:

1. Click **Status**.
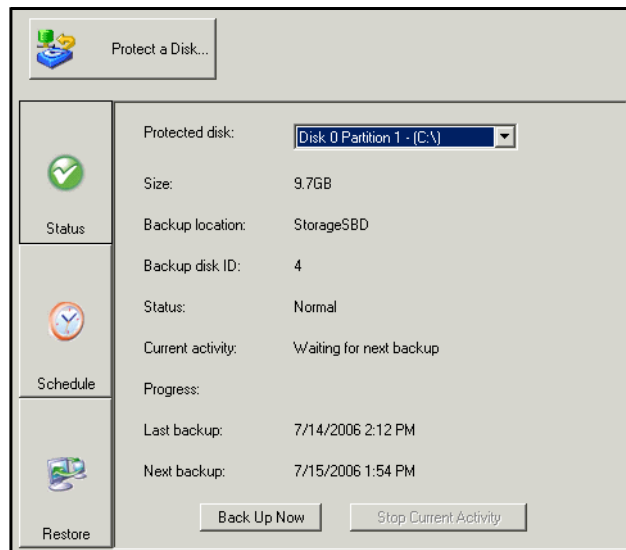
2. In the **Protected disk** list, select the disk that you want to back up.

3. Click **Back Up Now**.

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

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

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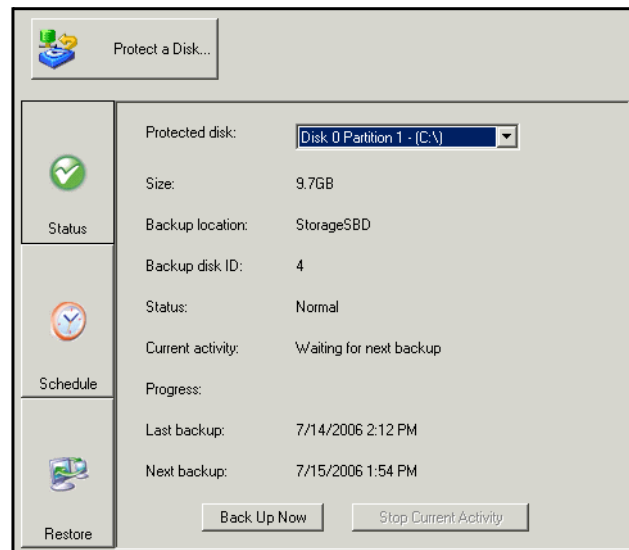
2. In the **Protected disk** list, select the disk whose backup or recovery you want to stop.

3. Click **Stop Current Activity**.

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

    If you're stopping a recovery, a confirmation message displays. 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 want backups to occur. However, you can change this schedule at any time as long as the **Status** page indicates 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**.

To change the backup schedule:

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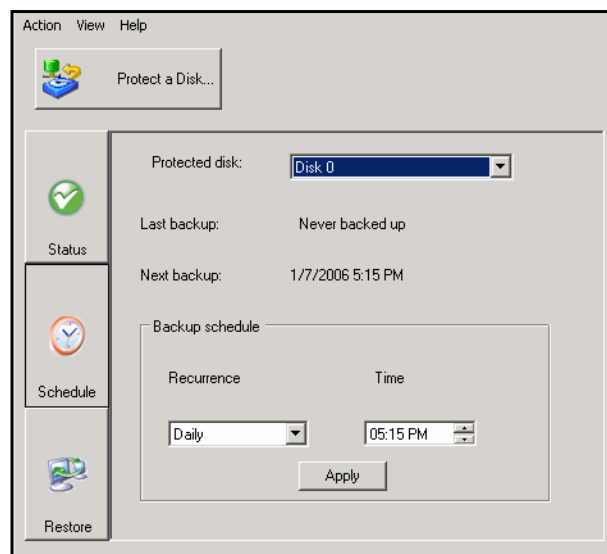
2. In the **Protected disk** list, select the disk whose backup schedule you want to change.

3. Specify when you want backups to occur.

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

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

4. Click **Apply**.

5. When the confirmation message displays, click **Yes**.

6. When the result message displays, click **OK**.

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

Receiving event notifications

When you install DiskSafe Express, the DiskSafe Express Agent is also installed. This program starts automatically whenever you start your computer, and the Agent icon displays in your system tray.

When the Agent is running, a pop-up message displays whenever a backup-related problem occurs (for example, if a scheduled backup did not occur because the storage system was not running).

You can close the Agent at any time. However, if you do this, notifications will no longer appear automatically. If you subsequently want to start the Agent again, you can do so using DiskSafe Express.

To close the Agent:

l   In the system tray, right-click the Agent icon ( ) and click **Exit DiskSafe Express Agent**.

To restart the Agent after you have closed it:

l   From the **View** menu, click **Agent**.

The Agent icon redisplays in the system tray.

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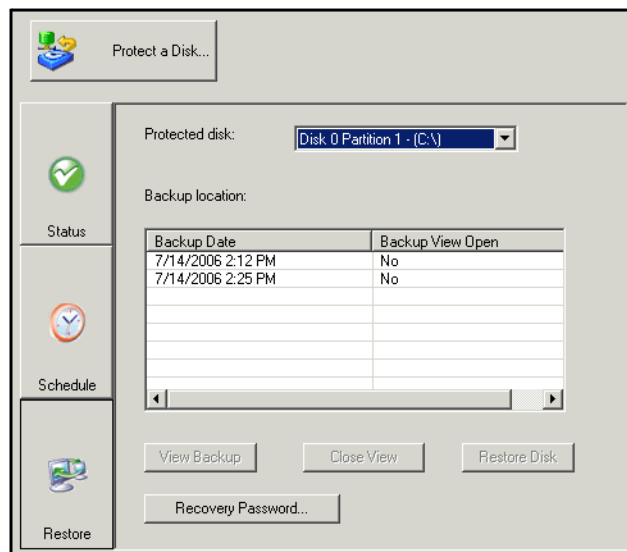
2. In the **Protected disk** list, select a disk whose backup resides on the storage system whose recovery password you want to change.

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

3. Click **Recovery Password**.

    The Reset Recovery Password dialog box displays.
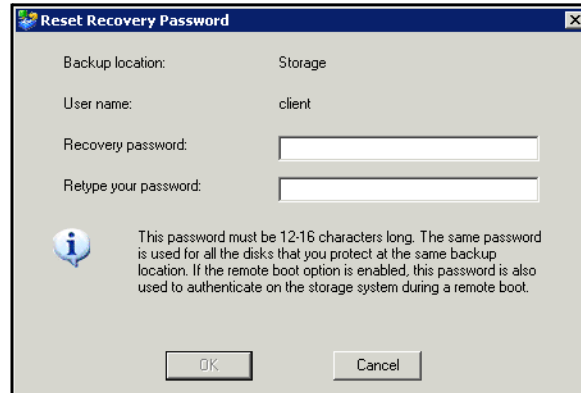
4. In the **Recovery password** text box, enter the desired password.

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

5. In the **Retype your password** text box, 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 using the recovery CD"). 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're not sure if 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:** 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 using the recovery CD" 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 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 using the recovery CD") 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:

l   Windows was installed on the first partition of the first disk in your computer.

l   DiskSafe Express was installed on that system disk.

l   You protected your system disk or partition.

l   You are accessing the computer directly rather than using Remote Desktop.

📝 **Notes:**

l   If DiskSafe Express was installed on the same disk but 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") and protect the entire disk (as described in "Protecting your disks").

l   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 want 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. This dialog box displays a list of all the NICs on your computer.
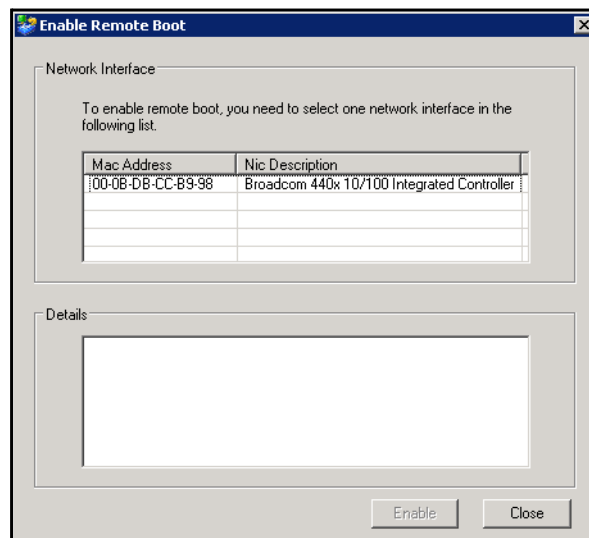
3. From the list, select the NIC that you want to use when remotely booting from the storage system.

4. Click **Enable**.

    A message displays, advising you that your network connection will be
    temporarily interrupted.
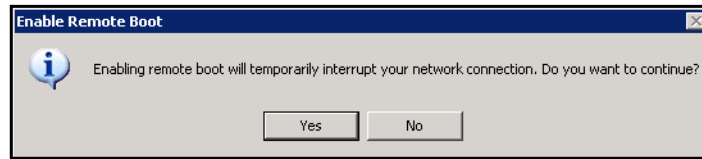
5. Click **Yes** to allow the temporary network interruption. (Your network connection
    will be restored immediately after this process is complete.)

    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 displays, advising you that drivers will be installed, click **OK**.

7. When the drivers are installed, one or more messages might appear, advising
    you that these drivers are not signed. This has no adverse effect on your
    system. Click **Continue Anyway** or **Yes** on each message to proceed with the
    installation.

    In addition, the Found New Hardware Wizard starts. Select **No, Not This Time**
    on the initial screen and complete the rest of the wizard, accepting all the default
    values.

    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 for some reason 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 116). 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").

    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"). 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. It is recommended that you save and close any open files on your system before you do this.

To disable remote boot:

1.   From the **Action** menu, click **Disable Remote Boot**.

     A progress bar displays, indicating the progress of the process.

2.   When the confirmation message displays, 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 want to do and the capabilities of your computer:

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

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

   For more information, refer to "Recovering files or folders".

l   **Recover an entire data 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.

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

   For more information, refer to "Recovering a data disk".

l   **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 want to duplicate the backup of an existing disk to 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 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 then recover your system disk. For more information, refer to "Recovering a system disk while booting remotely".

⚠️   **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 using the recovery CD" 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") 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 using the recovery CD") 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 or folders

To recover selected files or folders from a backup:

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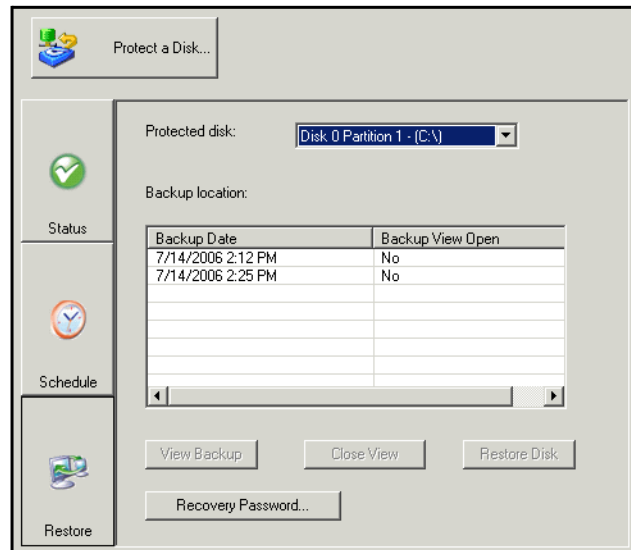
2. In the **Protected disk** list, select the disk that contains the files or folders that you want to recover.

3. In the **Backups** list, select the backup from the desired date and time.

   You can select only a backup for which **No** displays in the **Backup View Open** column.

4. Click **View Backup**.

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

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

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

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

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

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

l   If you open a backup view of a disk that contains multiple partitions, a drive letter is assigned to each partition.

l   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.

l   You can view more than one backup simultaneously. Simply repeat steps 3 and 4 for each backup that you want to view.

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

l   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).

l   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.

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

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

Recovering a data disk

You can recover a data disk or partition only as long as DiskSafe Express is not installed on that disk or partition, the disk or partition is not currently being backed up, and no backup view is open.

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.

Once the recovery of any data disk or partition is complete, your computer restarts automatically.

⚠️   **Caution:**   When you recover a data disk or partition, you will lose any data that was written to the disk after the time of the selected backup, as well as any backups that were performed after the backup you're recovering. You might want to copy any newer files that you want to keep to another disk before you recover the disk.

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 have to recover it using the recovery CD (or re-install the operating system if you did not protect your system disk).

To recover a data disk or partition:

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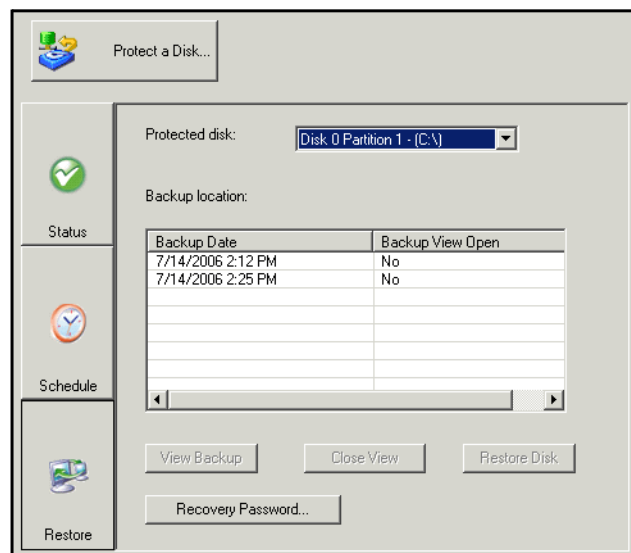
2. In the **Protected disk** list, select the disk or partition that you want to recover.

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

4.   Click **Restore Disk**.

5.   If you are restoring a partition, and at least one other partition on the same disk is also protected, a message displays, advising you that protection will be stopped for that partition during the recovery process. Click **Yes** to proceed.

6.   When the recovery confirmation message displays, click **Yes**.

7.   If any backup views are open (including backup views of disks other than the one you are recovering), click **Yes** to close them.

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 displays automatically. The **Current activity** area displays the percentage of the recovery that has completed, and the speed at which the data is being sent over the network. The **Progress** bar graphically indicates how much of the recovery is complete.

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

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

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

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

Recovering a system disk using the recovery CD

When you use the recovery CD, you boot your computer from that CD rather than from your local hard disk.

The recovery CD has a menu-style user interface. 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 displays in the brackets when the option is selected), and press Enter to make your selection. You can also tab between fields.

Note: The recovery CD does not support USB keyboards or mouse devices.

Although the recovery CD is used primarily for recovering a system disk or partition, you can also use it to recover data disks or partitions.

The recovery CD can recover multiple partitions to a disk with existing partitions. It can also create one partition on a new disk. However, if you want to recover multiple partitions to a new disk, you must format and partition the disk before you use the recovery CD to recover the partitions.

In some cases, when you recover a disk using the recovery CD, an additional backup is created on the storage system. If the maximum number of backups has already been performed, the oldest backup will be deleted to make room for this backup.

To recover a disk or partition using the recovery CD:

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

   For more information, refer to the documentation for your computer.

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

   A welcome screen displays while the CD initializes.

3. If you have already verified that the recovery CD supports your local hardware, or if you have received a new recovery driver from your vendor, wait 25 seconds for **Normal Mode** to start automatically and go to step 4.

   If this is the first time you have used the recovery CD, press any key to start **Diagnostic Mode**. The screen displays a list of all the devices found on your computer and whether or not they are compatible with the recovery CD. You can use the arrow keys to scroll through the list. If at least one supported network interface card (NIC) and one hard disk have been detected, select **Normal Mode** and go to step 4.

If no supported NIC is found, you can gather information about your computer and send it to Technical Support to see if an updated recovery CD or an appropriate driver is available. To do this, select **Save**, insert a formatted floppy disk or USB disk into your computer, and select the appropriate option (**Save to Floppy Disk** or **Save to USB Disk**). Once the file has been saved to the specified location, you can send it to Technical Support. Then select **Finish** and select **Yes** to restart your computer. At this point, you have 10 seconds to remove the recovery CD from your CD-ROM drive and boot from your local disk once more. Otherwise, your computer will boot from the recovery CD again.

4. When the hardware list displays, take the desired action:

To do this	Do this
Proceed with recovering data	Select **Next**.
	You can select **Next** only if at least one supported NIC is listed.
Load a new recovery driver	Select **Load Driver**, select the location from which you want to install the driver (**Load From System** for the local hard disk, **Load From Floppy Disk** for a floppy disk, **Load From CD** for a CD, or **Load From USB Disk** for a USB disk), insert the disk (if loading from a floppy disk, CD, or USB disk), and respond to the prompts.
See a complete list of the detected hardware	Select **Diagnostic Mode**.
	When you are done viewing the list, select **Normal Mode**.

5. Review the network settings for your NIC and select **Next**.

The recovery CD obtains the IP address to use from your DHCP server. If the displayed settings are not the ones you want to use, or if no IP address is displayed, select the NIC in the list, select **Config**, specify the desired IP address, subnet mask, and default gateway, and select **OK**.

If multiple NICs are listed, the recovery CD will use the last operational one (that is, the last NIC whose **Status** is **Enabled**). If you do not want to use the last listed NIC, select that NIC, select **Config**, and then select **Disable** to change the **Status** to **Disabled**. Repeat this procedure for each NIC that you do not want to use. Then select **Next**.

6. In the **Computer Name** field, enter the full computer name of this computer.

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

7.   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.

8.   In the **Storage System** 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 computer is in the same subnet as the storage system or if you manually registered the name with a DNS server in your network.

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, and then select **Next**.

If you don't remember your password, you can change it on the storage system (as described in "Changing the recovery password") and enter the new password here.

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

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

If you protected multiple disks or partitions, you can identify the right item by looking at the **Attr**, **Disk ID**, and **Size(M)** 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 partition and a data partition, the system partition will be labeled **PS**, and the data partition will be labeled simply **P**. If you protected disks of different sizes, the **Size(M)** column (which displays the number of megabytes) can also help you identify the right item. You can also compare the disk ID with the listed backup disk IDs in the Manager (as described in "Managing backups").

If you protected the same disk more than once (for example, if you removed protection and then protected the disk again without re-using the existing backup), the attributes and size of each backup of that disk will be the same. To determine which item to select, select each one individually and look at the times and dates in the right column. This can help you identify which image is the most recent.

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

> ⚠️ **Caution:**   Selecting a backup with a specific date/time stamp is strongly recommended.
>
> In most cases, selecting **Latest Backup** is the same as selecting the backup in the list with the most recent date/time stamp. However, if the most recent backup is marked **<Protect>**, the **Latest Backup** will be in an incomplete state. In that case, be sure to select one of the other listed backup dates rather than **Latest Backup**.
>
> In addition, if nothing displays in this column besides **Latest Backup**, do not recover this disk or partition. In this situation, **Latest Backup** represents only the empty storage space allocated for the backup and contains no data to recover. You can press Ctrl+Alt+Delete to exit the recovery CD.

If you select **Latest Backup**, an additional backup is created on the storage system, and this image is recovered. As a result, if the maximum number of backups has already been performed, the oldest backup is deleted to make room for this backup. Backups created by the recovery CD are identified in this list by the word **<Recovery>**.

To update the information on this screen, select **Refresh**. This is helpful if you're recovering data from one computer to another and a new disk was protected or a backup occurred after this screen was displayed.

12. If you selected a backup other than **Latest Backup**, specify whether or not to delete all backups that occurred after the selected backup by selecting or clearing **Delete all later backups**.

> **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 for differences between the backup and your local disk by selecting or clearing **Enable microscan**, and then select **Next**.

If you're simply overwriting corrupted data on your original disk, select this option. Only the data that differs between the backup and the local disk will be copied to the local disk. This can minimize the impact to the network, although the scanning process takes some additional time.

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

14. Select the local disk where you want to recover the data, and select **Next**.

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

15. If you selected a disk in step 10, go to step 18.

    If you selected a partition in step 10, select **Recover to an existing partition** to recover to an existing partition on the selected disk, or select **Reformat the local disk and recover to a new partition** to delete all the existing data on the selected disk and recover only the selected partition.

16. If you selected **Recover to an existing partition** in step 15, select the partition where you want to recover the data and press Enter. (Otherwise, go to step 18.)

    For system partitions, the **Active** column displays **Yes**.

17. If the selected partition is the original partition, go to step 18.

    If the selected partition is not the original partition, select **Yes** to use the selected partition, or select **No** and select a different partition.

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

> **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 **Cancel**. However, this leaves the local 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 displays, review the results and do one of the following:

To do this	Do this
Recover another disk or partition	Select **Recover Another Disk**.
	If you want to recover a different backup of the same computer from the same storage system, select **No** to retain the current configuration settings and return to step 10.
	If you want to recover a different computer's backup, or if you want to recover a backup from a different storage system, select **Yes** to modify the current configuration settings and return to step 6.
Restart the computer	Select **Restart Computer**.
	When the informational message displays, select **OK**.
	When prompted to confirm that you want to restart the computer, select **Yes**.
	You have 10 seconds to remove the recovery CD from the CD-ROM drive.

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

    If your computer is configured to boot from the local hard disk if no CD is in the CD-ROM drive, simply remove the recovery CD from the CD-ROM drive before restarting.

21. If you changed the recovery password on the storage system, reset it in the Microsoft iSCSI Initiator (as described in "Resetting the recovery password in the Microsoft iSCSI Initiator").

22. Start DiskSafe Express and remove protection from the recovered disk or partition (as described in "Removing protection").

23. Protect the recovered disk once again (as described in "Protecting your disks"), re-using the original backup.

Recovering a system disk while booting remotely

If your computer meets the necessary 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.
>
> In addition, 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:

l   The computer that you're remotely booting must be in the same subnet as the storage system.

l   Remote boot must be enabled for that computer (as described in "Enabling remote boot").

l   At least one backup must have been performed after remote boot was enabled.

l   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").

l   If you plan to remotely boot your computer from a different computer's backup, you 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".

l   If you want to remotely boot from any backup other than the most recent one, you must select the desired backup on the storage system. For more information, refer to "Configuring remote boot".

Recovering the disk

To recover a system disk or partition while booting remotely:

1. Start your computer.

2. Use the appropriate procedure for your computer to configure it to boot from the NIC.

   For example, you might press F12 when the boot menu displays. 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.

   You have a limited amount of time to do this.

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 don't remember your password, you can change it on the storage system (as described in "Changing the recovery password") and enter the new password.

6. If any error messages appear, click **OK**.

7. Log in as you normally would.

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

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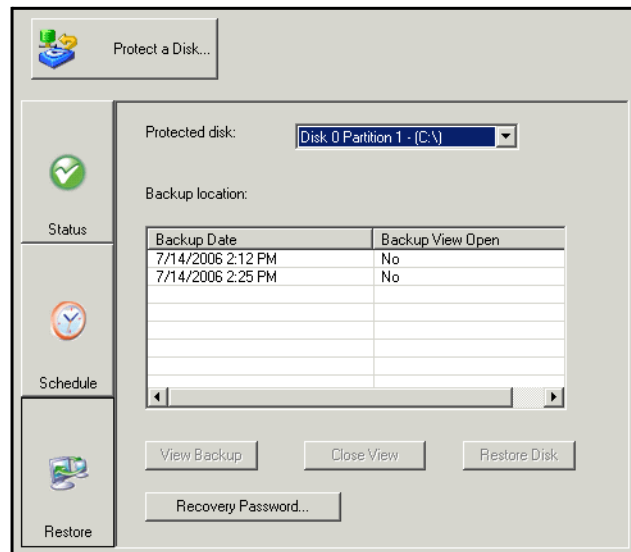
8. Start DiskSafe Express.

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

9. When a warning message displays, advising 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 the **Backups** list, 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"). Then restart DiskSafe Express.

12. Click **Restore Disk**.

The Restore dialog box displays.
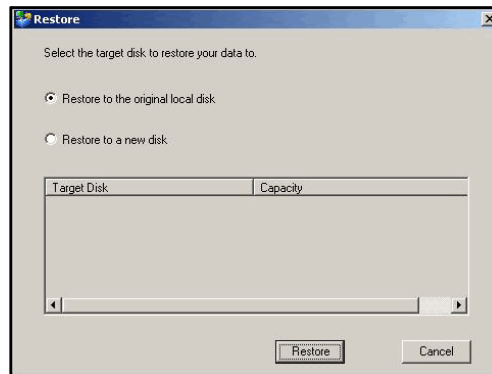
13. Specify whether you are recovering to the original disk or a new disk.

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

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

    The backup is recovered to your local disk, and the progress bar displays the progress of this process. You can cancel the recovery at any time by clicking **Stop** on 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 for your computer to configure it 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").

18. Start DiskSafe Express and remove protection from all your disks and partitions (as described in "Removing protection"). (This disables remote boot and restarts your computer.) Then protect your disks again (as described in "Protecting your disks"), reusing the existing backups.

    If you need to recover any other data disks or partitions, you can do so (as described in "Recovering a data disk"). 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").

Removing protection

If you no longer want to back up a particular disk or partition, you can remove protection as long as a recovery is not currently in progress for that disk or partition. (If a recovery is in progress, 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 for a disk for which remote boot is enabled, remote boot will be disabled and your computer will restart.

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 or folders" and "Recovering a data disk"). 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 using the recovery CD").

If you subsequently want to protect the same disk or partition again, you can re-use the existing 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 "Deleting a backup".

To remove protection:

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

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

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

   The disk disdisplays from the **Protected disk** list. If another disk is protected, that disk displays in the **Protected disk** list, and information about that disk now displays in the application window. If no other disk is protected, click **OK** on the informational message; the **Protected disk** list and application window are blank.

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

Software Specifications **A**

Operating System	Linux Kernel 2.6.10
Network Service	DHCP client/server (default IP address for Port 1 is 192.168.0.101)
Supported Web Browsers	▪ Microsoft Internet Explorer 6.0 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 ▪ CIFS users access shared folders using passwords

Disk Configurations B

Your storage system supports various types of disk configurations, including RAID (redundant array of independent disks), a disk subsystem that can increase performance, provide data protection, or both.

l **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.

l **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.

l **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.

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

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

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

l   **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.

l   **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. (Access to the disks is temporarily interrupted while the disk is being 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").

> ⚠️ **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.

Although you can add a disk of any size to a linear configuration, any new disk that you add to a RAID configuration must be the same size as or larger than the smallest existing disk in the RAID.

Adding hard disks to a linear or normal RAID configuration

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

1. Insert the hard disk into the storage system.

   You can do this whether the storage system is powered on or off.

2. Access the Manager or refresh the browser window.

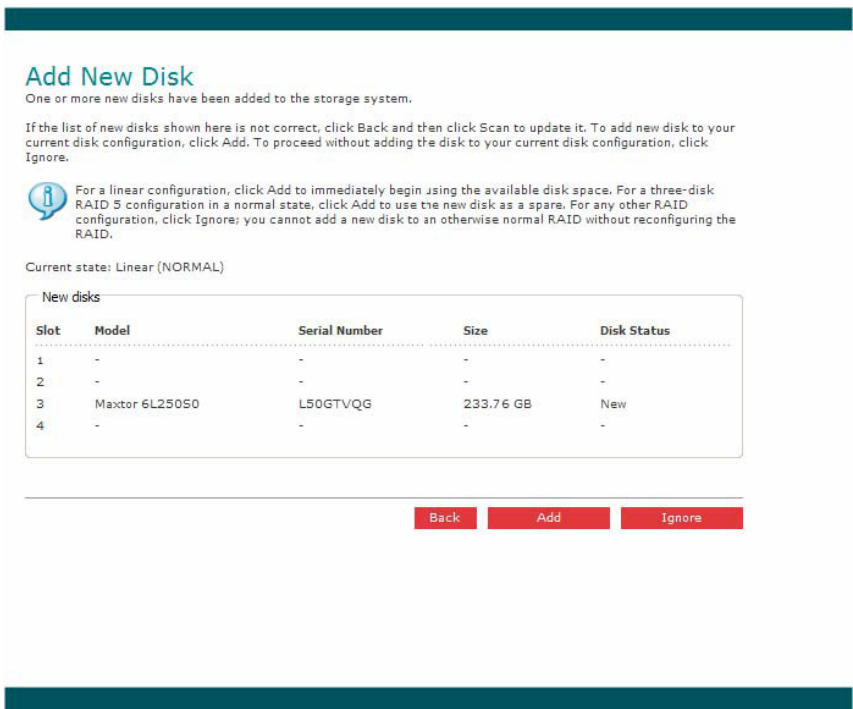   The **Disk Change Notification** page displays:

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

   If the information on this page is not correct, click **Scan** to scan the storage system again and update the page.

   You can also click **Shut Down** to shut down the storage system, but you will be presented with this page again the next time you access the Manager.

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

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"), 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 Manager or refresh the browser window.

    The **Disk Change Notification** page displays:

> **Note:**   Initially, the **Disk Status** for the new disk might display **Spare** rather than **Rebuilding**. If this occurs, refresh the page to update the status.

3. Click **Continue** to continue rebuilding the disk and return to the Manager.

    The **Disks** page shows the progress of the rebuilding progress.

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

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

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. However, this will not adversely affect any of the other disks.
>
> In addition, while a disk is being rebuilt, all the other disks are RED, since removing any one of them at this point will cause the RAID to fail.

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

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

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

> ⚠️ **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 displays when you access the Manager 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 Manager 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 displays when you access the Manager or refresh the browser window:

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

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

Current state: RAID 10 (DEGRADED)

Previous disks

Slot	Model	Serial Number	Size	Disk Status
1	ST3750840AS	3QD0J8S1	698.64 GB	RAID 10
2	ST3750840AS	3QD0J8RF	698.64 GB	RAID 10
3	ST3750840AS	3QD0D1FQ	698.64 GB	RAID 10
4	ST3750840AS	3QD0J8NJ	698.64 GB	RAID 10

Current disks

Slot	Model	Serial Number	Size	Disk Status
1	ST3750840AS	3QD0J8S1	698.64 GB	RAID 10
2	-	-	-	-
3	ST3750840AS	3QD0D1FQ	698.64 GB	RAID 10
4	ST3750840AS	3QD0J8NJ	698.64 GB	RAID 10

Scan | Shut Down | Continue

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 "Configuring your storage system"). **Caution:** Reconfiguring the storage system deletes all user information and all data on all the disks.

Swapping hard disks

If you're 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.

> **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 displays (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 Manager for the new unit (as described in "Accessing the Manager").

   As long as the new unit is in the same subnet as the old unit, you can access the Manager using the same procedure you used previously. However, if the new unit is in a different subnet, you might have to install the Console on a computer in the same subnet as the storage system and use the 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 displays, prompting you to update the flash memory on the storage system with the firmware from the hard disks. Click **Update** to proceed. If you don't want to upgrade the firmware at this time, click **Shut Down** to shut down the system.

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

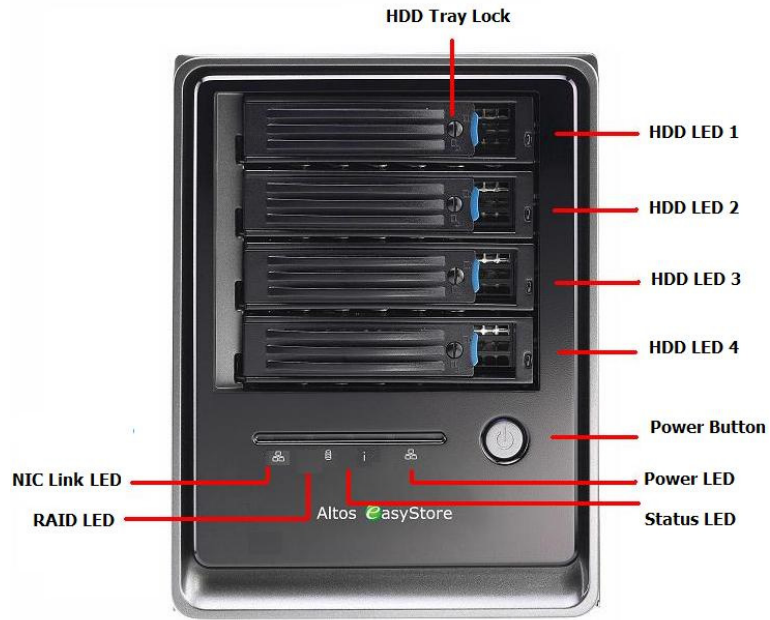If no message displays, you can manage the unit as you did before.

Hardware Specifications C

FEATURE	DESCRIPTION	
Platform	Processor	Intel® 80219 IOP
	Max.Speed	600 MHz
System Memory	Technology	DDR-SDRAM
	Socket	184-pin unbuffered DIMM x 1
		256MB default, 512MB max
Storage Interface	Embedded OS	Intel® 8MB NOR Flash
	Storage Capacity	Hard Drive bays x 4, up to 2 Terabytes
	Hard Drive Support	Serial ATA Interface [4 headers], Intel® 31244
	RAID levels	RAID 0, 1, 5, 10, and JBOD
	File Format Protocol	CIFS/SMB/NFS
Networking	Network Controller	Intel® i82541
	Bandwith	1Gb
I/O Interface	USB 2.0 x 2	Supports FAT/FAT32 file format for flash disk
		Supports ink jet printer with Line Printer Device protocol (print.server)
Client OS Supported		Microsoft Windows 2000 with Service Pack 2
		Microsoft Windows XP/2003
		UNIX
		Macintosh OS 7.X and later
		Linux
DiskSafe	Client Backup	Yes
	Client Recovery	Yes
	No. of Licenses	2
	Max Licenses	16
File Sharing	Network Protocol	FTP
		CIFS/SMB/NFS
		NTFS
	Network Service	DHCP client/server
	Active Directory Support	Yes
	Management Interface	Web Graphical User Interface
	Client Support Capabilities	Max. 256 Clients (128 Windows/OS X, 128 Linux)
		Max. 128 Groups
		Max. 128 Share Folders
Cooling	System.Fan	1 (92 x 92 x 25 mm)
Environmental Parameters	Temperature, ambient operating	0 to 40°C (32 to 104°F)
	Temperature, ambient non-operating	0 to 40°C (32 to 104°F)
	Temperature, ambient storage	-20 to 70°C (-4 to 158°F)
	Humidity (RH), ambient operating	10 to 90 percent non-condensing
	Humidity (RH), ambient non-operating and storage	5 to 90 percent non-condensing
Physical Dimensions	Dimensions (WxLxH)	16 x 24 x 21 cm , (6.3 x 9.45 x 8.27 in)
	Weight	4.5 kg (9.92 lb)

 Front Panel

 Rear Panel

Altos easyStore Manual
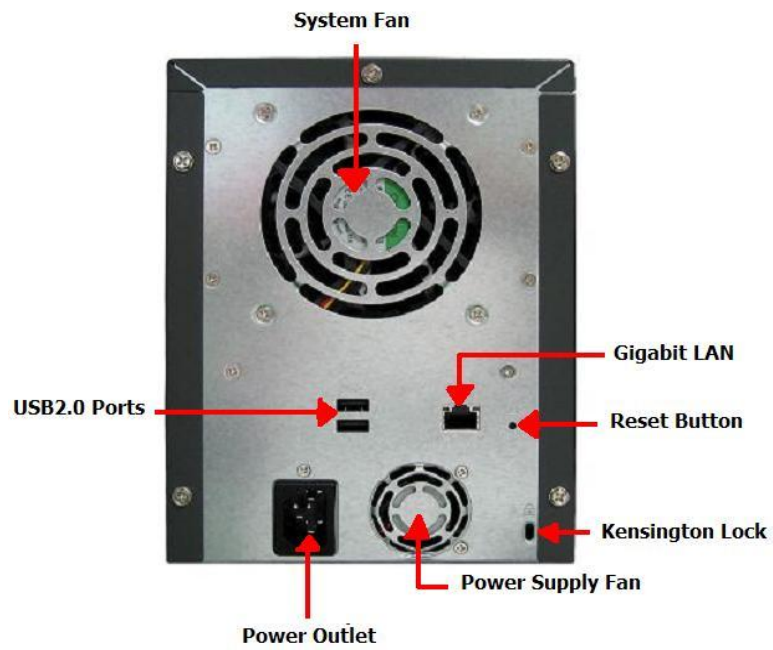
Technical Assistance

For technical assistance, contact your local dealer or distributor. You may also access the website (http://support.acer-euro.com) for information on how and where to contact the service centers available in your area.

Prior to contacting us, we ask that you first check the electronic product documentation for assistance.   Should you still have questions, we recommend you have the following information on hand in order to expedite the process:

- Model name
- Product Serial Number
- Local network configuration details
- Abnormal behavior and/or error messages reported by your system
- Detailed questions or a description of the problem you are experiencing

Glossary

backup view   A backup that has been assigned a drive letter and can be opened and explored using My Computer/Windows Explorer

Console   The Windows-based application that enables you to discover all the storage systems on your subnet, view their version and network information, access the Manager, and map drive letters to shared folders

data disk or partition   A hard disk or partition of a hard disk that is not used to run the computer operating system

group   A collection of one or more users that can be given access to a shared folder all at once

jumbo frame   A large packet size for transferring data between the storage system and computers in the network

Manager   The Web-based user interface that enables you to configure the storage system

NIC   An acronym for network interface card

NTP   An acronym for Network Time Protocol, a mechanism for synchronizing a computer's time with a standard time on a server

RAID   An acronym for redundant array of independent disks

Different levels of RAIDs provide different types of data protection and data duplication, as well as enhance the performance of your disks.

remote boot   The process of booting your computer from the storage system rather than from a local hard disk

shared folder   A folder on the storage system that can be accessed by authorized users

subnet   A portion of a local area network

Computers in a subnet typically have IP addresses that are the same except for the last three digits. For example, computers with IP addresses of 192.168.0.101, 192.168.0.102, and 192.168.0.103 would all belong to the same subnet.

system disk or partition   A hard disk or partition of a hard disk that the computer boots from

user   An individual or computer that can access a shared folder on the storage system