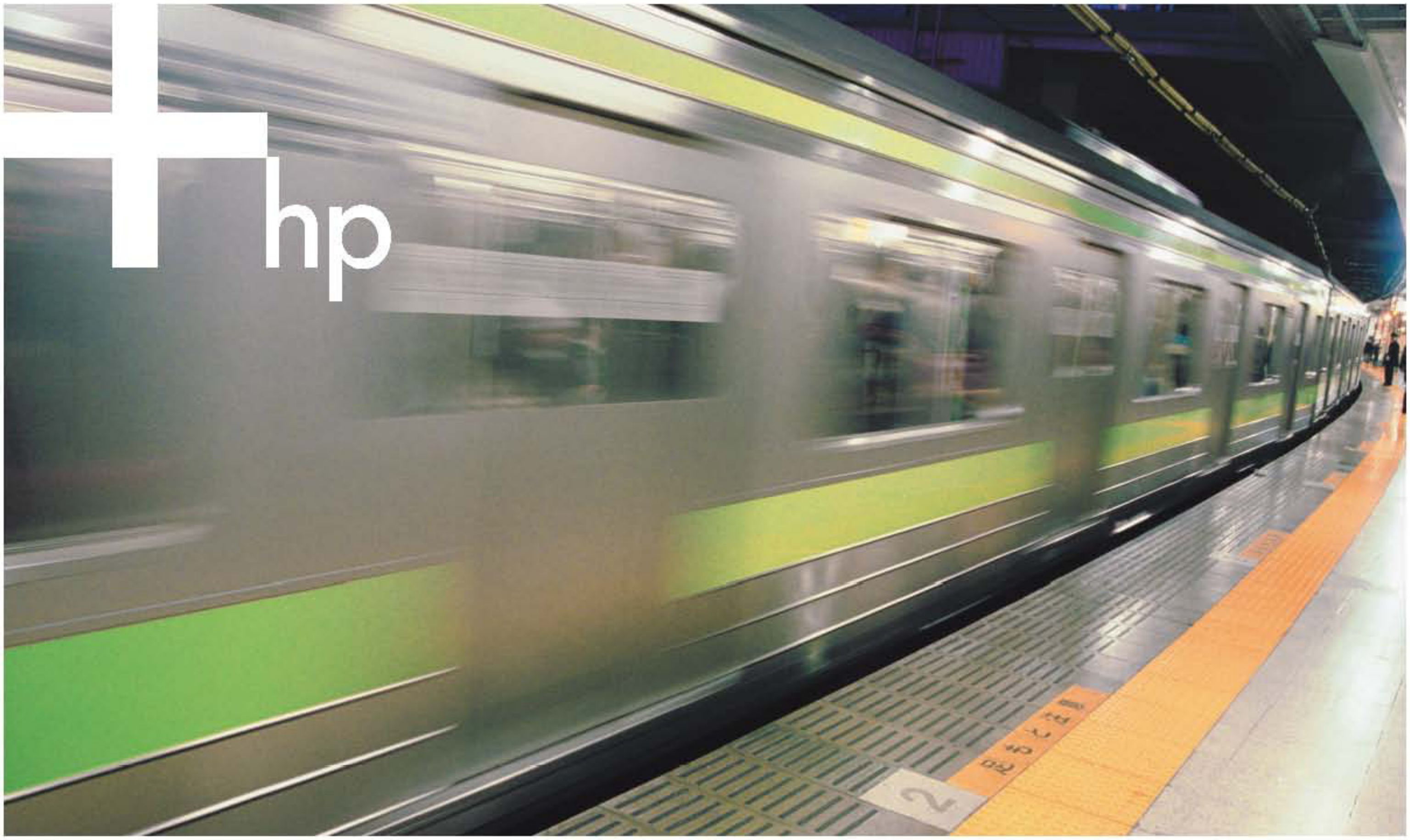
HP StorageWorks Data Protector Express



Users Guide and Technical Reference

Copyright

Part Number BB116-90023

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided ”as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.
www.hp.com

Trademarks

Windows® and Windows NT® are registered trademarks of Microsoft Corporation.

NetWare® is a registered trademark of Novell, Inc.

Linux® is a registered trademark of Linus Torvalds. Red Hat® is a registered trademark of Red Hat, Inc. SuSE® is a registered trademark of SuSE Linux Products GmbH, a Novell business.

Table of Contents

Before You Begin

This *User's Guide and Technical Reference* provides all of the information necessary to effectively implement and use all of the advanced features found in Data Protector Express. Information about installing Data Protector Express is available in the *Installation Guide*.

In this section

- Documentation
- Customer Support

Documentation

The following documentation is included with Data Protector Express to help you install and use all of Data Protector Express features and options.

NOTE: In the following sections:

<Lang> represents the language in which the document is written: **eng** (English), **fre** (French), **ger** (German), **ita** (Italian), **jpn** (Japanese) , **spa** (Spanish), **kor** (Korean), **chs** (Simplified Chinese), and **cht** (Traditional Chinese).

Printable documentation

The **/doc** directory on the Data Protector Express CD-ROM contains the following printable documentation:

- *Quick Start Guide* **(dpqks.pdf**): Contains basic information to help you install and run Data Protector Express (multiple languages in one version).
- *Installation Guide* **(dpins<Lang>.pdf**): Contains installation information for each supported platform.
- *User's Guide and Technical Reference* **(dpusr<Lang>.pdf**): Contains information for configuring and using Data Protector Express.
- *Addendum* **(dpadd.pdf**): Contains information on additional features (English only): This manual is provided only when necessary.

NOTE: You can also download these documents from the Data Protector Express website www.hp.com/go/dataprotectorexpress.

If you require printed copies of these manuals, you can print the PDF files. They were designed to be printed two-sided and new chapters always begin on an odd-numbered page.

To view or print this documentation, Adobe Acrobat Reader (version 4.0 or higher) must be installed on your Windows or X Window (Linux) computer. If not currently installed, you can install it from the Adobe Acrobat Reader website at *www.adobe.com/*.

NOTE: Adobe Acrobat Reader does not offer versions for NetWare systems. Therefore, you can only view or print the Data Protector Express documentation on Windows or X Window (Linux) systems.

To print the documentation, open the appropriate file into Adobe Acrobat Reader. Choose **Print Setup…** from the **File** menu and set the proper options for your printer. Then choose **Print…** from the **File** menu and print the document.

Release notes

Release notes are included with every service pack. Before using Data Protector Express, please read and print the release notes for additional information. The release notes are available in both HTML (**readme.htm**) and text (**readme.txt**) formats in the root directory of the Data Protector Express CD-ROM.

Online Help

Windows

To view online help while using Data Protector Express, select **Contents** from the **Help** menu. The online help is displayed in a pop-up window.

For task-related or context-sensitive help while using Data Protector Express, select a topic in the Dynamic Help list.

Non-Windows

You can view online help from most Data Protector Express screens by pressing **F1**.

Screen Shots

The screen shots in this manual may not be identical to the interface you see when you use Data Protector Express. Any differences will be small and will not prevent you from using this documentation. Note that because of the customizable nature of the Data Protector Express graphical user interface that the components of the GUI may be in different locations and colors in the documentation compared to the product in use.

Features

If you have a Proliant Edition or Single Server Edition of Data Protector Express software, not all of the features described in this document will be available to you. This document describes all the features in Data Protector Express. Both Data Protector Express Single Server Edition and Data Protector Express Proliant Edition can be upgraded to Data Protector Express with the appropriate license key. Please contact your HP partner to purchase this upgrade.

Customer Support

Customers under a support contract may receive their support by phone or by submitting an email.

Country specific details on both options can be found at *welcome.hp.com/country/us/en/wwcontact.html*.

If you require support and your support contract has expired, please contact your HP Partner or sales representative for information on obtaining a new HP Data Protector Express support contract

Chapter 1: About Data Protector Express

A backup and recovery system is an integral part of a company's data security. The ability to back up and restore business-critical data quickly and efficiently can mean the difference between survival and failure. Maintaining backups is often considered a tedious task, and many companies fail to protect their corporate data at all. Data Protector Express provides users with the capacity to back up and restore data across a network and the ability to administer a comprehensive backup plan. This section describes basic concepts of a backup and recovery system and presents how Data Protector Express provides a powerful, yet cost-effective and easy-to-use, management tool for protecting data on network file or application servers and PC desktops.

In this section

- Backup basics
- Backup environment

Backup basics

Whether your work environment consists of a single computer in a home or small office, several computers connected to a network server, or hundreds of computers connected to multiple network servers, a typical data protection plan involves at least the ability to back up and restore business files.

At a minimum, data that cannot be reloaded onto the system from installation disks, network-based security settings, company-generated databases should all be backed up for easy retrieval in the event of a data disaster. The important data might be a word processing file, e-commerce transactions, network user account and password information, and so on.

The data you protect and how long it remains available on storage media might depend on legal requirements for your industry or your own company policies. Whatever your data storage requirements might be, you should have a basic understanding of the types of backup operations and your own computer environment.

Typical backup and recovery operations

Backup: A backup is the process of copying a file or folder from its current location to a new location, typically media loaded in a backup device. The original data remains intact in its current location. During the backup process, an attribute associated with each file, known as an archive attribute, is altered within the Data Protector Express Selection tree to indicate that the file was backed up. Archive attributes may function differently on different operating systems, so the Data Protector Express catalog also tracks file changes.

Data Protector Express runs backups in one of four backup modes:

- **Full:** In full backup mode, the backup job copies all selected files in the job whether or not they have changed. During a full backup, the archive attribute and Data Protector Express catalog record for each selected file is updated to indicate that it has been backed up during a full backup.
- **Differential:** In differential mode, the backup job copies only those selected files that have changed since the *last full* backup. The Data Protector Express catalog record for these files is updated but the archive attribute is not reset by this backup.
- **Incremental:** In incremental mode, the backup job copies all selected files that have changed since the last backup *regardless of backup mode*. The Data Protector Express catalog record and archive attribute for these files is updated to reflect this backup.
- **Copy:** In copy mode, the backup job backs up all selected files, but has no effect on any future scheduled backups. The archive attribute is not changed during this backup.

Restore: A restore is the process of copying data from backup media to its original location or to a new location in the event that the original location is damaged or unavailable. Restore operations can also retrieve data to a file or folder other than the original one.

Disaster recovery: Often defined as the ability to recover information systems quickly, disaster recovery is the process of automatically partitioning and formatting the hard drive, and restoring operating system data that allows a computer or network to restart normally. Disaster recovery and general restore operations can be combined to quickly restore both the operating system and business-critical data.

Backup environment

A complete network backup system consists of three parts: backup devices, a catalog, and a backup management program.

Backup devices

Data Protector Express works with your existing computer network. A network connects file or application servers and PC desktops together in order to allow various users to work together on projects and with common files. Networks also allow users to share peripheral devices, such as disk drives, printers, fax machines, and modems. Sharing devices across a network makes economic sense, since several systems can use a single device. Backup devices, such as tape drives, hard disks, NAS appliances, and CD or DVD recordable devices, which back up or copy files onto tape, disk, or other media, may also be shared. For more information about using backup devices in network environments, see *Strategies for Faster Jobs* on page 156.

Sharing a backup device makes operational as well as economic sense. Sharing devices lowers costs and makes it possible to centralize backup operations across the network. Further, a single user, such as the network administrator, can have primary responsibility for backing up all the file or application servers and PC desktops on the network.

Sharing a backup device or tape drive across a network also poses problems.

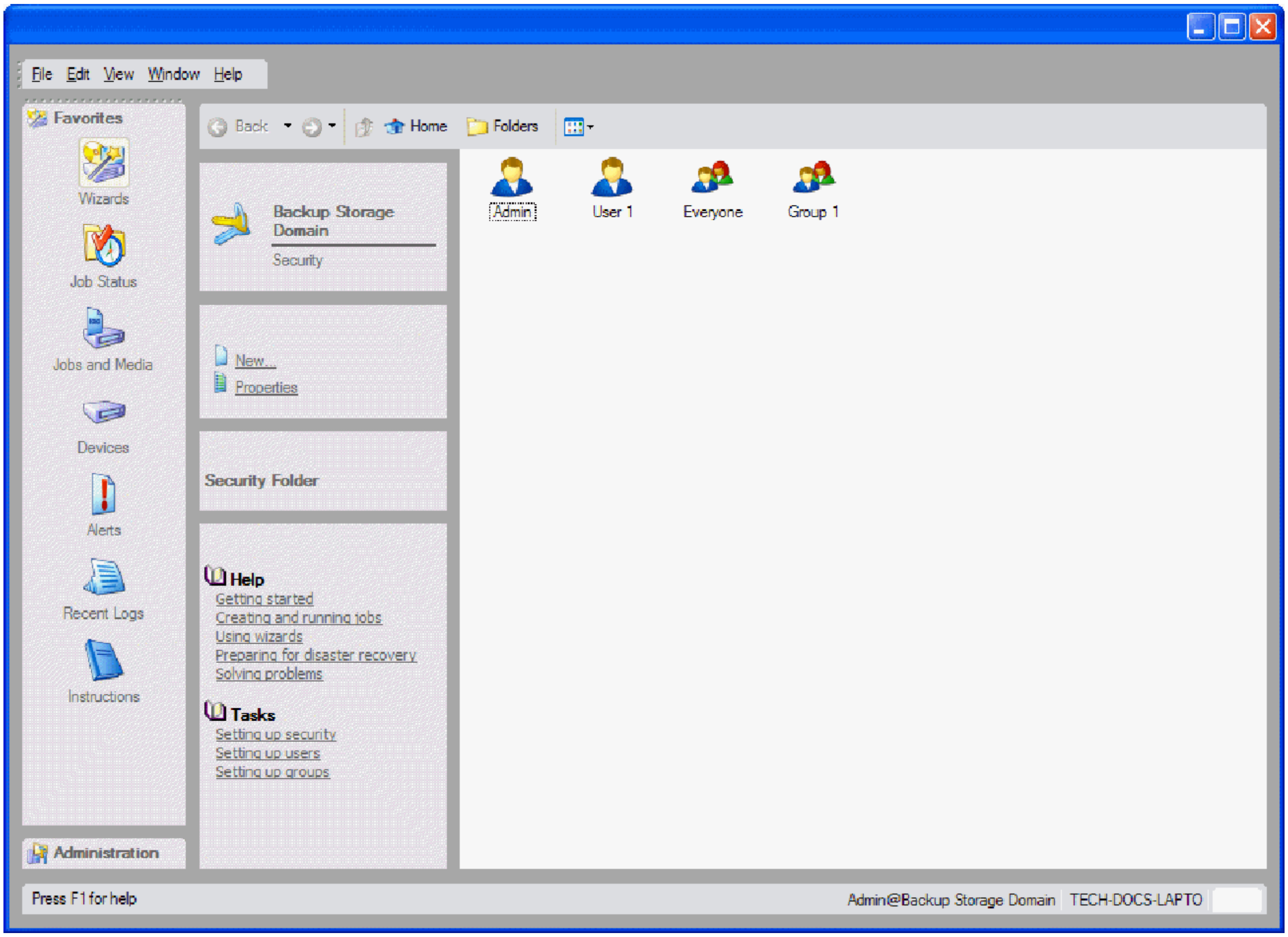
- **Security:** Most networks have elaborate security systems that prevent access by unauthorized users to sensitive or confidential data. However, unless you take protective measures, once these files are backed up onto tape or other media, any user in physical possession of the media can gain access to these files. Although it is possible to physically store the media in a secure location, a complete network backup system will help prevent unauthorized users from accessing confidential or classified information. Data Protector Express provides this level of backup security by providing passwords in order to access to the contents of backup media.

- **Tracking backed up files:** While a single user may be able to find a file copied onto a CD or floppy disk by manually searching through a stack of disks, this approach is unworkable for large networks. Without the appropriate software, locating a given occurrence of a file may be impossible, since there may be hundreds of thousands of files backed up on hundreds of media created over weeks or months.

Storage management catalog

To solve the problems of security and tracking files, Data Protector Express creates and manages a **storage management catalog** commonly referred to as the Data Protector Express catalog. The Data Protector Express catalog keeps track of used and available backup media and each file that is stored on that media. For each media, the catalog contains detailed information about the media, such as when it was created and who created it and about the files on the media, such as when they were backed up and on which media files are stored. For more information, see *Tips for Managing the Catalog* on page 153.

The Data Protector Express catalog also addresses issues surrounding security. Included in the catalog is information about which users can use or view which files. The catalog prevents unauthorized users from accessing files for which they have insufficient security rights. It tracks each user and ensures that only approved users have access to backup devices and files stored on the backup media. The following illustration shows the **Security** view of the Data Protector Express catalog.



Backup management program

Writing files to the backup media and managing the catalog requires an application program, such as Data Protector Express. Two of the most important functions of Data Protector Express are *managing the catalog* and *creating and running jobs.* Data Protector Express manages the catalog to keep track of files and to ensure security. Data Protector Express also creates and runs jobs, such as backup and restore jobs, which transfer files back and forth between backup devices (such as tape drives) and file or application servers or PC desktops.

Managing the Storage Management Catalog

Much of the power and usefulness of Data Protector Express comes from its extensive capabilities to manage the storage management catalog. There are three important concepts associated with the catalog: *objects, properties and Data Protector Express management domains*.

Objects

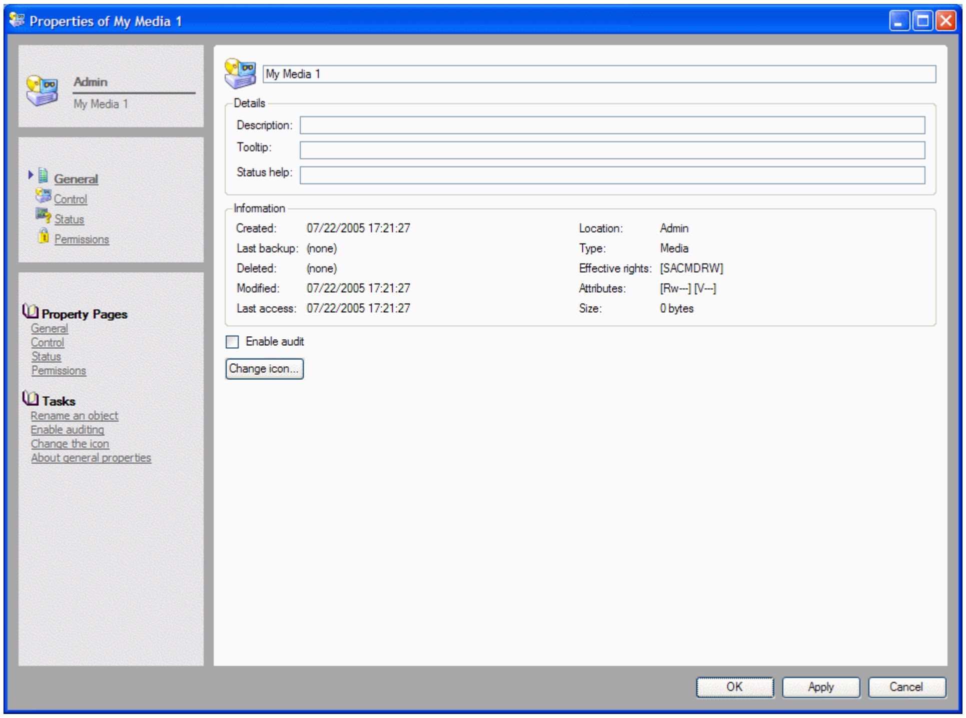
The catalog collects and organizes information about **objects**. An object is any file, machine, device, backup media or user about which Data Protector Express needs to store data. Examples of objects which Data Protector Express tracks in its catalog include backup media, tape drives, network servers, versions of files, backup jobs, custom templates, users, and so on.

Some objects can contain other objects within them. A simple example is a folder. It contains other objects within it, such as jobs, files, templates, user information, and so on. Data Protector Express also displays information about the contents of objects other than folders. When you view a list of the contents of the Data Protector Express management domain, you might see machines, networks, devices, libraries, and so on. Although not folders, these objects can contain other objects in them. For example, a library can contain storage slots, import/export slots, and so on. A network might contain file systems, network drives, printers, and attached backup devices.

Properties

The information about each object that Data Protector Express stores in its catalog are called **properties**. The properties of each object include important information about that object, such as what kind of object it is, who has security permissions to use it and its relationship to other objects. For more information on property pages, see *Chapter 13 – Objects and Properties Reference* on page 181.

For example, an individual backup media is an object in the Data Protector Express catalog. Some of the properties of that media stored in the catalog include its name, when it was created, who has security permissions to use the media and whether or not it can be erased.



My Media 1

Description:
Tooltip:
Status help:

Created: 07/22/2005 17:21:27
Last backup: (none)
Deleted: (none)
Modified: 07/22/2005 17:21:27
Last access: 07/22/2005 17:21:27
Location: Admin
Type: Media
Effective rights: [SACMDRW]
Attributes: [Rw--] [V--]
Size: 0 bytes

☐ Enable audit

Working with Data Protector Express objects and properties is easy. If you know how to use Windows Explorer, you already know most of what you need to use Data Protector Express.

Data Protector Express management domains

Data Protector Express may be licensed to support several catalogs. On a large network, it may be useful to have multiple catalogs, each addressing different data protection needs. For example, there may be a separate catalog for each work group or department, even though they are all on the same network.

If your network has several Data Protector Express catalogs, then you choose which catalog you wish to use by selecting a **Data Protector Express management domain** when you log on to Data Protector Express. Choosing a Data Protector Express management domain is simply a way to select which catalog you wish to use.

Each Data Protector Express management domain is overseen by a Data Protector Express **administrator**. It is the Data Protector Express administrator’s job to manage the security and integrity of the files in his or her Data Protector Express management domain.

You can switch to a different domain each time you log on to Data Protector Express. You can also set up domains from the Data Protector Express **Login** screen.

In the **Host Name** field, enter the hostname or IP address of the machine on which the Data Protector Express management $Option_masterserver$ is located, then select **OK**.

NOTE: When you edit a domain, you cannot edit the $Option_masterserver$ name.

Data Protector Express management domains and security

Data Protector Express management domains also help ensure network security. Data Protector Express uses Data Protector Express management domains to promote security in two ways: first, by preventing users from working with more than one Data Protector Express management domain at a time and, second, by allowing file or application servers and PC desktops to be the member of *only* one Data

Protector Express management domain. For more information, see *Chapter 12 – Advanced Permissions and Security* on page 166.

Note the following about machines, users, and Data Protector Express management domains:

- File or application servers and PC desktops can only be the member of one—and only one—Data Protector Express management domain. Because these machines belong to only one catalog, their peripherals, such as disk drives and backup devices, can belong to only one catalog.
- Backup media created in one Data Protector Express management domain cannot be used in another Data Protector Express management domain without following special procedures (e.g., importing media created on one Data Protector Express management domain into the Data Protector Express catalog of another Data Protector Express management domain). This ensures that there is no improper access to secure files and data.
- Each Data Protector Express management domain must have at least one backup device , such as a virtual library, tape library or CD device. This backup device can belong to only one Data Protector Express management domain; it cannot be shared among multiple storage domains. However, a Data Protector Express management domain could have multiple backup devices.
- From one PC desktop, users can work in other Data Protector Express management domains besides the storage domain to which their PC desktop belongs. This means they can administer jobs remotely for other Data Protector Express management domains besides the storage domain to which their PC desktop belongs. They cannot, however, work in more than one Data Protector Express management domain at the same time.
- Users can work from other machines with other Data Protector Express management domains besides the one to which their machine belongs. Their machine, along with its drives, peripherals and accompanying data, however, always remain in a single Data Protector Express management domain. That is, the data on their machine is always backed up and restored within a single Data Protector Express management domain. This helps to prevent the unauthorized sharing of data between Data Protector Express management domains that would occur if someone in a different storage domain were able to restore your data to their machine. Thus while users can work outside of their storage domain, the PC desktops and file or application servers they use always remain a part of the Data Protector Express management domain that was selected when Data Protector Express was installed on the machine.

Creating and running jobs

Data Protector Express creates backup media and restores files with **jobs**. Working with backup devices and a network, Data Protector Express jobs either back up network file or application servers and PC desktops onto physical or virtual media or restore files from media onto file or application servers or PC desktops. When you want Data Protector Express to back up or restore a file, you create and run a job.

There are several kinds of jobs: backup, restore, verify, media, and disaster recovery. Every kind of job you create and run has six components: *creating the job, permissions, selection, options, scheduling and running*. Setting up media rotation is an additional feature that you may include in your backup jobs.

Creating the job: You begin by creating a job, either a backup, restore, verify, media, and disaster recovery job. Refer to *Chapter 3 – Creating Jobs with Data Protector Express* on page 30 for more information.

Permissions: In order to create a job, you must have permissions to the objects that job will work with. For example, to create a backup job, you must have permissions to the tape drive, the tape, and the files you will back up. If you wish to back up files on another PC desktop, you must have permissions to that PC desktop and to the files on that PC desktop. Individual users are assigned permissions by the Data

Protector Express administrator, who is responsible for ensuring the security and integrity of the backup system. Refer to *Chapter 4 - Permissions* on page 42 for more information.

Selection: Once you have permissions to a file, you must select it to be included in your job. You might select all files, only a few files, or perhaps only a single file. You select files first by selecting them in the selection window and second by having Data Protector Express ‘sort’ them with **filters**, which apply additional selection criteria, such as date modified, type of file, and so on. Refer to *Chapter 5 – Selecting Files and File Versions* on page 54 for more information.

Options: After scheduling the job, you specify the job’s option settings. Some of the options you can specify include what backup device to use, what media to use, whether to automatically format the media, and so on. Refer to *Chapter 8 – Job Options* on page 107 for more information.

Scheduling: After selecting files, the job is scheduled to be run. A job may be scheduled to run later or to run immediately. It can be scheduled to run regularly or only once. Refer to *Chapter 6 – Scheduling Jobs* on page 90 and *Chapter 7 – Planning for Media Rotation* on page 98 for more information.

Media rotation: After selecting a schedule for a job, you must decide how to manage your media. Data Protector Express can manage your media automatically with default media rotation plans, or you can manage your media manually. Refer to *Chapter 7 – Planning for Media Rotation* on page 98 for more information.

Running the job: Finally, the job is run. Many scheduled jobs are run automatically by Data Protector Express, but you can manually run a job at any time. Refer to *Chapter 9 – Running Jobs* on page 121 for more information.

NOTE: When you recover the storage management catalog, jobs are placed on hold. To restart the jobs, select the jobs and select **Continue** from the command list.

Chapter 2: Data Protector Express Workplace

Data Protector Express is designed to be easy to use. This section will familiarize you with most Data Protector Express features, including keyboard shortcuts and mouse conventions.

NOTE: This manual documents the graphical user interface available on Windows and Linux systems running X Window. The console interface operates similarly on Windows, NetWare, and Linux systems.

In this section

- Starting Data Protector Express

- Starting Data Protector Express
- Main Data Protector Express Window
- Customizing the main Data Protector Express window
- Working with Objects in the Main Data Protector Express Window

Starting Data Protector Express

After you have installed Data Protector Express, you start it like any other program.

Windows

To start Data Protector Express in Windows, double-click the Data Protector Express shortcut on the desktop.

You can also click the **Start** button and select Hewlett-Packard Company from the **Programs** (or **All Programs**) submenu. Then select Data Protector Express**.**

NetWare

To start Data Protector Express on a NetWare machine, access the server console. Then type dp**Admin**. It is not necessary to specify a search path. For example, you can launch Data Protector Express on a NetWare computer by typing the following at a console prompt:

:

SERVER: dpAdmin

Linux

To start Data Protector Express on a Linux machine, open a terminal window. Then access the directory where you installed Data Protector Express. Type ./ dpadmin. For example:

[/usr/local/hp/dpx]# ./ dpadmin

To launch the CUI, type ./ dpadmin -c. For example:

```
[/usr/local/hp/dpx]# ./ dpadmin -c
```

Linux (X Window)

To start Data Protector Express on a Linux machine running X Window, open a terminal window. Then access the directory where you installed Data Protector Express. Type ./ dpadmin. For example:

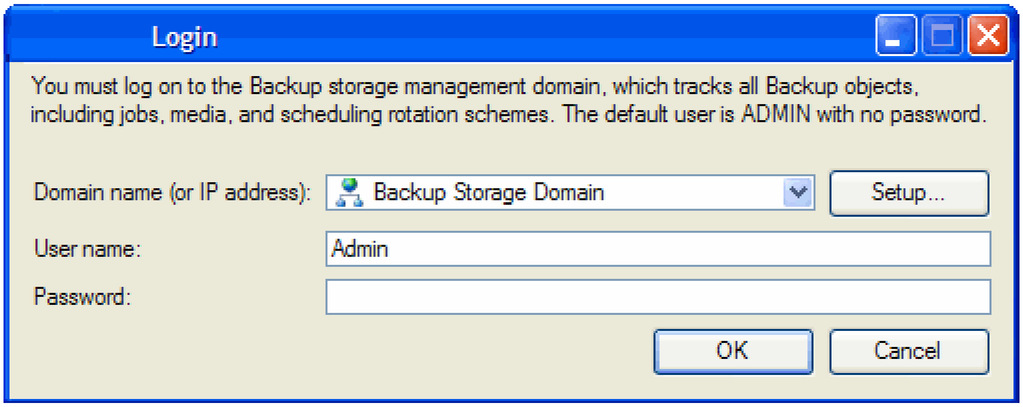
```
[/usr/local/hp/dpx]# ./ dpadmin
```

On Linux systems, you can create a shortcut on your KDE or GNOME desktop. (See the Data Protector Express *Installation Guide* for more information.)

NOTE: If you are running Red Hat Enterprise Linux 4, you may see an error message (such as “libstdc++.so.5 could not be found”) when you start Data Protector Express. This is because the C++ library version that the application was built with is not present on these systems, and the latest version “libstdc++.so.6” is not backwards compatible. If you are using Red Hat Enterprise Linux 4, you can use an RPM package called "compat-libstdc++.rpm" to install the necessary library. This can also be achieved by installing the “Developer’s Tools” package from the Red Hat Enterprise Linux 4 installation CDs.

Logon Window

Each time you start Data Protector Express, you are shown the Data Protector Express **Logon** window.



Login

You must log on to the Backup storage management domain, which tracks all Backup objects, including jobs, media, and scheduling rotation schemes. The default user is ADMIN with no password.

Domain name (or IP address): Backup Storage Domain

User name: Admin

Password:

To log on, you must select a Data Protector Express management domain and enter your user name and your password.

Logging on the first time

CAUTION: Data Protector Express administrators have unlimited access to all of the objects in the storage management catalog. Any user who logs on as the Data Protector Express administrator will have complete access to all of the files and machines contained in the Data Protector Express management domain.

The default user name for the Data Protector Express administrator is **Admin**. There is no default password required for this user to log on.

Your first security step should be to change the Data Protector Express administrator’s password. Refer to *Changing your password* on page 11 for instructions on changing your password.

Grace logons

Your Data Protector Express administrator may have set up your password to expire after a set period of time. For example, your password may expire after 60 days. This forces you to change your password regularly.

If your password has expired, Data Protector Express will prompt you to change your password. If you choose not to change your password, Data Protector Express may still let you log on, even with an expired password. Logging on with an expired password is called a **grace logon**. Your Data Protector Express administrator will determine how many grace logons you are allowed.

When your password has expired and you have used all of your grace logons, Data Protector Express will ask you to change your password when you log on.

Selecting a Data Protector Express management domain

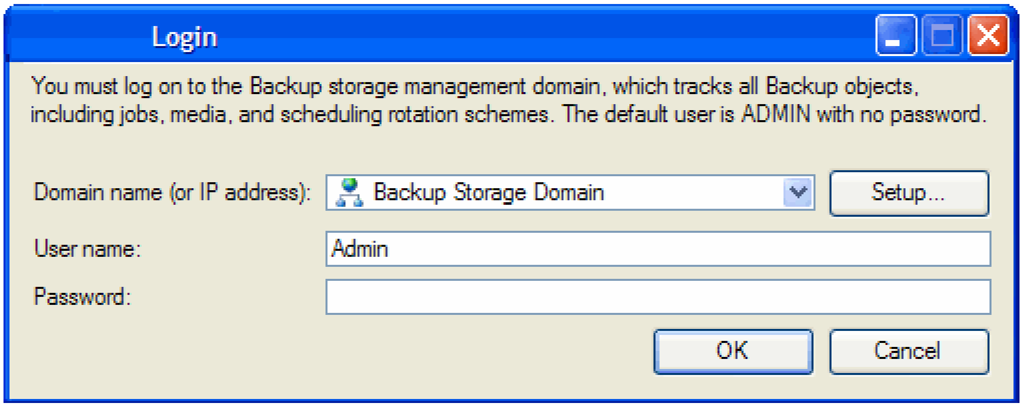
When your Data Protector Express administrator set up Data Protector Express to run on your network, your PC desktop was assigned to a Data Protector Express management domain. Your PC desktop, along with its drives and peripherals, **can only be a member of one Data Protector Express management domain**. The name of this storage domain is the *default* name that appears in the **Domain** list on the **Logon** window.

Normally, you should leave the default name in the list unchanged. This is because you will typically want to work with the Data Protector Express management domain to which your PC desktop belongs.

Occasionally, however, you may wish to work in a different storage domain. You might be asked by a co-worker or your Data Protector Express administrator, for example, to run a Data Protector Express job in a different Data Protector Express management domain.

To select a different Data Protector Express management domain

1. Use the drop-down menu to choose a Data Protector Express management domain from the **Domain name** list. (A list of possible Data Protector Express management domains will appear.)
2. Select the Data Protector Express management domain you wish to use and click **OK**.



You must log on to the Backup storage management domain, which tracks all Backup objects, including jobs, media, and scheduling rotation schemes. The default user is ADMIN with no password.

Domain name (or IP address): Backup Storage Domain

User name: Admin

Password:

NOTE: Although you can log on to different Data Protector Express management domains, you can only create and run jobs within a single Data Protector Express management domain. Further, you can only access files and devices in a single Data Protector Express management domain. This means, for example, that you will be unable to restore files backed up from PC desktops in one Data Protector Express management domain to PC desktops in another Data Protector Express management domain. (If you need to share data from one Data Protector Express management domain to a different Data Protector Express management domain, see *Import Media* on page 144.)

User name and password

After selecting a Data Protector Express management domain, type in your **User name** and **Password**.

If you type your name or password incorrectly, you will be asked to re-enter your user name and password.

In order to log on, your Data Protector Express administrator must first assign you a user name and a password. If you are having difficulty logging on, ask your system administrator to specify again the exact spelling of the user name and password assigned to you.

NOTE: Passwords are case-sensitive; that is, the password USER1 is not the same as the password user1.

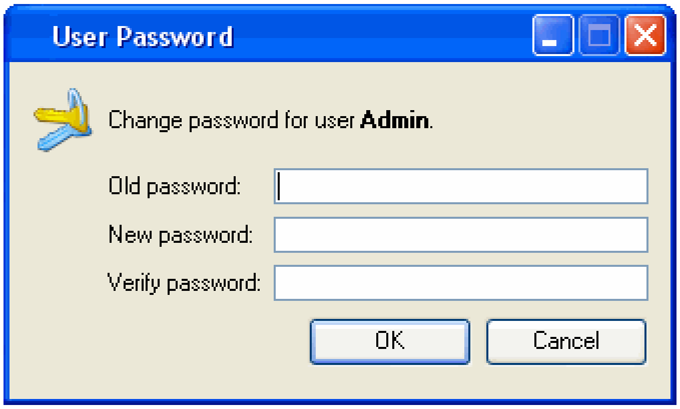
Changing your password

It is a good idea to regularly change your password, particularly if you are working with sensitive and important data.

To change your password

1. Open the **Administration** desk bar.
2. Select **Security**, and then click your **User** icon.
3. Open the **User Password** screen by either

- Selecting **Change Password…** from the **Commands** task pane
- Right-clicking the user and selecting **Change Password…** from the shortcut menu.


User Password

Change password for user **Admin**.

Old password:

New password:

Verify password:

1. Type in your old password and then your new password.
2. Confirm your new password and then click **OK**.

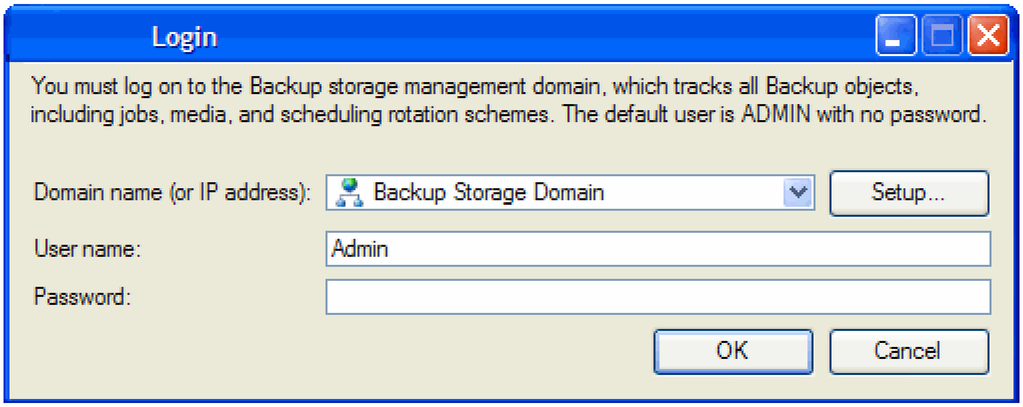
When selecting a password, remember that some passwords are notoriously easy to break. For example, because many people use their birth date or the name of their spouse, these are not good choices for passwords.

TIP: The Data Protector Express administrator can change a user’s password without knowing the user’s current password. Data Protector Express does not even ask you to enter the old password. This is useful when the user has forgotten his or her password.

Logging out

On occasions you may want to change the Data Protector Express management domain you are using or want to log on as a different user. Although you could quit Data Protector Express and restart the program, it is quicker and faster to log on again without quitting Data Protector Express.

To log on again, choose **Logout** from the **File** menu. You will be presented with the Data Protector Express **Logon** window and asked to log on again.



You must log on to the Backup storage management domain, which tracks all Backup objects, including jobs, media, and scheduling rotation schemes. The default user is ADMIN with no password.

Domain name (or IP address): Backup Storage Domain

User name: Admin

Password:

Logging out and running scheduled jobs

Data Protector Express can run scheduled jobs even when no one is logged on. (Only *scheduled* jobs can be performed when no one is logged on to Data Protector Express.) For more information, see *Running Scheduled Jobs* on page 123.

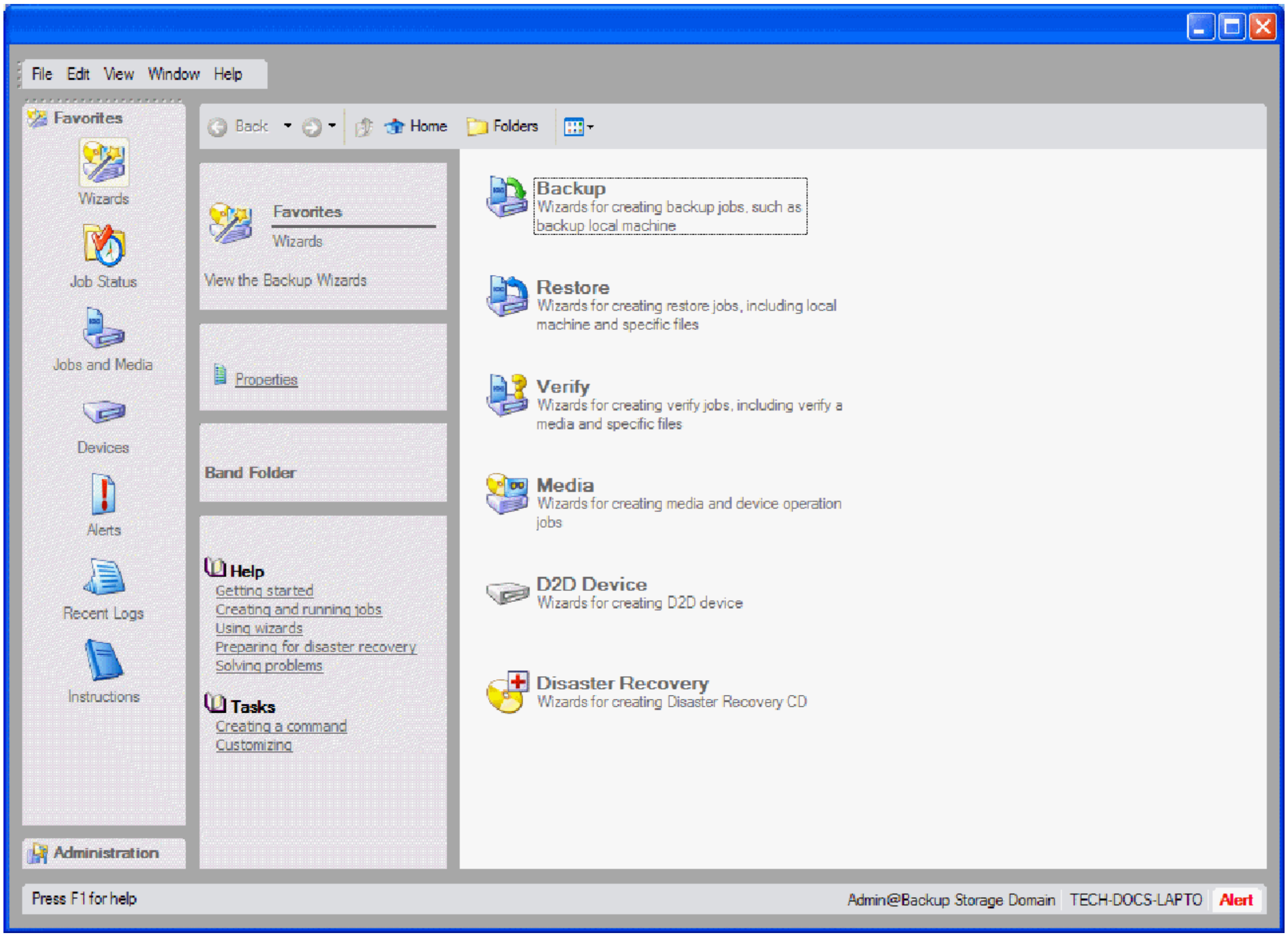
When you leave your PC desktop, you may need to leave Data Protector Express open. In order to prevent unauthorized access to the network, log out of Data Protector Express before leaving your PC desktop. Any scheduled jobs will still run, but no unauthorized users will be able to work with Data Protector Express unless they can log on. (This requires that the Data Protector Express Service be installed and running).

NOTE: If the Data Protector Express service is installed and running, you can close Data Protector Express and your scheduled jobs will still run (see *Appendix B - About the* Data Protector Express *Service* on page 246 for more information).

Main Data Protector Express Window

You use the main Data Protector Express window to view, create and manipulate Data Protector Express objects, such as jobs and tapes.

In addition to the menu bar, the Data Protector Express window has the following parts: menu bar, desk bar, toolbar, task and information panes, the object detail area and the status bar.



View the Backup Wizards

Getting started
Creating and running jobs
Using wizards
Preparing for disaster recovery
Solving problems

Creating a command
Customizing

Backup Wizards for creating backup jobs, such as backup local machine

Restore Wizards for creating restore jobs, including local machine and specific files

Verify Wizards for creating verify jobs, including verify a media and specific files

Media Wizards for creating media and device operation jobs

D2D Device Wizards for creating D2D device

Disaster Recovery Wizards for creating Disaster Recovery CD

Press F1 for help   Admin@Backup Storage Domain   TECH-DOCS-LAPTO   Alert

Menu bar

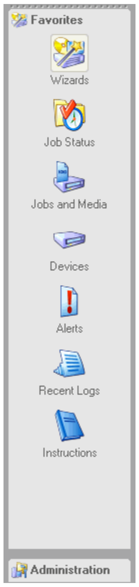
Located at the top of the screen, the menu bar contains several menus that group together similar commands.

To invoke a command from a menu, open the menu and then select a command. The available menus are **File**, **Edit**, **View**, **Window**, and **Help**. For example, to locate and update your Data Protector Express license, select **Licenses** from the **Help** menu.

You will find the menus easy to use and intuitive. Most of the menu commands are discussed in detail later in this manual. Commands on these menus are often related to the current active object in the object detail area. For example, select **File → Properties** to display the **General** property page for the current object. Other commands display menus related to general operation in Data Protector Express, like the **Preferences** page.

Desk bar

Along the left side of the screen is the main Data Protector Express desk bar.



Data Protector Express provides two desk bars to organize similar sets of tasks and commands. For example, you open the **Favorites** desk bar to display the **Wizards** view, which contains the wizards that Data Protector Express provides to help you quickly create jobs. The **Favorites** views also contains the **Job Status** view that lets you view the status of jobs that are scheduled, running or completed. The **Jobs and Media** view lets you work with backup, restore, verify and media jobs, and so on. To display a different view, click on the category heading along the desk bar. For information about creating a custom desk bar, see *Creating a custom desk bar* on page 18.

TIP: To organize long lists of jobs or objects in any view, sort the list by any column heading.

The **Favorites** desk bar contains the following views:

- **Wizards:** The **Wizards** view contains groups of pre-defined wizards that you can use to create backup, restore or verify jobs, work with media, create a virtual library, or create bootable CDs or DVDs for disaster recovery. For more information about these wizards, see *Working with Data Protector Express wizards* on page 25.
- **Job Status:** The **Job Status** view contains a list of jobs that are scheduled to run, have completed running, or that are currently running. To sort the list, click on any column heading.
- **Jobs and Media:** The **Jobs and Media** view contains a list of all of the jobs or media in Data Protector Express that you have created or for which you have permissions.
- **Devices:** The **Devices** view contains a list of any devices contained in the Data Protector Express management domain to which you have access. You might have access to a D2D device, a CD or DVD device, a library or one of many types of tape devices. Use this view to quickly locate a device and view its property information.

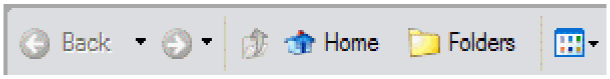
- **Alerts:** The **Alerts** view displays a list of alerts that Data Protector Express generates while jobs are running. You can view any alert displayed on this view. Also available from this view are evaluation alerts. An evaluation version of optional features in Data Protector Express is automatically installed when you originally install Data Protector Express. Each time you access an optional feature that is running as an evaluation, Data Protector Express displays an evaluation alert for 60 days. Use the **Clear Evaluation Alerts** command to clear all of these alerts at once, or you view each alert and clear them individually.
- **Recent Logs:** The **Recent Logs** view contains a list of logs that Data Protector Express has created as each job has completed.
- **Instructions:** The **Instructions** view contains a set of instructions for jobs that are scheduled to run on the current day. These instructions provide details about each job schedule to run that day including the job name, the time the job will run, who has set up the job, and the media required for the job. Use this information to prepare for jobs each day.

The **Administration** desk bar contains the following views:

- **Catalog:** The **Catalog** view contains a list of every object contained in the Data Protector Express management domain. These objects are organized in a hierarchical tree view similar to how data on a computer is organized. For example, expand **Job Status** to see a list of completed, running or scheduled jobs. Use the **Catalog** view to display property information about any job, device, media, user, or machine in the Data Protector Express management domain.
- **Security:** The **Security** view contains information about every user or group in the Data Protector Express management domain. Use this view to display, edit, or create user information including permissions and passwords.
- **Preferences:** Select **Preferences** from the **Administration** desk bar to display the **Preferences** property page for the current user. Use this page to set up general user preferences for the color scheme, animations, a web browser, and so on. For more information about the settings on this page, refer to *Preferences* on page 227.
- **Configure Domain Server:** Select **Configure Domain Server** to set up email settings for the Data Protector Express management domain. For more information about configuring email settings, refer to *Configuration page* on page 187.
- **Messages:** Select **Messages** to see the contents of the trace files that Data Protector Express creates while it is running. In contrast to job logs, information is displayed here if you enable logging for things like the network, the Data Protector Express catalog, specific devices, and so on. You can track information about these objects by enabling auditing on the **General** property page for the selected object. For example, to enable auditing for a device, open the Devices view from the **Favorites** desk bar, select a device and view its properties. Then select **Enable Auditing**.
- **Reports:** Select **Reports** to create a report on any object or group of objects in the catalog. For instructions on running reports, refer to *Reports*.

Toolbar

The toolbar contains several command buttons related to the main viewing area of the screen.



- Similar to clicking Back in a web browser, the **Back** button redisplays the most recent Data Protector Express menu or submenu. Click this button to return to that view quickly.

- Similar to clicking Forward in a web browser, the **Forward** button redisplays the previous menu or view since you pressed the **Back** button.
- The **Up** button changes the currently displayed folder (or container) to the next higher folder in the hierarchy, that is, the folder that contains (is the parent of) the current folder.
- The **Folders** button shows or hides a hierarchical tree view of the Data Protector Express management domain.
- The **Home** button takes you quickly to your Home folder which contains all jobs that you have defined and all media that is used by your jobs.
- The **Views** button lets you change how objects are displayed in the object detail area (e.g., **Tiles**, **Icons**, **List** or **Details**, etc.).

Task and information panes

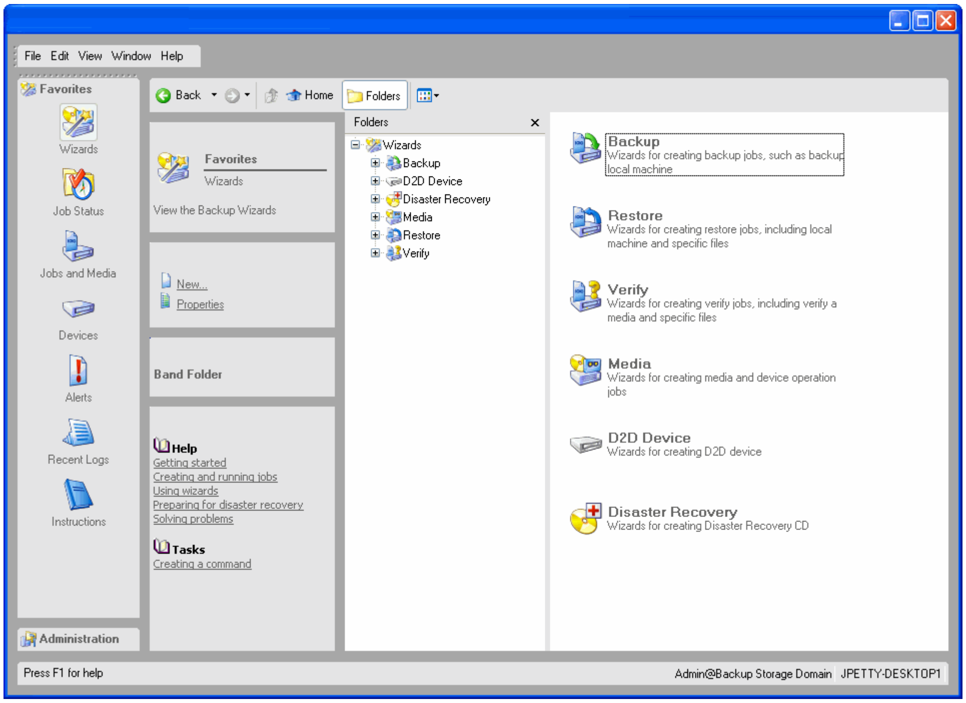
Task and information panes are located to the left of the main object detail area. These areas are updated as you work in Data Protector Express and always contain shortcuts to commands or tasks related to the active object. Tasks and information are organized together into different panes.

- **General:** Presents basic information about the current object, such as a job title and location in the storage management server
- **Commands:** Contains shortcuts to tasks that are related to the selected object, such as New, Run, Rename, etc.
- **Details:** Describes the current active object, such as type of object
- **Dynamic Help:** Contains links to task-related help and other topics of interest to the current object

Click the **Expand** arrow in the right corner of a pane to expand or collapse the information.

Detail viewing area

The remainder of the screen is the **detail area**. When you select the **Folders** command, the detail view area is split vertically into a hierarchical tree view of the current view on the left and a detail area on the right. The contents of this view change as you navigate within Data Protector Express. Selecting a view from the desk bar or the hierarchical tree updates the detail area to show the objects contained in that view or folder.



Backup
Wizards for creating backup jobs, such as backup local machine

Restore
Wizards for creating restore jobs, including local machine and specific files

Verify
Wizards for creating verify jobs, including verify a media and specific files

Media
Wizards for creating media and device operation jobs

D2D Device
Wizards for creating D2D device

Disaster Recovery
Wizards for creating Disaster Recovery CD

Press F1 for help | Admin@Backup Storage Domain | JPETTY-DESKTOP1

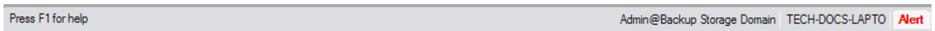
When working with objects presented in the object detail area, keep the following in mind:

- The hierarchical tree view displays folders, machines, and other devices that contain more files or folders. If an entry in the tree does not contain other files or folders, it is displayed only in the main detail area of the screen.
- To display the files in a folder, machine or other device, open it by clicking on it in the tree view area.
- To view the folders within a folder, expand the tree view by clicking on the **Expand tree** icon next to the folder. You can also double-click the folder and it will both expand and display its contents in the main detail area.
- To close a folder, click the **Collapse tree** icon next to the folder. You can also double-click the open folder and it will close.

There are numerous keyboard shortcuts available that make it easier to work with files, folders and other items in Data Protector Express. For more information, see *Keyboard shortcuts* on page 20.

Status bar

The **Status** bar displays short descriptive messages about the menu commands on its left side. The **Status** bar displays the current user's name, the storage domain to which the user is logged in, and the name of the machine at which the user is working.


Press F1 for help | Admin@Backup Storage Domain | TECH-DOCS-LAPTO | Alert

An **Alert** button appears in the lower right corner of the status bar. This button flashes when there is an issue that requires your attention. For example, Data Protector Express might not be able to locate a backup device you specified for a job and will send a message to the **Alert** window to notify you of the problem. When you click on the **Alert** button, Data Protector Express displays the **Alert** window so you can view any pending alerts.

You can also resize the Data Protector Express window. Point to the lower right corner of the **Status** bar and drag the window to the desired shape. To show or hide the **Status** bar, open the **View** menu and select **Status bar**.

Customizing the main Data Protector Express window

Several elements of the main Data Protector Express window can be rearranged or their appearance modified. Changes to settings are retained for future work sessions.

- Move the Menu bar and Desk bar to a new location on the screen. To move them, cursor over the area with the dots. The cursor changes to double arrows. Drag the bar to the new location. You can place them at the top or bottom of the screen, along the right or left side of the screen, or you can let them "float" anywhere on the screen.
- Show or hide the Status Bar. Click the **View** menu and select Status Bar to show or hide it.
- Change the appearance of the detail area. Click the **Views** button and select **Tile**, **Icons**, **List** or **Details**.
- Change the color scheme and animation settings for Data Protector Express. From the **File** menu, select **Preferences**.
- Organize jobs, commands, and other objects by creating a custom desk bar. See *Creating a custom desk bar*, below.
- Change an icon associated with an object. See *Changing the icon associated with an object* on page 18.
- Add custom descriptions for objects. See *Adding custom descriptions to objects* on page 19.
- Create a custom profile that contains only those settings and features that you want to use while running Data Protector Express. See *Customizing profiles* on page 19.

Creating a custom desk bar

A desk bar groups together similar objects and commands. You can create a custom desk bar and add jobs and tasks to it that you perform frequently or that you want to find easily. A custom desk bar can contain backup jobs, media jobs, job groups, custom folders or user information, and more. You create a custom desk bar or other menus by adding them to a profile folder. A profile folder contains all of the possible menus and commands that you might use in Data Protector Express. Alternatively, you can create a template that contains only a few of the menus and commands available in Data Protector Express.

To create a custom desk bar

1. Right-click the area in which you want to place the desk bar and select **New**.
2. Select **Band Folder** and type a name for the desk bar.
3. Click **OK**.
4. Right-click the new desk bar.
5. Add commands or jobs as needed.

Changing the icon associated with an object

You can change the icon associated with any object in Data Protector Express.

1. Select an object from the detail area on the screen then select the **Properties** command. You can also right-click the file, machine, task or other object and choose **Properties** from the **Shortcut** menu.

   The **General** property page appears.
2. Click the **Change Icon** button.
3. Select an icon from the Icon browser and click **OK**.

4. Save the new icon by clicking **Apply** or **OK** to closes the **Properties** screen.

TIP: To keep the existing icon associated with this object, click **Cancel** to close the properties page without saving your changes.

Adding custom descriptions to objects

You can add custom descriptions for any object in Data Protector Express. These descriptions appear under and object in the main detail area or in the Status bar at the bottom of the screen.

1. Select an object and display the **General** property page.
2. Enter a new description in any of the following fields:
    - **Description:** Enter a message here that will appear below the object icon in the main detail area.
    - **Tooltip:** If you have created a custom menu, enter a message here that will appear when you roll over the object.
    - **Status help:** If you have created a custom menu, enter a message here that will appear in the Status bar when you select the object.
3. Click **Apply** or **OK** to save your changes.

Customizing profiles

You can customize your profile in Data Protector Express so that it contains only those settings and features that you want to see when you run Data Protector Express. When you customize your profile, you enable any menu, view, job, or task that you want to see and you disable any menu, view, job, or task that you do not want to see. You can include or exclude any desk bar or only a few commands within a desk bar, any menu or only a few commands within a menu, any job type (backup, restore, etc.), and so on. Your custom profile could contain only custom menus with custom commands.

When a user starts Data Protector Express with a custom profile, he sees only those features that have been enabled. All other features are hidden from view. You might create a custom profile if you have users who need only a limited set of Data Protector Express features.

To customize a profile

1. Select **View → Administration → Catalog**.
2. In the **Folders** view, expand the tree under **Home** until you see the user name for which you want to modify the profile.
3. Expand the tree under the user name until you see the **.Default** profile.
4. Make a copy of the **.Default** profile to save the original settings.
    a. Right-click the .Default profile and click **Copy**.
    b. Right-click the user name and click **Paste**.

    Data Protector Express adds a new profile named **Copy of .Default** to the tree under the user name.

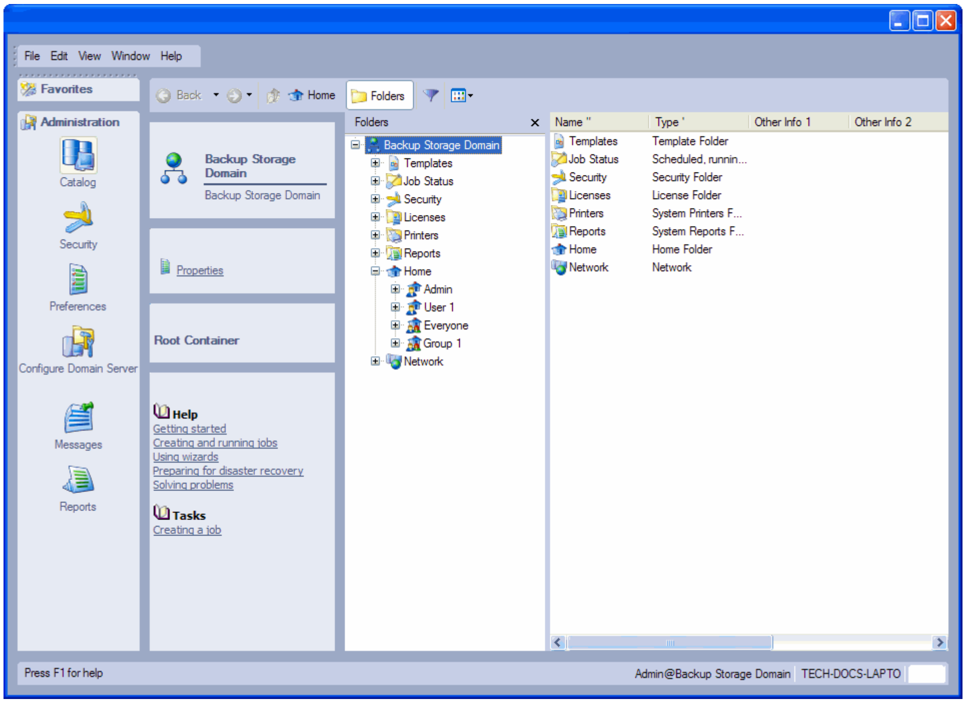
    c. Rename the new profile.
5. Expand the tree under the Default profile.
6. Modify the menus and job types that you want to include in the profile.
7. The next time a user starts Data Protector Express, he will use this profile.

Working with Objects in the Main Data Protector Express Window

You can easily change how objects are displayed in the object detail area. This will assist you in working more effectively and quickly.

Arranging objects

In the object detail area, you can arrange the objects in several different ways using either buttons on the toolbar or the **Arrange Icons by** submenu. Depending on the view, you can sort the objects by name, size, type or one of several other settings. You can also use the column head at the top of the object detail area to change how the objects are sorted when working in **Details** view.



Name	Type	Other Info 1	Other Info 2
Templates	Template Folder		
Job Status	Scheduled, runnin...		
Security	Security Folder		
Licenses	License Folder		
Printers	System Printers F...		
Reports	System Reports F...		
Home	Home Folder		
Network	Network		

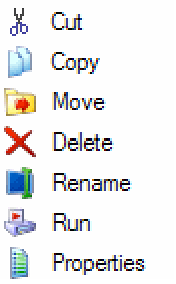
Keyboard shortcuts

Besides using the mouse to work with objects in the main Data Protector Express window, there are several keyboard shortcuts that will speed up your work. The next time you work with Data Protector Express, try these keyboard shortcuts. These shortcuts are available in the graphical user interface and in the character user interface.

- The TAB key will move the active or highlighted area to a different area of the window.
- The PLUS SIGN (+) on the numeric keypad or the RIGHT ARROW key *expands* the tree in the tree view area.
- The MINUS SIGN(-) on the numeric keypad or the LEFT ARROW key *collapses* the tree in the tree view area.
- The ARROW keys also select objects in the tree view area and in the object detail area, as well as change the active page.

Shortcut menus

When you right-click in most windows, the shortcut menu appears. The shortcut menu list commands that pertain to the active portion of the screen or to the currently-selected object. This is often the fastest and easiest way to create new objects and modify existing objects.



Find button

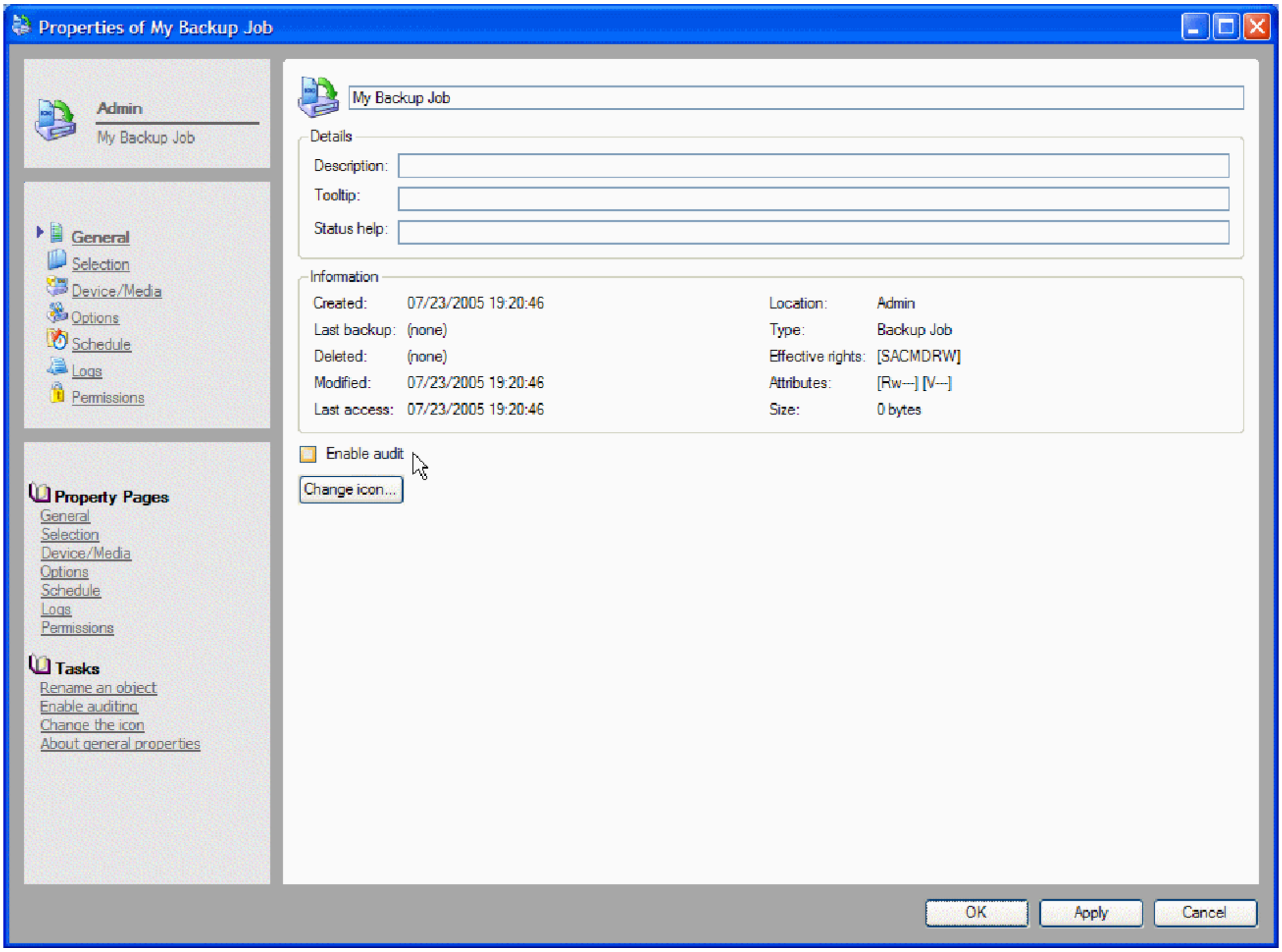
The **Find** button lets you locate objects in the storage management catalog quickly without searching through multiple volumes and directories.

To use the **Find** command, click on the **Find** button, select **Find...** from the **Edit** menu or press F3. In the **Find** window, type the name of the object you want to find. Data Protector Express will search through the catalog, attempting to locate that object. When the object is found, it will be displayed and highlighted.

Note that the **Find** command is not case-sensitive and you can use the wildcard characters **?** (question mark) and *(asterisk) .

Property pages

Every object in the Data Protector Express catalog has a set of **property** pages associated with it. Use these property pages to modify settings for an object and to view logs, messages, diagnostics or other reporting information that Data Protector Express generates.



Properties of My Backup Job

Admin
My Backup Job

My Backup Job

Details

Description:
Tooltip:
Status help:

Information

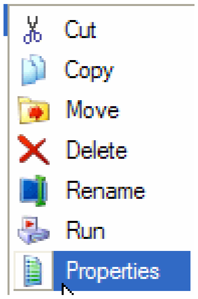
Created:	07/23/2005 19:20:46	Location:	Admin
Last backup:	(none)	Type:	Backup Job
Deleted:	(none)	Effective rights:	[SACMDRW]
Modified:	07/23/2005 19:20:46	Attributes:	[Rw---] [V---]
Last access:	07/23/2005 19:20:46	Size:	0 bytes

□ Enable audit

Opening property pages

You display the property page of an object in one of several ways:

- Select the object with the mouse or keyboard, and then click **Properties** on the **Command** task pane.
- Right-click the object to display a shortcut menu, then select **Properties**.
- Select the object, and then select **Properties** from the **File** menu.



Open a property page in one of several ways

NOTE: You can leave open property pages when you return to working in the main Data Protector Express window and you can have several property pages open at once.

Reports

Data Protector Express has a series of helpful diagnostic and summary reports available. These predefined reports are designed to gather specific information that is stored in the Data Protector Express catalog. Reports can contain summary information or detailed information.

Types of reports

Generating reports with wizards ensures that you have the reports you need whenever you need them. Data Protector Express provides the following report generation wizards. You can choose to produce either a summary report or a detail report from each wizard.

Objects at Risk wizard

Summary view: Generate a report that summarizes the objects in the Data Protector Express catalog that are at risk.

Detail view: Generate a report that contains a detailed account of the objects in the Data Protector Express catalog that are at risk.

Media Information wizard

Summary view: Generate a report that summarizes information about the contents of media that are part of the Data Protector Express catalog.

Detail view: Generate a report that contains detailed information about the contents of media that are part of the Data Protector Express catalog.

Catalog Listing wizard

Summary view: Generate a report that summarizes the contents of the Data Protector Express catalog.

Detail view: Generate a report that contains detailed information about the contents of the Data Protector Express catalog.

Additional reporting capabilities

Besides its reporting capabilities, Data Protector Express has several advanced features to help you track and compile information that Data Protector Express generates.

- Select **Alerts** on the **Favorites** desk bar to view Data Protector Express alerts. You can also open alerts by clicking the Alerts button in the lower right corner of the screen.
- Select **Recent logs** on the **Favorites** desk bar to view recent logs that Data Protector Express has generated. Use this command to print or save the log. You can also set up Data Protector Express to send the logs automatically to a specified email address. For more information about emailing logs, see *Emailing job logs* on page 131.
- Select **Instructions** on the **Favorites** desk bar to see which media and devices are required for the scheduled jobs. See *Viewing and printing scheduled job instructions* on page 126 for more details.
- Select **Messages** on the **Administration** desk bar to view or print information about the general operating state of the machine that do not require attention in order for Data Protector Express to continue running. Sometimes referred to as trace messages, this information is updated each time Data Protector Express performs an operation on an object for which you have enabled auditing. See *Audit Logs* on page 131 for additional information.

Printing reports

1. Select **Reports** from the **Administration** desk bar.
2. Select the Base object from which to generate the report. Predefined reports gather information for the entire storage domain. The report will generate information for all of the objects in the Data Protector Express hierarchy that are below the object specified as the base object. Click the **Browse** button to select a new object.

   NOTE: Media information reports do not require a base object.

3. Double-click an available report type in the main object detail area, for example, Media Information.

   The **Report** screen appears.
4. Choose the **Report type** that you want to run: Summary or Details.
5. Select a printer and font for the report.
6. Update the **Printer settings** and other information.
7. Click **Print**.

   The report is printed on the selected printer.

NOTE: These reports can output many hundreds of pages. Therefore, we recommend that you save the reports as a file. For instructions on saving a report as a file, follow the instructions below in the *Saving reports* section.

Saving reports

By default, reports are printed directly to a printer. If you want to save a report as a file, you can set up a printer that prints files to a filename. Depending on the type of printer you set up, you can save reports as PDF files, postscript files or plain text files. To create PDF files requires that you have access to Adobe® Acrobat® Distiller® or another product capable of creating PDF files. The following instructions describe how to create a generic text printer on a Microsoft Windows PC desktop.

To create a generic text printer

Add a new printer from the Windows Start menu. For example, in Windows XP, select Printers and Faxes on the Start menu, then select **Add a printer**.

1. Working through the printer wizard, create a local printer.
2. On the Select a Printer Port screen, select **FILE** (Print to File).
3. On the Install Printer Software screen, select **Generic** for the manufacturer and Generic/Text Only for the printer.
4. On the **Name Your Printer** screen, select a unique name for this printer so that it is easy to identify in Data Protector Express.
5. Do not use this printer as your default printer.
6. Continue through the wizard until the printer is created and accept any remaining default settings.
7. The printer is ready for use in Data Protector Express.

To save a report as a file

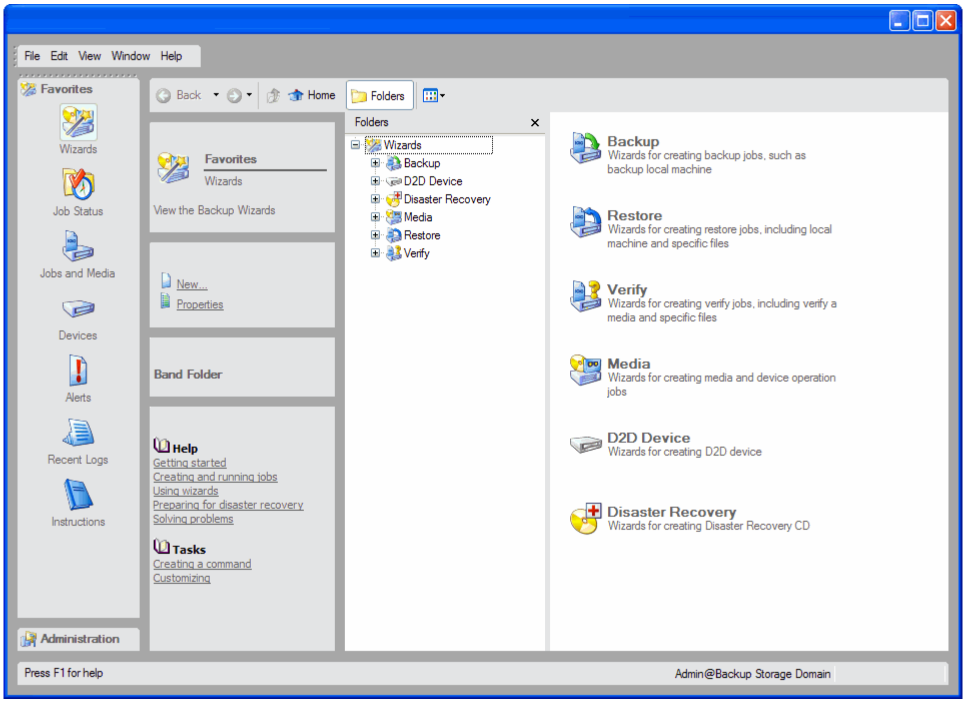
The next time you create a report in Data Protector Express, follow these steps to save the report as a file.

1. From the **Administration** desk bar, select **Reports** and choose the report you want to generate.
2. On the Report screen, select the printer you created above as the destination for your report.
3. As the report is generated, Data Protector Express will prompt you to name the file.
4. Enter the path and filename for the report (e.g., C:\ObjectReport.txt).

You can print this report or view it in a compatible editor. Generic text files can be viewed with most text editors like Notepad or Microsoft Word.

Working with Data Protector Express wizards

Data Protector Express wizards give you a fast and quick way to perform most tasks. You can use wizards to create and schedule backup jobs, restore jobs, verify jobs, and media jobs. You can also create a virtual library, test a library or device, or clean a device from the **Wizards** view or perform operations related to disaster recovery. Data Protector Express wizards will guide you through each step necessary to create and run the job or task you select.



Backup
Wizards for creating backup jobs, such as backup local machine

Restore
Wizards for creating restore jobs, including local machine and specific files

Verify
Wizards for creating verify jobs, including verify a media and specific files

Media
Wizards for creating media and device operation jobs

D2D Device
Wizards for creating D2D device

Disaster Recovery
Wizards for creating Disaster Recovery CD

The name of each Data Protector Express wizard option indicates what task that wizard helps you perform. The descriptions are self-explanatory. The **Backup**, **Restore**, and **Verify** wizards create jobs. For additional information about creating these jobs without the Data Protector Express wizards or about the jobs the Data Protector Express wizards created, review the rest of this manual. Media wizards help you format or erase media, organize media in a library, import the contents of media into the Data Protector Express catalog, and so on. The **Disaster Recovery** wizard helps you create a bootable CD or DVD for use during a disaster recovery operation. The **D2D Device** wizard helps you create a virtual library.

Data Protector Express walks you through the task that you have selected. You are prompted to name the job, select files or devices to include in the job, select media as appropriate, and set up a schedule to use when running the job. By the time Data Protector Express finishes the wizard, you have a job that is ready to run. You can also create custom wizards or edit existing wizards. To create a custom wizard, see

Custom wizards on page 28. To edit a job created with a wizard, select the job, and view the job's property pages.

Available wizards

Data Protector Express contains over twenty wizards grouped into logical categories. Use the **Wizards** view to select a category from which to create jobs and tasks efficiently. Wizards are grouped into the following categories.

Backup job wizards

Backup wizards help you create backup jobs that fit the most common backup situations. These wizards walk you through the process of setting up a job including selecting backup mode, backup devices, files to include in the job, scheduling information and media rotation. For more information about selecting files for backups, see *Backup Selection Concepts* on page 55. Data Protector Express provides the following backup job wizards:

Backup Local Machine: Use this wizard to back up the contents or a portion of the local machine.

Backup all Servers: Use this wizard to back up the contents or a portion of the contents of all servers in the Data Protector Express management domain.

Backup all Workstations: Use this wizard to create a backup job that backs up all or a portion of the data stored on all PC desktops included in the Data Protector Express management domain.

Backup all Machines: Use this wizard to create a backup job that backs up the data or a portion of the data on all machines included in the Data Protector Express management domain whether they are individual PC desktops or servers.

Backup Specific: Use this wizard to create a backup job that backs up only specific files stored on the local hard disk or on other PC desktops in the Data Protector Express management domain. Use this wizard to back up only a few selected files on a regular basis.

Restore job wizards

Restore wizards help you create restore jobs that fit the most common data restore situations. These wizards walk you through the process of setting up a job including selecting the correct versions of files to be restored, the media location of these versions, and the network destination for the restored files. For more information about restoring files, see *Restore Selection Concepts* on page 67. Data Protector Express provides the following restore job wizards:

Restore Specific: Use this wizard to restore certain files. This wizard will guide you through the process of locating a version of a particular file or files no matter where the file versions are located.

Verify job wizards

Verify wizards help you create verify jobs that fit the most common data verification situations. For more information about verify jobs, see *Verify Selection Concepts* on page 80. Data Protector Express provides the following verify job wizards:

Verify Media: Use this wizard to compare the contents of a particular media with the data that exists on a local PC desktop or file or application server. This wizard is useful when you need to verify the integrity of the backup data on a specific backup media.

Verify Specific: Use this wizard to compare a file on a local PC desktop or file or application server with its backup versions available on backup media. This wizard is useful when you need to verify the integrity of backup data for certain files.

Media job wizards

Media wizards help you create jobs to perform several common tasks related to backup media. Some backup devices do not support all of these tasks. If your backup device does not support a task, the wizard will not be available. If a wizard you want to use is not available, review the manufacturer's documentation for your backup device to see if you can perform the tasks manually. Data Protector Express provides the following media wizards:

Format Media: Create a job that formats media and assigns a name to it. You might use this wizard to schedule media formatting remotely or after normal business hours or to initialize virtual media.

Import Media (into the catalog): Create a job that imports media into the Data Protector Express catalog from another server. This wizard is useful if you want to import media without an administrator being present to monitor the job.

NOTE: This wizard is unavailable when working with virtual media.

Erase Media: Create a job to erase media whose data is no longer needed. You might use this wizard to schedule a job that erases the contents of several media outside of normal business hours.

Sort Media: Create a job that reorganizes the media in a library. Use this wizard to schedule a sorting task for a time when it will have the least impact on users attached to the Data Protector Express management domain.

Eject Media: Create a job that ejects media from the selected device. If this wizard not available, either your device does not support this command or no device is selected. You might use this wizard to eject media after a backup job is completed as a visual cue to your support staff that the job is done.

Move Media: Create a job that moves media from one storage slot in a library, drive, or mail slot to another. You might use this wizard to move media automatically at the end of a series of backups to help you manage media rotation more effectively.

Copy Media: Create a job that copies the contents of a selected media to another media. You might use this wizard to create redundant copies of media that you can store offsite for safekeeping.

Media Content: Create a job that determines the contents of the selected media. You might use this wizard to determine which files or file versions are available on a piece of media that is unidentifiable. You might then use the Import Media wizard to import the contents of the media into the Data Protector Express Catalog.

Test Device: Create a job that tests a backup device. You might use this wizard to ensure that Data Protector Express and a backup device are communicating properly.

Test Library: Create a job that tests a library. You might use this wizard to ensure that Data Protector Express and a library are communicating properly.

Insert Media: Create a job that inserts media into a library storage slot from an import/export slot.

Remove Media: Create a job that removes media from a library. You might use this wizard to schedule a job that removes several media from a library outside the normal business hours.

Clean Device: Create a job that inserts a cleaning cartridge into a library device and runs it through a cleaning cycle. You might use this wizard to schedule a cleaning cycle on a library device outside the normal business hours. This wizard is available only for devices that support automatic cleaning.

Identify Media: Create a job that identifies the media currently loaded in a device. You might use this wizard to routinely identify media in a library so that the latest information is available to Data Protector Express.

Retension Media: Create a job that rewinds the selected media to improve its tension. Media that has been wound and rewound several times loses its tension and is not as efficient during backup jobs. Retensioning media improves its overall life as well as the accuracy of backups.

Restore Catalog: Create a job that restores the catalog for the Data Protector Express management domain from any available media.

D2D device wizards

Create Virtual Library: Create a virtual library device and assign a storage folder to it. If you intend to make use of D2D2Any backups you must create a virtual device.

Disaster recovery wizards

Disaster recovery wizards help you perform disaster recovery preparation tasks that fit the most common situations. For more information about disaster recovery operations, see *Disaster Recovery* on page 249. Data Protector Express provides the following disaster recovery wizard:

Make Bootable CD: Use this wizard to create a bootable compact disk that you can use to start your system in the event of a data disaster. Each machine should have a bootable CD, and bootable media should be recreated when a PC desktop configuration is altered; that is when the operating system is modified or hardware changes occur on the PC desktop.

Custom wizards

To create a custom wizard, follow these steps.

1. Open the **Administration** desk bar, select **Catalog** and locate **Templates**.
2. Open the **.default** template and select either **Character Based UI** or **Graphical Based UI.**
3. Double-click **Desk Bar, Favorites,** and then **Wizards**.
4. Right-click in the details area and select **New …**.

   The **New Object** screen appears.
5. Enter a name for the wizard, select **Command** for the object type and click **OK**.
6. Set up the new wizard as follows:
   - On the **General** property page, enter a description and other information
   - On the **Command** property page, select the command that this wizard will run; if desired, select a specific on which to run the command
   - On the **Permissions** property page, select the users and groups that may run the wizard
7. Click **Apply** or **OK** to save your changes.

The wizard will be available to all users with permissions to the object.

Viewing optional features

If an option is not listed on a screen, e.g., **Disaster Recovery** on the **Wizards** view or **SQL Agent** on the **Catalog** view, it may be for one of the following reasons:

- The evaluation license for the option has expired. Optional features are installed automatically when you install Data Protector Express. Once the license expires, you can no longer use an optional feature without purchasing a license.

- The option is not available due to your license agreement. For example, you might be using a Standard edition of Data Protector Express and are looking for features that are available only in the Advanced edition.
- An error occurred when starting Data Protector Express. Review the alerts to see if an option failed to start properly when you started the application.

Chapter 3: Creating Jobs with Data Protector Express

To transfer files back and forth from backup devices to PC desktops and file or application servers attached to a network, you create and run **jobs**. You organize and store these jobs in **folders** you create on **job pages** in the main Data Protector Express administrator window.

In this section

- Jobs and Media view and the Job Status view
- Creating New Jobs
- Renaming, deleting, copying and moving jobs

Overview

You use backup jobs in order to protect against loss of data due to disasters or equipment malfunction, to archive important files and to create permanent historical records. Restore jobs allow you to transfer stored files on media back to file or application servers and PC desktops. Verify jobs compare the version of a file stored on media, such as tapes, with current versions of the file stored on machines on a network.

You can create folders to store these jobs on one of the job pages. These folders and the jobs stored within them can be renamed, deleted and moved to new locations.

Data Protector Express can create and run several types of jobs: backup jobs, restore jobs, verify jobs, media jobs, and disaster recovery jobs. You can also create several types of jobs and add them to a Job Group so that they will run together unattended.

Backup jobs

Backup jobs copy selected files *from* file or application servers and PC desktops *to* various storage media, such as tapes, writable CD or DVD media, or virtual media. These backups can be stored, preserving a copy of the file for future use. You might create and run a backup job for one of the following reasons:

- To ensure the integrity of data should a disk drive on a PC desktop or file or application server fail.

  This is perhaps the most common type of backup job. Its purpose is to protect valuable information in case of a disastrous data loss. This type of backup allows a company or organization to return to work quickly, even after the failure of a main file or application server. To be effective, these backup jobs must be run regularly (usually daily) *without exception* to ensure that recent changes to files can be safely restored. This type of backup job is for *disaster protection.*

- To remove files—from a PC desktop or file or application server—that are infrequently used.

  Some files are important to keep, but are never or rarely used. For example, you may wish to keep a copy of correspondence from last year for legal reasons, but have no regular need to access these files under normal circumstances. By backing up the files onto a tape or other media, you safely store the media, preserving a copy of the file and then delete the file from the PC desktop or file or application server. Data Protector Express will keep track of which files you have backed up and which media they are located on. As long as the media is undamaged and safely stored, you will be able to retrieve the file if necessary. Test the archive tape before you assume that it can be relied upon. This type of backup job is called an *archive job.*

- To store a copy of a particular historical version of a file.

  Sometimes you may wish to keep a permanent record of a particular version of a file. For example, you may need to preserve a copy of company records as they exist on a certain date or before they are converted for use in a new program. You can store a copy of the file as it exists on a certain date and instruct Data Protector Express to make certain that this file and the media it is on are not overwritten with other data. Data Protector Express will keep track of the file and the media in its catalog and you will be able to retrieve it if necessary. Unlike an archive job, the file that was backed up is not deleted from the file or application server or PC desktop. This type of backup job is sometimes called a *historical backup.*

You can also create several backup jobs and add them to a Job Group so that they will run unattended.

Restore jobs

Restore jobs copy files *from* backup devices *to* PC desktops and file or application servers. You might create and run a restore job when files on a PC desktop or file or application server have been lost because of a disk crash, when you need to view a file that has been archived (backed up onto media and then deleted) or when you need data from a particular historical version of a file. You can also create restore jobs and add them to a Job Group so that they will run unattended.

Verify jobs

Verify jobs compare a file on some media, such as a tape, with a file on a PC desktop or file or application server. These jobs *verify* that the two files are in fact the same file. A verify job is useful when you wish to make sure a particular file, such as a program file, has not been corrupted or modified. You can also create several verify jobs and add them to a Job Group so that they will run unattended.

Media jobs

Media jobs perform routine tasks on physical or virtual media such as formatting or erasing media, moving media from one storage slot to another in a library, or identifying the contents of the media. A media job is useful when you want to manage the media contained in your backup devices. You can also create several types of media jobs and add them to a Job Group so that they will run unattended.

Disaster recovery jobs

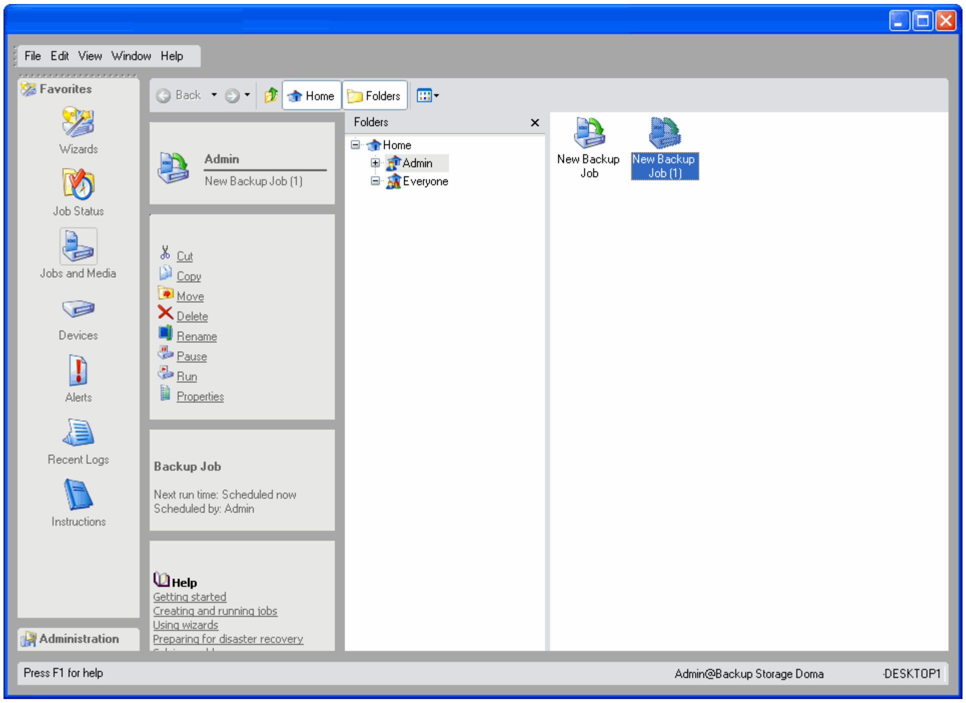
Disaster recovery jobs create bootable media which you use to recover your system configuration, software and data following a system or disk failure. You can use this media to boot your system and initiate the recovery process.

Job Group

A Job Group is a collection of jobs that will be run together either sequentially or simultaneously. Running jobs together from a single job group can streamline your data management procedures. You can include any type of job in a job group. With the exception of scheduling, each job retains all of its job settings including file selections, backup mode, media or device destination. The jobs use the schedule setting for the job group.

Jobs and Media view and the Job Status view

You can view your jobs by selecting **Jobs and Media** from the **Favorites** desk bar. You create, modify and run backup, restore, verify or media jobs with the **Jobs and Media** view. Within this view, jobs are organized by owner or access rights. Select the **Jobs and Media** view and notice that each user or group in the storage domain is listed. Expand your user name and you will see a list of all jobs that you created or to which you have access rights. For additional information about working with media on this view, refer to *Managing Media with the Jobs and Media View* on page 147.



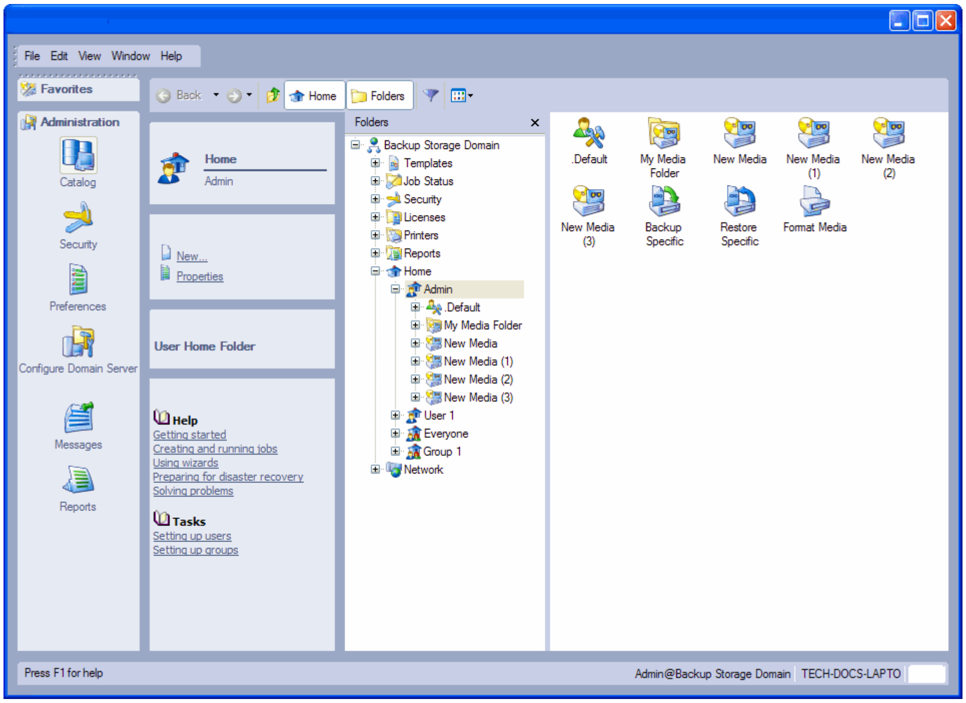
Admin
New Backup Job (1)

Backup Job
Next run time: Scheduled now
Scheduled by: Admin

Press F1 for help
Admin@Backup Storage Doma
DESKTOP1

The **Job Status** view on the **Favorites** desk bar displays a list of all jobs and all occurrences of a job. That is, for any job that runs repeatedly, an entry appears in this list each time it is scheduled to run. You can sort this view by status to organize the jobs more clearly. Doing so groups them together as completed, running or scheduled.

You can also view jobs in the **Catalog** view. Accessible from the **Administration** desk bar, the **Catalog** view keeps track of all of the objects in the Data Protector Express catalog, and it may appear very cluttered. Normally, when working with jobs, make the appropriate view active. In the following illustration, the **Catalog** view displays all jobs and objects created by the Admin user. For more information about the **Catalog** view, refer to *Catalog View* on page 151.



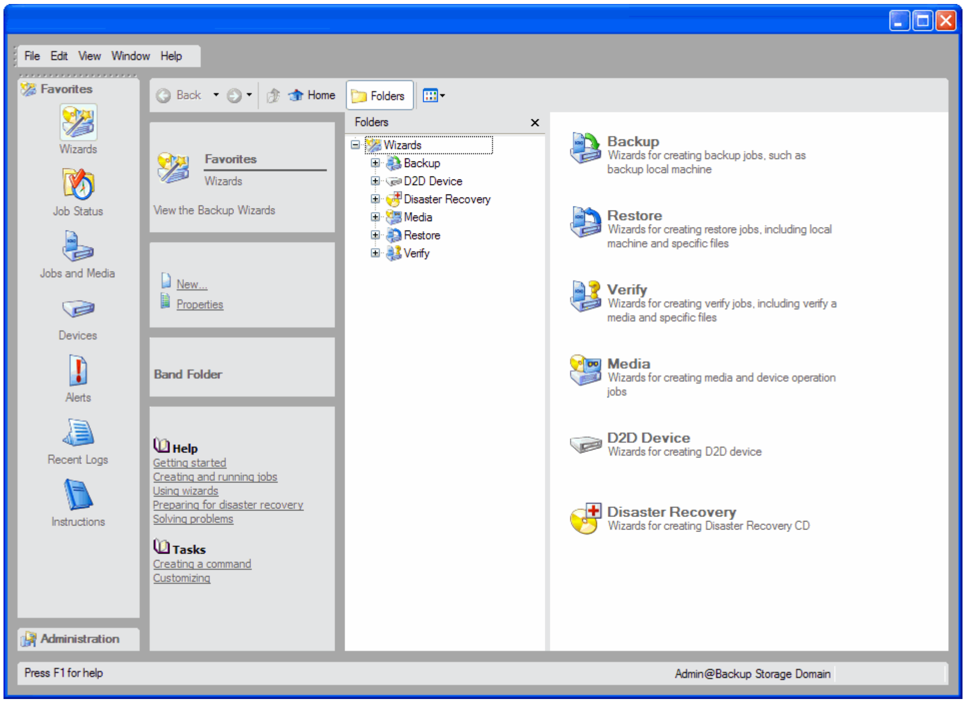
Creating New Jobs

There are three ways to create new jobs: with the *wizard*, from a *job view* and by *copying old jobs*.

Creating jobs with wizards

The Data Protector Express wizards will help guide you through all of the steps necessary to create and run a backup, restore or verify job. This is often the fastest way to create a new job, especially when you are inexperienced using Data Protector Express. After you answer a few questions, the Data Protector Express wizard will create the job for you. You can then work with this job in the catalog just like any other job.

The fastest way to activate the Data Protector Express wizard is to click on the **Wizards** view from the **Favorites** desk bar. Then click on the appropriate button to create either a new backup, restore or verify job.



Backup
Wizards for creating backup jobs, such as backup local machine

Restore
Wizards for creating restore jobs, including local machine and specific files

Verify
Wizards for creating verify jobs, including verify a media and specific files

Media
Wizards for creating media and device operation jobs

D2D Device
Wizards for creating D2D device

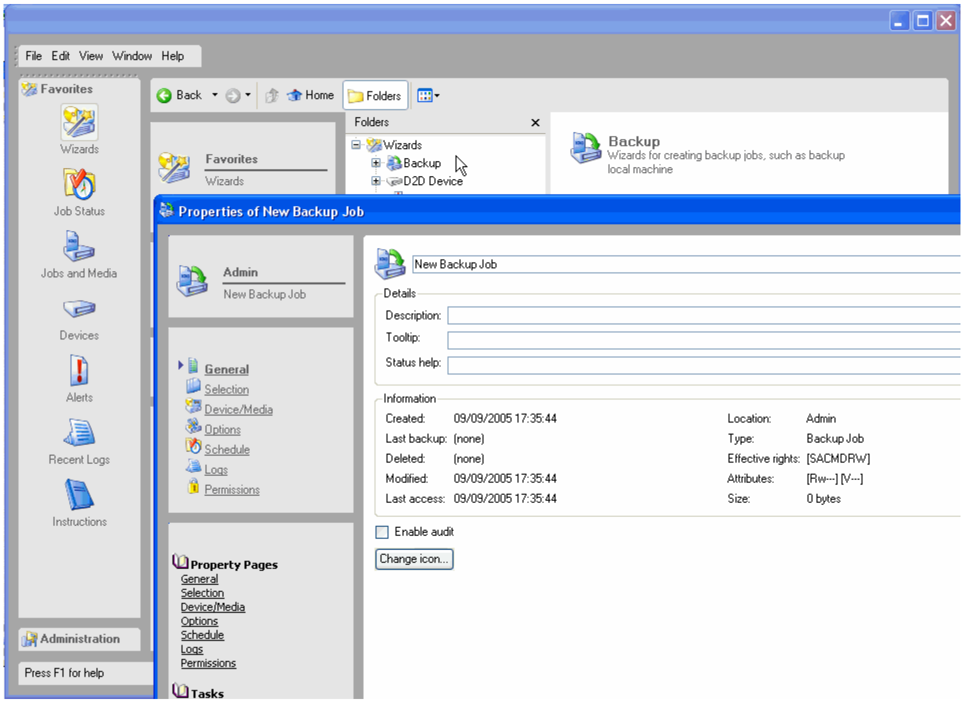
Disaster Recovery
Wizards for creating Disaster Recovery CD

You can also create a new job with a Data Protector Express wizard by either

- Selecting the **Wizards** view and selecting the appropriate category,
- Selecting **Wizards** from the **View** menu

Creating new jobs from the Jobs and Media view

Commonly, you will create jobs while working with the **Jobs and Media** view in the main Data Protector Express window. When you create a job this way, Data Protector Express opens the property page of the new job so you can name the job, select files and devices, set up logging and other options, and schedule it to run. Selecting files and scheduling a job to run are covered in detail in *Chapter 5 - Selecting Files and Versions*, *Chapter 7 - Planning for Media Rotation*, and *Chapter 8 - Job Options*.



New Backup Job

Details

Description:

Tooltip:

Status help:

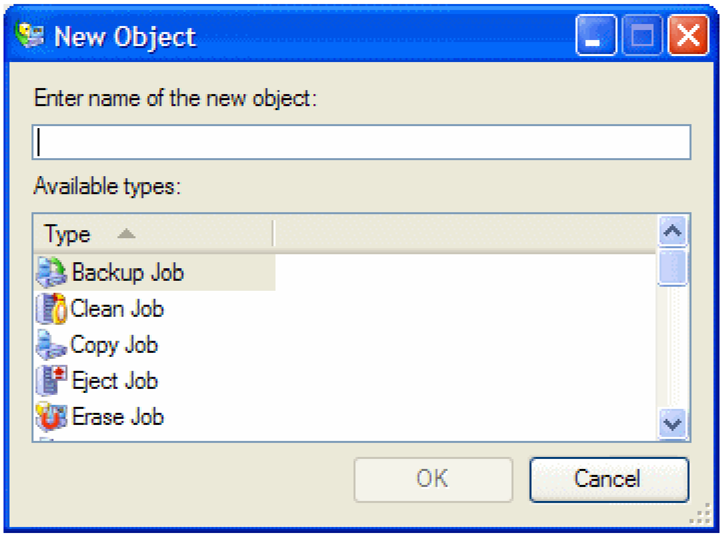
Information

Created:	09/09/2005 17:35:44	Location:	Admin
Last backup:	(none)	Type:	Backup Job
Deleted:	(none)	Effective rights:	[SACMDRW]
Modified:	09/09/2005 17:35:44	Attributes:	[Rw---] [V---]
Last access:	09/09/2005 17:35:44	Size:	0 bytes

□ Enable audit

To Create a New Job from the Jobs and Media view

1. Select **Jobs and Media** from the **Favorites** desk bar and open your **Home** folder.
2. To store the job in a specific folder, create or select a folder before you create the job. The contents of that folder are displayed in the object detail area. Data Protector Express will store your new job here.
3. Create the new job in one of these ways:
   - Select **New…** from the **File** menu and then select the appropriate job type in the **New Object** window
   - Right-click in the Data Protector Express object detail area and select **New…** from the shortcut menu
   - Click the **New…** button on the Commands pane and select the appropriate job from the **New Object** window.
4. Enter a name for the new job and select a type in the **Available Types** list.
5. Click **OK**.



Creating new jobs by copying

Creating a new job by copying an existing job is sometimes a useful method of creating a job. In particular, copying an existing job is appropriate when you want your new job to be like the old job in every way except for a few minor changes.

To Create a New Job by Copying an Existing Job

1. Copy the existing job you wish to duplicate in one of these ways:
   - Press the CTRL key as you drag the existing job to a new location, then skip to step 4 below
   - Select the existing job (with the mouse or keyboard) and press CTRL+C
   - Right-click the existing job and selecting **Copy** from the shortcut menu
   - Select **Copy** from the **Edit** menu.
2. Open the folder you want the new job to be stored in by selecting it in the tree view area. (To store the job in the same folder as the existing job, skip this step.)
3. Right-click the folder where you want the new job to be pasted and select **Paste** from the shortcut menu. Alternatively, highlight the location where you want the job pasted; then select **Paste** from the **Edit** menu or press CTRL+V.
4. Change the name of the new job.

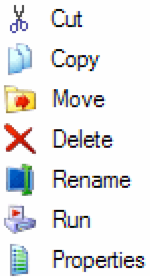
NOTE: Data Protector Express copies all job properties, including job logs, to the new job.

Renaming, deleting, copying and moving jobs

You can change the names of jobs or move them to new folders. Or, if you do not plan to use a job again in the future, you can delete it.

You rename, delete, copy and move jobs in one of these ways:

- Select the appropriate command from the **Edit** menu
- Right-click the job and selecting the appropriate command from the shortcut menu.



To move a job, drag it to a new location. You can also use the Delete key and the **Delete** command to delete jobs.

NOTE: When you run a backup job, Data Protector Express uses its catalog to keep track of the files you have backed up and the name of the media on which they are stored. Deleting a job does not affect how the catalog tracks files and media. Data Protector Express continues to track these files and media even after the job that created them has been deleted. However, the jobs associated with this job will also be deleted.

Creating job groups

Data Protector Express provides a special job type called a Job Group. Use this job to set up a list of jobs that you want to run together. As you select jobs to include in job group, they appear on the Jobs view. Scheduling options for job groups are similar to scheduling options for any other job type. You can select a Schedule Type, Start Time and Start Date; however, you cannot select or modify a Rotation Type or Job Mode. Each job retains its rotation type and job mode.

To create a job group

1. From the **Jobs and Media** view, select **New…** and select Job Group in the **Available Types** list.
2. Enter a name for the job group and click **OK**.
3. Set up the job group as follows:
   - On the **General** page enter description information, and check the **Enable Audit** box if you want Data Protector Express to keep a log for the job
   - On the **Options** page, select the jobs to include in the job group
   - On the **Schedule** page, select the days and times to run the jobs
   - On the **Permissions** page, select the users and groups that can run this job group
4. Click **Apply** or **OK** to save your changes.

Data Protector Express will run the job group based on the schedule. The job will be stored in your Home folder.

Organizing jobs with folders

Every backup, restore, verify and media job is stored by Data Protector Express inside a folder. By default, Data Protector Express stores all jobs in the Home folder of the user who creates the jobs. However, you can create new folders to help organize your jobs or you can use existing folders.

When the Data Protector Express administrator added you as a user, Data Protector Express created a personal folder for your use. Generally, because there may be many users in your Data Protector Express management domain, it is a good idea to store your personal jobs in your personal folder. Alternatively, you can store group jobs in the appropriate group folder.

Types of folders

Data Protector Express provides many types of folders: **User/Group folders**, **Job folders**, **Media folders**, and folders for any other type of object you might want to create**.** Each of these folders is a container, that is, they store other objects within them. They differ from each other according to the type of object that can be stored within them.

User/Group folders can only be stored in a special folder, called the **Home** folder. These folders can have either Job folders or Media folders within them; additionally, you can store jobs or media "loose" in these folders.

Job folders can only be stored in User/Group folders or in other Job folders. These folders usually have jobs stored within them, although you can also store additional job folders within them.

Media folders can only be stored in User/Group folders or in other Media folders. These folders usually have media stored within them, although you can also store additional Media folders within them. Media folders are discussed further in

Managing *Devices and Media* on page 134.

Data Protector Express organizes other objects and resources that you create in folders designated for those objects. For example, if you set up a secondary printer, you will find it in a printers folder in the **Catalog** view. Create a new user or group and Data Protector Express will store them in a **Security** folder.

Folders and job views

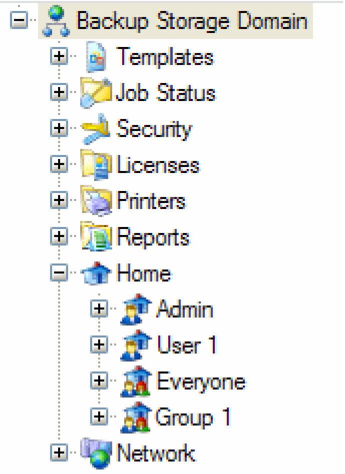
Job folders appear only on the **Jobs and Media** view for the users or groups that access to them and in the **Catalog** view. That is, a job folder appears only in the **Jobs and Media** view (and on the **Catalog** view) for the person who created the job or for users or groups who have access rights to it.

Similarly, User/Group folders appear only in the **Security** view as well as the **Catalog** view.

Media folders appear in the **Jobs and Media** and **Catalog** views.

Home, Admin, and Everyone folders

Three folders play a special role in every catalog: the **Home** folder, the **Admin** folder and the **Everyone** folder.



The **Home** folder is the folder that stores all of the User/Group folders within it. It is always at the top of the hierarchy in the tree view area of the **Jobs and Media** view. You are not allowed to store jobs “loose” in the **Home** folder, only inside other folders. You can, however, create a job folder in which to store other jobs. This folder would be available to any user with access rights to it.

The **Admin** folder is a special folder used by the Data Protector Express administrator. Normally, only the Data Protector Express administrator has permissions to the **Admin** folder. If you don’t see it inside your **Home** folder, this is because the Data Protector Express administrator has not given you permission to view it.

The **Everyone** folder is a folder to which every Data Protector Express user has permission. Your Data Protector Express administrator may place jobs in this folder to which he wants everyone to have access.

Everyone folder and permissions

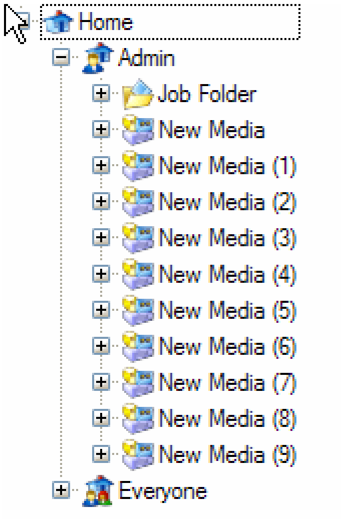
Because of the way Data Protector Express assigns permissions to new objects, if you create a new object inside the **Everyone** folder, normally everyone will have at least some permissions to it. For example, if you create a new backup job and store it in the **Everyone** folder, it is likely that every Data Protector Express user will have permissions to that folder and thus to the job.

To restrict the permissions of other Data Protector Express users to a job or folder, you should create a folder to which only you or your group have permission. Granting permissions is covered in detail in *Permissions* on page 42.

Creating job folders

Usually, the best strategy for organizing your personal jobs or the jobs of your group is to create a special folder in which to store them. Managing permissions to these jobs is much easier and quicker if you create a special folder for them.

When the Data Protector Express administrator adds a user or group, Data Protector Express creates a personal folder for that user or group. If you have the proper permissions, you can also create as many additional new job folders as you need and organize them in a convenient way. You can create additional job folders either inside your personal or group folder or inside the **Everyone** folder.



To create a new folder

1. From the **Jobs and Media** view on the **Favorites** desk bar select the existing folder in which you want to store the new job folder. (It cannot be the Home folder.)
2. Create the new folder one of these ways:
   - Select **New Object…** from the **File** menu and then select **Folder** from the **New Object** window
   - Right-click in either the tree view or object detail area and select **Folder** from the shortcut menu
   - Click the **New Object** button and select **Folder** from the **New Object** window.

   Data Protector Express creates the new folder inside the selected folder.
3. Type in the name of the new folder on its property page.

TIP: After creating a new folder, be certain to specify which users have permissions to it. This is the simplest and fastest way to assign permissions to multiple objects stored in the folder.

Moving, renaming and deleting folders

You can move, rename or delete a folder just like you can any other Data Protector Express objects, such as jobs; however, you cannot copy folders. When moving, deleting or renaming folders, keep the following in mind:

Moving Folders: Contents of a folder move with the folder to the new location. This may change the permissions of the objects stored in that folder.

Renaming Folders: Only the name of the folder is changed. Data Protector Express still treats that folder and any objects associated with it in the same manner.

Deleting Folders: Deleting folders also deletes their contents, including any other folders or jobs contained in that folder. Before deleting a folder, be certain that you intended to delete all of its contents.

WARNING: Once a folder has been deleted, its contents cannot be recovered. Be certain either that the folder is empty or that you no longer need the contents of the folder before deleting it.

Modifying folders

You can rename, delete and move folders using one of these methods:

- Select the appropriate command from the **Edit** menu
- Right-click the folder and select the appropriate command from the shortcut menu

Chapter 4: Permissions

Security is an important issue when managing a network. One of the most important functions of the Data Protector Express catalog is to handle security. The catalog prevents unauthorized users from working with objects to which they have not been granted sufficient security permissions. To ensure only authorized users can access sensitive data, Data Protector Express tracks the **permissions** of each user. The Data Protector Express administrator can grant different types of permissions to various users to ensure the security and integrity of the network data while efficiently implementing a productive backup program.

In this section

- Users and Groups
- Effective Permissions
- Types of Permission
- Examples of Permissions
- Granting Permissions to Other Data Protector Express Users

Overview

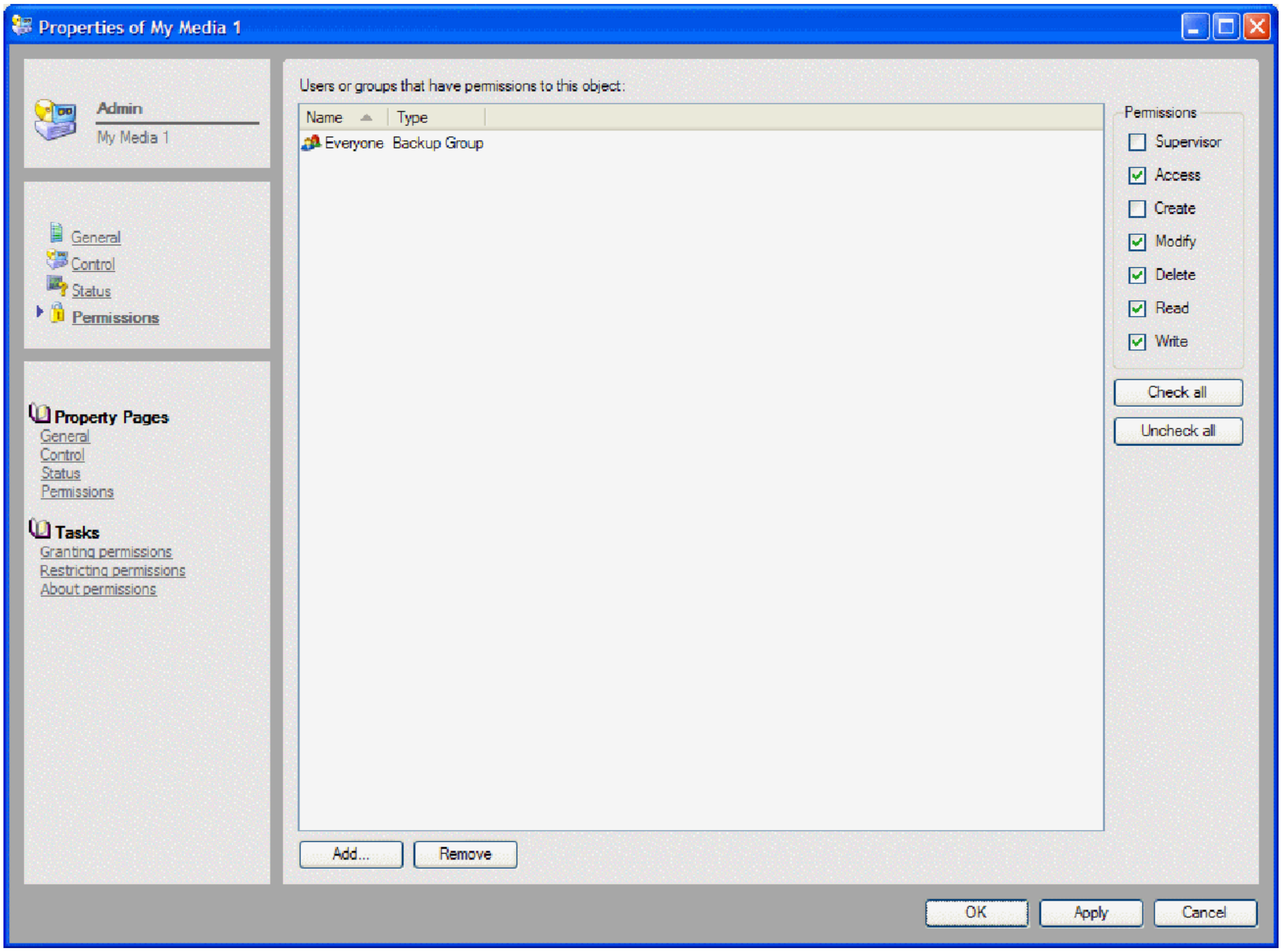
Before you can work with any object (directory, file, user, etc.) in the Data Protector Express catalog, you must have **effective permissions** to that object.

Different types of permissions restrict what type of operations can be performed on an object. For example, some permissions allow users to *write* to an object (such as a file, a storage media or a PC desktop) or *create* new objects (such as folders or jobs). Sometimes a user is granted unlimited permissions to an object or all objects. Usually, however, to protect the integrity of the data and for security reasons, most users have only limited effective permissions to some (not all) of the objects in the Data Protector Express catalog.

Maintaining the security of data on a network is the primary responsibility of the Data Protector Express administrator. Because of this, the following section is only an overview of security and permissions. This section will help the typical user understand how Data Protector Express handles security and permissions so that you can work efficiently with your Data Protector Express administrator.

Users and Groups

The Data Protector Express administrator grants permissions to objects in the Data Protector Express catalog to either a **user** or to a **group**. Individual Data Protector Express users have effective permission to an object either as a user or as the member of a group. A group is a set of users that are all granted permissions in the same way and at the same time. For example, the Data Protector Express administrator may grant permission to read the files on specific media to users individually, to a group of users or both to users and groups.



Users or groups that have permissions to this object:

Name	Type
Everyone	Backup Group

Permissions

□ Supervisor
☑ Access
□ Create
☑ Modify
☑ Delete
☑ Read
☑ Write

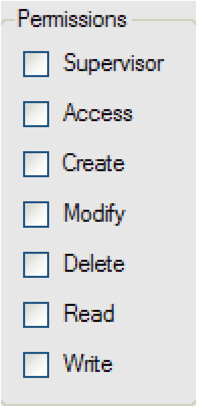
Individual Data Protector Express users can be a member of more than one group or in every group, depending on how the Data Protector Express administrator arranges the catalog security. The number of groups the Data Protector Express administrator creates and the assignment of members to those groups depends on the security needs of your particular network. For more information on setting up users and groups, see *Adding New Users and Groups* on page 168.

Everyone group

Normally most Data Protector Express users are a member of a special group, the **Everyone** group. Whenever a new user is added to a Data Protector Express management domain, Data Protector Express automatically assigns that user to the **Everyone** group. Typically, only limited permissions are granted to the **Everyone** group, although users can be granted more extensive permissions either individually or as members of other groups.

Effective Permissions

The permissions you have to an object in the Data Protector Express catalog are called your **Effective permissions**. You can view your effective permissions to an object on the **General** page of that object.



Permissions

□ Supervisor

□ Access

□ Create

□ Modify

□ Delete

□ Read

□ Write

Determining effective permissions

A user is assigned effective permissions to an object through by **direct permissions** or **inherited permissions**.

A user has *direct permissions* to an object if they are listed on the **Permissions** page of the object, if they are equivalent to a user who has direct permissions to the object or if they are a member of a group that is listed on the **Permissions** page of that object.

A user has *inherited permissions* to an object if they do not have direct permission when they have effective permissions to the container that contains the object. If you do not have direct permissions to an object, you must have effective permissions to the container in which the object is stored.

NOTE: Your effective permissions to a container object can be either direct or inherited. All that matters is that you have effective permissions to the container.

When determining a user's effective permissions to an object, Data Protector Express checks if the user has direct permission; if not, Data Protector Express checks if they have inherited permission.

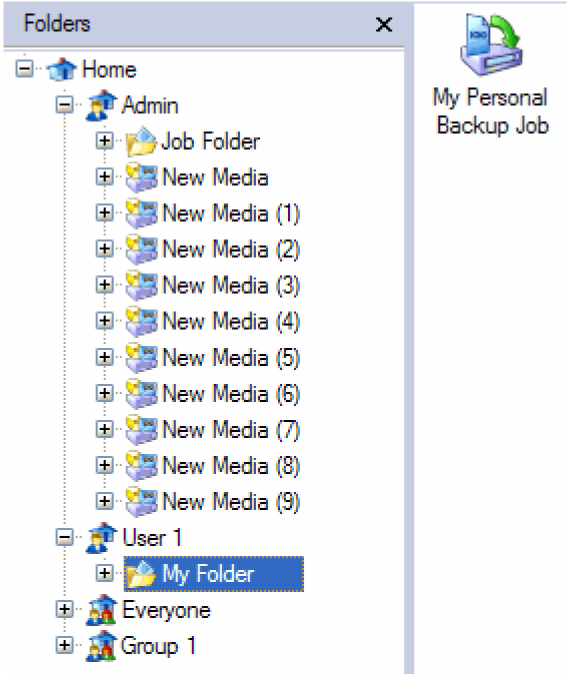
For example, if a user has the **Read** direct permission, but the group has the **Access** permission, the user's effective permission is **Access**.

Examples of determining effective permissions

The following two examples illustrate how Data Protector Express determines the effective permissions a user has to an object.

Effective permissions example #1

In this example, a user has direct permissions only to the User/Group folder named **My Folder**.

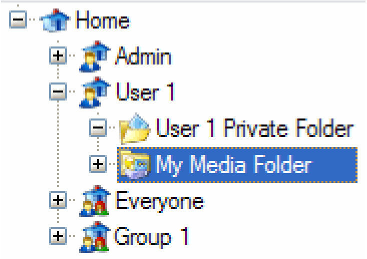


When determining the effective permissions the user has to **My Folder**, Data Protector Express first looks to see if he has direct permissions to the folder. Because the user is listed as a user on the **Permissions** page of the folder's property page, he has direct permissions to the folder. Data Protector Express uses this information to determine the user's effective permissions. Data Protector Express does NOT look to see if there are any inherited permissions to the folder.

When determining the effective permissions the user has to the backup job named **My Personal Backup Job** stored in **My Folder**, Data Protector Express first looks to see if he has inherited permissions to the job. Because the user does not have direct permissions, Data Protector Express checks to see if the user has inherited permissions to the folder that contains the job. In this case, Data Protector Express checks to see if he has direct permissions to **My Folder,** and because this user has direct permissions to this folder, Data Protector Express uses this information to calculate the effective permissions this user has to the job.

Effective permissions example #2

In this example, a user (User One) has direct permission to the media folder named **My Media Folder** *as a member of a group named Group One* and to any folders or jobs that he creates *as a user*.



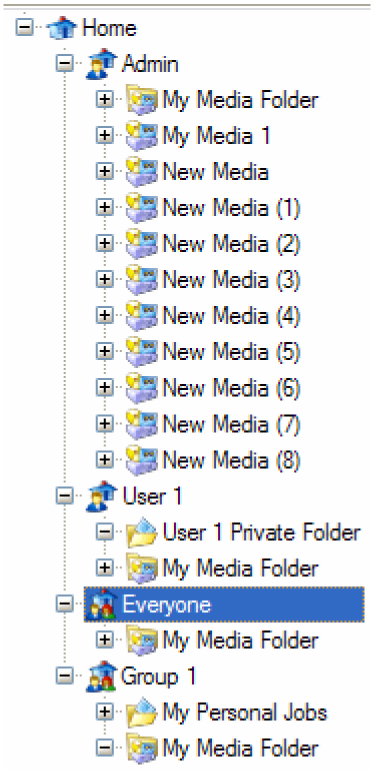
When determining the effective permissions that User One has to these folders, Data Protector Express first looks to see if he has direct permission to the folder. Because he is a member of **Group One** which has direct permissions to the folder, User One also has direct permissions to the folder. Data Protector Express uses this information to determine the user's effective permissions. Data Protector Express does NOT look to see if there are any inherited permissions to the folder.

When determining the effective permissions a user has to anything stored in the folder, Data Protector Express first looks to see if a user has direct permission to the object. If no users or groups have direct permissions to the object, Data Protector Express checks to see if the user has direct permissions to the folder. In this example, Data Protector Express checks to see if User One has direct permissions to **My Media Folder**; because User One has direct permissions to this folder, Data Protector Express uses this information to calculate his effective permissions to anything contained in the folder.

Similarly, Data Protector Express determines the effective permissions a user has to a folder by the direct permissions he or she has to that folder. Note that when determining the effective permissions to a folder, it makes no difference that a user also has effective permissions to the folder which contains this folder.

When determining the effective permissions a user has to a job contained in his or her personal folder, Data Protector Express checks to see if the user has direct permissions to the job. If he does not, Data Protector Express checks to see if the user has direct permissions to the folder that contains the job. If a user has direct permissions to the folder, Data Protector Express uses these direct permissions to determine his effective permissions to the job that is stored in the folder.

Note especially that the effective permissions a user has to a job or task are determined ONLY by the user's effective permissions to the *folder*—and NOT by his effective permissions to the group folder.

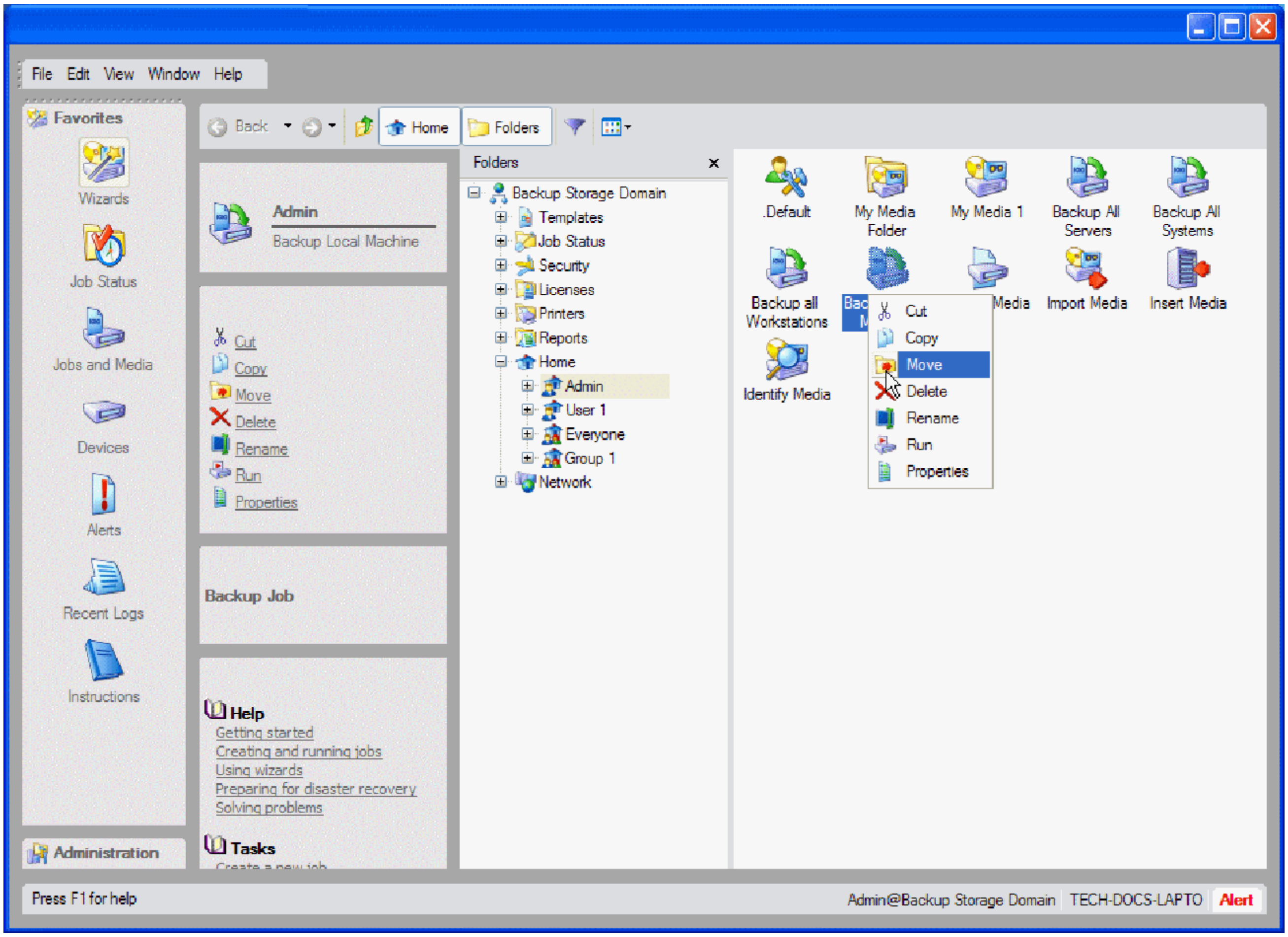


- Home
  - Admin
    - My Media Folder
    - My Media 1
    - New Media
    - New Media (1)
    - New Media (2)
    - New Media (3)
    - New Media (4)
    - New Media (5)
    - New Media (6)
    - New Media (7)
    - New Media (8)
  - User 1
    - User 1 Private Folder
    - My Media Folder
  - Everyone
    - My Media Folder
  - Group 1
    - My Personal Jobs
    - My Media Folder

How moving objects affects permissions

When an object is moved from one container to another, Data Protector Express determines the effective permissions of the object based on its new location.

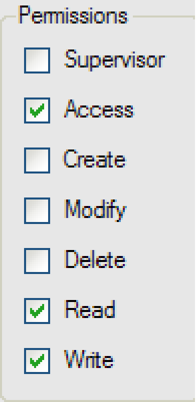
For example, suppose a user has effective permissions to a job because that job is stored in his or her User/Group folder, a container to which the user has been granted direct permission. If the job is moved from that folder to a new folder, the user's effective permissions to the job may change. If the job were moved to the **Admin** folder, the user would lose permission to it because he or she does not have direct permissions to the **Admin** folder. On the other hand, if the job were moved to the **Everyone** folder, the user would still be able to access the job, even though the effective permissions might be different.



Types of Permission

Data Protector Express controls access to objects in its catalog with seven different types of permission. The type of permission determines what actions a user can perform on an object. Users and groups can be granted all seven types of permission, only some of the permissions or none of the permissions.

The seven types of permission are **Supervisor**, **Access**, **Create**, **Modify**, **Delete**, **Read** and **Write**.



Permissions

☐ Supervisor

☑ Access

☐ Create

☐ Modify

☐ Delete

☑ Read

☑ Write

Supervisor

This is the most powerful permission. **Supervisor** permission grants the user three specific abilities:

- First, a user with **Supervisor** permission to an object is automatically granted the other six permissions to that object;
- Second, a user with **Supervisor** permission to an object automatically has effective permission to all the objects in the catalog below that object; and
- Third, a user with **Supervisor** permission to an object cannot be denied any of the seven permissions to any object in the catalog below that object.

The Data Protector Express administrator is automatically granted **Supervisor** permission to the highest container in the Data Protector Express catalog hierarchy (called the **System Container**). This means that the Data Protector Express administrator has full permissions to all the objects in the Data Protector Express catalog and that none of these permissions can be denied.

Often, only the Data Protector Express administrator will be assigned **Supervisor** permission.

Access

A user with **Access** permission to an object can grant other users and groups permissions to that object. For example, if you wish to grant a co-worker permissions to a tape you have created, you must have **Access** permission to that tape.

Access permission can be very powerful, since it allows a single user the ability to grant all other users in the Data Protector Express catalog extensive permissions to an object. For this reason, your Data Protector Express administrator may not grant you **Access** permission to objects even though you have other permissions to them. For example, your Data Protector Express administrator may grant you permission to read and write from a particular tape. Without **Access** permission however, you will not be able to grant other users or groups that same ability.

You can only grant permissions to other users or groups if you have **Access** permission. If you want other users to have permissions to an object, such as a job or tape, and do not have **Access** permission to that object, ask your Data Protector Express administrator to grant these users permissions for you.

Create

This permission allows a user to create new objects within a container object. For example, to create a new job within a folder, a user must have **Create** permission to the folder. Note that the **Create** permission applies *to the folder*, not to the job: it grants the user permission to create new objects *within* that folder.

If you want to create new folders or jobs, your Data Protector Express administrator must grant you **Create** permission. Your permission to create new jobs or folders might be limited to a single folder. For example, you may have **Create** permission only to the **Everyone** folder or to a personal folder that your Data Protector Express administrator has created for you or your group.

If you can't create a new job or folder, first make sure you have selected a folder in the tree view area to which you have **Create** rights. If you still cannot create a new job or folder, ask your Data Protector Express administrator to grant you **Create** permission to that folder.

Modify

This permission allows a user to change the name and location of an object, such as a job, in the Data Protector Express catalog. **Modify** permission also allows a user to change or modify the property pages of an object. If you have this permission, you will be able to move, rename and change the property pages of objects. For example, to change the name of job, a user must have **Modify** permission to that job. You must also have **Modify** permission to move a job from one folder to another.

Delete, Read and Write

These three permissions control user access to objects, such as tapes, devices and files, which are read, deleted or written to. These permissions are necessary in order to run backup, restore, and verify jobs as specified below.

- *To complete a backup job*, a user must be granted **Read** permission to the files to be backed up and **Write** permission to both the media and the backup device. If the backup job will *overwrite* the media with the new data (as opposed to merely *appending* the new data), the user must also have **Delete** permission to the media.
- *To complete a restore job,* a user must be granted **Write** permission to the volumes (disk drives) on which the files are going to restored and **Read** permission to the media and backup device. If the restore job will *overwrite* or *replace* old files, the user must have **Delete** permission to those files.
- *To complete a verify job,* a user must be granted **Read** permission to the files on the PC desktop or file or application server to be verified, to the media and to the backup device.

Examples of Permissions

The following two examples illustrate how the permissions work with each other.

Permissions example #1

In this example, a user has effective permissions to a folder named **My Backup Jobs**, to a drive (or volume) named **File System** and to a media set named **Media:1**.

Catalog Object	Effective Permissions
My Backup Jobs (Job folder)	`[--CMDRW]`
File System (Volume)	`[-----R-]`
Media:1 (Media)	`[-----R-]`

These permissions allow the user to do the following:

- Because the user has **Create** permission to the **My Backup Jobs** folder, he will be able to create new job folders within that folder and to create backup, restore and verify jobs inside that folder. The **Modify** permission allows him to move these jobs between folders, to change the name of the job and to change the property pages of these jobs. The **Delete** permission allows him to delete any jobs or folders inside this folder. The user also has **Read** and **Write** permissions to the **My Backup Jobs** folder and will have these same permissions to any object stored in that folder.
- Because the user also has **Read** permission to the volume named **File System**, he will be able to select files from that drive for backup. He will also be able to select files for restoring.
- Because the user has **Read** permission to both the media and to the volume, he will be able to create and run verify jobs—if he also has **Read** permission to the backup device.

These permissions do NOT allow the user to do the following:

- Although the user will be able to create a backup job, he will not be able to run the backup job because he does not have **Write** permission to the media. The job must be run by the Data Protector Express administrator or some other user to whom the Data Protector Express administrator grants **Write** permission to the media.
- Similarly, although the user will be able to create a restore job, he will not be able to run the restore job because he does not have **Write** permission to the disk drive. If the user wants to run the restore job, he must ask the Data Protector Express administrator to run it for him or to grant him the permissions necessary to run it.
- The user is prevented from granting permission to other users to his folder, to his drive and to his media because he lacks **Access** permission to these objects.

Permissions example #2

In this example, a user has effective permissions to a drive named **My Drive** and to a media set named **Media:2**. He is also a member of a group that has effective permissions to a folder named **Group Jobs.**

Catalog Object	Effective Permissions
My Drive (Volume)	User: `[-----R-]`
Media:2 (Media)	User: `[-----RW]`
Group Jobs (Folder)	Group: `[--CMDRW]`

These permissions allow the user to do the following:

- Because he is a member of the group, the user will be able to create jobs and folders within the **Group Jobs** folder. He will also be able to modify and delete any jobs or folders in that folder.
- Because the user has **Modify** permission to the folder and **Read** permission to the drive named **My Drive**, he will be able to select files from that drive to back up. Similarly, the user will be able to select files for restoring because he has **Read** permission to the media named **Media:2**.
- Unlike the user in example 1, this user will be able to run backup jobs because he has **Write** permission to the media. (This assumes he also has **Write** permission to a backup drive.)
- The user will also be able to create and run **Verify** jobs.

These permissions do NOT allow the user to do the following:

- Although the user will be able to create and run *backup* jobs, he will not be allowed to *restore* files from those tapes onto his drive because he has not been granted **Write** permission to his disk drive.
- When the user runs a backup job, he will be prevented from overwriting old files on the media with new files because he does not have **Delete** permissions to the tape. Thus the backup jobs he creates and runs must all be append jobs.
- This user, like the user in example 1, is prevented from granting permission to other users to either his drive or his tape because he lacks **Access** permission.

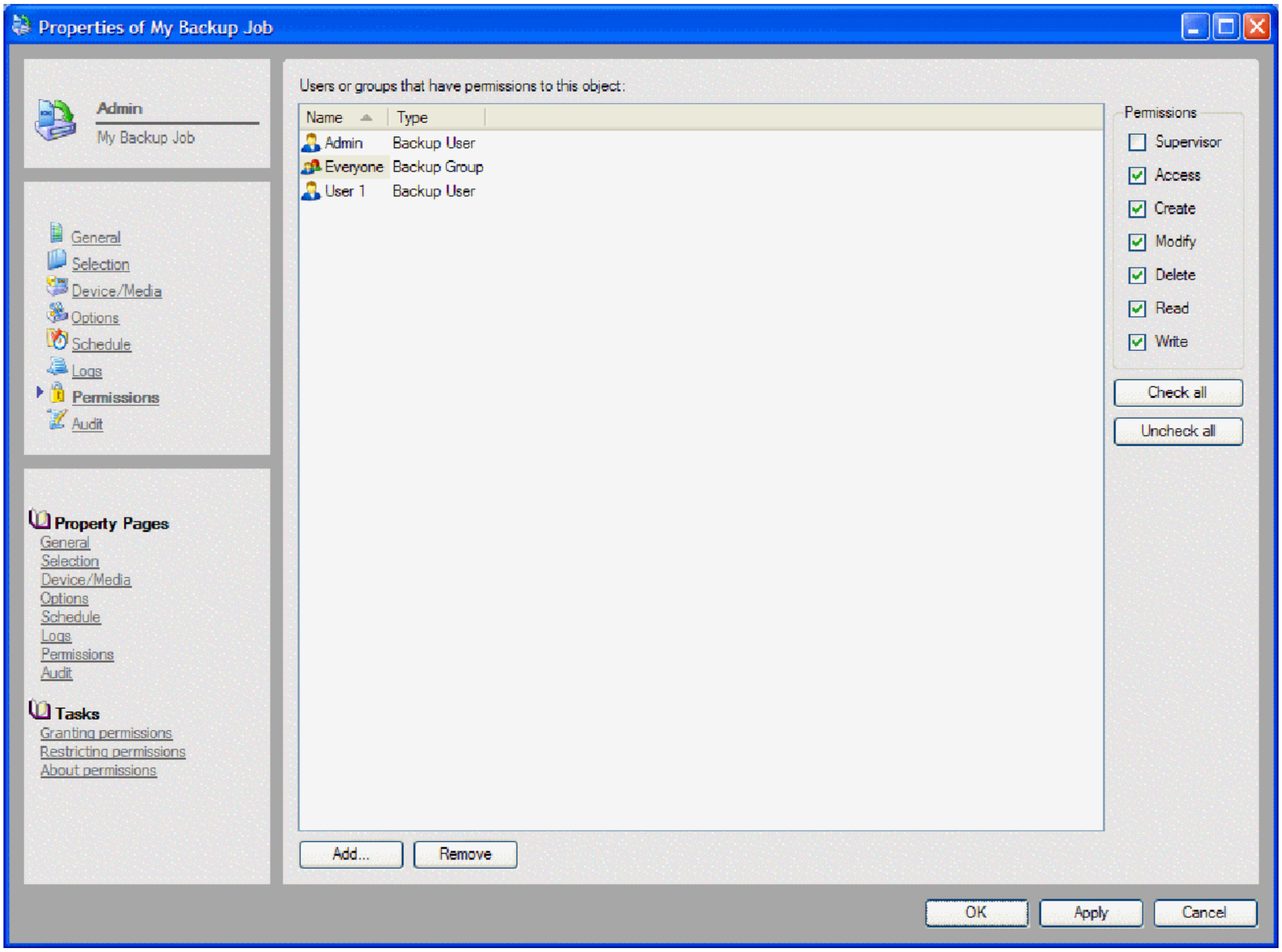
Other members of the group also have some permissions to the jobs and folders inside the **Group Folder**, including those created by this user. This affects them in the following ways:

- They will be able to view the folders and jobs each group member creates in the **Group Jobs** folder. Because they have **Modify** permission, members of the group will be able to modify the properties of any jobs or folders the group members create inside the **Group Jobs** folder.
- Because members of this group lack **Read** permission to this user's drive and media, they will be unable to change the files this user selected for backing up or restoring—even if they have **Modify** permission to a job this user created.
- No other members of this group can run one of this user’s jobs unless the Data Protector Express administrator grants them the appropriate **Read** and **Write** permissions.

Granting Permissions to Other Data Protector Express Users

If your Data Protector Express administrator has given you **Access** permission to an object, you will be able to grant other users and groups permissions to that object. Generally your Data Protector Express administrator will only grant you **Access** permission to objects in the Data Protector Express catalog when he or she wants you to be able to share this data with other users.

For example, if your Data Protector Express administrator has given you **Access** permission to an archive tape, you will be able to grant other users **Read** permission to the tape. This would allow other users to restore files from this tape to any drive they have **Write** permission to.



Users or groups that have permissions to this object:

Name	Type
Admin	Backup User
Everyone	Backup Group
User 1	Backup User

Permissions

- ☐ Supervisor
- ☑ Access
- ☑ Create
- ☑ Modify
- ☑ Delete
- ☑ Read
- ☑ Write

To grant permission to other Data Protector Express users

1. Display the properties for the object to which you wish to grant users or groups permission.
2. Select the **Permissions** page. (If you do not have **Access** permission to an object, you cannot modify permissions.)
3. Click the **Add…** button.
4. Select a user or group to add in the **Browse** window and then click **OK.**
5. With the user or group selected, check the appropriate permissions in the list at the right of the screen.
6. Click **Apply** or **OK** to save the permissions.

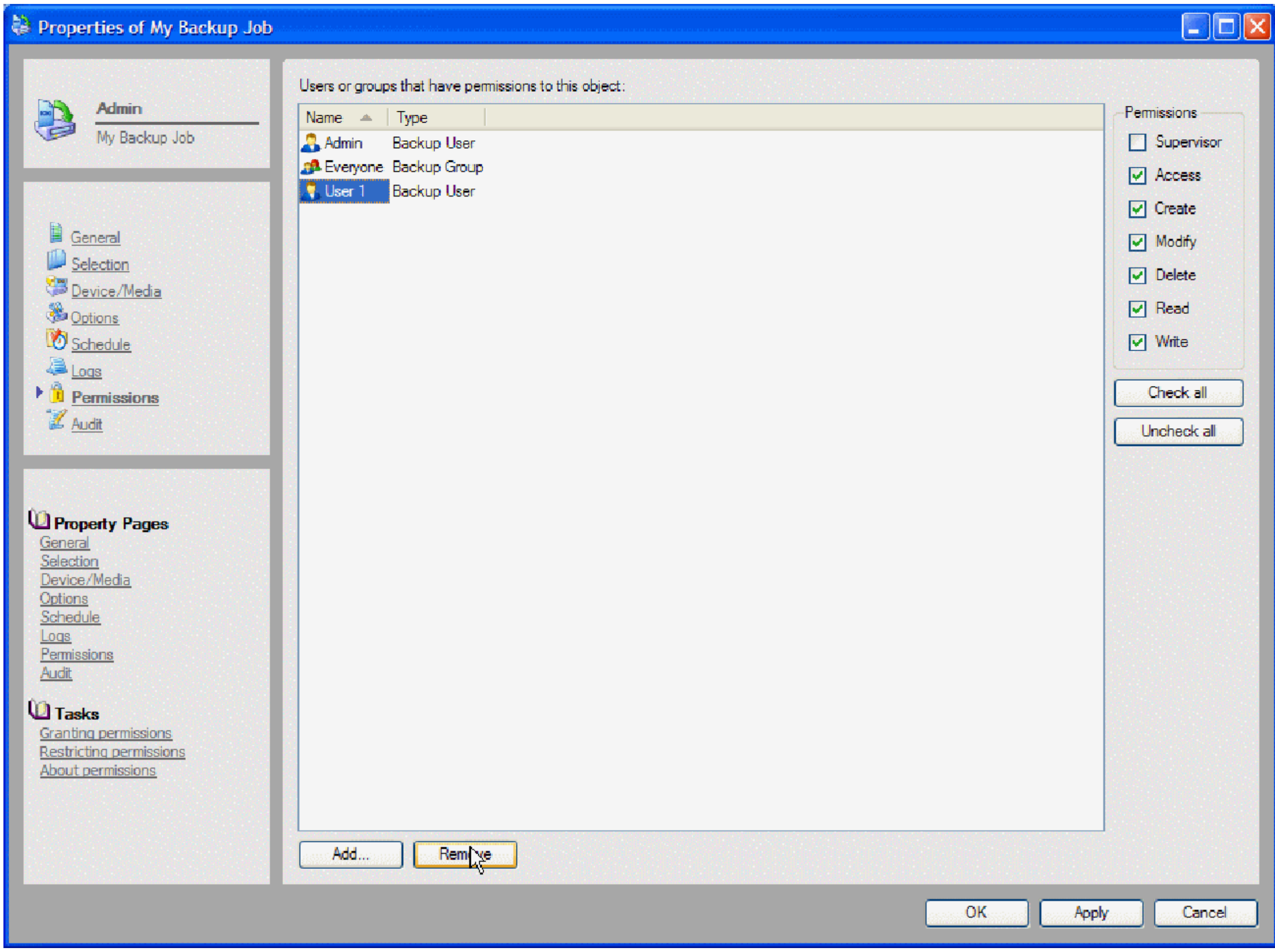
Restricting user permissions

In most cases you can restrict the permissions a user has to an object in the same way you grant permissions—by clearing the appropriate check boxes on the **Permissions** page of that object. If the user or group is not listed on the **Permissions** page of the object, you must first add that user or group to the list of users or groups that have direct permissions to that object.

To restrict permissions of other Data Protector Express users

1. Open the properties of the object to which you wish to restrict user or group permissions.

2. Select the **Permissions** page. (If you do not have **Access** permission to an object, you cannot modify permissions.)
3. If the user is not listed, first add the user or group by clicking the **Add…** button and then selecting a user or group to add in the **Browse** window.
4. With the user or group selected, clear the check boxes from the permissions list at the right of the screen.



Users or groups that have permissions to this object:

Name	Type
Admin	Backup User
Everyone	Backup Group
User 1	Backup User

Permissions

☐ Supervisor
☑ Access
☑ Create
☑ Modify
☑ Delete
☑ Read
☑ Write

5. Click **Apply** or **OK** to save the permissions.

When you restrict a user's direct permissions to a container, you also change that user's effective permissions to objects within that container—but only when the user's effective permissions to those objects are *inherited* from that container's effective permissions. For example, if you deny a user direct **Modify** permission to a job folder by clearing the **Modify** check box under that user's name, you also deny that user effective **Modify** permission to jobs stored in that folder—unless that user has direct permissions to those jobs.

Normally, your Data Protector Express administrator will have arranged the security of your Data Protector Express management domain to prevent unauthorized access to files and tapes. However, if you believe another user's permissions to an object should be restricted and you cannot restrict it yourself, notify your Data Protector Express administrator.

Chapter 5: Selecting Files and File Versions

You use the **Selection** property page of a job to select files for backing up, restoring and verifying. Data Protector Express's powerful selection filters allow you to select exactly the files you want and to automatically update your selection before the job is run.

In this section

- Backup Selection Concepts

Working with VSS snapshots

Backup jobs can create snapshots using Microsoft Volume Shadow Services (VSS) on platforms that support VSS.

VSS freezes the volume data at the point in time of the snapshot creation by creating a temporary snapshot. Any changes after that point in time will not be backed up until the next backup job. The snapshots are deleted after the job has finished. If VSS cannot create a snapshot the backup will proceed and the error will be noted in the job log.

Snapshots will affect an entire volume, not just the selected files. So jobs logs may indicate more space was snapped than you expect.

To turn off VSS for a job

1. Open the **Property** page for the job.
2. Select the **Options** page.
3. Click the **Advanced Options…** button
4. Deselect the **Enable Snapshots** checkbox

To turn off VSS for a specific machine

1. Open the **Catalog** view from the **Administration** desk bar.
2. In the main object detail area, select **Network**.
3. Select the machine for which VSS is being configured.
4. Select **System Drivers**.
5. Locate and select **Microsoft Volume Shadow Copy Services Agent**.

6. Right click and select **Stop.**

To re-enable the service, repeat the steps above and select **Run.**

- Selecting Files for Backup Jobs

- Restore Selection Concepts
- Selecting Versions of Files for Restore Jobs
- Restoring Files with New Names and Locations
- Verify Selection Concepts
- Selecting Versions of Files for Verify Jobs

Backup Selection Concepts

When you select files for a job, you want to select only those files which are necessary for your job and not any others. However, you also want your selection criteria to be flexible enough to automatically select new files that meet your criteria.

Data Protector Express allows files to be selected in several ways: by directly selecting volumes, folders and files; by using filters to sort through selected files; and by additional automated filters used by Data Protector Express when your job is run. For restore jobs, you can also specify which version of a file you wish to restore, what name that new file will have and what folder or directory the file will be restored to.

By specifying your selection criteria carefully, when Data Protector Express automatically updates the selected file list each time your job is run, you can be certain that the job will work with those files you intended to select.

This section discusses how to select files separately for each type of job: backup jobs, restore jobs and verify jobs. For each type of job, there is a discussion of concepts you'll need to be able to correctly and carefully select files. Be certain to read this section before proceeding.

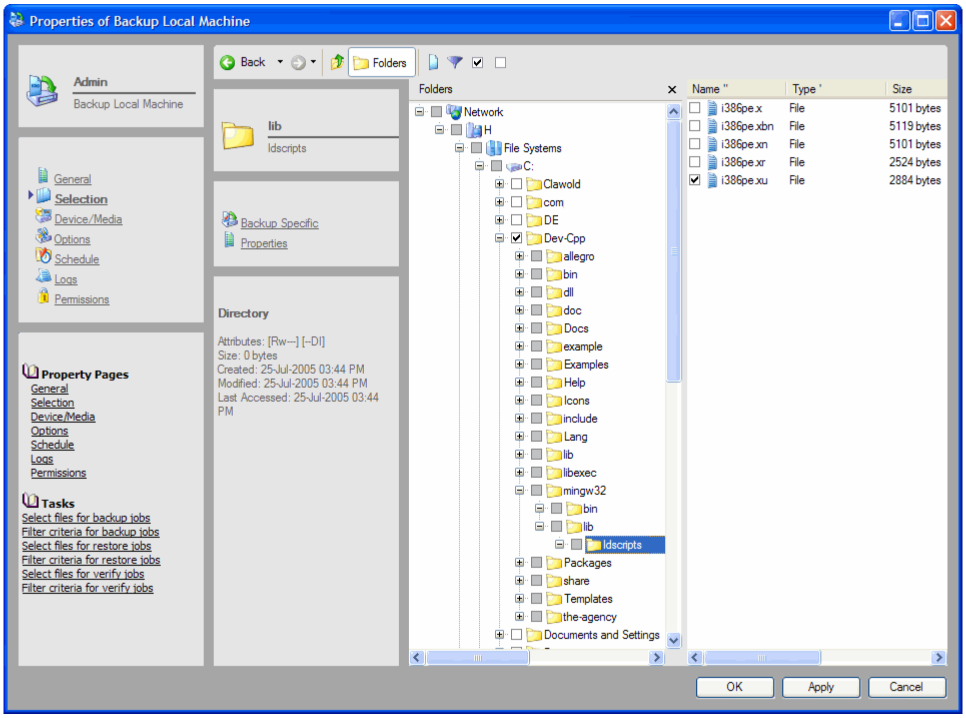
You use the **Selection** page of a job to select files for that job.

Files are selected for backup in three steps. In the first step, the appropriate files are selected by marking them with a check. In the second step, these marked files are sorted through using filter selection criteria. This step is optional. In the last step, as the job is run, Data Protector Express checks to see if it will back up all the files or only those files that have changed since the last backup job.

Marking files for backup

A file is selected for backup when the selection box next to the file is checked.

When the box next to a folder or other container is *shaded*, it means that this folder or container contains *some* selected files, even though it is not selected itself. When the box next to a folder or other container is *checked*, the folder itself is selected and may also contain selected files within it.



Directory

Attributes: [Rw--] [-DI]
Size: 0 bytes
Created: 25-Jul-2005 03:44 PM
Modified: 25-Jul-2005 03:44 PM
Last Accessed: 25-Jul-2005 03:44 PM

Name	Type	Size
☐ i386pe.x	File	5101 bytes
☐ i386pe.xbn	File	5119 bytes
☐ i386pe.xn	File	5101 bytes
☐ i386pe.xr	File	2524 bytes
☑ i386pe.xu	File	2884 bytes

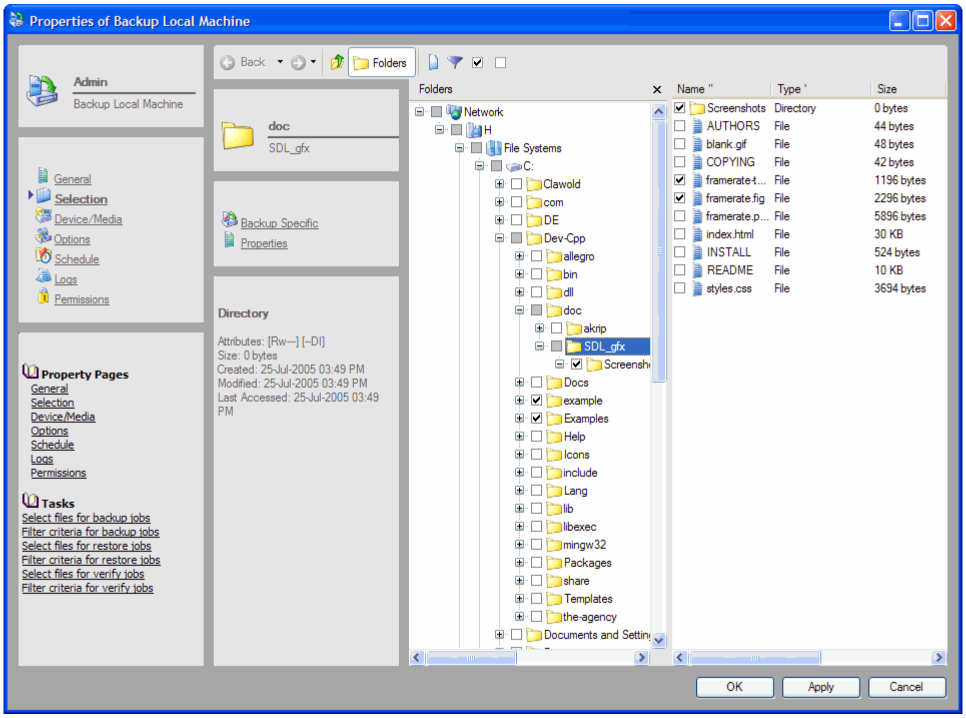
You can select or deselect a file for backup by checking or clearing the selection box next to the file. When you select a folder or volume, you automatically select all files contained in it.

Selecting folders or selecting files

You can select the contents of the folder in one of two ways: either by individually checking each object in that folder one-by-one or by checking the folder itself. Which method you choose is important because it affects which files Data Protector Express includes in the selection list *after changes have been made to that folder*.

If you select each file in the folder individually, when new files are added to the folder, Data Protector Express does not select them for backup. However, if you select the folder *itself*, when new items are created in that folder, Data Protector Express also includes these files in the backup job.

TIP: To speed up file selection on machines, consider organizing machines into workgroups. When you select a workgroup, Data Protector Express will back up selected files on all of the machines. This way, file selection is quicker and data for distinct groups within your organization is protected with a single backup job.



Directory

Attributes: [Rw--] [--DI]
Size: 0 bytes
Created: 25-Jul-2005 03:49 PM
Modified: 25-Jul-2005 03:49 PM
Last Accessed: 25-Jul-2005 03:49 PM

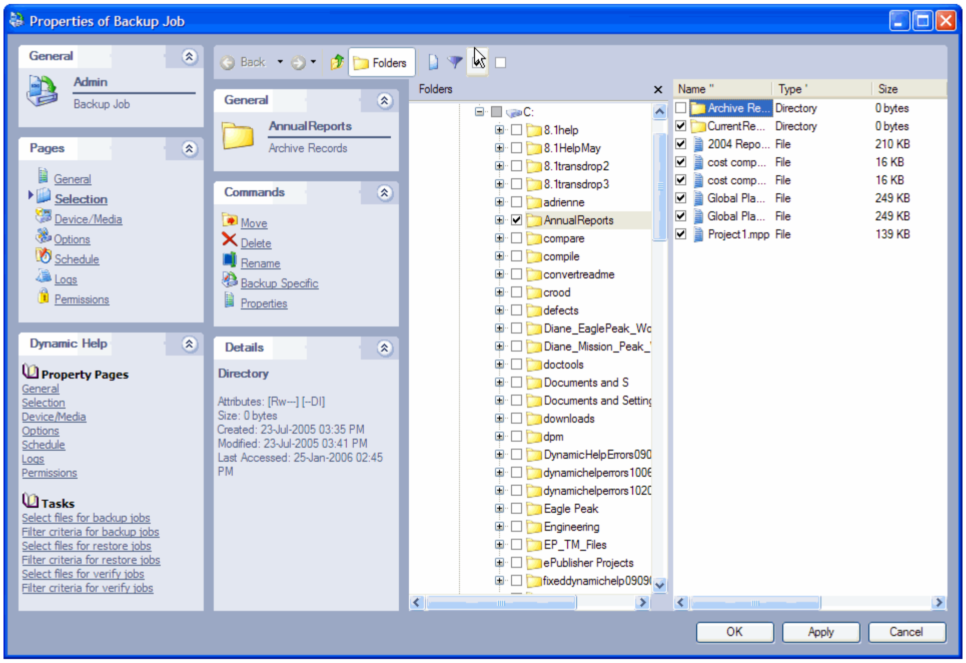
Name	Type	Size
☑ Screenshots	Directory	0 bytes
☐ AUTHORS	File	44 bytes
☐ blank.gif	File	48 bytes
☐ COPYING	File	42 bytes
☑ framerate-t...	File	1196 bytes
☑ framerate.fig	File	2296 bytes
☐ framerate.p...	File	5896 bytes
☐ index.html	File	30 KB
☐ INSTALL	File	524 bytes
☐ README	File	10 KB
☐ styles.css	File	3694 bytes

In general, when selecting files for backup, especially for jobs designed for disaster protection, begin by selecting containers at the top of the Data Protector Express management domain hierarchy. Then deselect containers or files lower in the hierarchy that you do not need to back up.

For example, you could begin by selecting the network icon at the top of the hierarchy. This will automatically select all of the machines on the network and all of the volumes on those machines. If there are machines, volumes or folders you do not want backed up, clear their check boxes. When new machines or volumes are added to the network (that is to the current Data Protector Express management domain), Data Protector Express will automatically select these machines and volumes.

There is an additional reason to select containers such as folders or volumes rather than the objects in the containers: to ensure that you do not miss any files stored loose in the container.

For example, suppose you want to back up a folder named **Annual Reports** and the folder named **Current Records** that is in it, but not the folder named **Archive Records**. If you check only the **Current Records** folder, your job will not back up any files in the **Annual Reports** folder that are not in the **Current Records** folder. Instead, check the **Annual Reports** folder and then clear the check box for the **Archive Records** folder. This selects all files in both the **Annual Reports** and **Current Records** folders—but not the files in the **Archive Records** folder.



Details

Directory

Attributes: [Rw---] [--DI]
Size: 0 bytes
Created: 23-Jul-2005 03:35 PM
Modified: 23-Jul-2005 03:41 PM
Last Accessed: 25-Jan-2006 02:45 PM

	Name	Type	Size
□	Archive Re...	Directory	0 bytes
☑	CurrentRe...	Directory	0 bytes
☑	2004 Repo...	File	210 KB
☑	cost comp...	File	16 KB
☑	cost comp...	File	16 KB
☑	Global Pla...	File	249 KB
☑	Global Pla...	File	249 KB
☑	Project1.mpp	File	139 KB

Selecting files with filters

Selection filters let you identify specific volumes, folders and files to exclude from the backup, restore or verify job. Click the **Selection Filters** button on the toolbar. Then specify the filter criteria for the job.

NOTE: The selection filters you specify are applied to all of the volumes, folders and files that have been marked for the job. You cannot apply different filters to different folders or volumes in the same job.

How selection filters work

By default, Data Protector Express backs up all volumes, folders and files that have been marked for the job. Selection filters let you identify specific criteria for excluding one or more of these marked objects. Data Protector Express applies these filter criteria at runtime, in effect unmarking any objects that do not meet the criteria.

For example, suppose you want to exclude all files that were created before 2004. Access the **Date Range** window for the **Create range** field. Select **On or after** for the **Range type**. Enter **1-Jan-2004** for the **Starting date**. When you run the job, Data Protector Express temporarily deselects all files with a creation date before 2004. They will be excluded from the backup.

You can change the filter criteria at any time. You can also mark or unmark objects before running the job. Data Protector Express does not apply the filter criteria to any marked object until it runs the job.

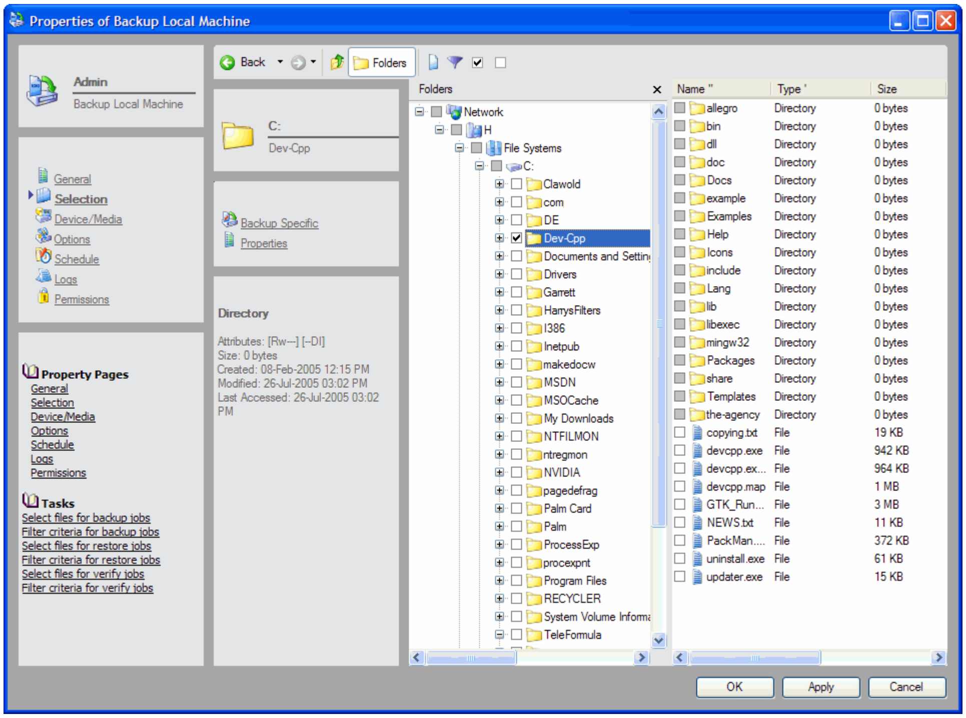
The use of filters can cause unexpected behavior. It’s recommended that you test any filters that you want to use before using them for backup.

NOTE: You cannot use selection filters to add unmarked objects to the job set. Selection filters are only used to exclude marked objects from the job set.

Filters and shaded folders

When you apply a filter to a marked folder, this may result in no files from that folder being selected. Although no files in that folder are selected, the folder will still appear with a shaded check box next to it.

The shaded check box indicates that if any new files that pass the filter criteria are created in that folder, they will be selected for the job.



Directory

Attributes: [Rw--] [--DI]
Size: 0 bytes
Created: 08-Feb-2005 12:15 PM
Modified: 26-Jul-2005 03:02 PM
Last Accessed: 26-Jul-2005 03:02 PM

Name	Type	Size
allegro	Directory	0 bytes
bin	Directory	0 bytes
dll	Directory	0 bytes
doc	Directory	0 bytes
Docs	Directory	0 bytes
example	Directory	0 bytes
Examples	Directory	0 bytes
Help	Directory	0 bytes
Icons	Directory	0 bytes
include	Directory	0 bytes
Lang	Directory	0 bytes
lib	Directory	0 bytes
libexec	Directory	0 bytes
mingw32	Directory	0 bytes
Packages	Directory	0 bytes
share	Directory	0 bytes
Templates	Directory	0 bytes
the-agency	Directory	0 bytes
copying.txt	File	19 KB
devcpp.exe	File	942 KB
devcpp.ex...	File	964 KB
devcpp.map	File	1 MB
GTK_Run...	File	3 MB
NEWS.txt	File	11 KB
PackMan....	File	372 KB
uninstall.exe	File	61 KB
updater.exe	File	15 KB

Selecting changed files only

When you run a job repeatedly, particularly backup jobs designed for disaster protection, many times you only want to back up files that have changed since the last time you ran a backup job. Data Protector Express handles this with the backup mode setting.

If you want to back up all selected files, use the **Full** backup mode setting; Data Protector Express does not deselect any selected files.

If you only want to back up files that have changed since the last *full* backup, use the **Differential** backup mode setting; Data Protector Express automatically deselects all the files that have not changed since the last *full* backup.

If you only want to back up files that have changed since the last backup, use the **Incremental** backup mode setting; Data Protector Express automatically deselects all the files that have not changed since the last backup.

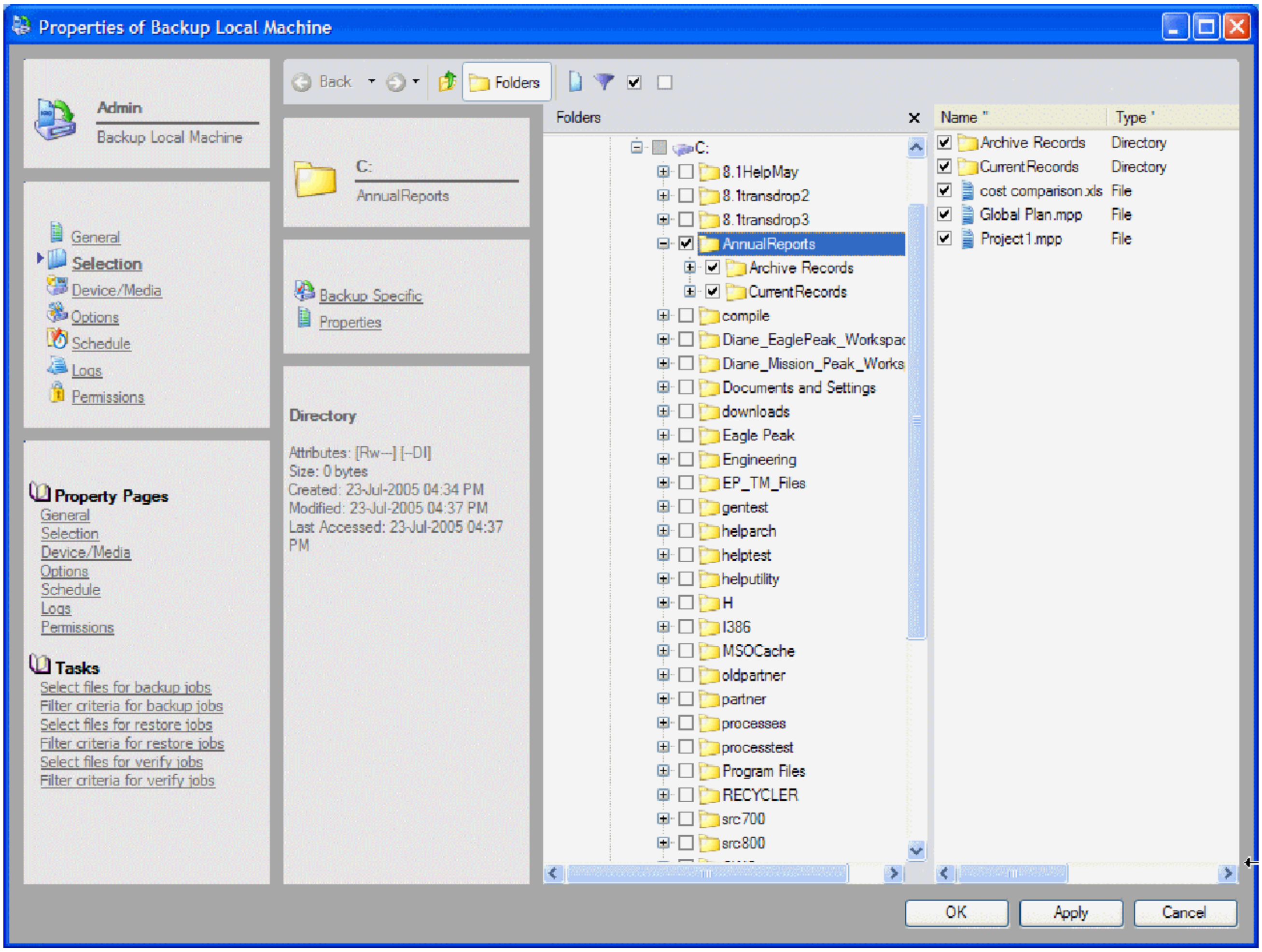
The job then runs with this updated selected file list.

Automatically selecting new files for backup

When you set up a job to run repeatedly, you want that job to adjust to changes made to any of the directories on your computer or any machine in your Data Protector Express management domain. Sometimes these changes include the addition of new files and directories that were not originally selected when the job was created. It may even include the addition of new machines on the network or any volumes on these machines that were not previously selected for backup.

If your selection criteria was carefully specified, Data Protector Express will also select these new files, folders, volumes and machines for backup. In general, a new file or container is selected for backup if (1) it is in a container selected for backup and (2) it meets the selection filter criteria.

For example, a new folder will be included in the backup selection list if it is in a selected container. If you create a new folder at the root level on a volume, that folder will be selected for backup if the volume was marked for backup. The files in that folder that pass through the selection filter criteria will be included in the backup job. However, if the volume itself was not selected, the new folder will not be selected.



Directory

Attributes: [Rw--] [--DI]
Size: 0 bytes
Created: 23-Jul-2005 04:34 PM
Modified: 23-Jul-2005 04:37 PM
Last Accessed: 23-Jul-2005 04:37 PM

- C:
  - □ 8.1HelpMay
  - □ 8.1transdrop2
  - □ 8.1transdrop3
  - ☑ AnnualReports
    - ☑ Archive Records
    - ☑ CurrentRecords
  - □ compile
  - □ Diane_EaglePeak_Workspac
  - □ Diane_Mission_Peak_Works
  - □ Documents and Settings
  - □ downloads
  - □ Eagle Peak
  - □ Engineering
  - □ EP_TM_Files
  - □ gentest
  - □ helparch
  - □ helptest
  - □ helputility
  - □ H
  - □ I386
  - □ MSOCache
  - □ oldpartner
  - □ partner
  - □ processes
  - □ processtest
  - □ Program Files
  - □ RECYCLER
  - □ src700
  - □ src800

Name	Type
☑ Archive Records	Directory
☑ CurrentRecords	Directory
☑ cost comparison.xls	File
☑ Global Plan.mpp	File
☑ Project1.mpp	File

If you want to see what files will be backed up, open up the **Selection** property page for the job. Whenever this page is opened, Data Protector Express recalculates which files should be selected for backup. Check the display to see that the files you intended to be backed up are selected.

NOTE: The **Selection** page shows all files that will be backed up by a full backup job. It does NOT indicate which files will not be backed up by a differential or incremental backup.

Working with mapped drives

Data Protector Express can be configured to include or exclude mapped drives during file selection. Once configured, these drives will appear on the **Selection** page of a job.

You must use the Data Protector Express Administrator, rather than the Data Protector Express service, to back up mapped drives because of the way that Windows implements mapped drives. The service must be stopped for the backup of the mapped drives to work.

NOTE: The HP Data Protector Express service must be stopped to allow the proper backup of mapped drives. The service cannot be running when you select mapped drives for backup because of the method Microsoft uses to authenticate mapped drive access. If the HP Data Protector Express service is not stopped when you select mapped drives for backup, the service will fail to authenticate to the selected mapped drives, and they will not be backed up. Because the HP Data Protector Express service must be stopped, you need to run Data Protector Express in application mode (the program must be open when the backup job is scheduled to occur), or the backup will not launch.

To enable or disable mapped drives

1. Open the **Catalog** view from the **Administration** desk bar.
2. In the main object detail area, select **Network**.
3. Select the machine whose mapped drives are being configured.
4. Select **System Drivers**.
5. Locate and select **File System Stream** and display its properties.
6. Select the **Configuration** page.
7. Enter a list of mapped drives in the appropriate list (e.g., JKLMQRSZX).

   You can enable or disable as many drives as you need. The list does not need to be listed in alphabetical order and Data Protector Express does not distinguish between capital and lower-cased letters for this purpose.

   For information about other options on this page, see *File system stream*.

Working with VSS snapshots

Backup jobs can create snapshots using Microsoft Volume Shadow Services (VSS) on platforms that support VSS.

VSS freezes the volume data at the point in time of the snapshot creation by creating a temporary snapshot. Any changes after that point in time will not be backed up until the next backup job. The snapshots are deleted after the job has finished. If VSS cannot create a snapshot the backup will proceed and the error will be noted in the job log.

Snapshots will affect an entire volume, not just the selected files. So jobs logs may indicate more space was snapped than you expect.

To turn off VSS for a job

1. Open the **Property** page for the job.
2. Select the **Options** page.
3. Click the **Advanced Options…** button
4. Deselect the **Enable Snapshots** checkbox

To turn off VSS for a specific machine

1. Open the **Catalog** view from the **Administration** desk bar.
2. In the main object detail area, select **Network**.
3. Select the machine for which VSS is being configured.
4. Select **System Drivers**.
5. Locate and select **Microsoft Volume Shadow Copy Services Agent**.
6. Right click and select **Stop.**

To re-enable the service, repeat the steps above and select **Run.**

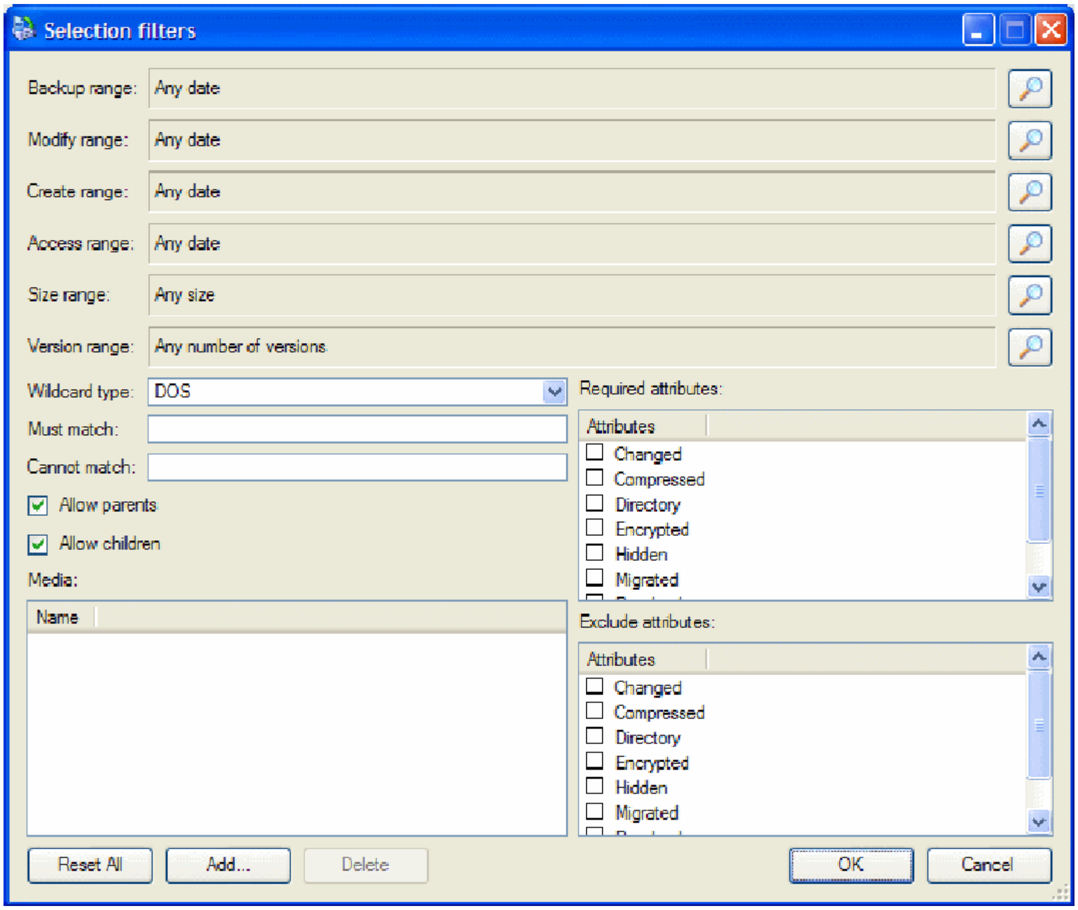
Selecting Files for Backup Jobs

To select files for backup jobs

1. View the properties of the backup job and click on the **Selection** page.
2. Check the selection boxes next to the files, folders or other containers you wish to include in the job.
3. Click the **Selection filters** button on the toolbar and specify filter selection criteria. (You can skip this step if you don't wish to apply any selection filters.)
4. Examine the tree view and object detail areas on the **Selection** page to ensure that the files you intended to select are marked for backup.

Applying filter criteria

When you click on the **Selection filters** button, the **Selection filters** window appears. This window has multiple selection filters you can apply to the files you have selected.



Backup range: Any date

Modify range: Any date

Create range: Any date

Access range: Any date

Size range: Any size

Version range: Any number of versions

Wildcard type: DOS

Must match:

Cannot match:

☑ Allow parents

☑ Allow children

Media:

Name

Required attributes:

Attributes

☐ Changed
☐ Compressed
☐ Directory
☐ Encrypted
☐ Hidden
☐ Migrated

Exclude attributes:

Attributes

☐ Changed
☐ Compressed
☐ Directory
☐ Encrypted
☐ Hidden
☐ Migrated

NOTE: Each filter criterion works **independently**. To be selected for backup, each file must pass every filter criterion specified. For example, if you specify that every file selected must have been created after January 1, 2004 and must have .doc as its extension, Data Protector Express will only select files which meet *both* selection criteria.

Filter selection criteria

This section contains a brief description of each selection filter Data Protector Express applies to the files and folders marked for backup.

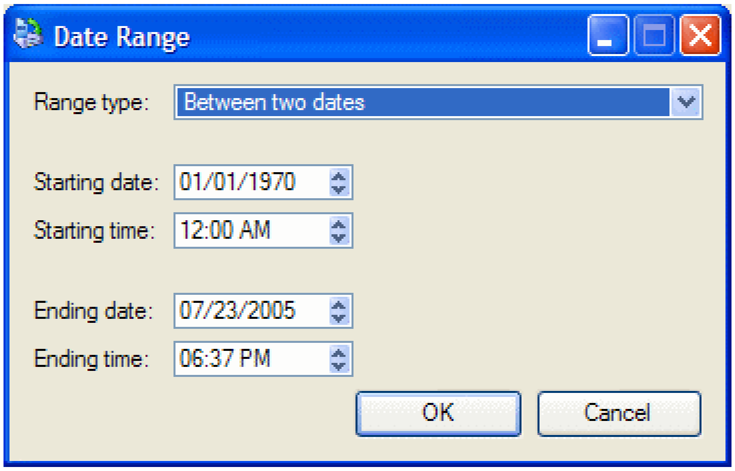
Note that some of the selection criteria are operating system-specific. Your Data Protector Express management domain may include multiple machines working with files created by different operating systems. If you select a filter criterion that is operating system-specific, files from other operating systems will be *automatically excluded* from the backup. This affects, in particular, the **Required attributes** and **Exclude attributes** filters.

NOTE: Data Protector Express calculates the century dates using the following process: if the year is 70 or smaller, the century is set to 20 (21st century); if the year is 71 or greater, the century is set to 19 (20th century). For example, if you set the date to 01-Jun-33, Data Protector Express calculates the date as June 1, 2033. If the date is set to 05-Apr-81, Data Protector Express calculates the date as April 5, 1981.

Backup Range

When a file is backed up, Data Protector Express stores the backup date in the catalog. This is called the **backup date**. Each time you back up a file, Data Protector Express changes the backup date to match this newer backup date. You can view information for all available backup versions file in the **Versions of…** window. You can use this information to filter files for verify jobs. You can use this filter for files that have been backed up on specific dates. More often, however, you would use this filter to filter out files that have been recently backed up.

To select files that have specific backup dates, click on the **Browse** button next to the **Backup range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.



Range type: Between two dates

Starting date: 01/01/1970

Starting time: 12:00 AM

Ending date: 07/23/2005

Ending time: 06:37 PM

Modify Range

Each time a file is modified, its modified date is updated. You can use this filter to back up files whose modified date matches your criteria. Data Protector Express checks the directory information on the volume to see if the file should be included for backup. For example, you can select only those files that were modified *after* a certain date and time or, alternatively, those that were modified *before* a certain date and time.

To select files that have specific modify dates, click on the **Browse** button next to the **Modify range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Create Range

When a file is first created, it is assigned a create date. You can use this filter to select only those files that match your criteria. Data Protector Express checks the created date for each file stored in the directory of the volume and uses this to select files for backing up.

To select files that have specific creation dates, click on the **Browse** button next to the **Create range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Access Range

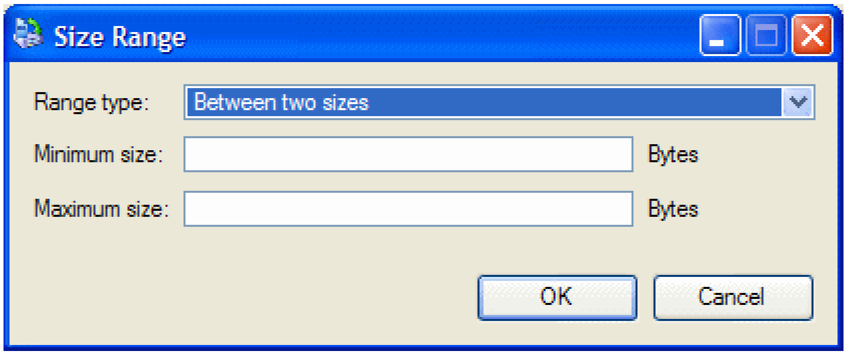
Each time a file is read, whether or not it is modified, its access date is updated. You can use this information to select files for backup. For example, you might want to back up only those files which have been accessed (opened or read) in the past two months. Alternatively, you could back up only those files which have *not* been accessed in the past two months.

To select files that have specific access dates, click on the **Browse** button next to the **Access range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Size Range

This filter lets you select files for backup according to their sizes. You might want to select only smaller files, larger files or files between two sizes.

To specify a filter that sorts files according to their sizes, click on the **Browse** button next to the **Size range** field and then select the appropriate criteria in the **Size Range** window that appears.



Range type: Between two sizes

Minimum size: Bytes

Maximum size: Bytes

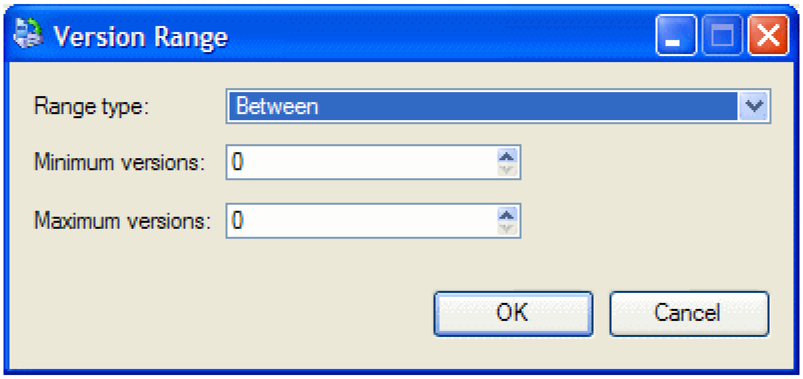
Version Range

Each time Data Protector Express backs up a file, it creates a new *version* of that file. For example, a file named **Expense Account Reporting Form** may have been backed up several times during the previous months and years. Typically, each version of the file is stored on the different media of a backup job. Data Protector Express tracks each version of a file separately in its catalog.

You can use this filter to instruct Data Protector Express to not back up files for which you already have multiple versions. For example, you may not want any more than three versions of a particular file backed up. When you set the **Range type** to **At most** and **Maximum versions** to **3**, Data Protector Express only backs up those files with less than three versions.

Note, however, that having several versions of a file does not ensure that the versions you have reflect the latest changes to the file. It may have been modified after the last time you backed it up. If so, your latest version may not match the file's current form.

To specify a filter that selects files according to their number of versions, click on the **Browse** button next to the **Version range** field and then select the appropriate criteria in the **Versions Range** window that appears.



Range type: Between

Minimum versions: 0

Maximum versions: 0

Wildcard Type

Select which wildcard format you wish to use from the list box. You can use any of the following formats:

- **Default:** Uses the default wildcard format for your operating system.
- **DOS:** Uses the 11-character name format with the eight-character primary name and the three-character extension, e.g., filename.txt.
- **Macintosh:** Uses the Macintosh native format.
- **NFS:** Network File System
- **FTAM:** File Transfer Access and Management
- **Long:** Uses the 256-character name format with a long primary name and an extension with multiple characters, e.g., Monday_backup.txt.

Must Match

Data Protector Express lets you use wildcard matches to include files. Only files that match the wildcard indicated in the **Must match** field are included in the backup set. For example, if you enter ***.exe**, Data Protector Express will only back up those files with the .exe file extension.

You can specify multiple wildcards by separating each with a semicolon (no spaces). For example, if you enter ***.exe;*.doc** in the **Must match** field, Data Protector Express selects all files that have *either* the .exe extension *or* the .doc extension.

Cannot Match

This wildcard field works just like the **Must match** field except that it *excludes* any files that match the wildcards. You can specify multiple wildcards by separating them with a semicolon (no spaces); if you specify multiple wildcards, Data Protector Express excludes any file that matches any one of the wildcards you specify.

Required Attributes

Operating systems track certain features of files called *attributes* that they use to manage these files. You can use these same attributes as a selection filter. In the **Required attributes** field, if an attribute is checked, Data Protector Express only selects those files which have these attributes. For example, if you check **Hidden**, Data Protector Express only selects those files which the operating system has assigned the **Hidden** attribute.

You can select multiple attributes. With this filter applied, Data Protector Express only selects those files that meet *all* of the required attributes.

Note that some of these attributes are only supported by certain operating systems. If you specify an attribute that is specific to a particular operating system, then only files created under that operating system will be selected for backup.

Exclude Attributes

This field works like the **Required attributes** field except that Data Protector Express excludes files that match these attributes. For example, if you have checked the **Execute Only** box, Data Protector Express will exclude from the backup job any files with the **Execute Only** attribute.

You can select multiple attributes. A file that has any one of these attributes will be excluded. For example, if you mark the **Hidden** and **System** attributes, any file that has *either* attribute will be excluded.

Allow Parents

When this option is checked, Data Protector Express backs up the directory information for the parent along with the file. This option must be checked in order for folders and other directory data to be backed up. When this ption is not checked, Data Protector Express will not back up any parent information for any file backed up.

Allow Children

When this option is checked, Data Protector Express backs up any files in the selected folders. If you want to back up only the marked directories, however, you can clear this option. When the **Allow Children** box is unchecked and the **Allow Parents** box is checked, Data Protector Express backs up the directory structure, but not the files stored in the directories (that is, in the folders).

This option can be useful for replicating a complex directory structure. Begin by marking the directory structure you wish to duplicate. Then clear the **Allow Children** option. Data Protector Express will back up only the directory structure. You can then replicate that directory structure to any volume by restoring the directory to that volume.

Media

Data Protector Express tracks versions of files and the media on which those versions are stored. You can use this information to sort files according to the media on which they appear. Only files with versions on the media in the **Media** field will be selected for the backup job. For example, if you select media named "Daily Set:1," Data Protector Express will only include files in the backup job which have a valid version on the media named "Daily Set:1."

To sort files according to the media on which they appear, click the **Add...** button and select the media from the **Browse** window. Note that you must select a Media object, not a Media folder or User/Group folder. If there are multiple media shown in the **Media** filter field, only files which have a valid version on *all* the media listed will be selected.

This filter has limited applications for backup jobs. One way to use it, however, would be in the case of media you know is corrupt or damaged. To back up a new version of every file on that damaged media, begin by creating a new job and then selecting the appropriate Network or Machine object on the **Selection** page. Then open the **Selection Filters** window by clicking on the **Selection Filters** button. Add the damaged media to the **Media** field. Then set the **Backup mode** on the job's **Options page** to **Copy.** When Data Protector Express runs the job, it will only back up files which had a version on the damaged media shown in the **Media** field.

Restore Selection Concepts

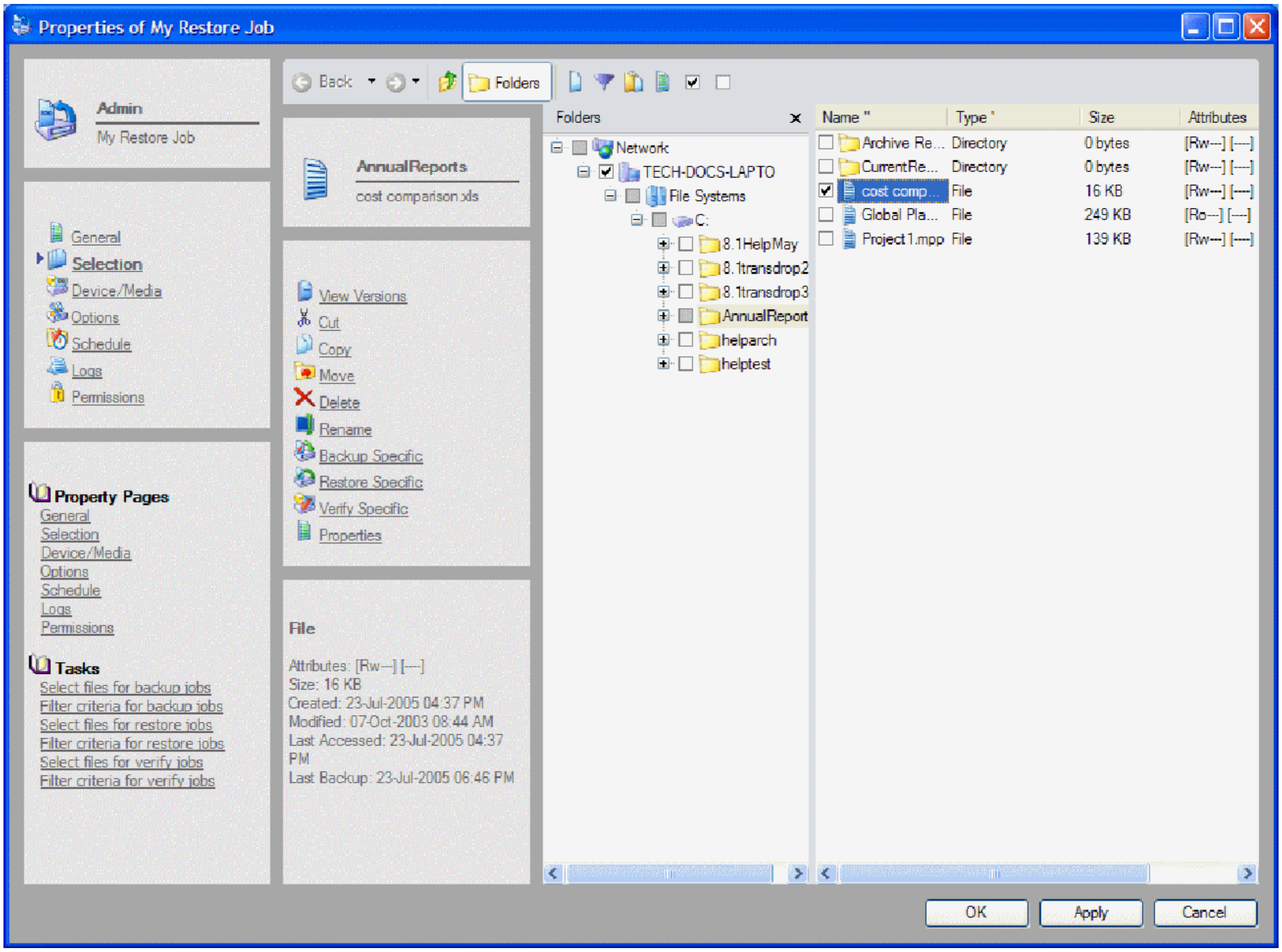
You select files for restoring the same way you select files for backing up; however besides selecting which files you wish to restore, you can also change the name of the restored file, restore it to a new location and create a new folder in which to restore the file. Additionally, when you select a file for restoring, you must specify which version of the file you wish to restore. (The most recent version is selected by default.)

Files are selected for restoring in four steps. In the first step, you modify the file tree to look the way you want it to appear when you restore the files. For example, you might make a new folder to store the restored files in. Second, the appropriate files are selected by marking them with a check and selecting the appropriate version. In the third step, these files are filtered using multiple selection criteria. In the last step, you can specify new names and locations for the restored files.

Selecting files for restoring

A file is selected for restoring when a check mark appears in the selection box next to the file.

When the box next to a folder or other container is shaded, it means that this container or folder contains selected files, even though it is not selected itself. When the box next to a folder or other container is *checked*, the folder itself is selected and may also contain selected files within it.

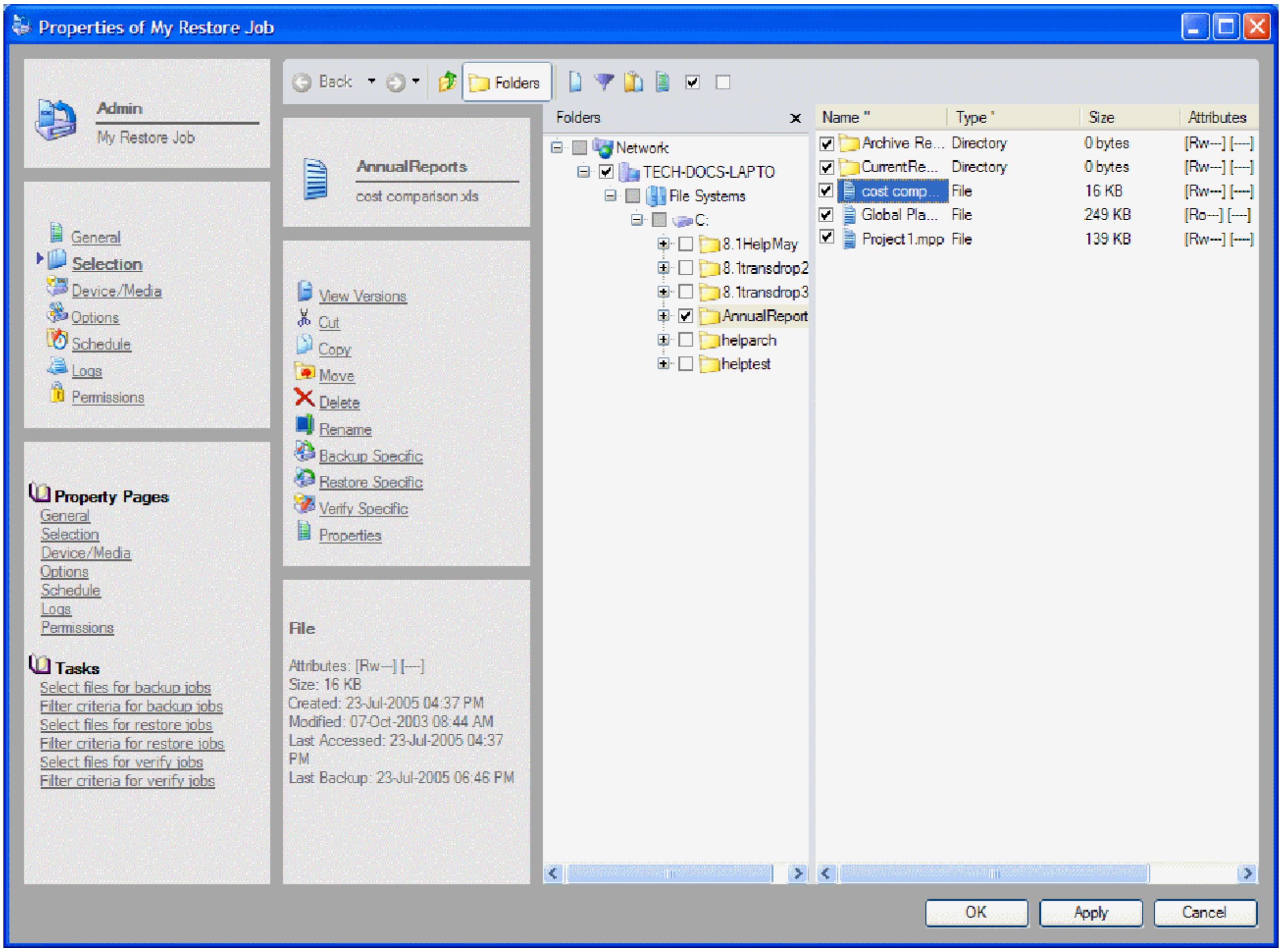


Name	Type	Size	Attributes
□ Archive Re...	Directory	0 bytes	[Rw--] [---]
□ CurrentRe...	Directory	0 bytes	[Rw--] [---]
☑ cost comp...	File	16 KB	[Rw--] [---]
□ Global Pla...	File	249 KB	[Ro--] [---]
□ Project1.mpp	File	139 KB	[Rw--] [---]

File

Attributes: [Rw--] [---]
Size: 16 KB
Created: 23-Jul-2005 04:37 PM
Modified: 07-Oct-2003 08:44 AM
Last Accessed: 23-Jul-2005 04:37 PM
Last Backup: 23-Jul-2005 06:46 PM

You can select or deselect a file for restoring by checking or clearing the selection box next to the file. You can also select the folder that contains the file and not the file itself. Notice that when you mark a container, such as a folder or volume, all of its contents, including all of the folders and containers in it, are also marked.



Name	Type	Size	Attributes
☑ Archive Re...	Directory	0 bytes	[Rw--] [----]
☑ CurrentRe...	Directory	0 bytes	[Rw--] [----]
☑ cost comp...	File	16 KB	[Rw--] [----]
☑ Global Pla...	File	249 KB	[Ro--] [----]
☑ Project1.mpp	File	139 KB	[Rw--] [----]

File

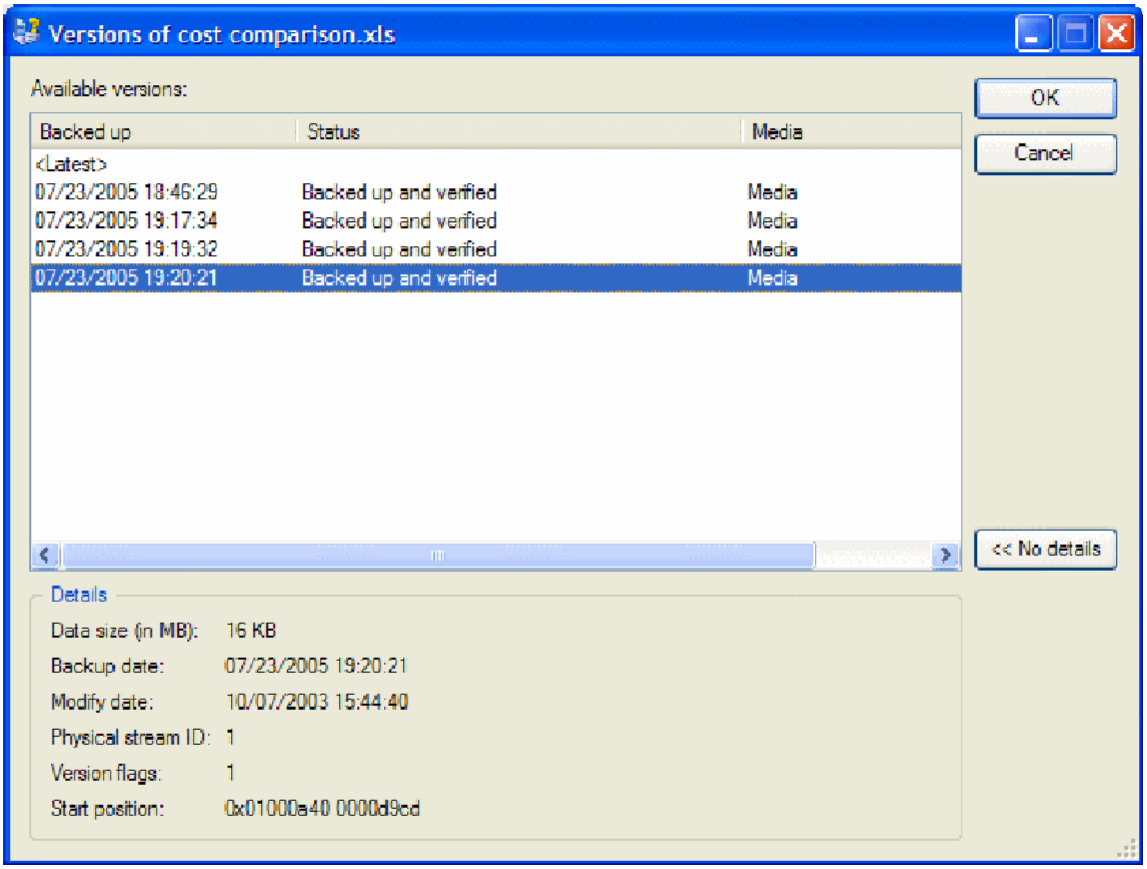
Attributes: [Rw--] [----]
Size: 16 KB
Created: 23-Jul-2005 04:37 PM
Modified: 07-Oct-2003 08:44 AM
Last Accessed: 23-Jul-2005 04:37 PM
Last Backup: 23-Jul-2005 06:46 PM

NOTE: The tree view and object detail areas are different for restore jobs than for backup jobs. For restore jobs, the files displayed in the tree view and object detail areas are the files for which Data Protector Express has versions in its catalog. For backup jobs, on the other hand, the files displayed are those currently present on the servers and PC desktops in the current storage domain.

Selecting versions of files

Each time a file is backed up, a *version* of that file is created. There may be several versions of files stored on different media created by different backup jobs. Data Protector Express keeps track of all the versions of each file in its catalog and the media on which each version is stored. When media is overwritten or deleted, Data Protector Express deletes those versions from its catalog as well.

When you select a file for restoring, Data Protector Express automatically selects the latest version. If you want to select a version other than the latest version of a backed up file, you must select that version in the **Versions of...** window. When you open the **Versions of...** window, the **Available versions** field shows a list of the versions of the file and the media on which those versions are stored. Select which version you want to restore by highlighting it. To display more information about a particular version of a file, click on the **Details** button. Data Protector Express displays various details it uses to manage the file in its catalog, including the file's backup date and its modify date.



Backed up	Status	Media
<Latest>		
07/23/2005 18:46:29	Backed up and verified	Media
07/23/2005 19:17:34	Backed up and verified	Media
07/23/2005 19:19:32	Backed up and verified	Media
07/23/2005 19:20:21	Backed up and verified	Media

Data size (in MB):	16 KB
Backup date:	07/23/2005 19:20:21
Modify date:	10/07/2003 15:44:40
Physical stream ID:	1
Version flags:	1
Start position:	0x01000a40 0000d9cd

If you select the latest version, Data Protector Express will restore the most recent version of that file or folder.

In general, if you want to restore a specific version of the file, you must select that file directly and specify which version you wish to restore in the **Versions of…** window.

Selecting versions of folders

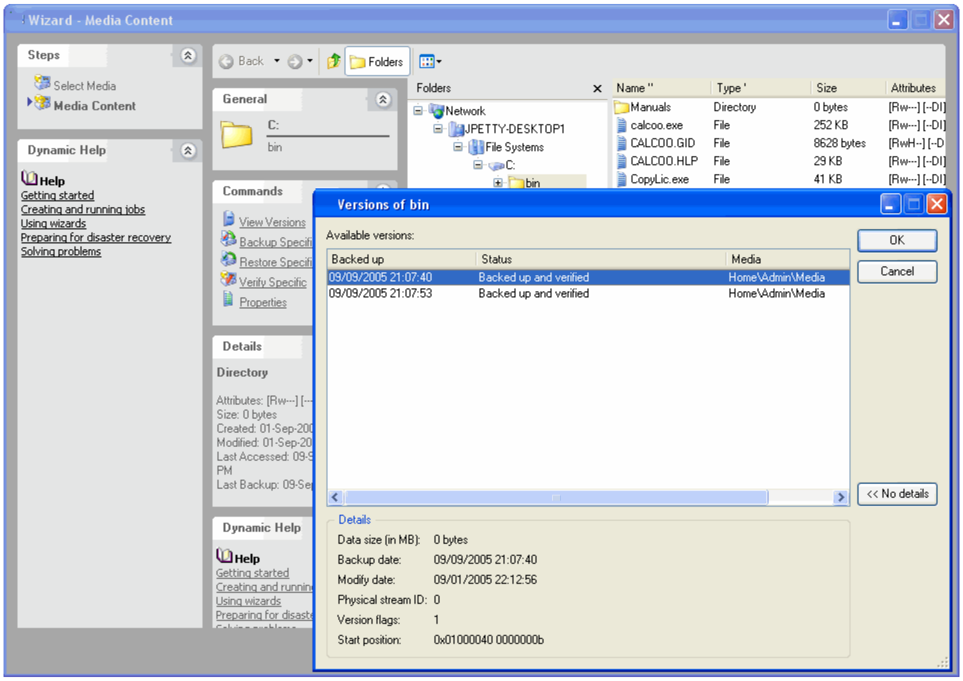
When you select a folder, Data Protector Express automatically selects the latest version for that folder and for every file within that folder. If you wish to specify another version, open the **Versions of…** window and highlight the version date to select it.

Data Protector Express uses the version you specified when you selected the folder to also select files contained within that folder. Specifically, a file is selected for restoring only if a version matches the folder version.

NOTE: When you specify a version date for a folder, volume or other container, files stored in that container are *only selected when they have a version date that matches the version date of the container.* Many times, files will not have version dates that match the dates of the containers they are stored in, for example, when you select a version date from an incremental or differential backup job. To be sure you select all of the files inside a container, select the latest version for that container.

Consider these two examples:

In the first example, by selecting the latest version of the folder, all of the files contained within the folder are selected because each of these files has a latest version. Note that *these versions may be from different dates and different backup jobs*, and consequently reside on different media. However, because each file has a latest version, each one will be restored.

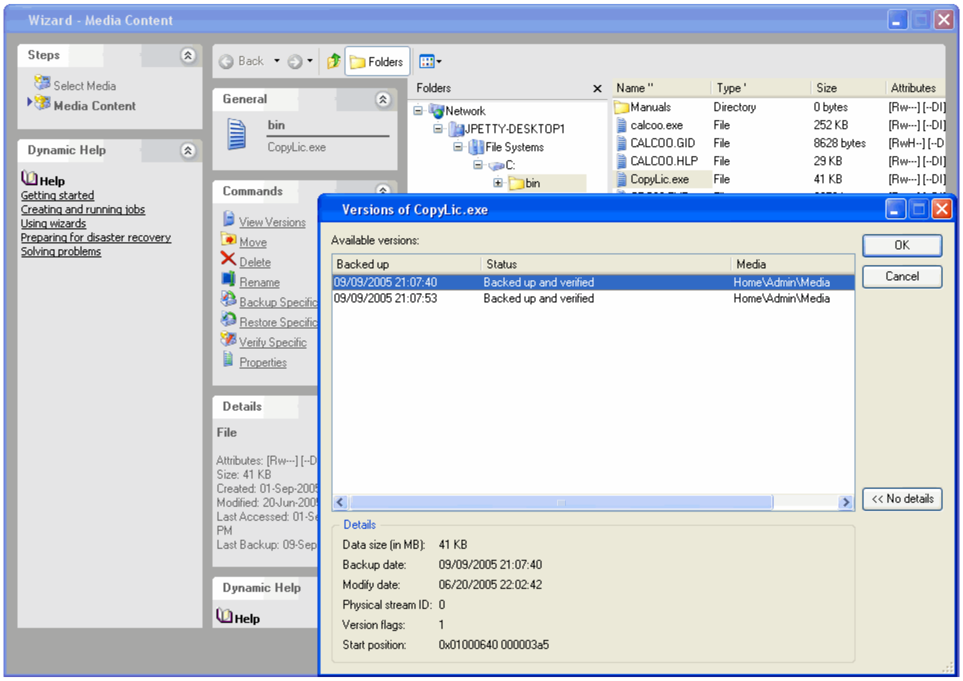


Name	Type	Size	Attributes
Manuals	Directory	0 bytes	[Rw---] [--DI]
calcoo.exe	File	252 KB	[Rw---] [--DI]
CALCOO.GID	File	8628 bytes	[RwH--] [--D
CALCOO.HLP	File	29 KB	[Rw---] [--DI]
CopyLic.exe	File	41 KB	[Rw---] [--DI]

Backed up	Status	Media
09/09/2005 21:07:40	Backed up and verified	Home\Admin\Media
09/09/2005 21:07:53	Backed up and verified	Home\Admin\Media

Data size (in MB): 0 bytes
Backup date: 09/09/2005 21:07:40
Modify date: 09/01/2005 22:12:56
Physical stream ID: 0
Version flags: 1
Start position: 0x01000040 0000000b

In the second example, another version besides the latest version was selected. In order for the files within the folder to be selected for restoring, they must have a version date that matches that selected for the folder. In this example, some files are not selected for restoring because they do not have an available version which matches the version date selected for the folder.



Name	Type	Size	Attributes
Manuals	Directory	0 bytes	[Rw---] [--DI]
calcoo.exe	File	252 KB	[Rw---] [--DI]
CALCOO.GID	File	8628 bytes	[RwH--] [--D
CALCOO.HLP	File	29 KB	[Rw---] [--DI]
CopyLic.exe	File	41 KB	[Rw---] [--DI]

Backed up	Status	Media
09/09/2005 21:07:40	Backed up and verified	Home\Admin\Media
09/09/2005 21:07:53	Backed up and verified	Home\Admin\Media

Data size (in MB): 41 KB
Backup date: 09/09/2005 21:07:40
Modify date: 06/20/2005 22:02:42
Physical stream ID: 0
Version flags: 1
Start position: 0x01000640 000003a5

In general, if you want to restore a specific version of the file, you must select that file directly and specify which version you wish to restore in the **Versions of…** window.

Selecting folders compared to selecting files

You can select the contents of the folder in one of two ways: either by individually marking the selection box of each object in that folder one-by-one or by marking the selection box of the folder itself. Which method you choose is important because it affects which files Data Protector Express includes in the selection list *after changes have been made to that folder.*

For example, if you select a folder for restoring by marking its selection box, all of the contents of that folder are restored. If a new backup job is run before the restore job is run, Data Protector Express selects files for restoring using the new folder's contents. So, for example, if a new file is created in that folder, Data Protector Express will also restore that file. Additionally, if you have selected a latest version of the folder, Data Protector Express will use the latest version of each file in its catalog. These files may be newer than the files you originally selected.

Versions and filters

You cannot use filters for selecting versions. The **Selection Filters** window can be used to sort through the versions you have otherwise specified in the **Versions of...** window, but filters will not change the selected version date.

Selecting files with filters

Selection filters let you identify specific volumes, folders and files to exclude from the restore job. Click the **Selection Filters** button on the toolbar. Then specify the filter criteria for the restore job.

NOTE: The selection filters you specify are applied to all of the volumes, folders and files that have been marked for restore. *You cannot apply different filters to different folders or volumes in the same job.*

How selection filters work

By default, Data Protector Express restores all volumes, folders and files that have been marked for restore. Selection filters let you identify specific criteria for excluding one or more of these marked objects. Data Protector Express applies these filter criteria at runtime, in effect unmarking any objects that do not fit the criteria.

For example, suppose you want to exclude all files that were created before 2002. Access the **Date Range** window for the **Create range** field. Select **On or after** for the **Range type**. Enter **1-Jan-2002** for the **Starting date**. When you run the job, Data Protector Express temporarily deselects all files with a creation date before 2002. They will be excluded from the restore.

You can change the filter criteria at any time. You can also mark or unmark objects before running the job. Data Protector Express does not apply the filter criteria to any marked object until it runs the job.

NOTE: You cannot use selection filters to add unmarked objects to the restore set. Selection filters are only used to **exclude** marked objects from the restore set.

Changing the name and location of restored files

When you restore a file, you may wish to restore the file with a new name or in a new location. If you restore a file to its original location using its original name, and that file currently exists there, Data Protector Express overwrites the current file with the restored file.

You can avoid overwriting current files by giving the file a new name or by restoring the file to a new directory. For example, to avoid replacing the current file named **Project List** with a previous, older version of the file, you can rename the file before restoring it or restore it to a different folder.

You can either select a different folder or, alternatively, Data Protector Express lets you create a new folder in which to restore the files.

Selecting Versions of Files for Restore Jobs

Each time you mark a selection box of a file or folder for restoring, Data Protector Express automatically selects the latest version. If you want to specify a different version, use the **Versions of…** window to select which version of the file you wish to restore.

You can also specify a particular version of a file or folder by highlighting it in the tree view or object detail areas and then clicking the **Select Version** button on the toolbar. Data Protector Express will show you the **Versions of…** window with a list of the available versions for that file.

Be certain to specify carefully which version of a file you wish to restore. A single Data Protector Express restore job can restore files backed up over a period of months or years on media created by many different backup jobs. You can easily restore all of the latest versions of the files by selecting the latest version in the **Versions of…** window. However, if you want versions of files that were created on different dates, you must select each version of each file individually.

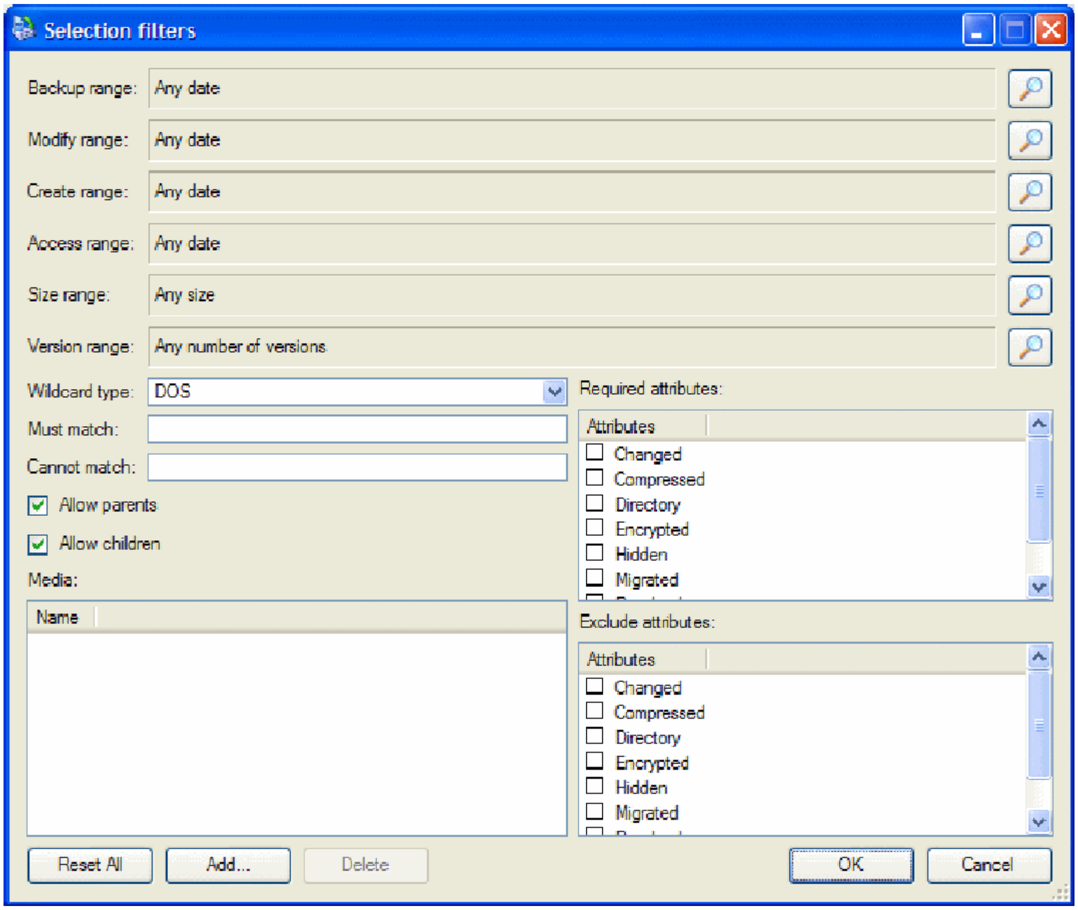
Note that you cannot restore multiple versions of the same file in a single restore job. If you want to restore more than one version of a file, you must create and run a separate job for each version.

To select versions of files for restore jobs

1. Open the **Properties** page of the restore job and click on the **Selection** page.
2. Check the selection boxes next to the files, folders or other containers you wish to include in the job.
3. To select a specific version of the objects you selected, highlight the folder or file and click the **Select Version** button. In the **Versions of…** window that appears, select the appropriate date of the version you wish to restore. If you want to include all of the files in a folder or on a volume, select the latest version.
4. Click the **Selection Filters** button on the toolbar and specify filter selection criteria. (You can skip this step if you don't wish to apply any selection filters.)
5. Examine the tree view and object detail areas on the **Selection** page to check that the files you intended are marked for restoring.
6. Additionally, you can change the names of the files and store them in new locations. This is discussed in *Restoring Files with New Names and Locations* on page 78.

Applying filter criteria

When you click on the **Selection Filters** button, the **Selection Filters** window appears. This window has multiple selection filters you can use to sort through the files you have selected for restoring.



Backup range: Any date

Modify range: Any date

Create range: Any date

Access range: Any date

Size range: Any size

Version range: Any number of versions

Wildcard type: DOS

Must match:

Cannot match:

☑ Allow parents

☑ Allow children

Media:

Name

Required attributes:

Attributes
□ Changed
□ Compressed
□ Directory
□ Encrypted
□ Hidden
□ Migrated

Exclude attributes:

Attributes
□ Changed
□ Compressed
□ Directory
□ Encrypted
□ Hidden
□ Migrated

NOTE: Each filter criterion works independently. To be selected for restoring, each file must pass every filter criterion specified. For example, if you specify that every file selected for restoring must have been created after January 1, 2002 and must have .doc as its extension, Data Protector Express will only select files which meet *both* selection criteria.

Filter selection criteria

This section contains a brief description of each selection filter Data Protector Express applies to the files and folders marked for restoring.

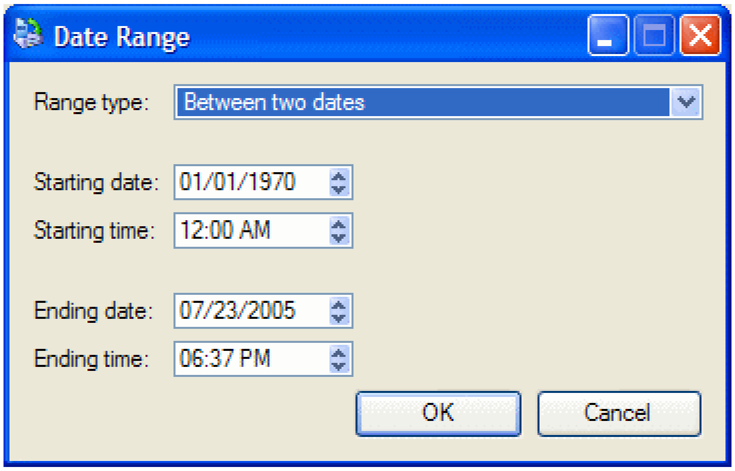
Note that the **Selection Filters** window for restore jobs is similar to the **Selection Filters** window for backup jobs. This allows you to use the same filters to select the files for restoring that you used for selecting files for backing up previously. This allows you to create a restore job that selects the same files as a backup job, no matter how widely distributed over the network these files may be.

NOTE: Data Protector Express figures the century dates using the following algorithm: if the year is 70 or smaller, the century is set to 20 (21st century); if the year is 71 or greater, the century is set to 19 (20th century). For example, if you set the date to 01-Jun-33, Data Protector Express calculates the date as June 1, 2033. If the date is set to 05-Apr-81, Data Protector Express calculates the date as April 5, 1981.

Backup Range

When a file is backed up, Data Protector Express stores the date the file was backed up in the Data Protector Express catalog. This is called the backup date. Each time you back up a file, Data Protector Express changes the backup date to the date of the backup. (You can view this information for all of the available versions in the **Versions of…** window in the **Backed up** field list.) You can use this information to filter files for restore jobs.

To select files that have specific backup dates, click on the **Browse** button next to the **Backup range** field. In the **Date Range** window that appears, select the appropriate range type, and the starting and ending dates and times.



Range type: Between two dates

Starting date: 01/01/1970

Starting time: 12:00 AM

Ending date: 07/23/2005

Ending time: 06:37 PM

Modify Range

Each time a file is modified, its modified date is updated. You can use this filter to restore files whose modified date matches your criteria. Data Protector Express checks the directory information on the volume to see if the file should be included in the restore job. For example, you can select only those files that were modified *after* a certain date and time or, alternatively, those that were modified *before* a certain date and time.

To select files that have specific modify dates, click on the **Browse** button next to the **Modify range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Create Range

When a file is first created, it is assigned a create date. You can use this filter to select only those files that match your criteria. Data Protector Express checks the created date for each file stored in the directory of the volume and uses this to select files for restoring.

To select files that have specific creation dates, click on the **Browse** button next to the **Create range** field. In the **Date Range** window that appears, select the appropriate range type, and the starting and ending dates and times.

Delete Range

This filter gives you an easy way to select files to restore that have been deleted from the volume, but for which Data Protector Express has valid versions stored in its catalog and on valid media.

When files that have once been backed up are later deleted, Data Protector Express marks these files with a special icon, indicating that they have been deleted. In addition, Data Protector Express assigns the file a delete date, which you can view on the **General** page of that file's property page.

This filter instructs Data Protector Express to only restore files which have a delete date that matches the criteria you have set. Note that if a file has not been deleted from the volume, it will be excluded by this filter and thus will not be selected for restoring.

You can easily select every file deleted for restoring by first marking the selection box of the volume and selecting the latest version. This will cause all of the files to be selected initially. Then, click on the **Browse** button next to the **Delete range** field and then select **On or before** from the **Range type** list box. Next select a random future date, for example, February 6, 2106. Data Protector Express will exclude all of the files that have not been deleted from the set of files to be restored. When you return to the **Selection** page, only those files that have been deleted will be checked.

On the other hand, you can also *not* restore files that have been deleted. In this case, set the **Delete range** filter to **On or before** some random early date, such as January 1, 1980. Any file that has been deleted will be filtered out by this filter, so that no deleted files will be restored. This can be useful if you don't want to unnecessarily restore files that were properly deleted in the first place.

Access Range

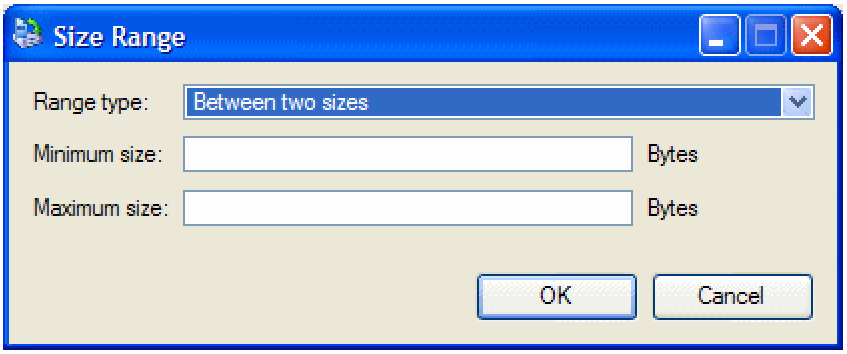
Each time a file is read, whether or not it is modified, its access date is updated. You can use this information to select files for restoring. For example, you might want to restore only those files which have been accessed (opened or read) in the past two months. Alternatively, you could restore only those files which have *not* been accessed in the past two months.

To select files that have specific access dates, click on the **Browse** button next to the **Access range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Size Range

This filter lets you select files to restore according to their sizes. You might want to select only smaller files, larger files or files between two sizes.

To specify a filter that sorts files according to their sizes, click on the **Browse** button next to the **Size range** field and then select the appropriate criteria in the **Size Range** window that appears.



Range type: Between two sizes

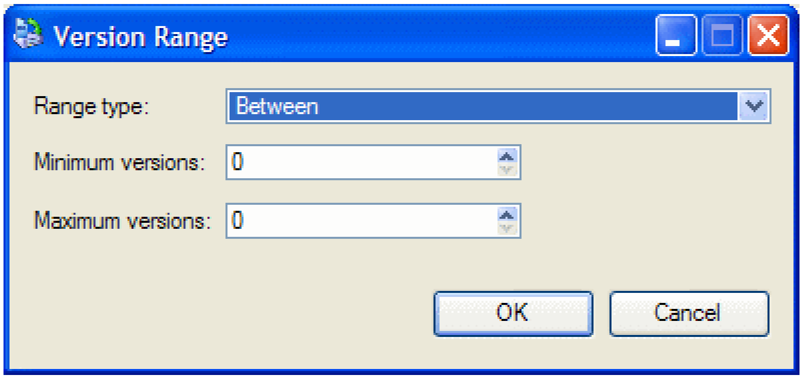
Version Range

Each time Data Protector Express backs up a file, it creates a new *version* of that file. For example, a file named **Expense Account Reporting Form** may have been backed up several times during the previous months and years. Typically, each version of the file is stored on the backup media of a different job. Data Protector Express tracks each version of a file separately in its catalog.

You can use this filter to instruct Data Protector Express to select files according to the number of versions that exist in the catalog. You might, for example, instruct Data Protector Express to restore all of the files for which there is only one version. When you set **Range type** to **At most** and **Maximum versions** to **1**, Data Protector Express only restores those files with a single version.

Note, however, that having multiple versions of a file does not ensure that the selected versions reflect the latest changes to the file. If it was modified after the last time you backed it up, your latest version may not match the file's current form.

To specify a filter that sorts files according to their number of versions, click on the **Browse** button next to the **Version range** field and then select the appropriate criteria in the **Versions Range** window that appears.



Range type: Between

Minimum versions: 0

Maximum versions: 0

Wildcard Type

Select which wildcard format you wish to use from the list box. You can use any of the following formats:

- **Default:** Uses the default wildcard format for your operating system.
- **DOS:** Uses the 11-character name format with the eight-character primary name and the three-character extension, e.g., filename.txt.

- **Macintosh:** Use the Macintosh native format.
- **NFS:** Network File System
- **FTAM:** File Transfer Access and Management
- **Long:** Uses the 256-character name format with a long primary name and an extension with multiple characters, e.g., Monday_backup.txt.

Must Match

Data Protector Express lets you use wildcard matches to include files. Only files that match the wildcard indicated in the **Must match** field are included in the restore set. For example, if you enter ***.exe**, Data Protector Express will only restore those files with the .exe file extension.

You can specify multiple wildcards by separating each with a semicolon (no spaces). For example, if you enter ***.exe;*.doc** in the **Must match** field, Data Protector Express selects all files that have *either* the .exe extension *or* the .doc extension.

Cannot Match

This wildcard field works just like the **Must match** field except that it *excludes* any files that match the wildcards. You can specify multiple wildcards by separating them with a semicolon (no spaces); if you specify multiple wildcards, Data Protector Express excludes any file that matches any one of the wildcards you specify.

Required Attributes

Operating systems track certain features of files called *attributes* that they use to manage these files. You can use these same attributes as a selection filter. In the **Required attributes** field, if an attribute is checked, Data Protector Express only selects those files which have these attributes. For example, if you check **Hidden**, Data Protector Express only selects those files which the operating system has assigned the **Hidden** attribute.

You can select multiple attributes. In this case, Data Protector Express only selects those files that meet *all* of the required attributes.

NOTE: Some attributes are only supported by certain operating systems. If you specify an attribute that is specific to a particular operating system, then **only files created under that operating system** will be selected for restore.

Exclude Attributes

This field works like the **Required attributes** field except that Data Protector Express excludes files that match these attributes. For example, if you have checked the **Execute Only** box, Data Protector Express will exclude from the restore job any files with the **Execute Only** attribute.

You can select multiple attributes. A file that has any one of these attributes will be excluded. For example, if you mark the **Hidden** and **System** attributes, any file that has *either* attribute will be excluded.

Allow Parents

When this option is checked, Data Protector Express restores directory information for any selected folder or volume. For example, if you have marked a folder, Data Protector Express will restore that folder only if this option is checked. When this option is not checked, directory information about folders and volumes is not restored.

Allow Children

When this option is checked, Data Protector Express restores files. When this option is unchecked, Data Protector Express does not restore files. This is useful if you want to restore a complex directory structure, but not the files in that directory. To restore a directory structure, but not the files (children) stored in the directories, begin by marking the directory for restoring. Then clear the **Allow Children** option. Data Protector Express will restore only the directory structure to the volume you specify.

Media

Data Protector Express tracks versions of files and the media on which those versions are stored. You can use this information to sort files according to the media on which they appear. Only files with versions on the media in the **Media** field will be selected for the restore job. For example, if you select media named “Daily Set:1,” Data Protector Express will only include files in the restore job which have a valid version on the media named “Daily Set:1.”

To sort files according to the media on which they appear, click the **Add...** button and select the media from the **Browse** window. Note that you must select a Media object, not a Media folder or User/Group folder. If there are multiple media shown in the **Media** filter field, only files which have a valid version on *all* the media listed will be selected.

This filter can be useful for restore jobs if you want to restore files only from a particular media. For example, you may have imported media from another Data Protector Express management domain and may wish to limit the files restored to those on that particular media. In this case, you can ensure that only files on that media are selected by adding that media to the **Media** field.

Note, however, that under ordinary circumstances, you should let Data Protector Express track the versions of particular files and restore files *not according to the media on which they appear,* but rather *according to their version date.* For example, if you want to restore the most recent version of a file, simply select the file. Data Protector Express will automatically select that file and identify the proper media on which that version is stored. Data Protector Express will then prompt you for the correct media when the job is run.

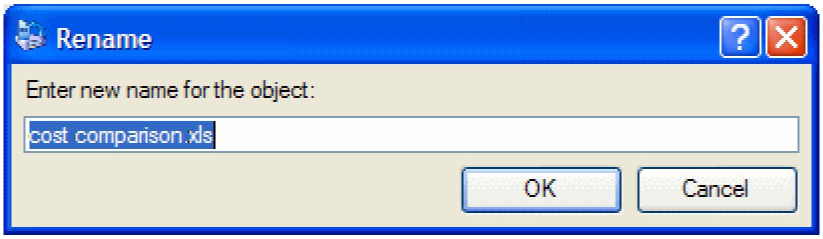
Restoring Files with New Names and Locations

You can change the name and location (folder) of a file when it is restored. Often referred to as a redirected restore operation, you can also create a new folder in which to store the file.

Restoring a file with a new name

After a file has been selected for restoring, you can rename the file. When you rename the file, Data Protector Express restores the file with the new name. This can be useful for not overwriting versions of the file that currently exist on disk.

To rename a file, right-click the file name on the **Selection** page of the restore job, select **Rename** from the shortcut menu and type the new name. Once you run the job the renamed file will be restored to the directory in which the original file was located.



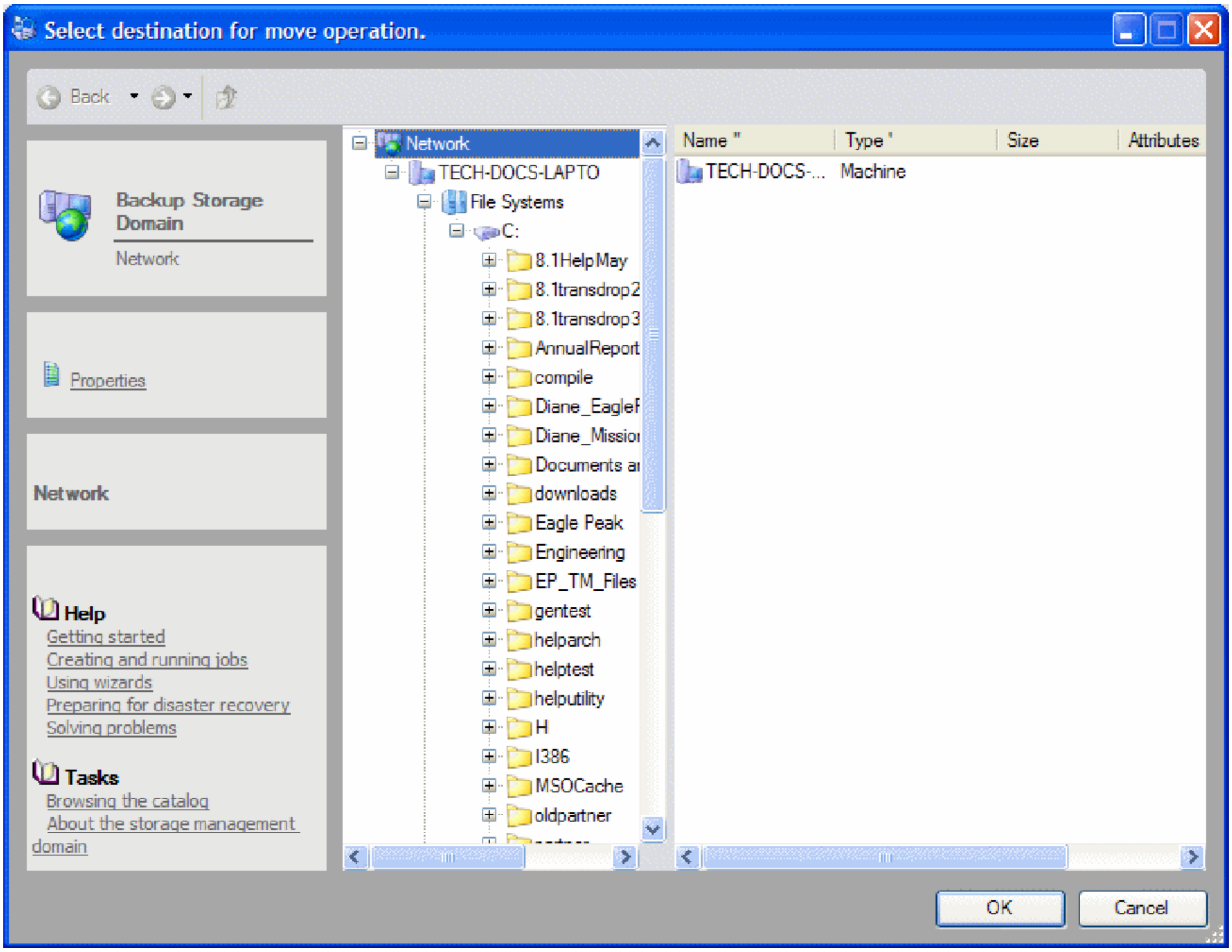
cost comparison.xls

Note that when you rename a version, you are *only* renaming that file for the purposes of restoring it with this particular restore job. *Only the current restore job will assign the new name to that file*. When you create a new restore job, you will see the file displayed with its original name. Similarly, the **Catalog** view always displays files with the names they had when they were backed up.

Restoring files to a different folder

You can also restore files to different folders. When Data Protector Express restores the file, it creates a new file in the new location. Similarly, you can restore folders in new locations as well. This is useful in order to prevent overwriting files and folders that currently exist on disk.

To restore a file to a different folder, right-click the file name on the **Selection** page of the restore job and select **Move…** from the shortcut menu. (**Move** is not displayed in the list of commands.) In the **Select destination for move operation** window, select a target location. Data Protector Express will move the file to the destination you select.



You can also restore folders and volumes in new locations. The contents of these containers move with them and are restored, along with the folder or volume, in the new location.

Note that when you move a version on the **Selection** page of a restore job, the changes you make are only recorded for that restore job. Only the current restore job will assign the file or folder the new location. When you create a new restore job, you will see the files and folders in their original locations. Likewise, the **Catalog** view will continue to display files in their original locations.

Restoring files to a new folder

You can create a new folder and restore files to that new folder. When Data Protector Express restores the files, it creates the new folder and restores the files you specified to that new location. Similarly, you can restore folders and their contents in new folders you create.

To create a new folder during a restore job

1. Create a restore job and select the file to be restored in a new folder.
2. Right-click the file and select the **Move** command from the shortcut list.
3. Select the location you want to create the new folder in the tree view area.
4. Select the **New** command from the **Commands** task pane. The **New** command is available only when you select a location for which it is appropriate for the operating system to create a directory.

5. Enter a name for the folder.

   Data Protector Express creates the new folder in the specified location and restores the selected file files to this new folder once you run the job.

Note that any new folder you create on the **Selection** page of the restore job is only created in the current restore job. Only the current job will show this new folder. When you create a new restore job or open another restore job, the new folder you created in the current job will not be displayed. Likewise, the new folder you created will not be displayed on the **Catalog** view either.

Verify Selection Concepts

You select files for verifying the same way you select files for backing up or restoring, including selecting which version to verify.

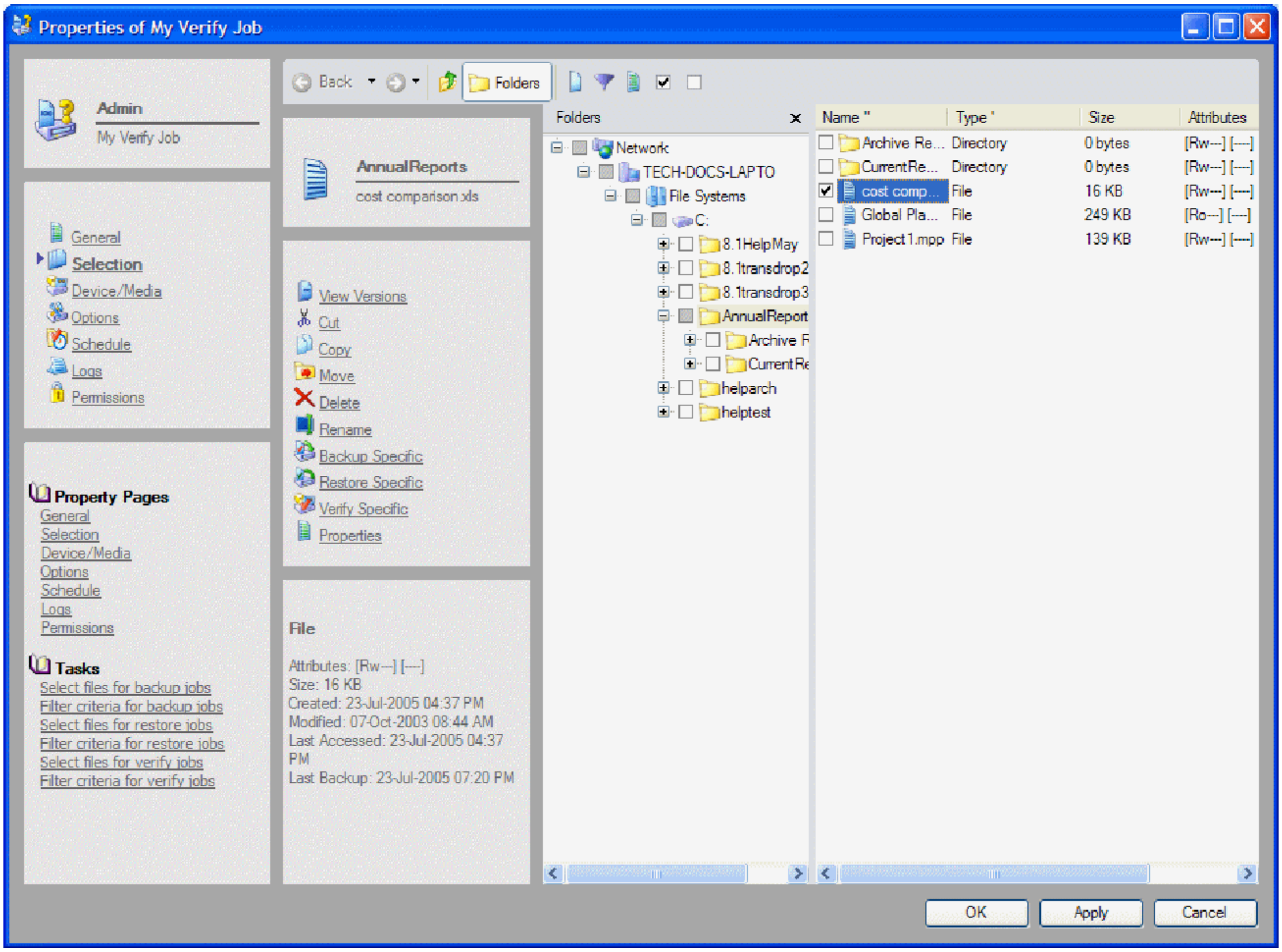
Files are selected for verifying in two steps. In the first step, the appropriate files are selected by marking them with a check and selecting the appropriate version. In the second step, these files are filtered using multiple selection criteria.

TIP: You can quickly check to see if a file was verified when it was backed up by opening the **Versions of…** window for that file. The **Status** field will show either **Backed up and verified; Backed up but verify failed; Backed up, possibly corrupted; Backed up, probably corrupted;** or **Backed up, not verified** depending on whether or not that file was successfully verified or not when the job was run.

Selecting files for verifying

A file is selected for verifying when a check mark appears in the selection box next to the file.

When the box next to a folder or other container is gray, it means that this container or folder contains selected files, even though it is not selected itself. When the box next to a folder or other container is *shaded and checked*, the folder itself is selected and may also contain selected files within it.

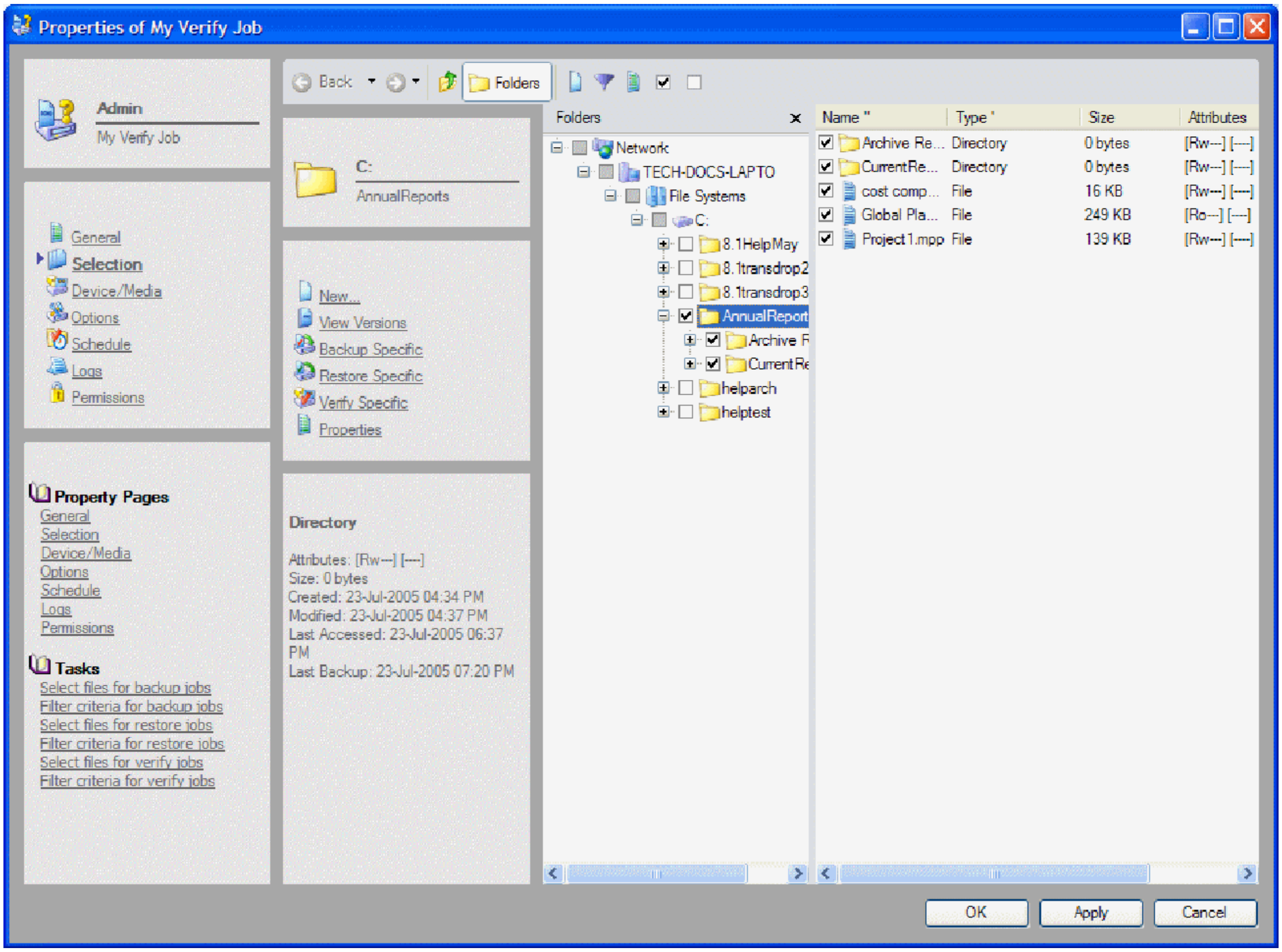


File

Attributes: [Rw---] [----]
Size: 16 KB
Created: 23-Jul-2005 04:37 PM
Modified: 07-Oct-2003 08:44 AM
Last Accessed: 23-Jul-2005 04:37 PM
Last Backup: 23-Jul-2005 07:20 PM

Name	Type	Size	Attributes
☐ Archive Re...	Directory	0 bytes	[Rw---] [----]
☐ CurrentRe...	Directory	0 bytes	[Rw---] [----]
☑ cost comp...	File	16 KB	[Rw---] [----]
☐ Global Pla...	File	249 KB	[Ro---] [----]
☐ Project1.mpp	File	139 KB	[Rw---] [----]

You can select or deselect a file for verifying by checking or clearing the selection box next to the file. You can also select the folder that contains the file and not the file itself. Notice that when you mark a container, such as a folder or volume, all of its contents, including all the containers and folders that it contains, are also marked.



Name	Type	Size	Attributes
☑ Archive Re...	Directory	0 bytes	[Rw---] [----]
☑ CurrentRe...	Directory	0 bytes	[Rw---] [----]
☑ cost comp...	File	16 KB	[Rw---] [----]
☑ Global Pla...	File	249 KB	[Ro---] [----]
☑ Project1.mpp	File	139 KB	[Rw---] [----]

Directory

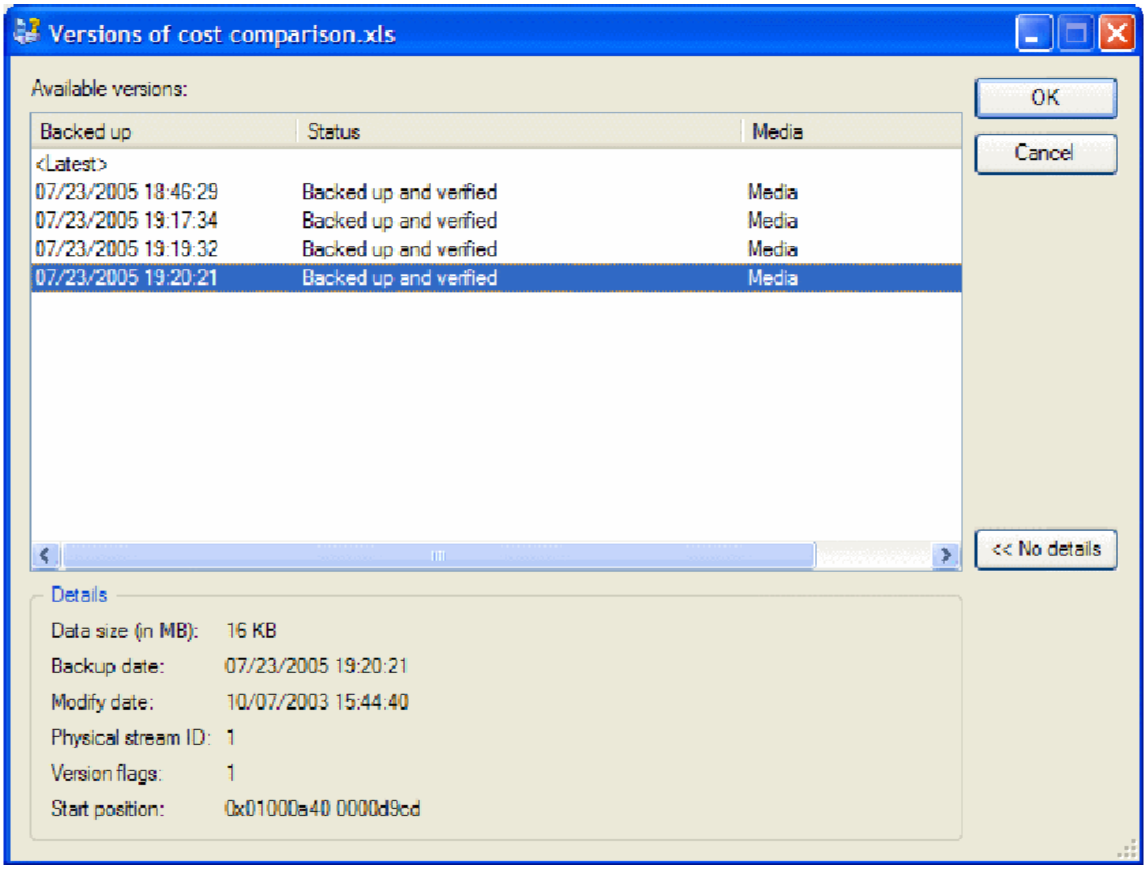
Attributes: [Rw---] [----]
Size: 0 bytes
Created: 23-Jul-2005 04:34 PM
Modified: 23-Jul-2005 04:37 PM
Last Accessed: 23-Jul-2005 06:37 PM
Last Backup: 23-Jul-2005 07:20 PM

NOTE: The tree view and object detail areas are different for verify jobs than for backup jobs. For verify jobs, the files displayed in the tree view and object detail areas are the files for which Data Protector Express has versions in its catalog. For backup jobs, on the other hand, the files displayed are those currently present on servers and PC desktops in the current storage domain.

Selecting versions of files

Each time a file is backed up, a *version* of that file is created. There may be multiple versions of files stored on different media created by different backup jobs. Data Protector Express keeps track of all the versions of each file in its catalog and the media on which each version is stored. When media is overwritten or deleted, Data Protector Express deletes those versions from its catalog as well.

When you select a file for verifying, Data Protector Express automatically selects the latest version. If you want to select a version other than the latest version of a backed up file, you must select that version in the **Versions of...** window. When you open the **Versions of...** window, the **Available versions** field shows a list of the versions of the file and the media on which those versions are stored. Select which version you want to verify by highlighting it. To display more information about a particular version of a file, click on the **Details** button. Data Protector Express displays various details it uses to manage the file in its catalog, including the file's backup date and its modify date.



Versions of cost comparison.xls

Available versions:

Backed up	Status	Media
<Latest>		
07/23/2005 18:46:29	Backed up and verified	Media
07/23/2005 19:17:34	Backed up and verified	Media
07/23/2005 19:19:32	Backed up and verified	Media
07/23/2005 19:20:21	Backed up and verified	Media

Details

Data size (in MB):	16 KB
Backup date:	07/23/2005 19:20:21
Modify date:	10/07/2003 15:44:40
Physical stream ID:	1
Version flags:	1
Start position:	0x01000a40 0000d9cd

If you select the latest version, Data Protector Express will verify the most recent version of that file or folder.

In general, if you want to verify a specific version of the file, you must select that file directly and specify which version you wish to verify in the **Versions of…** window.

Note that when you specify a version date for a container, such as a folder or a volume, only those files which have matching version dates will be selected. If a file does not have a version date that matches the date of the container, it will not be selected. On the other hand, if you want only certain files to be verified, you can specify the version date of a container to only select those files with matching version dates.

Selecting folders compared to selecting files

You can select the contents of the folder in one of two ways: either by individually marking the selection box of each object in that folder one-by-one or by marking the selection box of the folder itself. Which method you choose is important because it affects which files Data Protector Express includes in the selection list *after changes have been made to that folder.*

For example, if you select a folder for verifying by marking its selection box, all of the contents of that folder are verified. If a new backup job is run before the verify job is run, Data Protector Express selects files for verifying using the new folder's contents. So, for example, if a new file is created in that folder, Data Protector Express will also verify that file. Additionally, if you have selected the latest version of the folder, Data Protector Express will use the latest version of each file in its catalog. These files may be newer than the files you originally selected.

Selecting files with filters

Selection filters let you identify specific volumes, folders and files to exclude from the verify job. Click the **Selection Filters** button on the toolbar. Then specify the filter criteria for the verify job.

NOTE: The selection filters you specify are applied to all of the volumes, folders and files that have been marked for verify. *You cannot apply different filters to different folders or volumes in the same job.*

How selection filters work

By default, Data Protector Express verifies all volumes, folders and files that have been marked for verification. Selection filters let you identify specific criteria for excluding one or more of these marked objects. Data Protector Express applies these filter criteria at runtime, in effect unmarking any objects that do not fit the criteria.

For example, suppose you want to exclude all files that were created before 2002. Access the **Date Range** window for the **Create range** field. Select **On or after** for the **Range type**. Enter **1-Jan-2002** for the **Starting date**. When you run the job, Data Protector Express temporarily deselects all files with a creation date before 2002. They will be excluded from the verify.

You can change the filter criteria at any time. You can also mark or unmark objects before running the job. Data Protector Express does not apply the filter criteria to any marked object until it runs the job.

NOTE: You cannot use selection filters to add unmarked objects to the verify set. Selection filters are only used to exclude marked objects from the verify set.

Selecting Versions of Files for Verify Jobs

Each time you mark a selection box of a file or folder for verifying, Data Protector Express automatically selects the latest version. If you want to specify a different version, use the **Versions of…** window to select which version of the file you wish to verify.

You can also specify a particular version of a file or folder by highlighting it in the tree view or object detail areas and then clicking the **Select Version** button on the toolbar. Data Protector Express will show you the **Versions of…** window with a list of the available versions for that file.

Be certain to specify carefully which version of a file you wish to verify. A single Data Protector Express verify job can verify files backed up over a period of months or years on media created by many different backup jobs. You can easily verify all of the latest versions of the files by selecting the latest version in the **Versions of…** window. However, if you want versions of files that were created on different dates, you must select each version of each file individually.

Note that you cannot verify multiple versions of the same file in a single verify job. If you want to verify more than one version of a file, you must create and run a separate job for each version.

To select versions of files for verify jobs

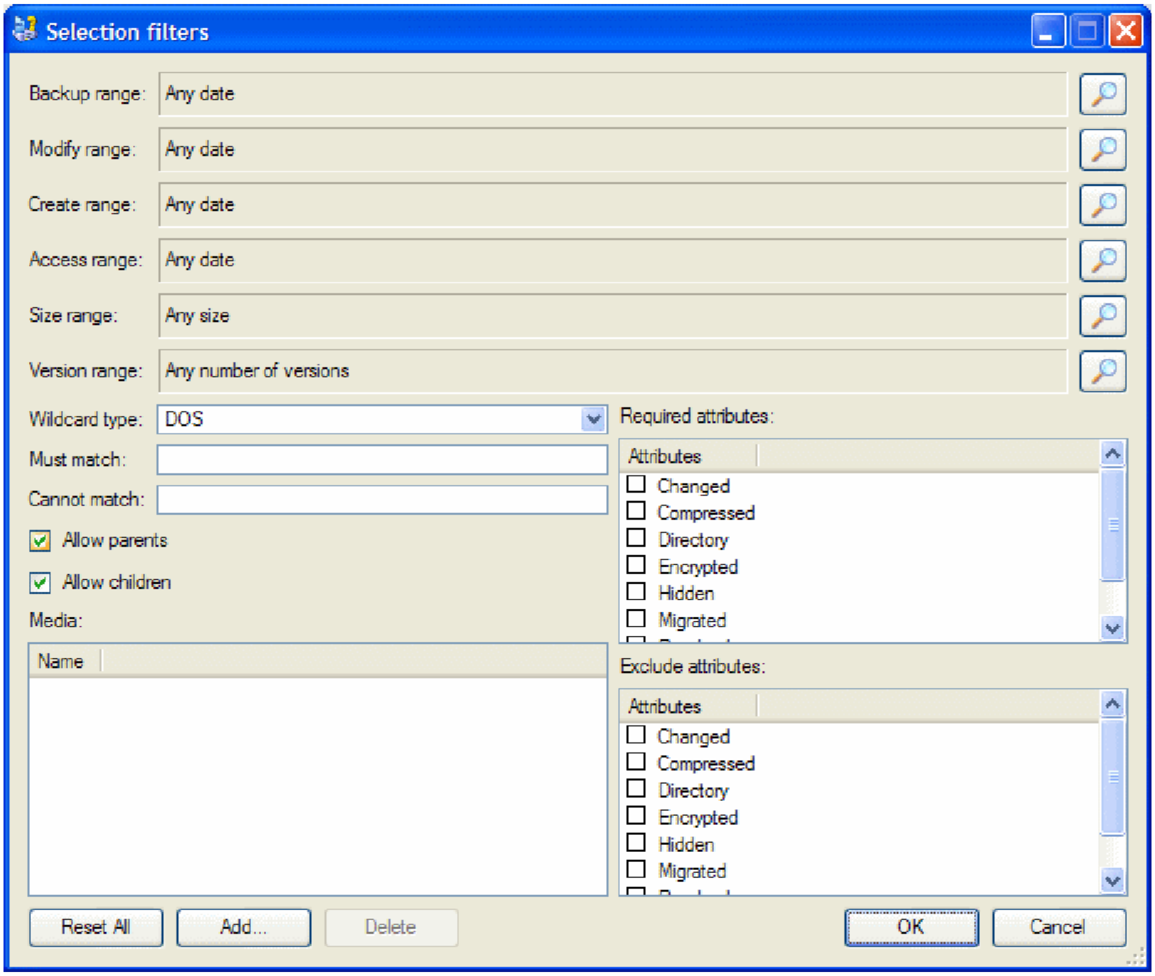
1. Open the property page of the verify job and click on the **Selection** page.
2. Check the selection boxes next to the files, folders or other containers you wish to include in the job.
3. To select a specific version of the objects you selected, highlight the folder or file and click the **Select Version** button. In the **Versions of…** window that appears, select the appropriate date of the version you wish to verify. If you want to include all of the files in a folder or on a volume, select the latest version.

4. Click the **Selection Filters** button on the toolbar and specify filter selection criteria. (You can skip this step if you don't wish to apply any selection filters.)

5. Examine the tree view and object detail areas on the **Selection** page to check that the files you intended to select are marked for verifying.

Applying filter criteria

When you click on the **Selection Filters** button, the **Selection Filters** window appears. This window has multiple selection filters you can use to sort through the files you have selected for verifying.



Backup range: Any date

Modify range: Any date

Create range: Any date

Access range: Any date

Size range: Any size

Version range: Any number of versions

Wildcard type: DOS

Must match:

Cannot match:

☑ Allow parents

☑ Allow children

Media:

Name

Required attributes:

Attributes

□ Changed
□ Compressed
□ Directory
□ Encrypted
□ Hidden
□ Migrated

Exclude attributes:

Attributes

□ Changed
□ Compressed
□ Directory
□ Encrypted
□ Hidden
□ Migrated

Note that each filter criterion works independent of every other. In order to be selected for verifying, each file must pass *every* filter criterion specified. For example, if you specify that every file selected for verifying must have been created after January 1, 2002 and must have .doc as its extension, Data Protector Express will only select files which meet *both* selection criteria.

Filter selection criteria

This section contains a brief description of each selection filter Data Protector Express applies to the files and folders marked for verifying.

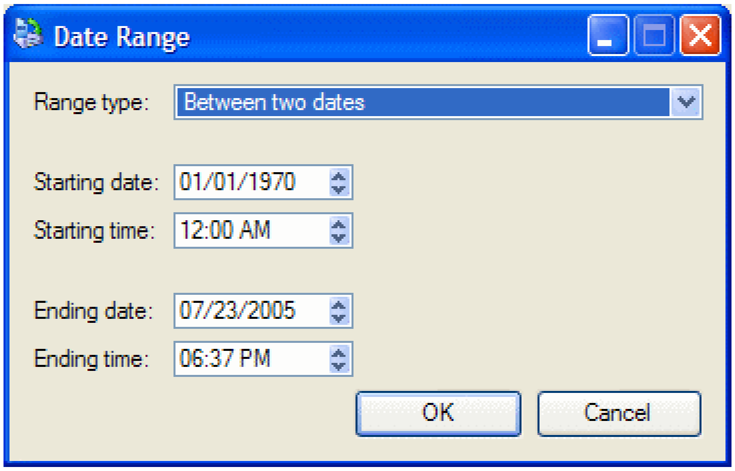
Note that the **Selection Filters** window for verify jobs is similar to the **Selection Filters** window for backup jobs. This allows you to use the same filters to select the files for verifying that you used for selecting files for backing up previously. This allows you to create a verify job that selects the same files as a backup job, no matter how widely distributed over the network these files may be.

NOTE: Data Protector Express figures the century dates using the following algorithm: if the year is 70 or smaller, the century is set to 20 (21st century); if the year is 71 or greater, the century is set to 19 (20th century). For example, if you set the date to 01-Jun-33, Data Protector Express calculates the date as June 1, 2033. If the date is set to 05-Apr-81, Data Protector Express calculates the date as April 5, 1981.

Backup Range

When a file is backed up, Data Protector Express stores the date the file was backed up in the Data Protector Express catalog. This is called the backup date. Each time you back up a file, Data Protector Express changes the backup date to the date of the backup. (You can view this information for all of the available versions in the **Versions of…** window in the **Backed up** field list.) You can use this information to filter files for verify jobs.

To select files that have specific backup dates, click on the **Browse** button next to the **Backup range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.



Range type: Between two dates

Starting date: 01/01/1970

Starting time: 12:00 AM

Ending date: 07/23/2005

Ending time: 06:37 PM

Modify Range

Each time a file is modified, its modified date is updated. You can use this filter to verify files with a modify date that matches your criteria. Data Protector Express checks the directory information on the volume to see if the file should be included in the verify job. For example, you can select only those files that were modified *after* a certain date and time or, alternatively, those that were modified *before* a certain date and time.

To select files that have specific modify dates, click on the **Browse** button next to the **Modify range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Create Range

When a file is first created, it is assigned a create date. You can use this filter to select only those files that match your criteria. Data Protector Express checks the created date for each file stored in the directory of the volume and uses this to select files for verifying.

To select files that have specific creation dates, click on the **Browse** button next to the **Create range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Access Range

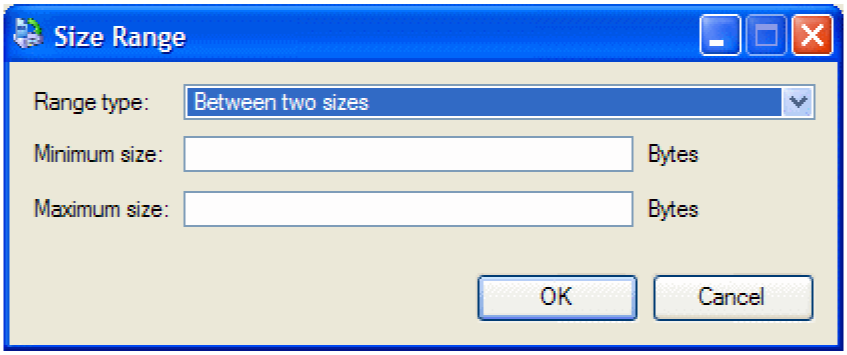
Each time a file is read, whether or not it is modified, its access date is updated. You can use this information to select files for verifying. For example, you might want to verify only those files which have been accessed (opened or read) in the past two months. Alternatively, you could verify only those files which have *not* been accessed in the past two months.

To select files that have specific access dates, click on the **Browse** button next to the **Access range** field. In the **Date Range** window that appears, select the appropriate range type and the starting and ending dates and times.

Size Range

This filter lets you select files for verifying according to their sizes. You might want to select only smaller files, larger files or files between two sizes.

To specify a filter that sorts files according to their sizes, click on the **Browse** button next to the **Size range** field and then select the appropriate criteria in the **Size Range** window that appears.



Range type: Between two sizes

Minimum size: Bytes

Maximum size: Bytes

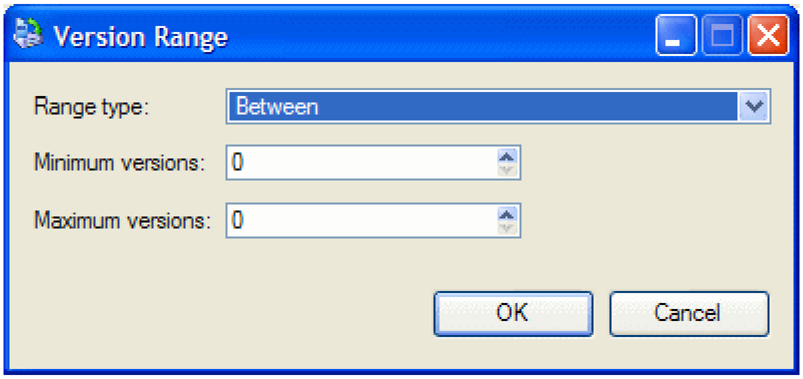
Version Range

Each time Data Protector Express backs up a file, it creates a new *version* of that file. For example, a file named **Expense Account Reporting Form** may have been backed up several times during the previous months and years. Typically, each version of the file is stored on the backup media of a different job. Data Protector Express tracks each version of a file separately in its catalog.

You can use this filter to instruct Data Protector Express to select files according to the number of versions that exist in the catalog. You might, for example, instruct Data Protector Express to verify all of the files for which there is only one version. When you set **Range type** to **At most** and **Maximum versions** to **1**, Data Protector Express only verifies those files with a single version.

Note, however, that having multiple versions of a file does not ensure that the versions you have reflect the latest changes to the file. It may have been modified after the last time you backed it up. So your latest version may not match the file’s current form.

To specify a filter that sorts files according to their number of versions, click on the **Browse** button next to the **Version range** field and then select the appropriate criteria in the **Versions Range** window that appears.



Range type: Between

Minimum versions: 0

Maximum versions: 0

Wildcard Type

Select which wildcard format you wish to use from the list box. You can use any of the following formats:

- **Default:** Uses the default wildcard format for your operating system.
- **DOS:** Uses the 11-character name format with the eight-character primary name and the three-character extension, e.g., filename.txt.
- **Macintosh:** Uses Macintosh native format.
- **NFS:** Network File System
- **FTAM:** File Transfer Access and Management
- **Long:** Uses the 256-character name format with a long primary name and an extension with multiple characters, e.g., Monday_backup.txt.

Must Match

Data Protector Express lets you use wildcard matches to include files. Only files that match the wildcard indicated in the **Must match** field are included in the verify set. For example, if you enter ***.exe**, Data Protector Express will only verify those files with the .exe file extension.

You can specify multiple wildcards by separating each with a semicolon (no spaces). For example, if you enter ***.exe;*.doc** in the **Must match** field, Data Protector Express selects all files that *either* have the .exe extension *or* the .doc extension.

Cannot Match

This wildcard field works just like the **Must match** field except that it *excludes* any files that match the wildcards. You can specify multiple wildcards by separating them with a semicolon (no spaces); if you specify multiple wildcards, Data Protector Express excludes any file that matches any one of the wildcards you specify.

Required Attributes

Operating systems track certain features of files called attributes that they use to manage these files. You can use these same attributes as a selection filter. In the **Required attributes field**, if an attribute is checked, Data Protector Express only selects those files which have these attributes. For example, if you check **Hidden**, Data Protector Express only selects those files which the operating system has assigned the **Hidden** attribute.

You can select multiple attributes. In this case, only files which have all of the specified attributes will be selected.

Note that some of these attributes are only supported by certain operating systems. If you specify an attribute that is specific to a particular operating system, then only files created under that operating system will be selected for verifying.

Exclude Attributes

This field works like the **Required attributes** field except that Data Protector Express *excludes* files that match these attributes. For example, if you have checked the **Execute Only** box, Data Protector Express will exclude from the verify job any files with the **Execute Only** attribute.

You can select multiple attributes. A file that has *any* one of these attributes will be excluded. For example, if you mark the **Hidden** and **System** attributes, any file that has *either* attribute will be excluded.

Allow Parents

When this option is checked, Data Protector Express verifies the directory information for any selected folder or volume. For example, if you have marked a folder, Data Protector Express will verify that folder only if this option is checked. When this option is not checked, directory information about folders and volumes is not verified.

Allow Children

When this option is checked, Data Protector Express verifies files. When this option is unchecked, Data Protector Express does not verify files. This is useful if you want to verify a complex directory structure, but not the files in that directory. To verify a directory structure, but not the files (children) stored in the directories, begin by marking the directory for verifying. Then clear the **Allow Children** option. Data Protector Express will verify only the directory structure on the volume you specify.

Media

Data Protector Express tracks versions of files and the media on which those versions are stored. You can use this information to sort files according to the media on which they appear. Only files with versions on the media in the **Media** field will be selected for the verify job. For example, if you select media named “Daily Set:1,” Data Protector Express will only include files in the verify job which have a valid version on the media named “Daily Set:1.”

To sort files according to the media on which they appear, click the **Add...** button and select the media from the **Browse** window. Note that you must select a Media object, not a Media folder or User/Group folder. If there are multiple media shown in the **Media** filter field, only files which have a valid version on *all* the media listed will be selected.

Chapter 6: Scheduling Jobs

Data Protector Express offers flexible job scheduling. Jobs can be scheduled to run only occasionally or as frequently as every minute. For ease of use and maximum data security, use one of the Data Protector Express default job schedules. You can also create a customized schedule to meet your business needs for data retention.

In this section

- Choosing a Schedule Type
- Customizing Schedules
- Managing Backups with or Without Media Rotation
- Backup Job Schedule Type Descriptions
- Scheduling Restore Jobs
- Scheduling Verify Jobs

Overview

This section covers scheduling concepts as they appear on the **Schedule** property page of a Data Protector Express job, which controls when and how often a job is run. To learn about media rotation concepts that appear on this property page, see *Planning for Media Rotation* on page 98.

Although schedule information is relevant to all job types, it is especially important for backup jobs. The **Schedule** property page allows you to set up a comprehensive backup schedule many years into the future, to run a job just once or to set up a job that you can run only occasionally.

The first part of this section reviews schedule types for backup jobs, while the second part explains how to create and modify backup job schedules. The final part of this section reviews these concepts for restore and verify jobs.

Choosing a Schedule Type

Data Protector Express lets you set up jobs that run automatically on regular schedules—at a certain minute in the hour every hour, daily, weekly, monthly, and yearly. You can also set up a job that you run manually once, immediately, or at a specified time. Or you can create a job that contains no schedule at all.

To determine which type of backup job you should create, ask yourself these questions:

- *Do I need to run the job at a specific time on a regular basis or only once in awhile?*

  Backup jobs are either *not scheduled* or *scheduled*. Some jobs may run once or only occasionally. These jobs are usually not scheduled because they only run when you instruct them to do so.

  Data Protector Express includes three default schedule types for jobs that run infrequently: **Not scheduled**, **Run on specific day**, and **Run now**. These jobs are designed to be run either periodically when you select them from Data Protector Express, or only once after you complete setting up the job. They are not designed to be run automatically even if Data Protector Express is running as a service.

- *If the job is scheduled, how frequently do I want to run it?*

  If you want a backup job to run automatically at a time or day that you specify, you should select one of the default schedules that Data Protector Express provides. You can create a job that runs as infrequently as only a few selected days or as often as every hour. Scheduled backup jobs are generally designed for disaster recovery protection and are therefore run at regular intervals, normally daily. For a job to run automatically, either Data Protector Express or the Data Protector Express service must be running.

  There are several default schedule types that are designed to be run automatically on a schedule: **Run on selected days (of the week),** or **Run repeatedly**.

- *If the job is scheduled, do I want to run it on a complex schedule?*

  If you want a backup job to run automatically on a complex schedule, or if you need to create a specialized backup schedule, use one of these schedules: **Run on selected days** or **Run repeatedly.** These schedules let you choose the specific days on which the job should run.

- *What is the purpose of this job—to protect from disasters or to maintain a historical record?*

  Data Protector Express runs jobs in one of four backup modes: full, incremental, differential, or copy. Jobs that are set to **Run repeatedly** use the backup type shown in their schedule. Other jobs use the backup type defined on the **Options** tab which is set to "full" by default. You can change the backup mode for a job on the Options property page or by changing the interval settings in a **Run repeatedly** job. Full backups provide the best backup for data recovery purposes because they include necessary system information. Backup jobs that are not run specifically for data recovery purposes can use any of the other backup modes and can be used for general data restoration purposes. To set up a flexible backup schedule that includes jobs run in more than just full backup mode, choose **Run repeatedly** so that you can set the backup mode for any job in the schedule.

TIP: To change the default backup mode for a job that does not include media rotation, open the **Options** property page and change the **Backup Mode** setting.

TIP: For the most flexible complex backup schedule, choose **Run repeatedly**.

How or whether or not you schedule a job and the type of schedule you select depends on several factors. Before proceeding, consider the following questions:

- What degree of risk to your data is reasonably allowable?
- Will the amount of traffic on your network require that backup jobs be scheduled to run during non-peak periods? Are there certain days of the week when running lengthy jobs will interfere with other uses of your network? Do I need to schedule jobs to run several times a day?

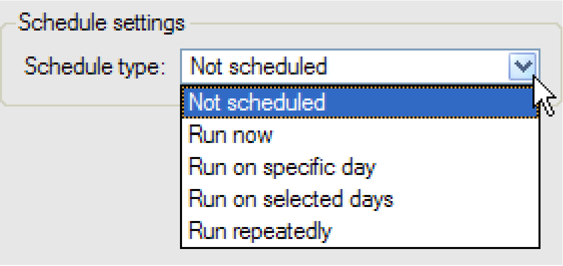
- Are there times when your tape drive will be unavailable?
- Will someone monitor the job as it runs?
- How large will a full backup job be?
- How much data can the backup media hold? How many media does my budget allow me? Or, alternatively, how many tapes does my library hold?

As you review the following sections, keep these questions in mind to help you determine which backup job schedule to select for any particular job.

Non-scheduled backup jobs

Some jobs may run once or only occasionally. Historical files provide a record of the data stored on the computer or network at particular times such as the end of the week or the end of the month. For jobs that do not need to run automatically on a regular schedule, Data Protector Express provides four options: **Not scheduled**, **Run now**, **Run on specific day**, and **Run on selected days**. By default, backup jobs are not scheduled. You must start these jobs manually each time you want to run them. To use a different schedule type, you must select it from the **Schedule Type** list on the **Schedule** property page for the job. A backup job that uses the **Run now** schedule type, will begin as soon as you finish setting it up.

NOTE: No jobs will start until the database server has been running for a minimum of five minutes. This allows the user a chance to shut down jobs that should not run immediately after the server is restarted.



Schedule settings

Schedule type: Not scheduled

NOTE: If you plan to set up media rotation, choose **Run repeatedly**. If you intend to manage your media manually, select any type other than **Run repeatedly**.

TIP: Backup jobs designed to protect data from disaster should always be scheduled. This is the most effective way of insuring that your data will be safely stored on media with regular backups. Media rotation also helps protect your data by insuring that media is not over-used.

Scheduled backup jobs

Backup jobs designed for disaster protection are run routinely, usually daily. Data Protector Express contains the Run repeatedly schedule type that is designed to provide different levels of data availability for recovery in the event of data loss or a hard disk failure. This schedule type allows backup jobs to be run at different intervals: **Minute**, **Hour**, **Day**, **Week**, **Month**, or **Year**.

For more information on how these scheduling options affect media rotation see *Chapter 7 – Planning for Media Rotation*.

Customizing Schedules

CAUTION: It is strongly recommended that you use the default schedules for disaster recovery. These schedules are specially designed to secure your data against catastrophic loss over time. If you need a custom schedule, try reviewing a default schedule—and using it as a model—rather than creating an entirely new schedule.

To create a customized schedule, use the **Run Repeatedly** schedule with rotation type set to **Custom** rotation. For information on modifying the custom interval schedule, see *Modifying the Run at custom interval Schedule* below.

Modifying a custom schedule

1. Select the **Schedule** property page of a job.
2. Select **Run repeatedly** as the **Schedule type**.
3. Select the start time and date of the job. This indicates when the schedule, as a whole, should start. The first scheduled event will start at this time.
4. Select **Custom rotation** as the **Rotation type**.
5. Select the **Type of fixed rotation**. Suggestion: use the **Fixed by day of week** default. For more information on this option see Chapter 7.
6. Click **Minute**. If you want to schedule jobs on certain minutes select **Enable scheduling by minute**. Set the number of minutes apart you want this schedule to run. Then select the **Type of backup** to use at this interval. (Suggestion: use scheduling by minute very sparingly. Many devices may take several minutes to properly mount their media. This may cause unintended behavior.) Select the number of rotation sets. Skip the next set to use. (This field stores the number that will be used in naming the tape rotation the next time the job is run.)
7. Repeat step six for each of the intervals: **Hour**, **Day**, **Week**, **Month**, and **Year**.
8. Edit the job settings for any other calendar days by doing one of the following:
   - Right-click the calendar and select the appropriate backup type from the shortcut menu
   - Navigate to the day in the calendar and select the backup type by typing its shortcut key
9. Apply the changes to the job.

NOTE: A schedule interval overrides any previous schedule interval. For example, suppose you want to create a job that runs every hour as a differential backup, and then run a full backup at the end of every day. First, set the job to start at midnight of the coming evening. Make sure that each of the intervals other than **Hour** and **Day** is disabled. On the **Hour** interval, enable the interval, give it a value of 1, set the **Backup type** to **differential**, and the **Number of rotation sets** to twenty-three. Then select the **Day** interval and set the **Backup type** to **full** and the **Number of rotation sets** to seven. Your first rotation will be the **Day** rotation since **Day** takes precedence over all previous intervals (**Minute** and **Hour**).

CAUTION: Jobs set up with this schedule type run automatically. If you do not set up media rotation with this schedule, Data Protector Express may overwrite any media in the backup devices. Setting up a media rotation ensures that Data Protector Express will prompt you for the correct media based on the rotation type.

Scheduling Restore Jobs

Restore jobs can be run with any of the schedules provided in Data Protector Express. If you only need your job to run when you start it manually from Data Protector Express, select **Not scheduled**. To run a restore job only once, use the **Run on specific day** or **Run now** schedule. For restore jobs that should run at regular schedules, use any of the other schedules.

Scheduling Verify Jobs

Verify jobs can be run with any of the schedules provided in Data Protector Express. If you only need your job to run when you start it manually from Data Protector Express, select **Not scheduled**. To run a verify job only once, use the **Run on specific day** or **Run now** schedule. For verify jobs that should run at regular schedules, use any of the other schedules.

Backup Job Schedule Type Descriptions

Not scheduled: Run a job manually any time you start it from Data Protector Express.

Run now: Run the job as soon as soon as you finish setting it up.

Run on specific day: Run the job only at the scheduled time so long as Data Protector Express or the Data Protector Express service is running.

Run on selected days: Run the job automatically only on those days that you select on the calendar at the specified time, with no rotation.

Run repeatedly: Run the job automatically at a custom schedule based on your selections. Media rotation is optional.

NOTE: Jobs run automatically so long as the Data Protector Express service is running or if Data Protector Express is open.

Tips for Working with Scheduled Jobs

This section provides useful tips for running scheduled jobs.

Running a failed rotation job again

Manually set the correct options and “force” the job to run again.

Suppose a scheduled job has failed to run correctly. In order to ensure the integrity of the data, the job must be run again.

Consider this example. Suppose it is discovered on Monday morning that a full backup job has failed to run as scheduled on Friday evening. If a full backup job is not run before the next incremental job, the ability to fully reconstruct data will be compromised. It is vital that the full backup job be run soon.

However, you cannot merely “force” the job to run again. Recall that when Data Protector Express runs a scheduled job, it automatically updates four settings on the **Options** and **Device/Media** property pages of the job: Backup mode, Write mode, New media location, New media name and Media.

Note that Data Protector Express does NOT automatically update these fields when you manually “force” a scheduled job to run. For example, when Data Protector Express automatically runs a scheduled backup job on a Monday, it changes (updates) the **Backup Mode** from **Full** to **Incremental**. But when this job is “forced” to run before its scheduled time, Data Protector Express does not automatically update these fields.

Before forcing a failed job to run again, open the job log of the failed job, noting the appropriate options. If needed, print the job log. Next, open the **Options** and **Device/Media** property pages of the failed job. Set the settings on the options page to match those of the failed job. In particular, check the **Backup mode**, **Write mode**, **New media location**, **New media name** and **Media**.

You will also want to select the appropriate media in the **Media** field on the **Device/Media** page. Use the **Browse** button to select the same media as the failed job was to use. When the options of the job match the options the failed job would have used, run the job.

If you have changed the **Media** field, be certain that this field is set back to its original specification so that scheduled jobs will automatically select the proper media.

An alternative method would be to copy the failed job, change the schedule type to **Not Scheduled** and then set the options settings to match the failed job. Manually “force” the job to run and delete it after it has successfully completed.

Scheduling a job to run once only

Turn off all the dates on the **Manual** schedule except the desired date.

When you want to run a job only once, you should set the **Schedule Type** field on the **Schedule page** to **Not scheduled**. Then you can run the job from the **Backup**, **Restore, Verify or Media** job views at any time. If you need to run the job once during off-peak hours, you can set the **Schedule Type** field to **Run on specific day**.

But what if you only need to run a job once during off-peak hours?

Create a new backup job that runs only once

1. From the Backup job view, create a new job.
2. When the **General** page appears, give it a name, such as **One-Time Backup**.
3. Open the **Selection** page and select the objects (directories, files, etc.) to back up. Consider selecting the **Network** or computer name check boxes to back up all data on the computer or on the network.
4. Select **Run on specific day** in the **Schedule Type** field on the **Schedule** page.
5. Set the **Start time** and **Start Date** for the job.
6. Click **OK** to close the backup job properties window. The job will run once on the selected day at the selected start time.

Scheduling simple backup jobs

Many computer users do not need the power of one of Data Protector Express’s default schedules. They can manage their backups best with a simplified backup plan, such as the simple daily backup or the simple five-day rotation described below.

Simple daily backup

Create a **Run repeatedly** at a daily interval schedule to run a full backup every day of the week at the same time.

If a library is not installed, you can create the following simple daily backup plan. It does not require different media for different days, though you can rotate your media if desired. It also does not require a lot of your attention. You can set it up quickly and let it run.

Create a new backup job that runs daily

1. When the **General page** appears, give it a name such as **Daily Backup**.
2. Click the **Selection page** and select the objects (directories, files, and so on) to back up. Many people select either the **Network** or computer name check boxes to back up all data on the computer.
3. Click the **Options page**. The **Backup mode** should be set to **Full** by default.

NOTE: Always select **Full** from the **Backup mode** list for this job. Otherwise, the backup job will not copy all of your data.

4. Select **Overwrite all media** from the **Write mode** drop-down list.
5. If your backup device does not support compression, select **None** from the **Hardware compression** drop-down list.
6. If your backup device supports automatic eject, you can configure the job to eject the media after the job finishes. Click **Advanced Options**. When the **Advanced Options** dialog box appears, select **Auto eject** and click **OK**.
7. Open the **Schedule page**.
8. Select **Run repeatedly** from the **Schedule Type** field.
9. Set the **Start time** and **Start Date** for the job.
10. Select no rotation plan from the **Rotation Type** field.
11. Adjust the days on which the jobs will run from the calendar. (The default is Monday through Friday).
12. Click **OK** to close the backup job properties window. The job will run at the selected time on each selected day.

Simple five-day rotation

Create separate media folders and backup jobs for each day of the week.

If a library with five or more slots is installed, you can create the following simple five-day rotation plan. It requires separate media for each day of the week, one in each library slot. You can set it up quickly and let it run. You can also use different tape magazines to create separate sets of backups for different weeks. For example, set A for the first week of the month, set B for the second week and so on.

Create separate media folders for each day of the week

1. Start in the **Home** folder for the user that will administer this job.
2. Select the **Admin** folder
3. Create media folders:
   a. Right-click the blank space in the Details area (in the right window pane).
   b. Select **New…** and **Media Folder**.
   c. Name the new media folder Monday.
4. Repeat step 3 for new folders Tuesday, Wednesday, Thursday and Friday.

5. Create new backup jobs for each day of the week:
   a. Right-click in the blank space in the Details area (in the right window pane).
   b. Select **New…** and **Backup Job**.
   c. When the **General** properties page appears, name the job Monday.
   d. Click the **Selection** page and select the objects (directories, files, and so on) to back up. Many people select either the Network or computer name check boxes to back up all data on the computer.
   e. Click the **Options** page. The **Backup mode** should be set to Full by default.

   NOTE: Always select **Full** from the **Backup mode** list for this job. Otherwise, the backup job will not copy all of your data.

   f. Select **Overwrite all media** from the **Write mode** drop-down list.
   g. If your backup device does not support compression, select Standard from the **Compression** type drop-down list.
   h. Select the existing **Home\Admin** folder in the Media pane.
   i. Click the **Delete** button under the Media pane and click **OK**.
   j. Click **Add**.
   k. Click the **Browse** button next to **New media location**.
   l. Browse to Home\Admin Folder\Monday and click OK.
   m. Click the **Schedule** page.
   n. Select **Run on specific day**.
   o. Set the start time and date.
   p. Click **OK** to close the backup job properties window. The job will run at the selected time on the selected days.
6. Repeat step 5 for Tuesday, Wednesday, Thursday and Friday.

Related topics

For more tips on setting up backup jobs, see *Tips, Techniques and Strategies* on page 153. For more information on media rotation, see *Planning for Media Rotation* on page 98.

Chapter 7: Planning for Media Rotation

Data Protector Express offers flexible media rotation features. The primary purpose for media rotation is to maximize your data security and to provide an easy means to recover your data in the event of data loss. Media rotation also protects you from data loss due to overuse of the backup media. For ease of use and maximum security, you can use the default media schedules with the default media rotations found in Data Protector Express. Or, alternatively, you can exclude media scheduling, and its associated rotations, from your backup jobs and manage your media manually.

In this section

- Media Rotation Concepts
- Media Sets
- Which Rotation Type to Select
- Adding Media Rotation to a Backup Job
- Modifying Rotation Types
- Managing Backups with or Without Media Rotation

Media Rotation Concepts

Backup jobs performed for disaster protection are often run daily. Ensuring that you have all the files you need to restore your system often involves creating and maintaining one or more sets of media (such as tape cartridges) for use during a recovery. Rather than use new media each time a backup job is run, Data Protector Express recycles or reuses media. This is efficient because it keeps costs down by limiting the amount of media needed and still provides for data security, should any media fail or be otherwise unavailable.

The process of recycling or reusing media is referred to as **media rotation**. Data Protector Express rotates media by creating media sets named to correspond to a job's scheduled backup intervals, and reuses media using a fixed number of sets. The media set names can be based either on the scheduled interval or on the type of fixed rotation.

When two intervals in a schedule are scheduled to run at the same time, they have the following precedence: **Year**, **Month**, **Week**, **Day**, **Hour**, **Minute**. For example, if a job was scheduled to run every hour using the **Hour** interval, and once every day using the **Day** interval—then once each day the daily backup would take precedence over the hourly backup.

A Sample Media Rotation

Many users use what is called the “Grandfather, father, son” media rotation concept. In our example schedules these are marked by using the acronym “GFS.” In a GFS rotation you use progressively larger intervals with fuller backups. The GFS-20 schedule uses a total of 20 sets. Six sets are used for the **Day** backup interval. Six sets are used for the **Week** backup interval. Six sets are used for the **Month** backup interval. Two sets are used for the **Year** interval.

Using this GFS-20 schedule, the first media set used would be “*Yearly Set 1*” since all the time intervals would try to run as soon as they were scheduled to, and the **Year** interval would have precedence over all of the other intervals.

NOTE: You can also create a job in Data Protector Express that does not contain any media rotation. If you do so, Data Protector Express will not prompt you to insert specific media in a backup device; instead you are responsible for reusing media based on your own media rotation plan. To avoid over-using your media, and for maximum data availability when rotating media manually, be sure you always use the oldest backup media each time you run the backup job.

Media Sets

Data Protector Express organizes rotated media into groups and sets based on the rotation type and schedule interval. You can use these sets of media to recover data in the event of a disaster or other data loss. Data Protector Express tracks which versions of files are stored on any set of media to ensure successful data recovery.

Each time you run a backup job, Data Protector Express copies data onto backup media. Data Protector Express organizes the media used to complete a single backup job into distinct media sets. Whether the job requires several media or only one media to complete, they are identified in the Data Protector Express catalog as a set. If you need to restore a specific version of a file, Data Protector Express will locate the data based on its media set.

When planning scheduled backup jobs, it is important to know whether one media or several will be required to complete a backup job. This can usually be estimated by comparing the size of the backup selection to the capacity of the selected media. If you do not want Data Protector Express to use more than one media for a backup job, then you must select fewer files (or “objects”) to back up.

For fixed rotation types, Data Protector Express will select media sets based on the day of the week, week of the month, day of the month or day of the year. Data Protector Express assigns names to media sets in a fixed rotation using the schedule below.

Fixed Rotation Type Descriptions

Not fixed. Media sets are named for the interval that has been run. They follow the form *[Interval] Set [number]*. For example, the first time an hourly backup job runs, the name of the media set will be “*Hourly Set 1*.” Other examples are “*Daily Set 1*,” “*Weekly Set 1*,” “*Monthly Set 1*,” and “*Yearly Set 1*.”

Fixed by day of week. An example of an hourly media set is “*9:00 PM Hour*.” An example of a daily media set is “*1st Monday*.” An example of a weekly media set is “*1st Week of the Month*.” An example of a monthly media set is “*1st Month*.” An example of a yearly media set is “*Yearly 1*.”

Fixed by week of month. An example of an hourly media set is “*9:00 PM Hour*.” An example of a daily media set is “*Monday 1st Week*.” An example of a weekly media set is “*1st Week of the Month*.” An example of a monthly media set is “*1st Month*.” An example of a yearly media set is “*Yearly 1*.”

Fixed by day of month. An example of an hourly media set is “*9:00 PM Hour*.” An example of a daily media set is “*1st Day of the Month*.” An example of a weekly media set is “*1st Week of the Month*.” An example of a monthly media set is “*1st Month*.” An example of a yearly media set is “*Yearly 1*.”

Fixed by day of year. An example of an hourly media set is “*9:00 PM Hour*.” An example of a daily media set is “*Day 1 of the Year*.” An example of a weekly media set is “*1st Week of the Month*.” An example of a monthly media set is “*1st Month*.” An example of a yearly media set is “*Yearly 1*.”

Each of these media rotations either relies on a predefined set count as described or makes use of the set count in the interval. To change the interval’s set count select the interval and enter the number of sets you want to keep in the **Number of rotation sets** field. When a rotation runs out of sets it starts again at set one and *overwrites* the media for set one.

Since a set may span multiple media you should not assume that a set is equal to a single piece of media. Generally you should multiply the number of media sets by the number of pieces of media that a single backup job uses in order to know how many pieces of media you should have. For example, if your backup normally takes three pieces of media—and you want two sets of this media—you should have six pieces of media.

NOTE: When a rotation is written to media and needs to know the set number it should use for the media’s name it pulls this information from the **Next set to use** field in the interval. If a backup failed to run correctly or if for some reason the set numbers are now out of synch you can use this value to change the name used the next time that interval is run.

Which Rotation Type to Select

Besides the **No media rotation** option, Data Protector Express provides several default media rotation types. The rotation types vary in several ways: the number of days for which full data recovery is available, access to historical files based on backup type (full, differential, incremental, etc.), the minimum number of tapes or other media needed, and how long media is retained.

Full data recovery period

All the media rotation types provide for full data recovery in case of disaster. The full data recovery period is the number of days prior to the data loss for which every file backed up can be recovered. You will also be able to reconstruct the data for any day during that period that you ran a full backup and for which a set is available that has not been reused.

Each media rotation type provides full data recovery periods for different number of days preceding the last backup. For example, a **GFS 30-tape** media rotation type can reconstruct the data from any day of the past three weeks (except weekends), while a **Simple 4-tape** media rotation type provides for reconstruction of only the past two days. See *Comparing rotation types* for more information.

TIP: To facilitate disaster recovery operations, Data Protector Express provides an optional disaster recovery agent.

Access to historical files

Rotation types vary according to how much access to historical files they provide. Historical files provide a record of the data stored on the computer or network at particular times such as the end of the week or the end of the month.

Because the backup contains only those files present on the system at the time the backup is run, data that was deleted since the last available historical backup will not be accounted for in the backup. For example, suppose you maintain four sets of monthly backups to serve as historical records of your data. You would schedule these backups to be performed on the last day of each month. Files that were created and deleted within a month will not appear in any of the historical backups.

Different rotation types give you different levels of historical access to previous weeks, months and years. For example, a **GFS 30-tape media** rotation type has eight weekly tapes, seven monthly tapes and two yearly tapes. This provides you with historical files of *at least* the end of the week for the past eight weeks, the end of the month for the past seven months and the end of the year for the past two years. On the other hand, a **Simple 4-tape** media rotation type provides end-of-week and end-of-month backups in full mode of only the last week and month.

Consider, for example, the yearly backup. Each of the three GFS default rotation types contains two yearly backups. The first time you run one of these rotation types, you create a yearly backup. The next yearly backup is made at the end of the current calendar year. The following year, the first media is recycled, that is, its data is overwritten with new data and information about the files backed up in the first year is deleted from the Data Protector Express catalog. This process continues with the second media being recycled the following year and so on.

NOTE: Yearly backups only provide you with access to files present on your computer or network on that one day each year. No copy exists for files that were created after the oldest yearly backup and then deleted before the most recent yearly backup.

It is the responsibility of the user to manage the retention of media containing critical business data.

Minimum number of tapes or media

The name of many rotation types indicates the minimum number of tape or media sets used by the backup job. For example, the Simple 4-tape rotation type will use at least four media sets (or individual tapes) to complete the media rotation.

Note that each media set may contain more than one tape or media. Several factors determine how much media you will need: the type of backup being performed (e.g., full, differential, incremental), the amount of data to be backed up during a full backup, and the media's storage capacity. If the total size of a full backup is larger than the capacity of the tape, additional tapes are required. Your historical usage is the best guide to determining how many tapes these jobs will require.

Because incremental and differential backup jobs usually back up fewer selected files than full backup jobs, additional tapes may not be required.

Deciding how frequently to overwrite media

Data Protector Express overwrites media in two ways: by overwriting the oldest media in a rotation type, and by overwriting media on a fixed schedule based on the day of the week, month, or year. How long you retain media depends on your business needs. If you need to retain media for longer than a few days or weeks, consider using one of the fixed media rotation types. If you have a limited supply of backup media and do not need to retain media for a long time, consider the other rotation types.

Comparing rotation types

NOTE: This table assumes that no job uses more than one media set or group and presents the default rotation type settings for the **Run Repeatedly** schedule type.

The following table compares the historical backups and full data recovery capabilities of each of the rotation types provided in Data Protector Express.

Media Rotation type	Full Data Recovery Available for Previous…	Historical backups Available for Previous…
GFS 62 set (every hour)	three 5-day weeks or two 7-day weeks (15 business days)	eight end-of-week sets eight end-of-month sets two end-of-year sets 24 hourly sets 18 every-fifteen-minute sets
GFS 54 set (every hour)	three 5-day weeks or two 7-day weeks (15 business days)	eight end-of-week sets eight end-of-month sets two end-of-year sets 24 hourly sets
GFS 30 set	three 5-day weeks or two 7-day weeks (15 business days)	eight end-of-week sets eight end-of-month sets two end-of-year sets
GFS 25 set	two 5-day weeks (10 business days)	eight end-of-week sets seven end-of-month sets two end-of-year sets
GFS 20 set	one 7-day week (7 business days)	six end-of-week sets six end-of-month sets two end-of-year sets
Fixed by Day of Week	one 7-day week (seven business days)	five end-of-week sets two end-of-month sets one end-of-year sets
Fixed by Day of Month	one 31-day month (31 business days)	five end-of-week sets three end-of-month sets two end-of-year sets
Fixed by Day of Year	one 366-day year (366 business days)	two end-of-week sets 12 end-of-month sets five end-of-year sets
Simple 12 set	five days	four end-of-week sets four end-of-month sets
Simple 11 set	five days	four end-of-week sets three end-of-month sets
Simple 10 set	five days	four end-of-week sets two end-of-month sets
Simple 6 set	five days	one end-of-week set, two end-of-month sets
Simple 4 set	two days	two end-of-week sets

Adding Media Rotation to a Backup Job

Before you can include media rotation in a backup job, you must select a backup schedule that permits media rotation, provide basic information such as the job start date and time, and then select a rotation type.

WARNING: If you choose a schedule type that does not support media rotation, it is your responsibility to have the correct media inserted in your backup device before you run the job. Schedule types that do not provide media rotation are **Not scheduled**, **Run on specific day**, **Run now**, or **Run on selected days**.

To add media rotation to a scheduled job

1. On the **Schedule** property page of a backup job, select a schedule type that supports media rotation in the **Schedule Type** list. The **Run repeatedly** schedule type support media rotation.
2. Specify a time and date for the job in the **Start time** and **Start Date** boxes. Data Protector Express will run the job at this time.
3. Select a media rotation type in the **Rotation** list. Data Protector Express displays default media set information under **Interval Settings**.

NOTE: You can change the number of media sets that Data Protector Express uses to rotate media for any type of backup in the job (e.g., daily, weekly, monthly, etc.) if you have set the **Rotation type** to Custom rotation.

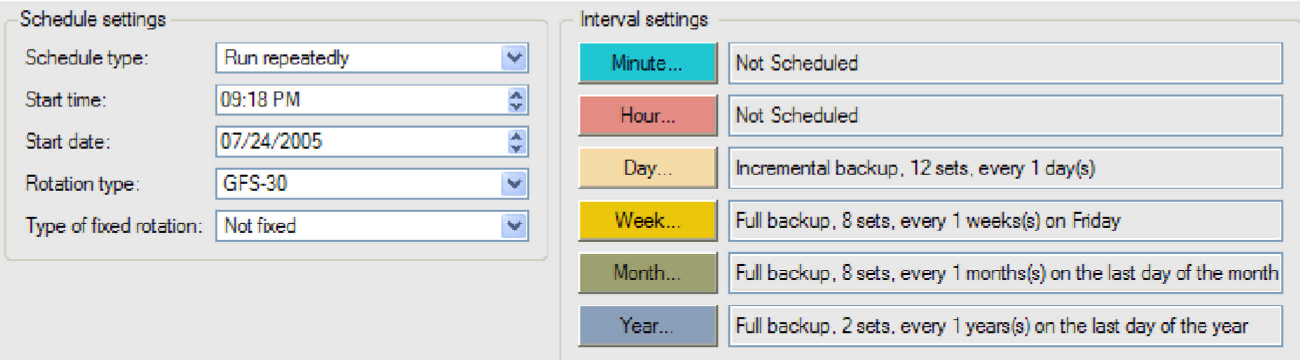
4. If available, modify the **Interval** settings.
5. In the calendar, change the type of backup performed by right-clicking the calendar and selecting the appropriate backup type from the shortcut menu
6. Apply the changes to the job.

NOTE: You can create a backup job to run as frequently as every minute or as rarely as once a year. To best protect your data, select every day of the week in which new and important data is generated (i.e., every business day).

Modifying Rotation Types

Rotation types can be set up to create media sets and groups for **Day, Week, Month,** and **Year** backups. This is helpful when the default settings do not fit your business needs or when a job fails to run because of a network problem or malfunction.

You select the rotation type as part of the settings for a schedule that is run repeatedly.



Schedule settings

Schedule type: Run repeatedly

Start time: 09:18 PM

Start date: 07/24/2005

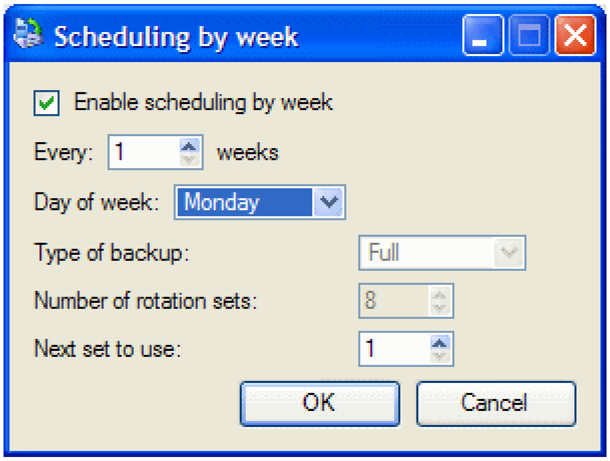
Rotation type: GFS-30

Type of fixed rotation: Not fixed

Interval settings

Minute...	Not Scheduled
Hour...	Not Scheduled
Day...	Incremental backup, 12 sets, every 1 day(s)
Week...	Full backup, 8 sets, every 1 weeks(s) on Friday
Month...	Full backup, 8 sets, every 1 months(s) on the last day of the month
Year...	Full backup, 2 sets, every 1 years(s) on the last day of the year

You can modify the **Interval Settings** based on the rotation type. For example, for some reason a **Weekly** backup job has failed to run when scheduled. It is important that this job be run as soon as possible to retain your full data recovery plan. In the following example, the **Weekly** backup job that was scheduled to run on Saturday is rescheduled to run on Monday by changing Monday from a **Daily** backup to a **Weekly** backup.



Scheduling by week

☑ Enable scheduling by week

Every: 1 weeks

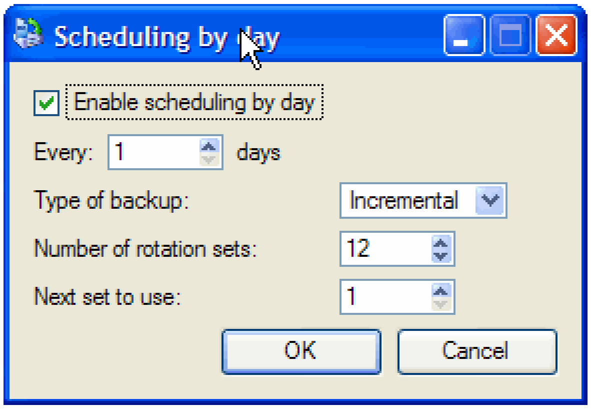
Day of week: Monday

Type of backup: Full

Number of rotation sets: 8

Next set to use: 1

In another example, you have specifed a Custom Rotation, and you decide to change the backup mode setting for all **Daily** backups from **Full** to **Incremental**



Scheduling by day

☑ Enable scheduling by day

Every: 1 days

Type of backup: Incremental

Number of rotation sets: 12

Next set to use: 1

Changing the tape set count

You can change either the length of the full data recovery period or the level of access to historical copies for media rotation plans. By modifying the tape set count, you can lengthen or shorten the period in which full data recovery is available or the period of time for which historical files are available.

For example, you may wish to increase the number of yearly historical tapes available from two to three or more. To do so, change the number in the **Sets** box for **Yearly** set types on the **Schedule** property page to the desired number of historical backups.

Alternatively, you may wish to expand the full data recovery period, while limiting the number of historical backups. As you change the number of media groups you want to maintain, Data Protector Express updates the number of sets required for the backup job.

To view when a group will be used during the life of the backup job, select **Sample**.

Managing Backups with or Without Media Rotation

If you create a backup job that does not include media rotation, you must manage your backup media sets manually. That is, you are responsible for ensuring that the expected media is in a backup device before a job runs. Data Protector Express will not prompt you to insert the correct media in a backup device because there is no media rotation plan to follow.

The schedule types **Run now**, **Run on specific day**, **Run on selected days**, and **Not scheduled** all require you to manage your own backup media sets. To make data recovery easier, Data Protector Express sets the backup mode to **Full** for any job created with these schedules. Running a job in **Full** backup mode ensures that you can use the media set to recover data easily. To change the backup mode for these jobs, edit the **Backup Mode** setting on the **Options** property page.

For all other schedules, you must choose whether or not to include media rotation. You can also alter the backup mode if the default settings do not suit your data recovery needs. By default, Data Protector Express sets the **Rotation Type** to **No rotation**.

Follow the guidelines below to determine how best to manage your media and how to set the backup mode.

Determining the length of the full data recovery period

Full reconstruction of data can be accomplished in two ways. The first method requires the most recent full backup media and all of the incremental backup media since the last full backup tape. The second method requires the most recent full backup media and the differential job from the previous day.

For example, to reconstruct the data for a Wednesday from a Simple-6 set rotation type, you will require one of two media sets: *either,* the full backup media (or media set) from the previous end of week and all of the incremental media sets from that week (that is, Monday's, Tuesday's and Wednesday's); *or*, the full backup media set from the previous end of week and the differential media set from Wednesday. (In some circumstances, the preceding full backup media set will be a monthly or yearly job and not a weekly job.) As long as none of these media sets has been overwritten, full data recovery is possible.

The length of the data recovery period is determined by the number of daily incremental or differential media sets, the number and frequency of full backup jobs (usually weekly jobs), and the media rotation you selected for the job.

Incremental jobs and full data recovery

Incremental jobs are the shortest and smallest jobs to run, but they present some issues related to full data recovery. The difference between an incremental and a differential backup is important -- incremental backup jobs back up only files that have changed since the last full, differential or incremental backup, while differential backup jobs back up all files changed since the last *full* backup. If incremental backup media sets are overwritten or recycled before another full backup is performed, this can create a gap in available data if you need to recover files from the overwritten media.

Exclusive use of incremental backup jobs to ensure full data recovery after a disaster is not recommended, *unless you are using a schedule that retains one full backup and all subsequent incremental backups* before overwriting any media. However, to ensure successful data recovery with incremental jobs, follow these guidelines:

- Have at least as many incremental media as there are days between full or differential backup jobs. For example, if you run full backup jobs every five days, have at least four incremental media; if you run full backup jobs every seven days, have at least six incremental media.
- Never recycle incremental media between differential or full backup jobs. If you run more than one incremental job in a row, be certain to not recycle any of the media used during this string of incremental jobs.

Related topics

For more information about planning backups, see *Tips, Techniques and Strategies* on page 153. For a description of the default backup schedules, see *Scheduling Jobs* on page 90.

Chapter 8: Job Options

Data Protector Express uses settings on a job's **Options** page to control various features necessary for running a job. Data Protector Express's default values are designed to be easy and secure to use, but you can modify the job option settings to meet your particular needs.

In this section

- Backup Job Options
- Advanced options for backup jobs
- Restore Job Options
- Advanced Options for Restore Jobs
- Verify Job Options
- Media Job Options

Overview

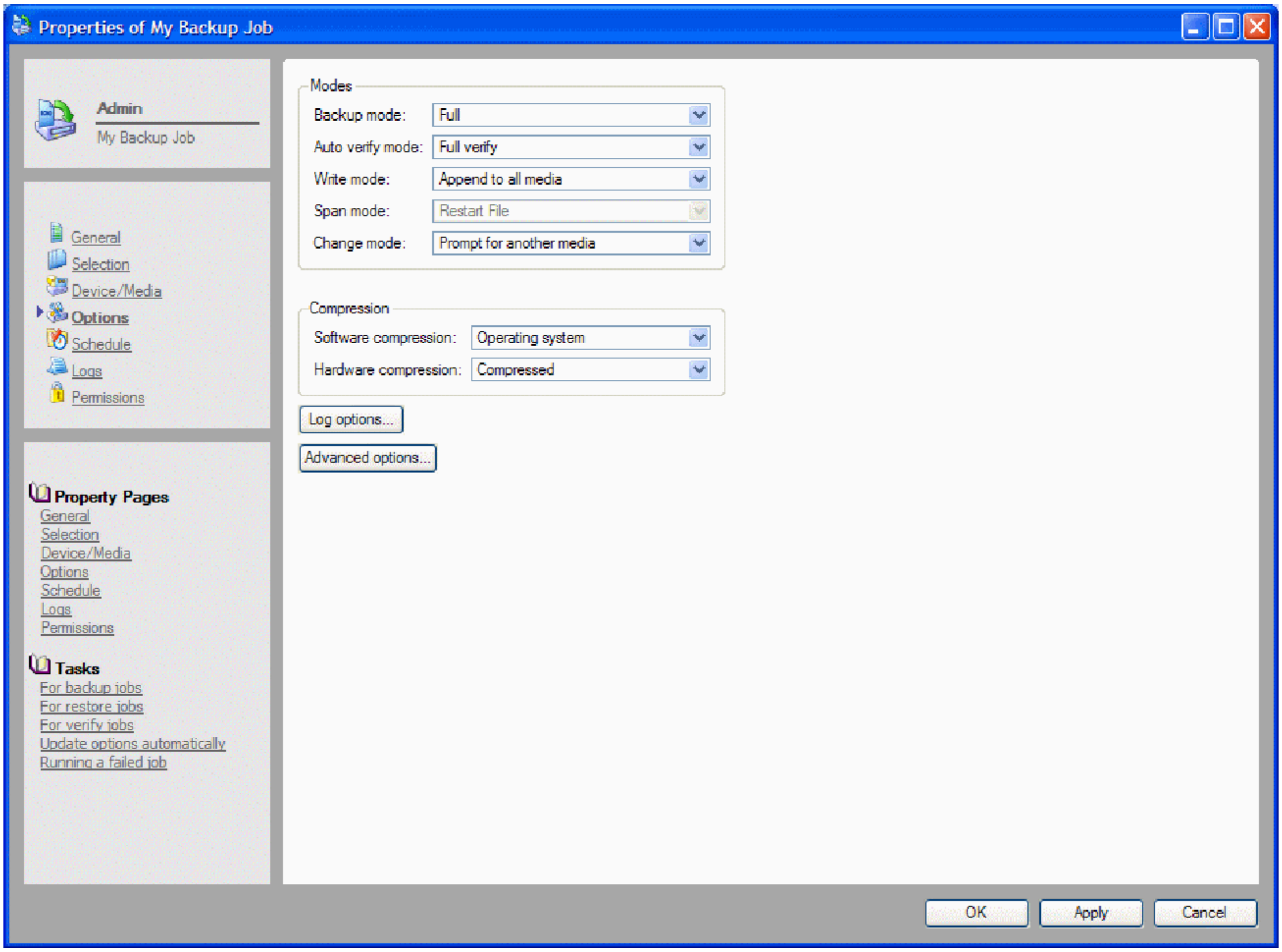
This section covers the **Options** page. This property page controls various features of the job, such as how files are written to backup media, whether files can be overwritten and how alerts are handled.

Although this page is relevant to all job types, the **Options** page is especially important for backup jobs. Some types of backup schedules, such as automatic rotation jobs, treat certain job option settings differently than do others, such as manual rotation jobs.

The first part of this section focuses on backup job options, while the second part explains the advanced options settings used by backup and verify jobs. Finally, options for media jobs are described.

Backup Job Options

The **Options** page on the property page of each backup job controls various settings important to how Data Protector Express runs a backup job. Although there are numerous choices, the default values have been chosen to provide the maximum degree of security and ease of use. Use the default values unless your particular backup needs require different settings.



Properties of My Backup Job

Admin
My Backup Job

Modes

Backup mode: Full
Auto verify mode: Full verify
Write mode: Append to all media
Span mode: Restart File
Change mode: Prompt for another media

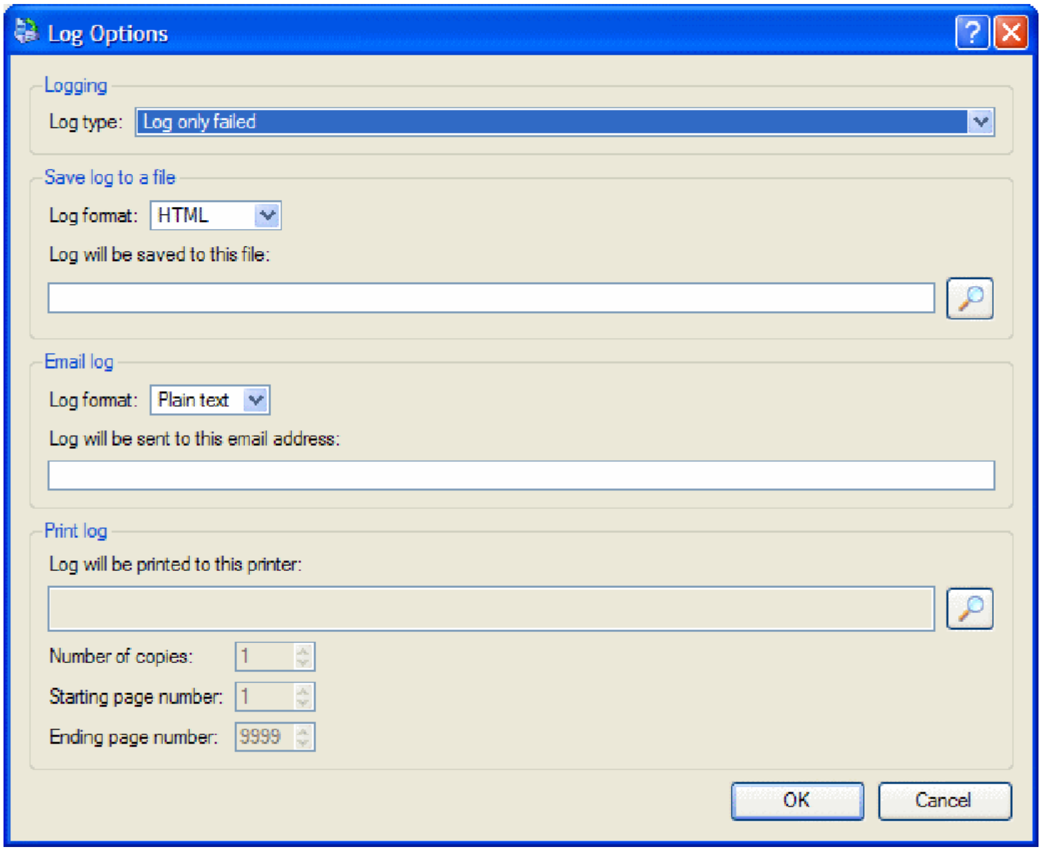
Compression

Software compression: Operating system
Hardware compression: Compressed

The following section describes each option setting and some of the possible ways each might be used.

Log options

Click the **Log options** button to select the information that will be contained in log files for the backup job. Valid choices are **None**, **Log only failed**, **Log only completed** or **Log all**.



Log Options

Logging

Log type: Log only failed

Save log to a file

Log format: HTML

Log will be saved to this file:

Email log

Log format: Plain text

Log will be sent to this email address:

Print log

Log will be printed to this printer:

Number of copies: 1

Starting page number: 1

Ending page number: 9999

Data Protector Express keeps a log of which files are backed up while running a job. To see which files were successfully backed up after a job is run, you can view or print the log, email it automatically to a designated email address, or save the log and view it later. The default value is **Log only failed**, which writes in the log any files which were not successfully backed up. This is particularly useful for locating any problems with running the backup job.

For a complete description of the logging options, see *Options page* on page 217.

File settings

To determine the layout of a log file, select from the following settings:

Log format: Data Protector Express can generate several file types. Select the log format that works best for you:

- **HTML:** Choose this file type to save log files as fully formatted HTML files. These files can be read by most Internet browsers.
- **XML:** Choose this file to save the log files as well-formed XML documents. These files can be read by most Internet browsers.
- **Excel CSV:** Choose this file type to save the log files in a format that can be opened in Microsoft Excel. CSV stands for Comma Separated Value. The information saved to a file formatted for Excel CSV will display in columns and rows.
- **Plain Text:** Choose this file type to save the log files in a format that can be read by any text editor.

Log will be saved to this file: Data Protector Express lets you select a file in which to store the job logs. Click the **Browse** button to select a file. Data Protector Express always saves a copy of the log in addition to the settings you choose here.

Span mode

Span mode determines how Data Protector Express will handle a file if the backup media is too full to fit on the current media. Available options are **Restart file** or **Split file**.

Restart file: Choose the option to instruct Data Protector Express to back up files to media only if they will fit on the media. Data Protector Express will check the available storage on the media for each file in the backup job. If a file will not fit, Data Protector Express will skip the media for the larger file and will locate media on which the file will fit.

Split file: Choose this option to instruct Data Protector Express to split a file across two media if it will not fit on the current backup media.

Backup mode

he **Backup mode** is either **Full**, **Incremental**, **Differential** or **Copy**. For scheduled automatic rotation jobs, Data Protector Express uses the backup mode for each backup set as indicated on the **Schedule** page; for unscheduled or manual jobs, Data Protector Express uses the settings set by the user. For more information, see *Backup options automatically updated* on page 112.

Full: This setting instructs Data Protector Express to back up all selected files. For each file, Data Protector Express resets the archive bit in the catalog and the archive bit on disk.

Differential: This setting instructs Data Protector Express to back up all selected files that have changed since the *last full* backup. When a file changes, its archive bit has been set. Data Protector Express does not reset the archive bit.

Incremental: This setting instructs Data Protector Express to back up all selected files that have changed since the *last* backup. For each file, Data Protector Express resets the incremental bit in the catalog and the archive bit on disk.

Copy: This setting instructs Data Protector Express to back up *all* selected files, but it has no effect on any future scheduled job. (A copy backup job does not reset the archive bit after backing up all the selected files.) Use this option when you wish to make a record of files or systems at a particular time, but do not wish to disrupt the normal backup schedule.

Change mode

The **Change mode** is either **Force to append** or **Prompt**. This option determines what action Data Protector Express will perform when it fails to find the media it was expecting to use for a job. When Data Protector Express runs a job, if the job uses specific media, Data Protector Express scans the network for devices with that media. If it does not find the media it expects, its response is determined by the **Change mode** setting.

Force to append: This setting instructs Data Protector Express to append data to whatever media it finds in the designated backup device, as long as the media is in the catalog. If it cannot find the correct media, Data Protector Express appends data to whatever media is available. This option will ensure that the job runs, if the media contains enough room to complete the job.

Prompt: This setting instructs Data Protector Express to continue to scan for the expected media and to send an alert warning that the proper media has not been found. This option will not allow a job to run with any other media except with the expected media. Additionally, this option will not search for another device that might contain the proper media.

Write mode

The Write mode is either **Append to all media**, **Append to first media, overwrite others** or **Overwrite all media**. For automatic rotation jobs, Data Protector Express overwrites all media. For other jobs, Data

Protector Express uses the write mode settings set by the user. For more information, see *Backup options automatically updated* on page 112.

This mode determines whether the old data on the media is *overwritten* with new data or whether the new data is *appended* to the end of the old data. When media is overwritten, all of the data previously stored on it is lost. Appending data will preserve the old data.

Unless the media is meant to be stored permanently, select **Overwrite all media**. This is because when media are rotated (reused), Data Protector Express overwrites it. If you have appended data to the media, overwriting will result in the loss of not just the oldest material, but all of the data on the media, including the most recent. For this reason, use **Overwrite all media** for media you wish to reuse through rotation, such as media that are part of a set of daily incremental backups, and **Append to all media** or **Append to first media, overwrite others** for media meant for permanent storage.

Appending is useful if the number of media is limited or if the media are several times larger than the size of the job. For example, a one gigabyte media could hold the contents of four jobs that are less than 250 Mbytes if these jobs were appended. However, if overwrite mode is selected, only one job will be stored on media at once. Similar comments apply to other types of media.

Append to all media: This setting instructs Data Protector Express to append all data to the end of the media. No data is overwritten. Select this setting for permanent storage.

Append to first media, overwrite others: This setting instructs Data Protector Express to append data to the end of the first media, but to overwrite all media that follows. For example, Data Protector Express will not overwrite the first media inserted, but will overwrite the second, third and later media. This setting is useful if you have a set of media with old data you no longer need. By selecting this option, Data Protector Express preserves your most recent data on the first media, but overwrites older, unneeded media.

Overwrite all media: This setting instructs Data Protector Express to overwrite all media. All data on media that is overwritten is lost. Use this option for media that are going to be recycled.

Auto Verify Mode

The Auto verify mode is either **No verify**, **Full verify** or **Quick verify**.

After Data Protector Express backs up a file onto a piece of media, it can verify that the file was backed up correctly. Data Protector Express reads the file from the media and compares it to the original file (**Full verify** mode). If any discrepancies between the two files are found, the file is considered to have failed the backup.

It is strongly recommended that the **Auto verify mode** be set to **Full verify**. Verifying that data has been correctly written to the media is an essential part of a comprehensive backup program. Also, verifying the files ensures that the media and the media drive are working correctly. Restoring data after a disaster is no time to discover that the data was incorrectly stored to begin with.

No verify: This setting instructs Data Protector Express to skip the verification step. It is not recommended.

Full verify: This setting instructs Data Protector Express to compare every selected file stored on the media with the original file from the PC desktop or file or application server. This default option is strongly recommended.

Quick verify: This setting instructs Data Protector Express to be certain that every file backed up onto the media is in readable condition. It does not verify that the data is correct, only that the data stored on the media (incorrect or not) can be read. While selecting this option can save time, it is nonetheless not recommended.

Compression

Data Protector Express can make use of both hardware and software compression during backups. Data can also be backed up without compressing it. Software compression types are: **None**, **Software**, **Operating system** or **Both**. Hardware compression types are **None** or **Compressed**.

This setting controls how Data Protector Express compresses or maintains the compression of files and directories.

None: When set to None, Data Protector Express writes all data to the backup media in a decompressed format. If the file is stored on disk in a compressed format, the file will be decompressed before writing. This option is useful if the device supports hardware data compression and the files are to be restored to a different operating system.

Software: When set to Software, Data Protector Express writes all data to backup media in the Data Protector Express compression format. If the file is stored on disk in a compressed format, the file will be decompressed before Data Protector Express re-compresses it. This option is useful if the backup device does not support hardware data compression and the files are to be restored to a different operating system.

Operating system: When set to Operating system, Data Protector Express writes all data to backup media in the same mode it is stored on disk. If the file is stored on disk in compressed format, Data Protector Express will write the data in the host's compressed format. If the file is not compressed on disk, Data Protector Express will store the file on media in a non-compressed format. This option is useful if the hardware supports data compression and the files are to be restored to the same operating system. This option also gives better performance.

NOTE: If the backup device supports hardware compression, be sure to select the **Compressed** from the **Hardware compression** drop-down list.

Both: When set to Both, Data Protector Express writes all compressed data in its compressed format. Any uncompressed files will be stored in the Data Protector Express compression format. This option is useful if the hardware does not support data compression and the files are to be restored to the same operating system.

Backup options automatically updated

The settings shown on the **Options** page fall into two categories: (1) settings that are updated automatically when Data Protector Express runs a scheduled *automatic media rotation* job (default or custom), but specified manually in *unscheduled* and *manual media rotation* jobs; and (2) settings that are always specified manually by the user. For more information, see *Forcing scheduled jobs to run* on page 125.

Data Protector Express jobs can be scheduled in several ways. For more information, see *Choosing a Schedule Type* on page 90.

When an automatic media rotation job is scheduled, the job appears on the **Job Status** view with an indication of the date and time the job is scheduled to run. When Data Protector Express runs these scheduled jobs listed on the **Job Status** view, it automatically updates the several settings on the **Options** page: **Backup mode** and **Write mode**.

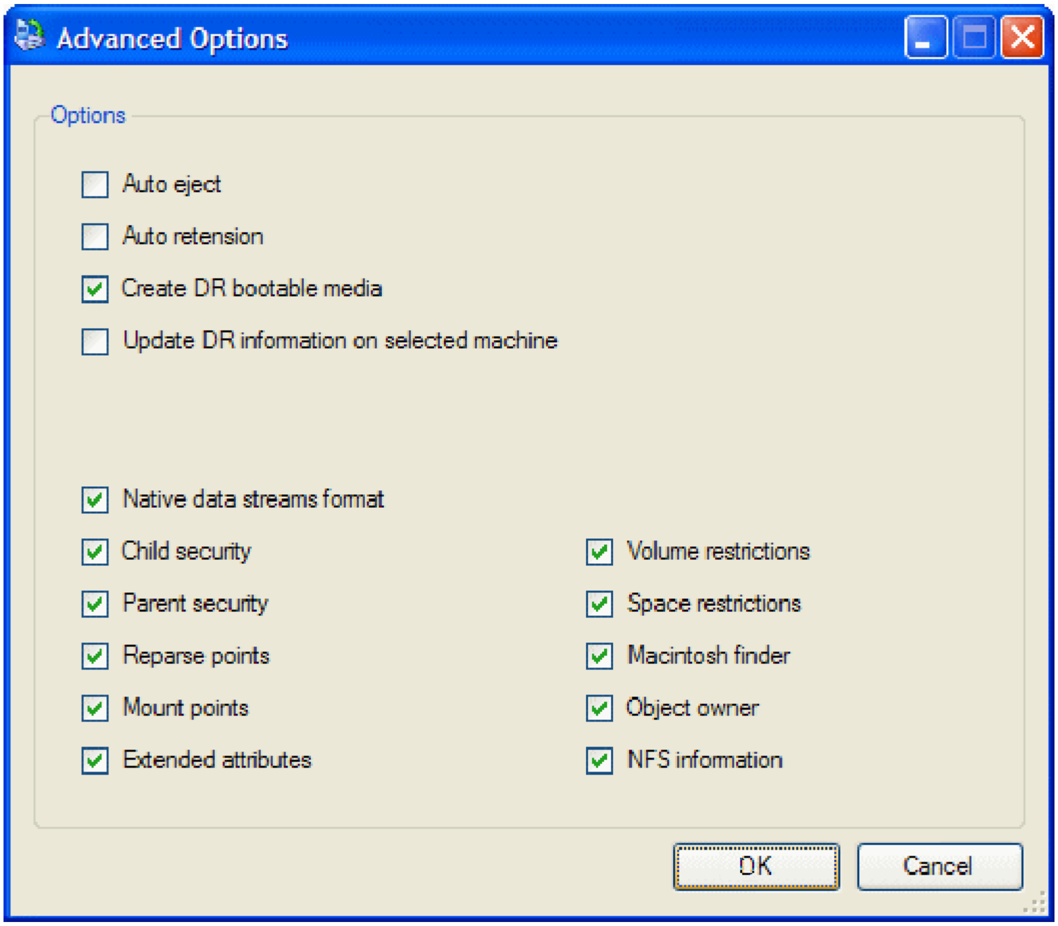
Note that Data Protector Express does NOT automatically update these five settings when you manually "force" a scheduled job to run. For example, when Data Protector Express automatically runs a scheduled backup job on a Monday, it changes (updates) the **Backup Mode** from **Full** to **Incremental**, but does not automatically update these settings.

When you run an unscheduled or manual rotation job, Data Protector Express always uses the settings selected by the user.

Advanced options for backup jobs

The **Advanced Options…** button on the **Options page** allows the user to specify certain settings controlling how files are stored on media and several post-job operations. In particular, these options specify whether the data on the media is stored in the same form as it was transmitted across the network. Data Protector Express can either store the data in a format specific to a particular network platform or in a generic format. Similarly, Data Protector Express can store all of the data it receives or filter out some of the data used by particular network platforms or operating systems.

In general, the default values should be used. These options are provided only for advanced users who need to customize their backup jobs for unique circumstances. These options might be used in one of two circumstances: when transferring data from one network platform or operating system to another; or when demands on network traffic require that a backup job be run as quickly as possible. *Unless you have specific needs that require changes to the advanced options, leave the default values unchanged.*



☐ Auto eject

☐ Auto retension

☑ Create DR bootable media

☐ Update DR information on selected machine

☑ Native data streams format

☑ Child security

☑ Parent security

☑ Reparse points

☑ Mount points

☑ Extended attributes

☑ Volume restrictions

☑ Space restrictions

☑ Macintosh finder

☑ Object owner

☑ NFS information

These options are applicable to both *backup* and *restore* jobs. Note that both job types can filter out certain data, such as security information. However, restore jobs cannot *add* data that was not originally stored on the media.

Advanced options are organized by platform. Select a platform-specific type to choose a specific setting.

Settings for all platforms

Auto Eject: When this option is checked, Data Protector Express automatically ejects the media at the end of the backup job. This feature only works on devices that support software eject.

Auto Retension: When this option is checked, Data Protector Express automatically retensions the media at the beginning of the backup job. This feature winds the tape cartridge end-to-end, applying equal tension to the entire media for maximum media life and data integrity. Your device must support auto retension to use this feature.

Create DR bootable media: Check this option to write DR system information to tape or an optical device.

Update DR information on selected machine: Check this option to generate DR system information for the selected machine.

Native data streams format: Different network software transmit data across the network to Data Protector Express in different formats. In particular, Windows, NetWare, and Linux use different data stream formats. If you are going to share data from one network platform to another, the data should be stored on media in a common data format, not in the native data streams format.

Check this option when you do not plan to share data between different network platforms. When this option is checked, Data Protector Express generally runs backup jobs more quickly.

Clear this option when you plan to share data between different network platforms, such as from a Windows server to a NetWare server.

CAUTION: Security is an issue to consider when checking this option. When this option is checked, Data Protector Express backs up all security information that network software includes in the data stream. If the option is unchecked, Data Protector Express uses a generic format that removes security information.

Reparse points: Check this option to back up the reparse point data. When this option is deselect, Data Protector Express will back up the file that the reparse point data indicates.

Mount Points: When checked, Data Protector Express includes the mount point information in the backup. If this option is not checked, Data Protector Express filters out the mount point information from the backup job.

Enable snapshots: The backup job creates snapshots using VSS by default. Deselect this checkbox to disable snapshots.

Settings for NetWare

Parent Security: When checked, Data Protector Express includes Windows, NetWare, and Linux parent security information, that is, the access control list and trustee information that controls who can see and modify the *directories*. If this option is unchecked, Data Protector Express filters out the parent security information that it receives from the network during a backup job and that it would transmit across the network during a restore job.

Child Security: When checked, Data Protector Express includes Windows, NetWare, and Linux child security information, that is, the access control list and trustee information that controls who can see and modify the *files*. If this option is unchecked, Data Protector Express filters out the child security information that it receives from the network during a backup job and that it would transmit across the network during a restore job.

Volume Restrictions: NetWare controls the maximum amount of space a user can use on a volume. When this option is checked, Data Protector Express includes this information about the volume in the backup media. If this option is unchecked, Data Protector Express filters out the volume restrictions that it receives from the network during a backup job and that it would transmit across the network during a restore job.

Space Restrictions: NetWare controls the maximum amount of space a directory can use on a volume. When this option is checked, Data Protector Express includes this information about the directories in the backup media. If this option is unchecked, Data Protector Express filters out the space restrictions that it receives from the network during a backup job and that it would transmit across the network during a restore job.

Extended Attributes: When this option is checked, Data Protector Express includes the extended attributes for objects on PC desktops or servers running operating systems that use extended attributes. Since many operating systems use extended attributes, this option can affect backups from servers and PC desktops running different operating systems. If this option is unchecked, Data Protector Express filters out the extended attributes during a backup job. As a result, these attributes will not be available during a restore job.

Macintosh Finder: When this option is checked, Data Protector Express includes the Finder information for files and directories on PC desktops or files servers that are using the Macintosh file system. If this option is unchecked, Data Protector Express filters out the Finder information that it receives from the network during a backup job and that it would transmit across the network during a restore job.

Object Owner: When this option is checked, Data Protector Express includes the object owner information for files and directories on PC desktops or file or application servers running NetWare. If this option is unchecked, Data Protector Express filters out the object owner information that it receives from the network during a backup job and that it would transmit across the network during a restore job.

Hardware Compression: When this option is checked, Data Protector Express enables hardware compression. This feature only works on devices that support software control of hardware compression.

NOTE: We recommend that you select **Operating system** for **Compression type** on the **Options** page.

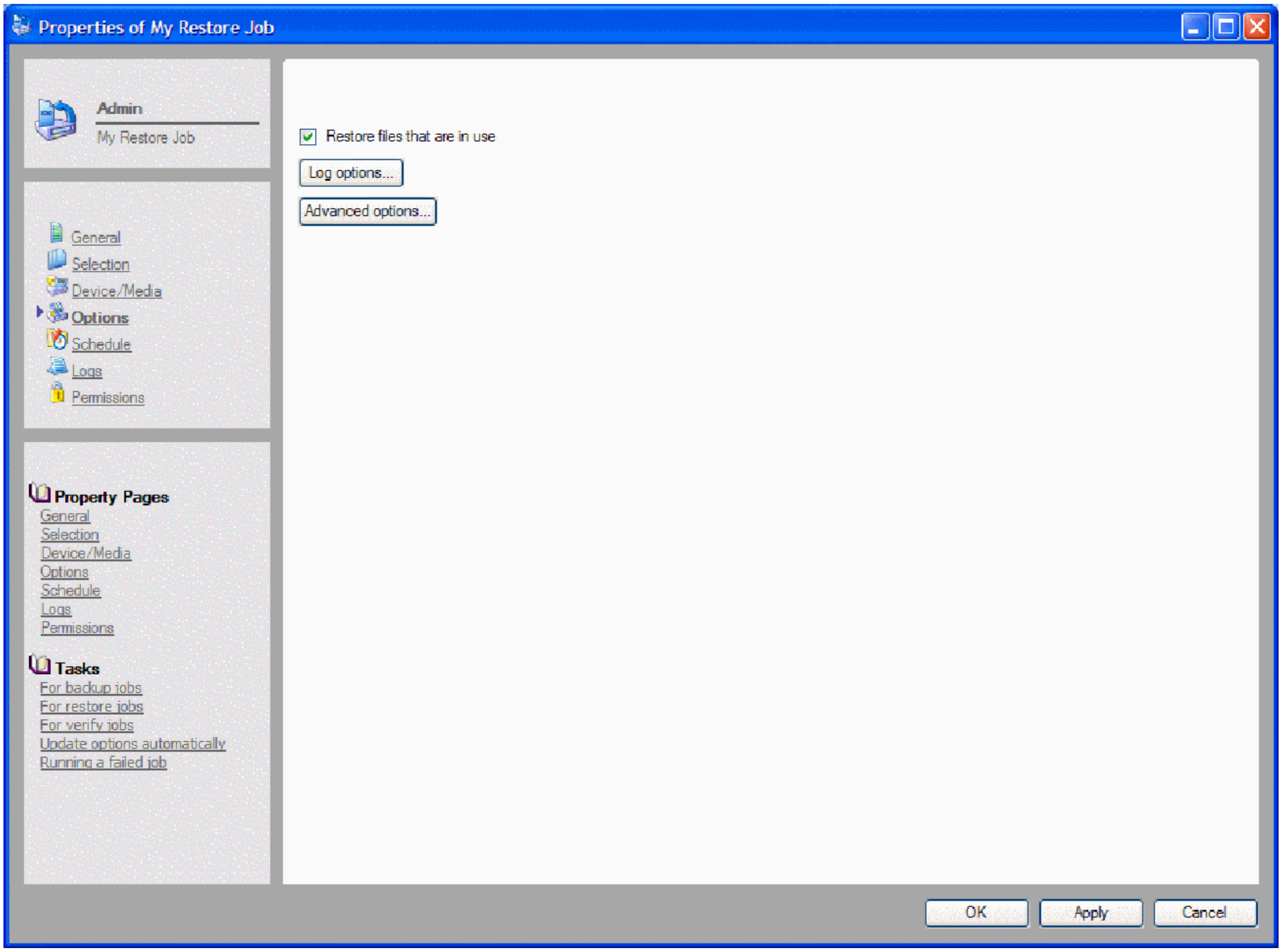
Settings for Windows

Settings for Windows platforms do not require changing during backup jobs. For information on platform-specific settings for this platform while running restore jobs, see *Settings for Windows.*

Recover databases: Check this option to process database transactions when the last incremental restore is complete.

Restore Job Options

There are fewer and simpler options for restore jobs. In general, these options are similar to options for backup jobs.



☑ Restore files that are in use

Restore files in use

The **Restore files which are in use** option tells Data Protector Express what to do when files to be restored are in use.

Select this option to restore the backup copy of the open file. (On Windows platforms, you can access the restored file after you restart the computer.) If you select this option, the restored file will replace your open file. As a result, your current changes may be lost.

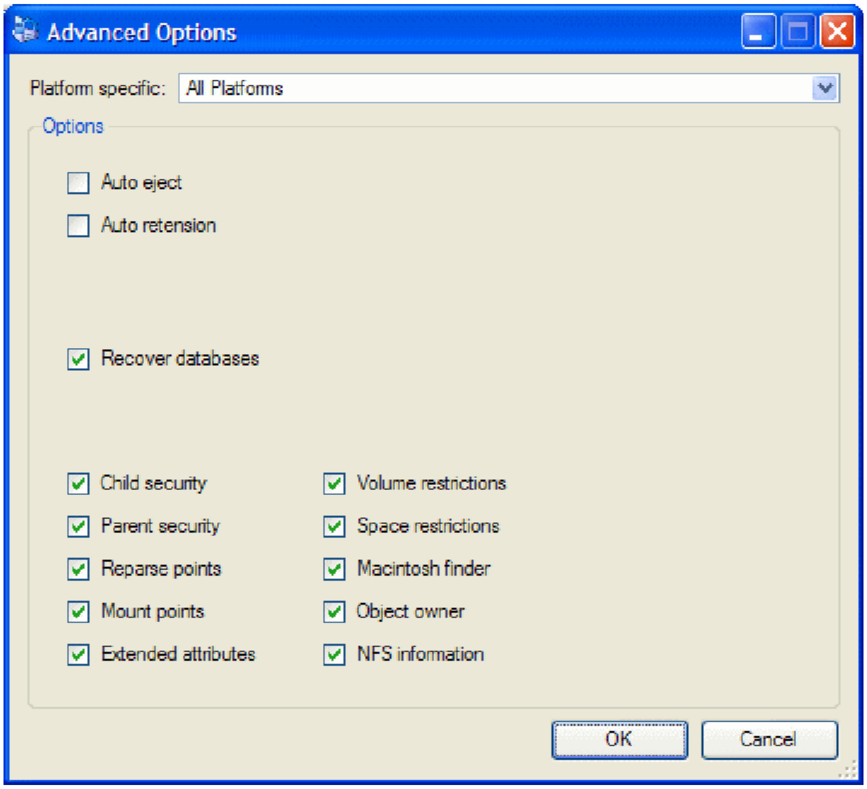
Deselect this option to skip over all selected files that are in use. This is useful if the open files are more current than the backed up files.

Log options

Log options settings for restore jobs are identical to those for backup jobs. For a complete list of options, see *Log options* on page 108.

Advanced Options for Restore Jobs

For restore jobs, you may also specify advanced options. As with backup jobs, advanced options are organized by platform. In addition to the advanced options that are available for backup jobs, the following settings are available for restore jobs.



Platform specific: All Platforms

Options

□ Auto eject

□ Auto retension

☑ Recover databases

☑ Child security

☑ Parent security

☑ Reparse points

☑ Mount points

☑ Extended attributes

☑ Volume restrictions

☑ Space restrictions

☑ Macintosh finder

☑ Object owner

☑ NFS information

All Platforms

Recover databases: Check this option to process database transactions when the last incremental restore is complete.

Settings for Windows

The following Windows settings are available only for restore jobs.

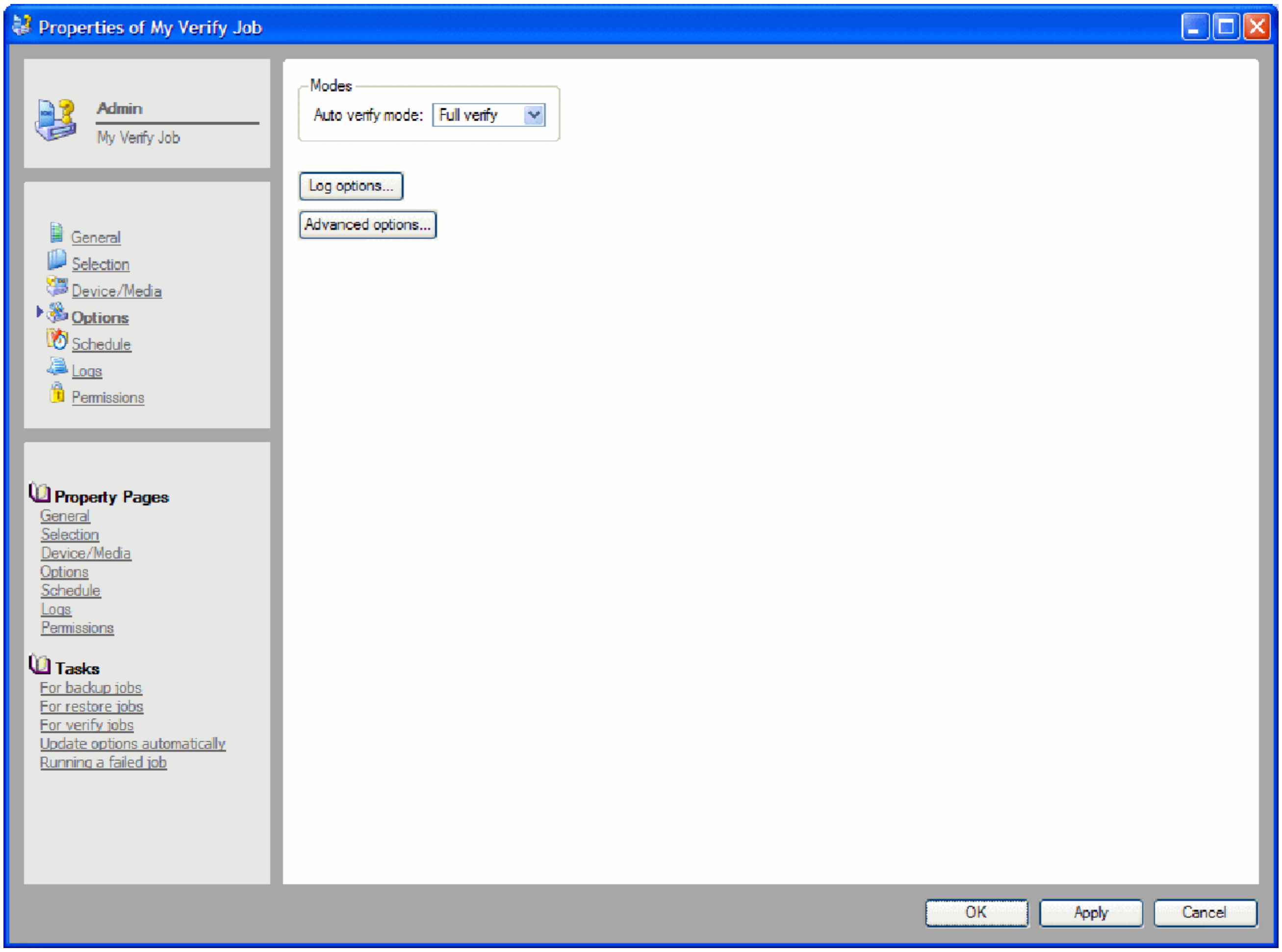
Registry: When checked, Data Protector Express restores all registry keys to the Windows Registry.

Replication: When checked, Data Protector Express rebuilds the Windows system volume tree.

NOTE: Data filters, such as security information and directory attributes, cannot restore data that was not originally backed up to the media. For example, if you did not select **Volume restrictions** for the backup job, Data Protector Express cannot restore this information because it was never stored on the media.

Verify Job Options

There are fewer and simpler options for verify jobs.



Auto verify mode: Full verify

Log Options

Log options settings for verify jobs are identical to those for backup jobs. For a complete list of options, see *Log options* on page 108.

Verify Mode

The Verify mode is either **Full verify** or **Quick verify**.

When Data Protector Express runs a verify job, it checks to see if the data on the media is readable and whether or not it matches data from the original source (that is, from the PC desktop or file or application server).

Full verify: This setting instructs Data Protector Express to compare every selected file stored on the media with the original file from the PC desktop or file or application server. This default option is strongly recommended.

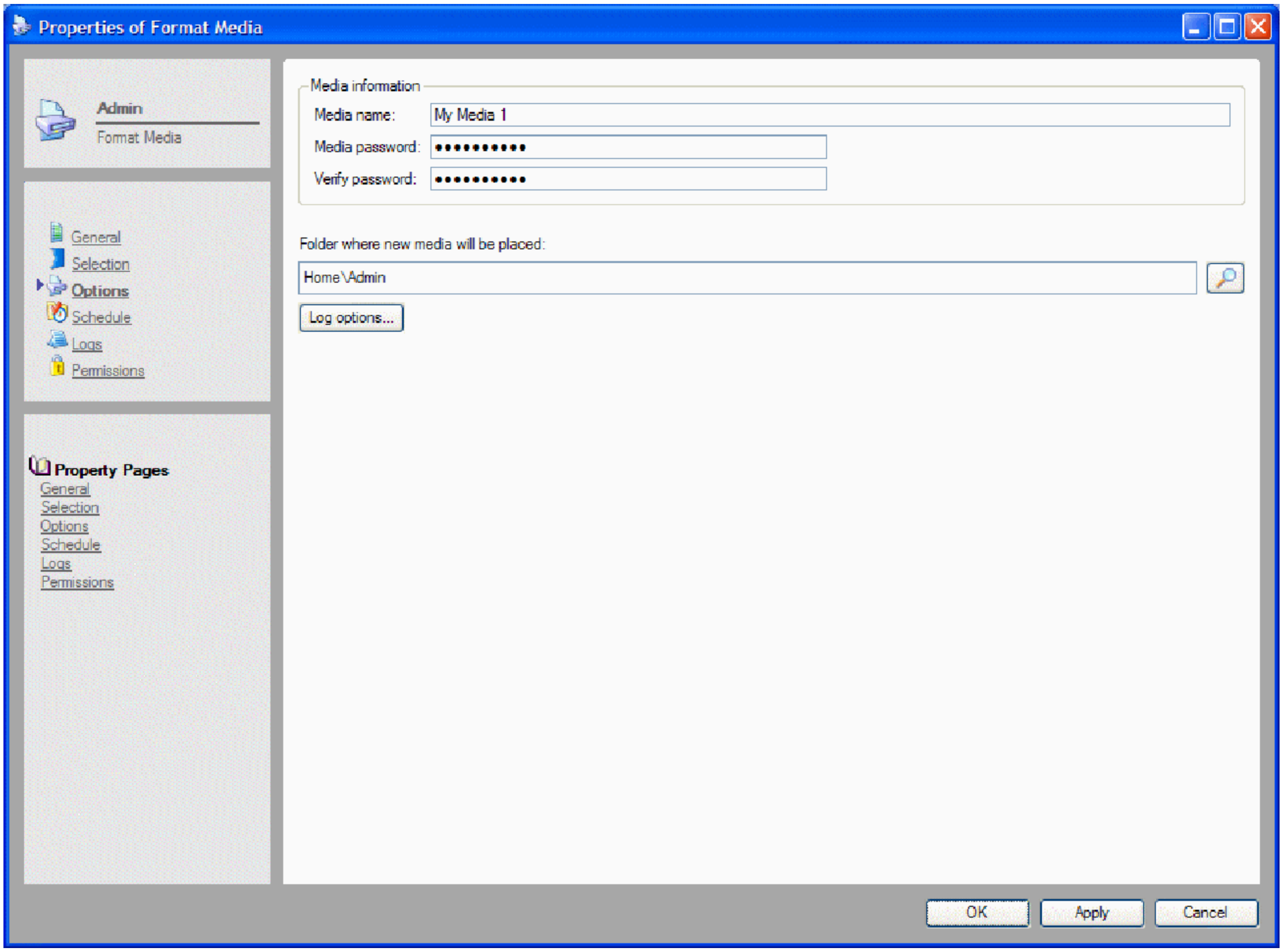
Quick verify: This setting instructs Data Protector Express to be certain that every file backed up onto the media is in readable condition. It does not verify that the data is correct, only that the data stored on the media (incorrect or not) can be read. While selecting this option can save time, it is nonetheless not recommended.

Advanced options for verify jobs

For verify jobs, you may also specify advanced options. Generally, these options work just like they do for backup and restore jobs. For a description of these advanced options, see *Advanced options for backup jobs* on page 113.

Media Job Options

There are fewer options for media jobs. The **Options** property page for selected media jobs controls settings like logging options, name and password.



Media information

Media name: My Media 1

Media password: ●●●●●●●●●●

Verify password: ●●●●●●●●●●

Folder where new media will be placed: Home\Admin

Log options

Log options settings for media jobs are identical to those for backup jobs. For a complete list of options, see *Log options* on page 108.

Additional settings for media jobs

The following media jobs include the following options. For more information about these options, see *Media job options* on page 223.

- Erase media job: Logging options and erase options

- Format media job: Logging options, media information and folder destination
- Import media job: Logging options, media information, and folder destination
- Move media job: Logging options, library and slot assignment
- Sort media job: Logging options and sort order (ascending or descending) and sort key

Chapter 9: Running Jobs

Data Protector Express will automatically run jobs that are scheduled. You can view jobs scheduled to be run on the **Job Status** view and you can track the progress of a job as it runs from the job's **Status** page or from the **Job Status** view.

NOTE: If the storage management server is turned off when a job is scheduled, the job will run when that machine is started again. Jobs scheduled to run will begin running five minutes after you start Data Protector Express. (If Data Protector Express is run as a service, this will be five minutes after startup.) This five-minute lag allows you to modify, update or cancel any pending jobs before they run.

In this section

- Job Status View
- Running Scheduled Jobs
- Running Unscheduled Jobs
- Status property
- Job Logs
- Audit Logs

Overview

For jobs that are not scheduled, Data Protector Express will only run the job when you instruct it to do so. Scheduled jobs run automatically as scheduled. You can view what jobs are scheduled to run on the **Job Status** view, which indicates when a job is scheduled to run and provides a short summary of a job's progress as it runs. When Data Protector Express automatically runs a scheduled job from the **Job Status** view, it updates the option settings for that job before running it.

You can also "force" scheduled jobs to run before they are scheduled. When a scheduled job is forced to run, Data Protector Express does not automatically update settings on the job's **Option** page. Forcing a job to run can also affect the permissions Data Protector Express uses when it runs the job. Be certain to read *Forcing scheduled jobs to run* on page 125 for more information on how forcing a scheduled job to run affects the settings Data Protector Express uses to run the job.

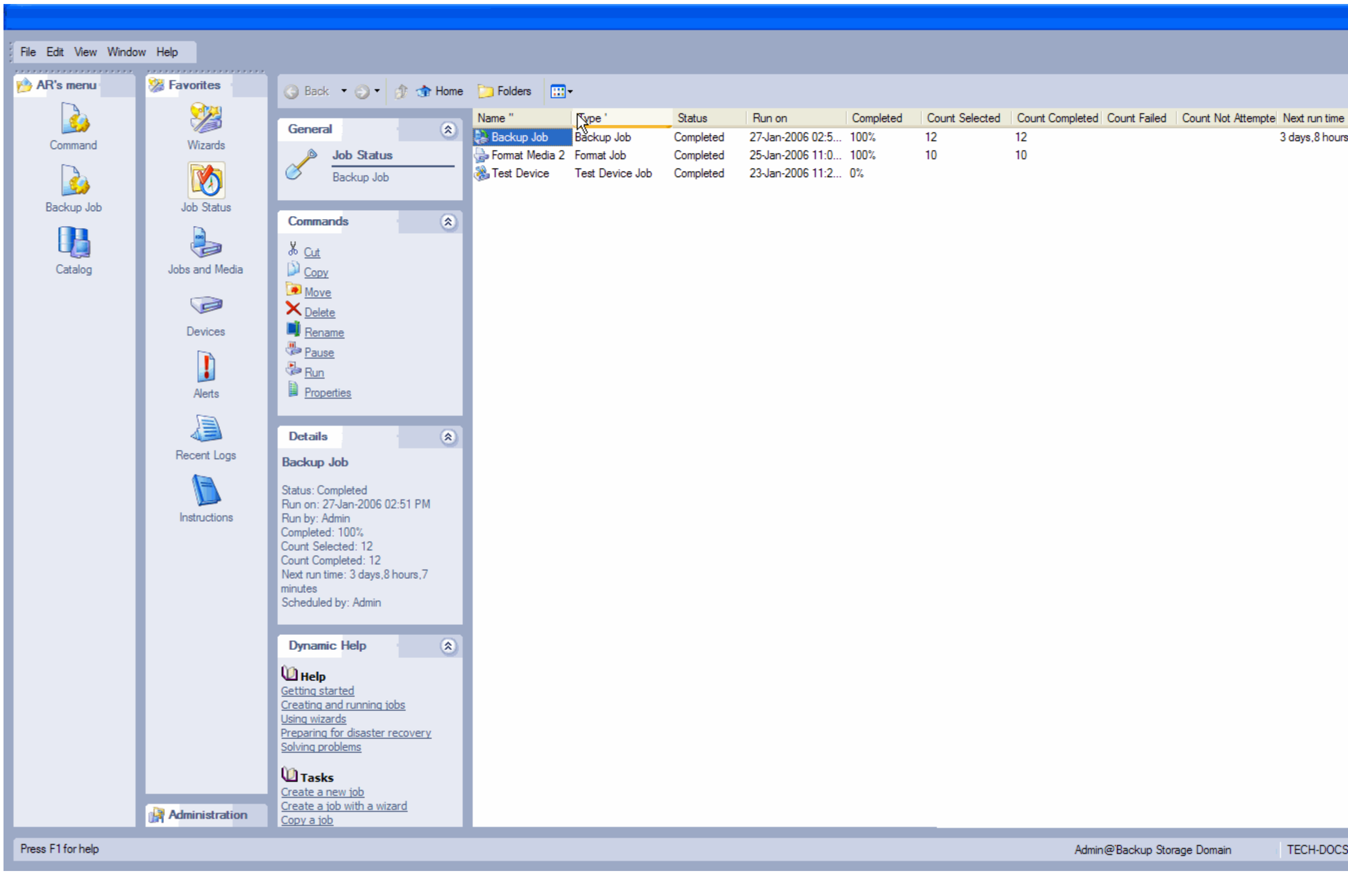
The **Status** window provides detailed information about the progress and status of jobs as they run. You can use this window to see that a job is running properly. After a job has completed running, you can view and print the **Job Log** to check what files were successfully or unsuccessfully backed up, verified or restored.

Job Status View

After a job has been scheduled to run, Data Protector Express displays the job and information about it on the **Job Status** view. Accessible from the **Favorites** desk bar, you can review the list of jobs to verify that a particular job or task completed as you expected.

This view shows all of the jobs that are scheduled to run, that have been completed, or that are running. As new jobs are created and scheduled, they are listed on the **Job Status** view. An entry for each occurrence of a scheduled job is listed using information for the each scheduled time that job is to run.

As a scheduled job runs, it status is updated to Running and then to Completed. Unscheduled jobs that Data Protector Express has been instructed to run also appear on the **Job Status** view, but only after you run them manually.



Name "	Type '	Status	Run on	Completed	Count Selected	Count Completed	Count Failed	Count Not Attempte	Next run time
Backup Job	Backup Job	Completed	27-Jan-2006 02:5...	100%	12	12			3 days,8 hours
Format Media 2	Format Job	Completed	25-Jan-2006 11:0...	100%	10	10			
Test Device	Test Device Job	Completed	23-Jan-2006 11:2...	0%					

Details

Backup Job

Status: Completed
Run on: 27-Jan-2006 02:51 PM
Run by: Admin
Completed: 100%
Count Selected: 12
Count Completed: 12
Next run time: 3 days,8 hours,7 minutes
Scheduled by: Admin

Tasks and jobs listed on this view can be organized by resorting the list with the **Details** view. If the **Details** view is not active, select View from the toolbar and change the view to **Details**.

Job Status details view

The **Details** view on the **Job Status** view provides the most useful and important information about completed, scheduled or running jobs.

The **Name** and **Type** fields show the name of the job and whether it is a backup, restore or verify job. The **Next Run Time** field indicates the date and time the job is next scheduled to run

The **Status** field provides a short summary of a job’s current status. The **Status** field indicates if the job is currently running, completed or scheduled.

Additional fields provide information about when the job was run or when it is scheduled to run, how many files are included in the job, and so on. You can customize this view by adding or removing fields to the table. To do so, right-click in the table heading and select **Insert column**. Then right-click the new column and select the information that you want to include in the list.

Running Scheduled Jobs

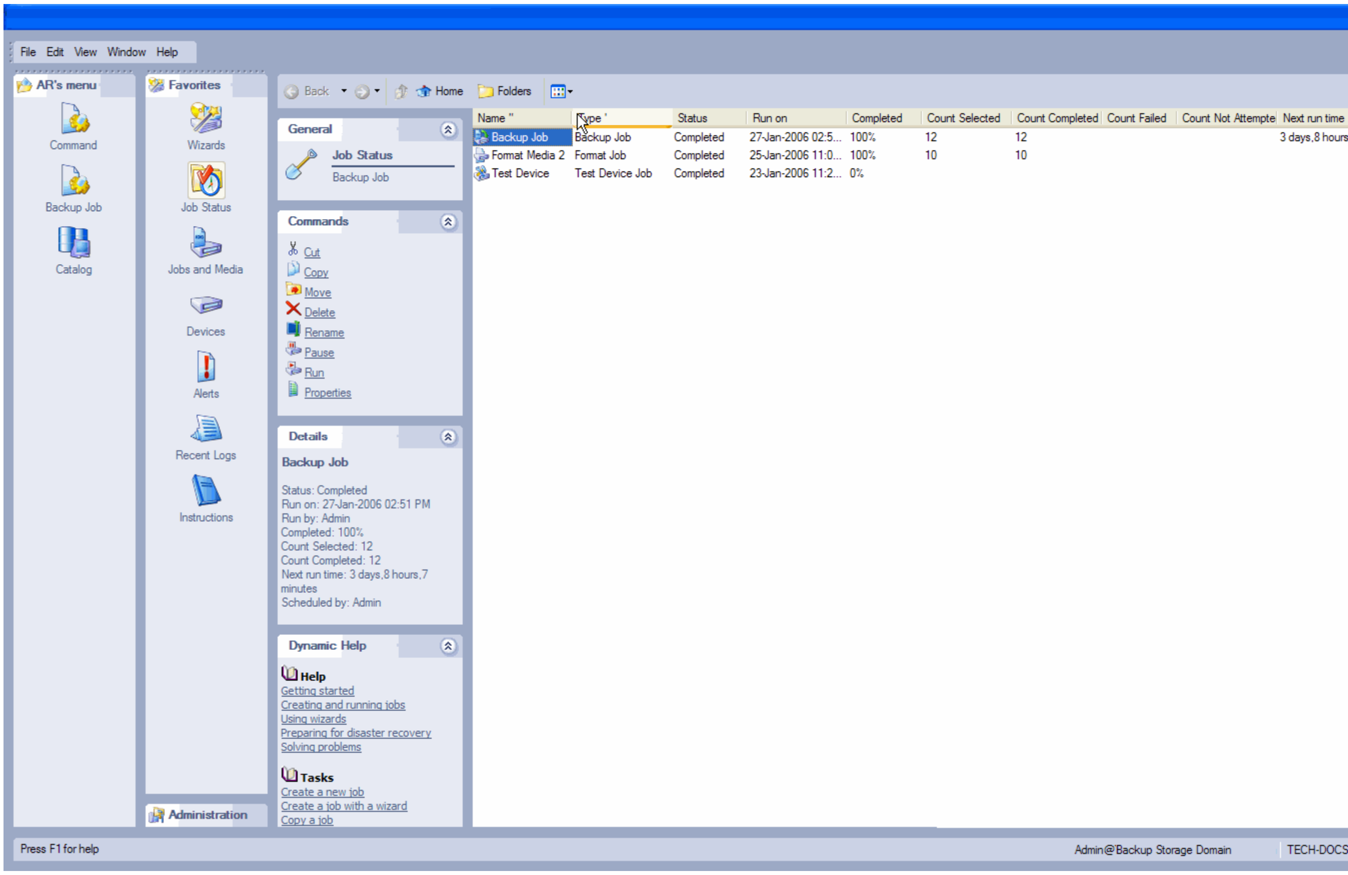
Scheduled jobs are normally run automatically by Data Protector Express, but you can also “force” a scheduled job to run.

Automatically running scheduled jobs

When you close the property page of a job, Data Protector Express calculates the next time the job is scheduled to run and places the job on the **Job Status** view.

TIP: To see a list of details about the jobs, use the **Details** view.

The **Next Run Time** field on the **Job Status** view shows the date and time the job is scheduled to run. This is true for jobs scheduled with automatic or manual rotation schedules.



Name	Type	Status	Run on	Completed	Count Selected	Count Completed	Count Failed	Count Not Attempte	Next run time
Backup Job	Backup Job	Completed	27-Jan-2006 02:5...	100%	12	12			3 days,8 hours
Format Media 2	Format Job	Completed	25-Jan-2006 11:0...	100%	10	10			
Test Device	Test Device Job	Completed	23-Jan-2006 11:2...	0%					

Details

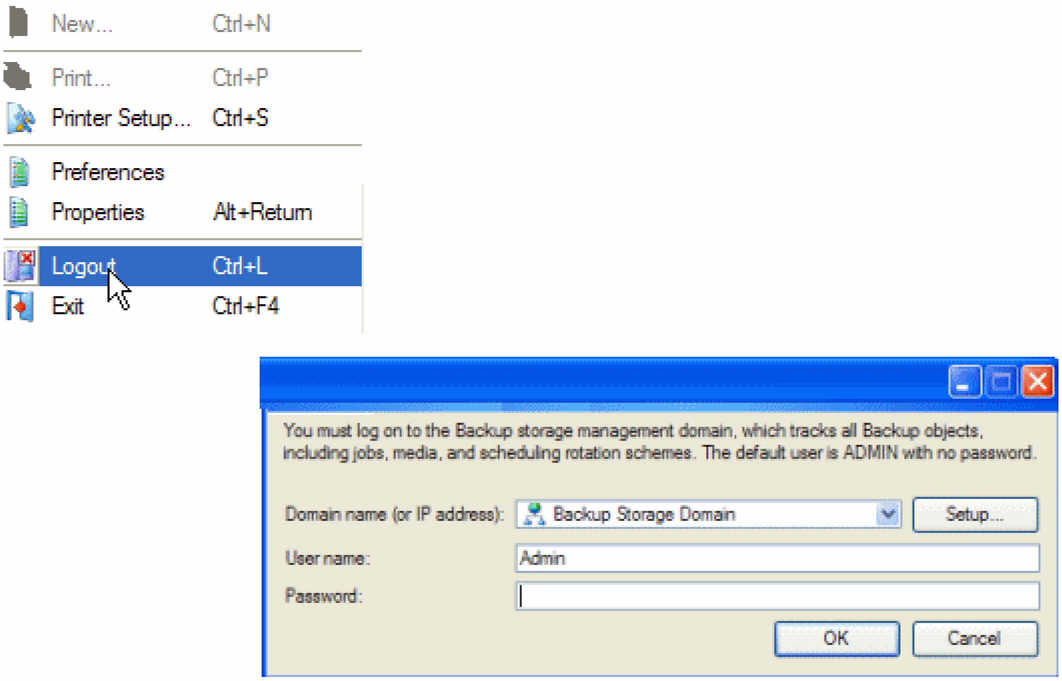
Backup Job

Status: Completed
Run on: 27-Jan-2006 02:51 PM
Run by: Admin
Completed: 100%
Count Selected: 12
Count Completed: 12
Next run time: 3 days,8 hours,7 minutes
Scheduled by: Admin

These jobs will run automatically if Data Protector Express is open at the scheduled date and time. It is not necessary for a user to be logged on to Data Protector Express for the job to run. Data Protector

Express will run scheduled jobs even if the user who created the job has logged out so long as Data Protector Express is still open or the Data Protector Express service is running.

For example, suppose you have scheduled a job to run at 11:00 p.m. tonight. When you leave your PC desktop, log out of Data Protector Express. *Do not exit or close* Data Protector Express. When the Data Protector Express **Logon** window appears, click the minimize button to close the window. Although no user will be logged on, Data Protector Express will still be open and will execute the job at the scheduled time.



You must log on to the Backup storage management domain, which tracks all Backup objects, including jobs, media, and scheduling rotation schemes. The default user is ADMIN with no password.

Domain name (or IP address): Backup Storage Domain

User name: Admin

Password:

Select Logout, then minimize the Login screen

TIP: You can install Data Protector Express as a service on machines running Windows and Linux. On NetWare systems you can install the Data Protector Express agent. When installed as a service or agent, Data Protector Express will start automatically each time the system starts up and run in the background without any user interface. If you want to make sure that scheduled jobs always run, install Data Protector Express as a service. For more information, see *Appendix B - About the* Data Protector Express *Service* on page 246.

NOTE: If the storage management server is turned off when a job is scheduled, the job will run when that machine is started again. Jobs scheduled to run will begin running five minutes after you start Data Protector Express. (If Data Protector Express is run as a service, this will be five minutes after startup.) This five-minute lag allows you to modify, update or cancel any pending jobs before they run.

Security and scheduled jobs

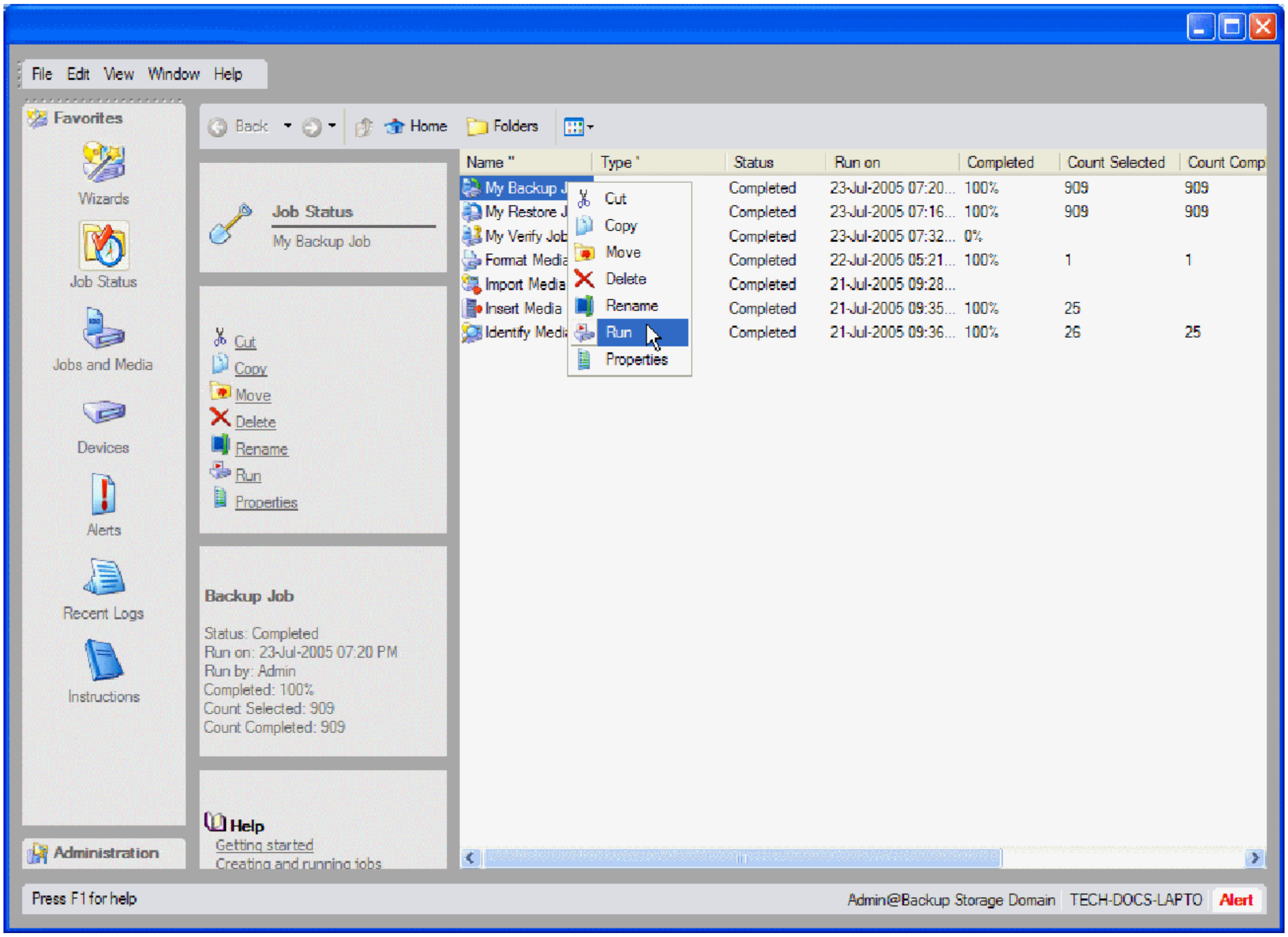
Scheduled jobs will run whether you log out or not, as long as Data Protector Express is open or the Data Protector Express service is running. If you have not logged out, however, unauthorized users will be able to work with your security clearance. For this reason, be certain to log out or exit Data Protector Express before leaving your PC desktop. This is the only way to ensure that no unauthorized users gain access to sensitive data.

CAUTION: Do not leave the main Data Protector Express window open when you are not at your PC desktop. Doing so allows users without security clearance unauthorized access to the network. Be certain to log out of Data Protector Express before leaving your PC desktop. If you have jobs scheduled to run, either log out instead of exiting Data Protector Express or make sure the Data Protector Express service is running.

Forcing scheduled jobs to run

You can “force” scheduled jobs to run prior to their scheduled time by selecting the job and clicking the **Run** command from the **Commands** task pane. Alternatively, you can select the job from the job view, right-click and select **Run** from the shortcut menu. You can also run the job from the **Job Status** view. Data Protector Express will execute the job immediately.

Note that forcing a job that is scheduled for the same day marks the job as complete for that day. Data Protector Express resets the job on the next day so it will run as scheduled. As a result, if you force a job to run on the same day that it is scheduled to run, it only runs once on that day.



Name "	Type '	Status	Run on	Completed	Count Selected	Count Comp
My Backup J		Completed	23-Jul-2005 07:20...	100%	909	909
My Restore J		Completed	23-Jul-2005 07:16...	100%	909	909
My Verify Job		Completed	23-Jul-2005 07:32...	0%		
Format Medi		Completed	22-Jul-2005 05:21...	100%	1	1
Import Media		Completed	21-Jul-2005 09:28...			
Insert Media		Completed	21-Jul-2005 09:35...	100%	25	
Identify Medi		Completed	21-Jul-2005 09:36...	100%	26	25

Backup Job

Status: Completed
Run on: 23-Jul-2005 07:20 PM
Run by: Admin
Completed: 100%
Count Selected: 909
Count Completed: 909

Select a job, then run it from the Shortcut menu

How forcing jobs to run affects job settings

When you force a scheduled job to run before its scheduled time, Data Protector Express does not automatically update certain settings on the **Options** and **Device/Media** property pages of the job. Recall that when a scheduled job *with an automatic rotation* is run, Data Protector Express updates the **Backup mode**, **Write mode**, **New media location**, **New media name** and **Media** settings on the **Options** and

Device/Media property pages of the job to reflect that job's place in the rotation schedule. However, when a job is forced to run before its scheduled time, Data Protector Express does not update these settings.

For example, suppose that a backup job is scheduled to run as an incremental job in the evening. If it is forced to run before its scheduled time, Data Protector Express will not update the **Backup Mode** setting. In this case, if the last time the job was run, it was as a full backup job, the **Backup Mode** setting on the job's **Option** page will still be set to **Full**. As a result, when you force the job to run, it will be run as a full backup job, even though it is next scheduled to run as an incremental job.

Forcing a job to run can be useful when a job failed to run for some reason. For example, suppose a full backup job is scheduled for a Saturday, but a network equipment malfunction prevented the job from being run as scheduled. It is important that another *full* backup job be run before the next *incremental* job. This is the only way to ensure that the full data recovery period is not compromised. On Monday, you can force the failed backup job to run again after the network connections are restored. Before you run the job, open the job's property page and make sure the proper job type and media are selected.

Before forcing a scheduled job to run, you should always check the **Options** page of the job to see that the option settings are set correctly. If you are forcing the job to run because an earlier job failed to run properly, you can look at the log of the failed job to see which settings the job would have used.

How forcing jobs to run affects permissions

When a job is run, Data Protector Express will check for the appropriate permissions to the device, files, media, and so on. Data Protector Express calculates these permissions by using the permissions of the user who scheduled the job. The **Scheduled by** field lists the user who scheduled the job. The **Run by** field lists the user who forced the job to be run. After a job is run, the job owner is reset to the last user who changed the job properties; forcing a job to run does not permanently change the job owner.

When the Data Protector Express administrator creates and schedules a job, the owner of the job is the administrator. Data Protector Express will use the Data Protector Express administrator's permissions when running the job. Similarly, if another user creates and schedules a job, that user will be the job's owner and Data Protector Express will calculate the job's permissions using that user's permissions.

However, if a scheduled job is forced to run, the person who forces the job to run becomes the job's new owner. So, for example, if the Data Protector Express administrator forces a job to run that another user has created, the Data Protector Express administrator becomes the job's new temporary owner and Data Protector Express calculates the permissions using the Data Protector Express administrator's permissions.

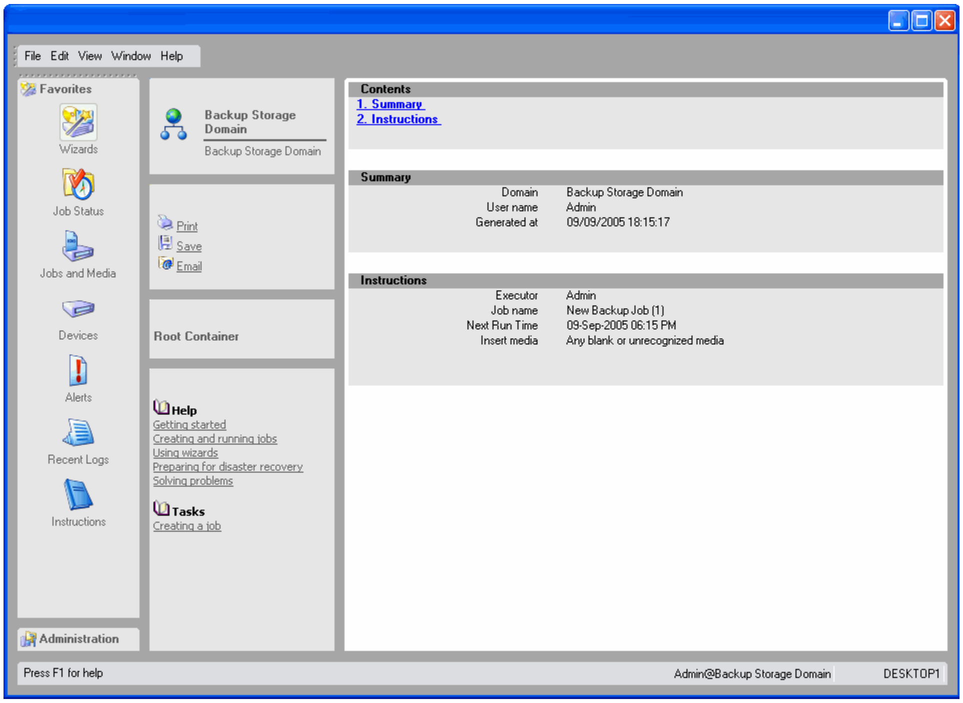
Changing the job's owner can be useful for managing security. A user can create and schedule a job, even though that user lacks the proper permissions to run that job. Another user, such as the Data Protector Express administrator, can then force that job to run with their own permissions.

Viewing and printing scheduled job instructions

Whenever a job is scheduled and placed on the **Job Status** view, Data Protector Express creates a set of *instructions* for that job. Included in a job's instructions is information about which media set must be available to be used and which backup devices it may be inserted into. For example, when running an automatic rotation job, the instructions for that job include the name of the media Data Protector Express is expecting to use when that job runs next, such as “Daily Set 1” or “Yearly Set 2”. The instructions also include the name of the backup devices which Data Protector Express expects to be available when the job runs.

TIP: You can use the instructions to ensure that all of your jobs run correctly by planning ahead to see that each job has the media it requires before it runs. For example, you can print the instructions and then assign a co-worker the task of inserting the proper media into various backup devices by the required time.

You can view the instructions for the jobs currently scheduled on the **Job Status** view by selecting **Instructions** from the **Favorites** desk bar.



Contents

1. Summary
2. Instructions

Summary

Domain	Backup Storage Domain
User name	Admin
Generated at	09/09/2005 18:15:17

Instructions

Executor	Admin
Job name	New Backup Job (1)
Next Run Time	09-Sep-2005 06:15 PM
Insert media	Any blank or unrecognized media

Choose an appropriate command to **Print**, **Save** or **Email** the instructions.

Running Unscheduled Jobs

If you did not schedule the job, then you must manually instruct Data Protector Express to run the job each time you want it to run. To run the job, select it from the **Jobs and Media** view and then select the **Run** command. Data Protector Express asks you to confirm and then executes the job immediately.

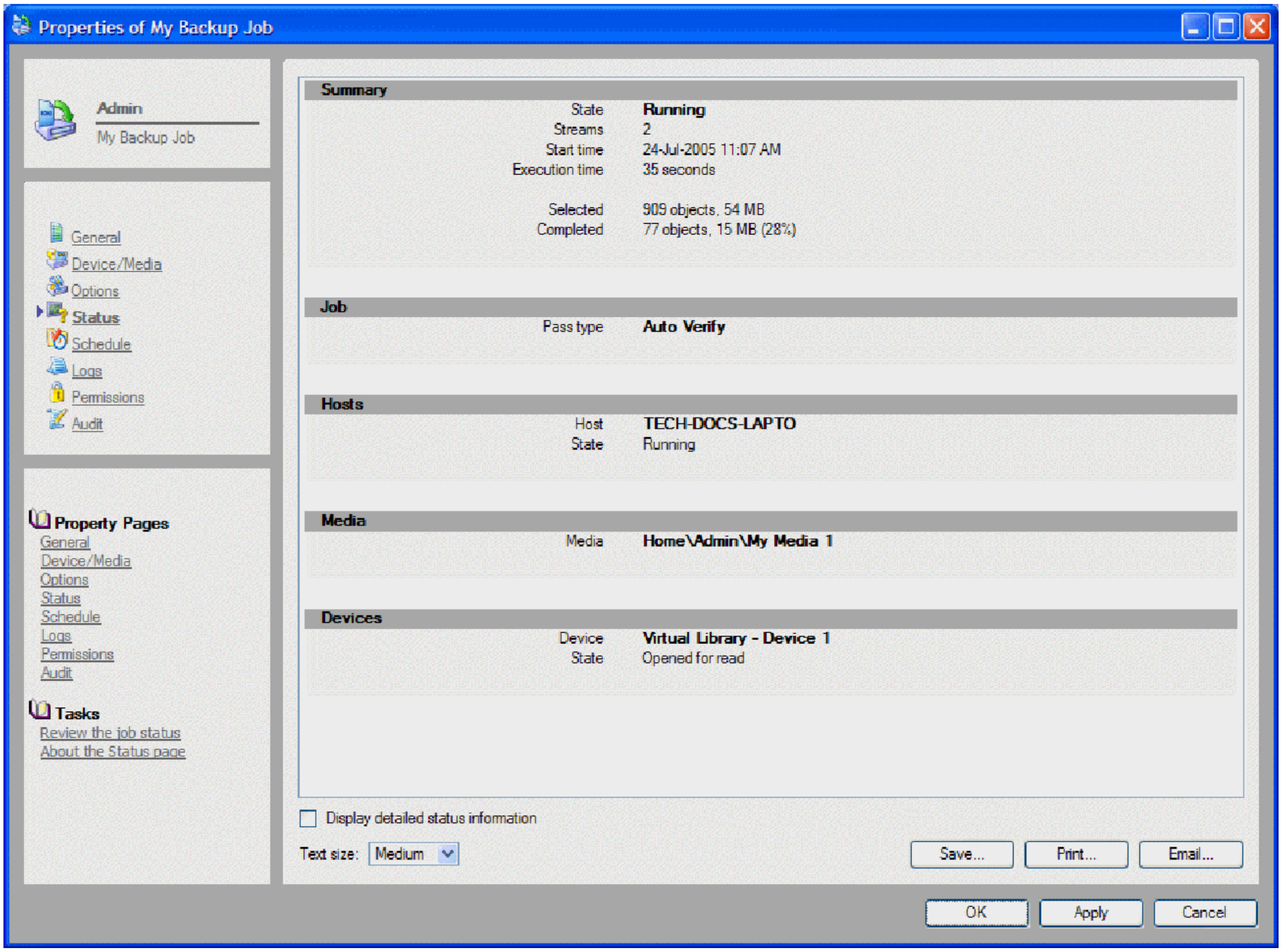
Unscheduled job settings and permissions

When an unscheduled (or manual rotation) job is run, Data Protector Express uses the current settings on the job's **Options** page.

Similarly, the owner of the job is the person that instructed Data Protector Express to run the job. Data Protector Express calculates the permissions of the job using this user's permissions, that is, the permissions of the job's owner. Note that the creator of a job and its owner are not necessarily the same user.

Status property page

Each time Data Protector Express runs a job, it goes through a series of predetermined steps. Many of these steps are indicated on the **Status** page of the job. The **Status** page is available whenever a job has run and Data Protector Express has new status information. Status information appears in the **Details** information pane. Once the job finishes running, this status information disappears. To review the details of the status information for a job, open the job's property pages and select the **Status** page.



Summary

State: Running
Streams: 2
Start time: 24-Jul-2005 11:07 AM
Execution time: 35 seconds
Selected: 909 objects, 54 MB
Completed: 77 objects, 15 MB (28%)

Job

Pass type: Auto Verify

Hosts

Host: TECH-DOCS-LAPTO
State: Running

Media

Media: Home\Admin\My Media 1

Devices

Device: Virtual Library - Device 1
State: Opened for read

□ Display detailed status information

Text size: Medium

To change how much information is displayed on the **Status** page check **Display detailed status information**. Commands are also available to save, print or email the status log.

Job status messages

As jobs are run, Data Protector Express displays messages in the **Status** message box indicating the progress of the job. These messages are also displayed in the job's **Status** field on the **Job Status** view. Which messages are displayed depends on the type of job being run. The following short descriptions indicate what procedures Data Protector Express is performing as each message is displayed.

Building…Selection List: The first step is to create a list of files to be backed up, verified or restored. For backup jobs, Data Protector Express uses the selection criteria and the backup job type (whether full, incremental or differential) to create a list of files to be backed up. The number of files and the total size of the selected files are indicated in the **Objects** and **Size** fields under **Selected**.

Mounting Media: Data Protector Express displays this message as it mounts the media. During this step, Data Protector Express reads identification information stored on the media. Data Protector Express then checks to see if the media already exists in the catalog and whether or not the current job can be run using this media.

If Data Protector Express can use the mounted media with the current job, it proceeds to the next step.

If the mounted media cannot be used for this current job, the next step is determined by the settings specified on the **Options** page for the job. For example, Data Protector Express only formats a blank media if that option is selected.

Scanning for Device: This message is displayed when Data Protector Express is looking for a device to use with the current job. This message might be displayed when the current media cannot be used with this job or when Data Protector Express cannot find a device on the network.

NOTE: Many times this message will be accompanied by an alert. You can view any current alerts by clicking the **Alert** button on the **Status** bar.

Formatting Media: If the media is already formatted, Data Protector Express proceeds to the next step. Otherwise, Data Protector Express formats the media according to the **Auto format mode** setting on the **Options page** for the job.

Opening Device: Once the media is mounted and formatted, Data Protector Express readies the media and device for the job.

Running: After opening the device, Data Protector Express runs the job. As the job is run, the **Status** window automatically displays current information about the job, including which files are being backed up, restored or verified, which streams are active and the rate (or **throughput**) at which files are being written to media or volumes. You can use the **Display** list box to check the progress of individual streams or the throughput of a specific device.

Closing Device: When Data Protector Express closes a device, it displays this message.

Building Logs and Audit Trails: After closing the device, Data Protector Express updates the catalog with new information from the job, such as which files were backed up, and creates a log of the job. The specific log contents depend on the **Log options** setting on the **Options page** for the job. For more information, see *Audit Logs* on page 131.

Merging Groups: After a backup job has run, Data Protector Express updates the catalog to reflect any changes to media or files created by the current job. Prior to running a restore or verify job, Data Protector Express sorts all the selected files into the order in which they appear on the media and displays this message.

Completed: This message is displayed after the job is finished.

Failed: When a job is forced to quit, Data Protector Express displays this message.

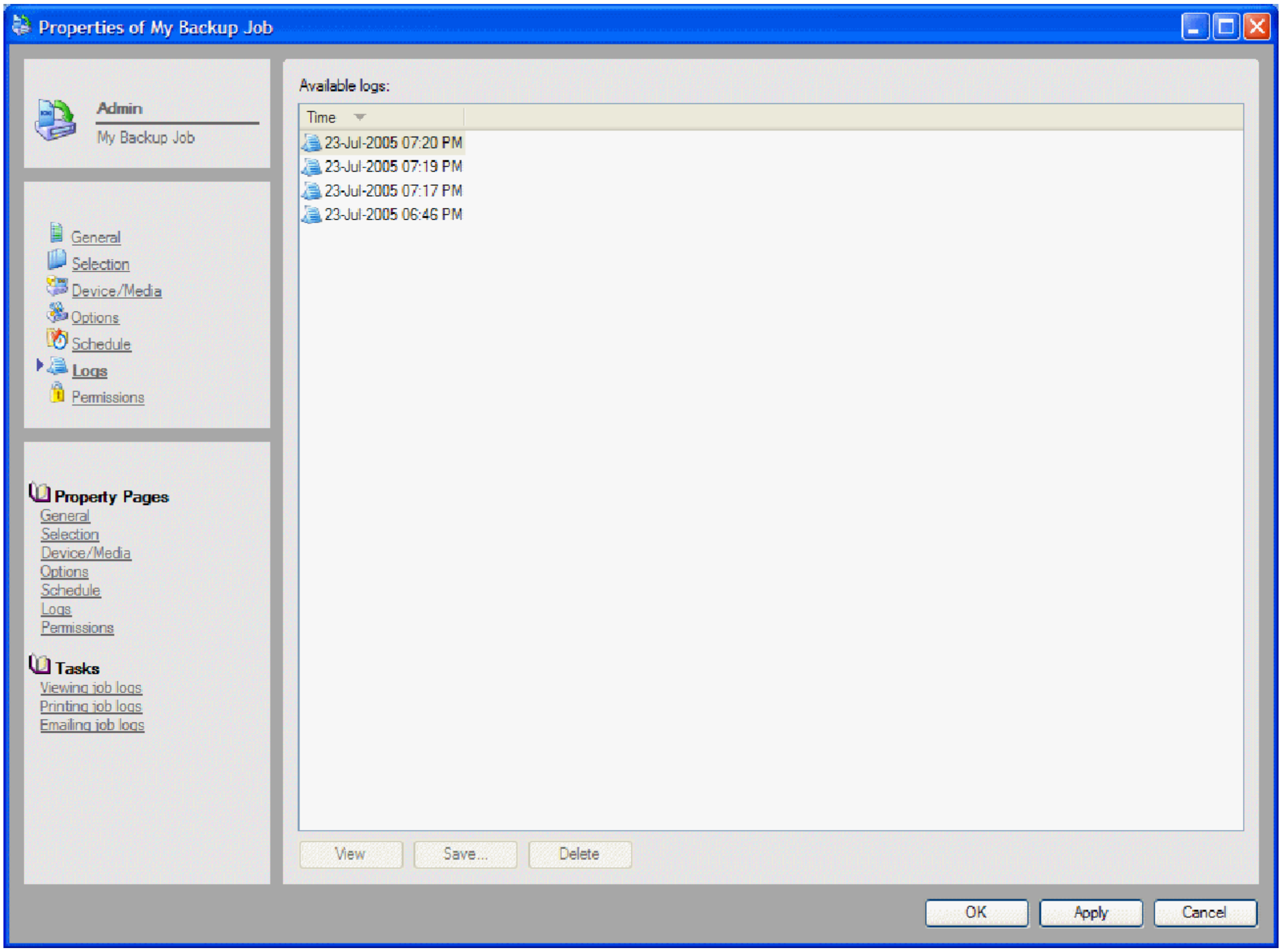
Job Logs

Each time a job is run, Data Protector Express creates a new log for that job. You can use this information to check if a job is running as you intended and to keep a permanent record of that job. After a job finishes, you can view or print the log, print the log automatically or have Data Protector Express email it to one or more addresses.

You can specify the information Data Protector Express should write to the log on the **Options** page of the job by clicking the **Log options** button. The log always includes summary information about the job, which includes useful information about which option settings the job used when it ran. Depending on which **Log options** setting you select, Data Protector Express will also include information about which files were successfully or unsuccessfully restored, verified or backed up.

Viewing job logs

You can view the logs for a job on the job’s **Logs** page. Note that there is a separate log for each time a job is run.



Time
23-Jul-2005 07:20 PM
23-Jul-2005 07:19 PM
23-Jul-2005 07:17 PM
23-Jul-2005 06:46 PM

To view the log of a particular job, open the **Logs** page of the job. Select the appropriate log in the **Available logs** list. You can double-click the log to open it, or click the **View** button. To change how the log is displayed, change the **Text size**.

To print an open log, click the **Print** button. Note that some logs can be very long; check the length of the document before printing it. To save an open log, click the **Save** button.

If you run a job repeatedly, you may want to delete old logs. Simply select the one or more of the job logs and click **Delete**. Use the CTRL and SHIFT keys while you select logs, or drag the mouse over a series of logs.

NOTE: The maximum number of logs per job is 250. Data Protector Express will overwrite the oldest log when you reach this maximum.

Automatically printing job logs

Data Protector Express provides a convenient method for you to print the job log automatically. This way you don’t have to manually print a copy of each job log.

The **Printer** page appears on the property page of each user in the **Security** view. You can select a specific printer, font, print range and number of copies. Data Protector Express prints the job log automatically as soon as the job finishes, according to the autoprint settings of the job owner.

For more information about setting up printing, see *Printer page* on page 229.

To configure this feature, access the group or user from the **Security** view, then click the **Autoprint** page. Update your settings and click **OK**.

NOTE: You must also select the **Print log** setting on the **Options** page of the job to automatically print the job log. For more information, see *Logging options* on page 220.

Emailing job logs

Data Protector Express can send you an email automatically when a job has completed. This way you can know for certain that a job has run successfully or the reason why a job has failed to run correctly. If you can retrieve your email remotely, you can monitor your jobs, even if you are away from the office.

NOTE: If a job fails before it can generate a log, Data Protector Express cannot email you the job log.

To use this feature, you must configure the email support option (see Appendix A - Configuring Email on page 245).

The job log is sent to the addresses listed on the **Log Options** screen of the **Options** page for each job. To specify several addresses, separate each address with a semicolon (no spaces). Additionally, you can enter the same address if you want to send a copy of *every* job log to the same user. For example, you might send the Data Protector Express administrator the log of every job that runs. Alternatively, consider setting up a separate email account for the sole purpose of receiving job logs.

Audit Logs

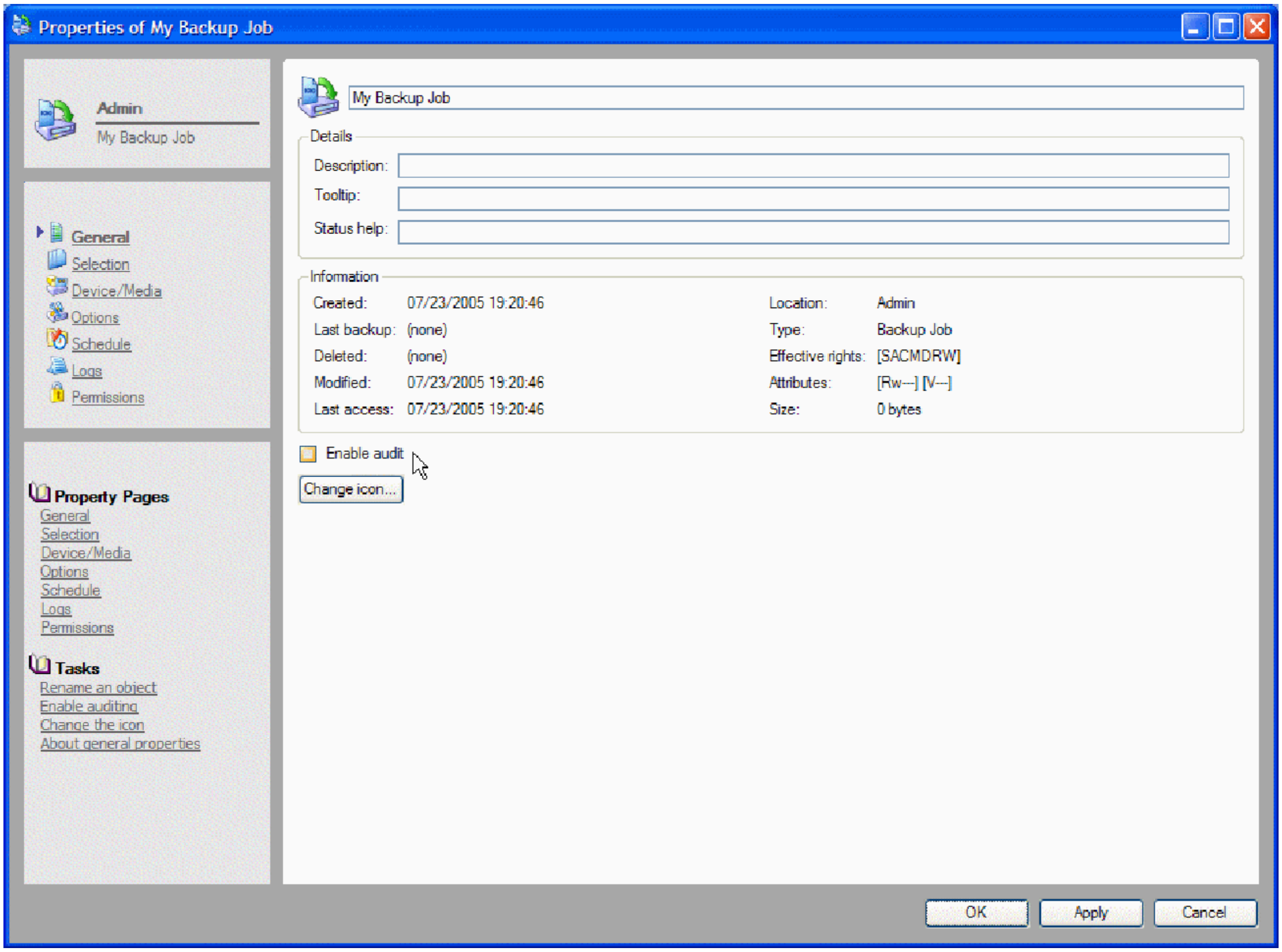
Some files, such as databases, are mission critical and regular backups of these files are essential. It is also essential that system administrators be able to verify that these files have been regularly backed up. The Data Protector Express *audit trails* feature allows you to collect, store and print such information about selected files and databases.

You can use the Data Protector Express audit trails feature to track how often and when a file, folder, volume or database is backed up, verified and restored. Data Protector Express will create an *audit trail* for each object for which auditing is enabled. Each time an action is performed on this object, the audit trail or log is updated with information about when that object was backed up, restored, and so on. The audit log also includes information about the media on which versions of a file are stored.

By default, auditing is disabled for most objects. To create an audit log for an object, you check **Enable Audit** on the **General** property page.

Auditing is turned on for User, Exchange, and SQL objects by default. For objects that can be backed up (for example, Exchange, SQL), turning on the auditing flag for the object causes a special job log entry to be made when that object is backed up. This feature calls your attention to important items, to confirm they have been backed up, even if they don’t have logging turned on.

NOTE: **Enable Audit** does not apply to all objects in Data Protector Express. If **Enable Audit** does not appear on the **General** property page of the selected object, this setting is not available for that type of object.



My Backup Job

Details

Description:

Tooltip:

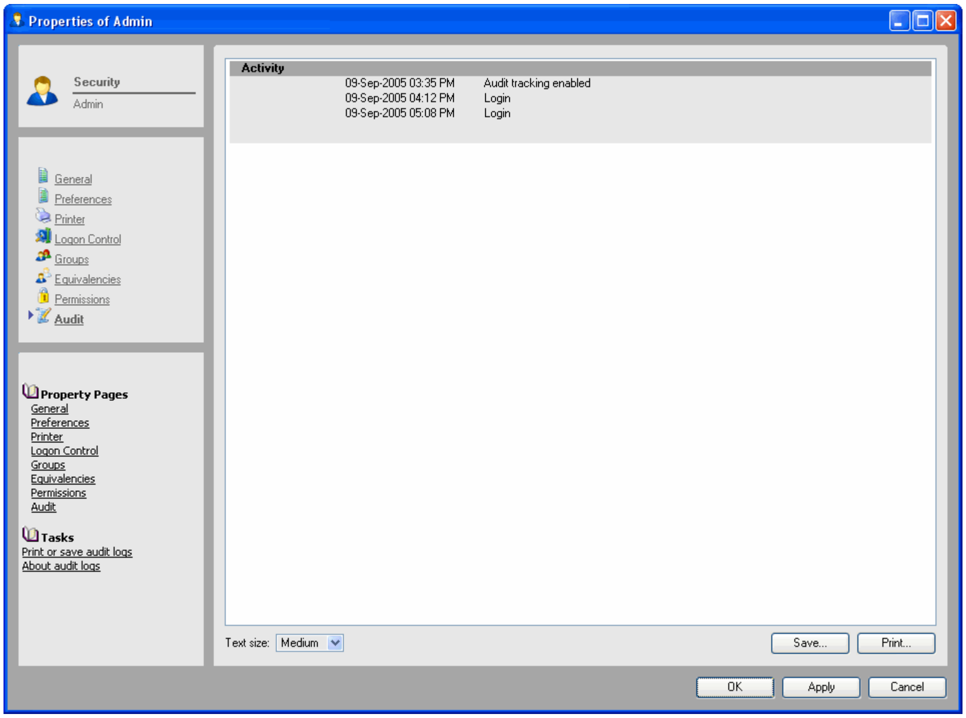
Status help:

Information

Created:	07/23/2005 19:20:46	Location:	Admin
Last backup:	(none)	Type:	Backup Job
Deleted:	(none)	Effective rights:	[SACMDRW]
Modified:	07/23/2005 19:20:46	Attributes:	[Rw--] [V--]
Last access:	07/23/2005 19:20:46	Size:	0 bytes

☐ Enable audit

When the audit log has been enabled for an object, a new page appears in the list of property pages, the **Audit** page. Click on this page to view the audit trail of that object. You can also print the audit log or save it to a file.



Activity

```
09-Sep-2005 03:35 PM    Audit tracking enabled
09-Sep-2005 04:12 PM    Login
09-Sep-2005 05:08 PM    Login
```

Text size: Medium

Chapter 10: Managing Devices and Media

In Data Protector Express you can manage backup devices and media to make the best use of available resources. With Data Protector Express you can create a backup system that includes individual media drives attached to a local PC desktop, tape libraries with multi-terabyte capacities accessible by way of a company network, and virtual tape devices that emulate libraries and allow you to perform disk-to-disk backups.

This section discusses how to create and manage backup devices and how to create and manage media in Data Protector Express.

NOTE: Performing disk-to-disk (D2D) backups is a standard feature in Data Protector Express. Enhanced support for disk-to-disk-to-tape (D2D2T) backups and for disk-to-disk-to-any media (D2D2Any) backups are available based on the license that you purchase. See Disk-to-Disk-to-Any Backups on page 135 for more information about these backups.

In this section

- Disk-to-Disk Backups
- Disk-to-Disk-to-Any Backups
- Creating a Virtual Library
- Moving Backups From a Virtual Library
- Devices view and Catalog view

Backup Concepts

Typical backup operations copy files from a local hard disk or network to a physical backup device. Physical backup devices are varied: they can be as simple as a writable DVD drive, a single- or multi-cartridge tape device connected to a local machine by way of a SCSI cable, or as complex as a robotic library with storage capacity for 200 or more tapes and accessible over a network. All optical disks (CD-ROM, DVD, etc.) and tape cartridges have a limited capacity; that is, only a certain amount of data can be copied to them. Common capacity limits for tape cartridges are 40 GB, 80 GB, and so on. Compact disks and DVDs might store 700 MB or more of data.

NOTE: Storage capacity varies widely among manufacturers. To determine the maximum capacity of the tape cartridge, CD-ROM, DVD or other backup media that you are using, check with the manufacturer's documentation.

Alternative backup operations copy files from a local hard disk to other disk drives, either locally or across a network. Often referred to as disk-to-disk (D2D) backups, the destination for these jobs is actually a folder or other location on a hard disk or network drive. D2D backups provide increased speed and improved access to data for both backup and restore. Data Protector Express provides default support for D2D backups through the use of virtual tape libraries, drives, and cartridges.

To further enhance backups to disk is the ability to then transfer these backups from the disk location (virtual media) to physical backup media. Often referred to as disk-to-disk-to-tape (D2D2T), this process of backing up files first to a virtual device and then to a physical device creates a flexible backup and restore environment.

Disk-to-Disk Backups

Data Protector Express supports the creation of virtual backup devices on both a local hard disk or on a network. Virtual backup devices emulate standard tape libraries and can be set up with any number of storage slots. Once created, you can back up data to the virtual device (D2D) instead of to physical media. You can also select the virtual device along with other available physical devices and let Data Protector Express use it along with physical devices during normal processing of jobs.

Disk-to-Disk-to-Any Backups

Data Protector Express supports disk-to-disk (D2D) backups for high speed backup and restores. A common problem for D2D backup systems is how to represent and manage the backup disks. Simply copying files to a backup disk will eventually fill it up and additional backups will not be possible unless you manually delete backed up files that are no longer needed. What is required is an automated way to reuse space on backup disks. Data Protector Express provides this automation through the use of D2D libraries.

A Data Protector Express D2D library is functionally equivalent to a physical, or real, tape library. Like a physical tape library, a Data Protector Express D2D library has one or more tape drives and a set of storage elements (slots) containing tape cartridges. These tape drives, storage elements, and tape cartridges are all virtual (that is, they appear to be real tape drives, storage elements, and tape cartridges to Data Protector Express, but they are not real devices or media and only exist within Data Protector Express). All operations, such as backup, restore, and most media operations, can be performed using the D2D library.

To perform D2D backups, simply create a regular backup job and select a D2D library as the backup device.

To illustrate how Data Protector Express D2D libraries automate reuse of space on backup disks, consider of a backup job using a Simple-12 media rotation schedule and a D2D library as the backup device. A Simple-12 media rotation schedule will use 4 tapes (or tape sets) for daily incremental backups, 4 tapes (or tape sets) for weekly full backups, and 4 tapes (or tape sets) for monthly full backups. This provides full data recovery for the previous week, plus end-of-week backups for the previous month, plus end-of-month backups for the previous 4 months. In this example, the backup job will use 4 (virtual) tape cartridges for monthly full backups over the first 4 months. Thereafter, it will overwrite (or reuse) the oldest monthly backup to create new monthly backups. This will automatically reclaim space on the backup disks used by the D2D library.

To create a D2D library run the Create D2D Library wizard from the **Wizards** view.

Creating a Virtual Library

1. Open the **Favorites** desk bar, **Wizards**, and **D2D Device** to display the **D2D Device** wizards.
2. Select the **Create Virtual Library** wizard to create a new virtual library.

3. Enter a name for the library then select a machine where the library will be located.

   Use the **Browse** button to select a machine within the Data Protector Express management domain.

4. Select **Next** to move to the **Configuration** page of the wizard

5. Enter or scroll to the desired number of tape drives and storage slots (tape cartridges).

   Selecting 2 or more tape drives can improve performance by allowing multiple concurrent backups to occur to the virtual library.

6. To complete the configuration select the desired storage folder to use. Select **Add** to create additional storage folders or select an existing one.

   A dialog box appears.

   Use the **Browse** button to locate a folder on the network that you want to use as a storage folder. You can add a maximum of eight folders. Set the size of the storage folder. Size is measured in Gigabytes.

   Set the minimum disk space in Megabytes.

   Click **OK** to accept the folder and return to the previous screen.

   NOTE: HP recommends that you select a storage folder with at least as much free space as data you are planning to back up. This insures that all backups will succeed without exhausting all available disk space. Select storage folders on a different disk drive from the disk drive containing the data you are backing up. This enhances performance and insures data recovery if the source data disk fails.

7. Optionally specify the maximum tape cartridge capacity and the Secure Erase policy. Setting the maximum cartridge capacity ensures that the no single virtual tape cartridge consumes the entire capacity of the storage folder.

   If Secure Erase is enabled, each time data is deleted from a tape cartridge in a virtual library, the underlying disk storage is overwritten to insure that the original data is no longer present in the storage folder (i.e., on any backup disk).

8. Click **Finish**.

The virtual library will be available for future jobs. To view details about the virtual library, select it from the **Devices** view of the **Administration** desk bar.

Moving Backups From a Virtual Library

If you have purchased the D2D2Any option, you can automate the process of moving backup data from a virtual library to any other backup device, including another virtual library. When the D2D2Any option is enabled, you will find additional options on the virtual library wizard or configuration page.

The first option is to select the desired copy device. This is where backups written to the virtual library will be copied.

The remainder of the configuration options are the default media policies for backups to a virtual library that has been set up to support disk-to-disk-to-any backups. These options can be overridden for each virtual tape cartridge by accessing the property pages of individual virtual tape cartridges.

Copy policy: This setting determines whether or not to copy backups written to a virtual tape cartridge. If set to **Copy to device** then backups written to the virtual tape cartridge are copied to a destination device. If set to **Do Not Copy**, then backups written to the virtual tape cartridge are never copied to the copy device. You can optimize the use of the copy device and its media by selectively copying backups to it. For example, you may decide to copy only weekly or monthly full backups to the copy device, and leave daily incremental backups on the virtual library. This policy would reduce the number of media required for the copy device.

CAUTION: If you select the **Do Not Copy** policy, then the only version of the backup data is on the virtual library. If the disks on which the storage folder resides crash, then data may be permanently lost.

Destination device name: This setting determines the destination device for backups that are stored on this virtual library. Use the **Browse** command to locate a device that is available in the Data Protector Express management domain. HP recommends that you select specific devices instead of selecting any device on the network. You can also select or exclude different types of devices instead of selecting specific devices. You can select or exclude all tape devices, all virtual libraries, or all CD/DVD devices. This setting is applicable only if the copy policy is set to **Copy to device**.

Delay: This setting determines how soon following the completion of a backup job to perform the copy operation. This timeout (or delay) is only applicable if the copy policy is set to **Copy to device**. Enter or scroll to the number of minutes following a backup to start the copy operation.

Retention policy: This setting determines how long data is retained on the virtual library. There are three options for the retention policy.

- **Retain data until overwritten:** Backup data will be retained in the virtual library until it is specifically overwritten or erased by a backup or media job. This is a good policy to use for backups that you want to stay “online” for fast restores from a virtual library at any time.
- **Retain data until copied:** Backup data will be retained in the virtual library until it is successfully copied to the copy device. In this case, space in the storage folder will be freed up after the copy operation completes. This is a good policy to use if you want to fully optimize the use of space in the storage folder.
- **Retain data until space is needed:** Backup data will be retained in the virtual library until it is successfully copied to the copy device, and the storage folder is not full. If during a subsequent backup the storage folder becomes full, the backup data will be automatically deleted from the storage folder to make room for the new backup. Only backups that have been successfully copied to the copy device will be removed under this policy. This policy is the best one to use for normal operations. It will provide the best balance of retaining backups in the virtual library and optimization of storage folder space. Data will be removed from the storage folder following least-recently-used (LRU) order.

Copy log options: Use this command to set up the log options for each copy job. Identical to the Log options command on the **Options** property page of any job, you can set up a log that Data Protector Express will save, print or email to a designated user each time a copy job is run. For more information about job logs, refer to *Log options* on page 108.

When a backup is copied under the D2D2Any option, every object (file, folder, etc.) in the original backup is copied to the copy device, and each version is recorded in the Data Protector Express catalog. Upon normal restores, Data Protector Express will automatically select the most current version of an object to restore, regardless of the media on which it resides. Data Protector Express makes this selection based on the time and date that the object was backed up, and the most efficient device/media to get it from.

In the case of backups done under the D2D2Any option, upon a restore, Data Protector Express may discover the desired object to be on a virtual library virtual tape cartridge, on media written to the copy device, or both places. If it is found in both places, restores will normally come from the virtual library as it is usually the most efficient device to restore from. In the case of a backup that has not yet been written to a copy device (either the time out has not occurred, the policy was set to **Do Not Copy**, or the copy operation failed), then the restore will come from the virtual library. For cases when the data has been removed from the virtual library (the **Copy** policy is selected, and either **Retain data until copied** or **Retain data until space is needed** options is selected and data has been removed from the virtual library), the restore will come from the copy device.

The Data Protector Express D2D2Any option not only optimizes space usage in storage folders, it also optimizes the use of media/storage in the copy device. When data is automatically copied from a virtual library to the copy device, Data Protector Express remembers the source and destination media (tapes). The D2D2Any option “remembers” or “associates” these media so that the destination media is retained (and not erased or overwritten) until the source media is erased or overwritten. To illustrate this concept, consider a backup to a virtual library that’s subsequently copied to a physical tape cartridge in a physical loader. When this happens, Data Protector Express will associate the physical tape cartridge with the virtual library virtual tape cartridge. Regardless of the retention policies on the virtual library virtual tape cartridge, the associated physical tape cartridge must not be erased or overwritten by any other backup or media job until Data Protector Express determines that the data can be safely overwritten. The D2D2Any option determines that it is safe to erase or overwrite the physical tape cartridge when the original backup has been erased or overwritten under a regular tape rotation schedule.

The “association” described in above is very important for managing and optimizing physical media usage. For example, without this capability each backup to the virtual library under the D2D2Any option would eventually lead to consuming another physical tape cartridge, ultimately consuming all available physical media. Knowing when it is safe to reuse physical media is critical for a cost effective automated disk-to-disk-to-any solution.

The “association” is accomplished by Data Protector Express when the copy operation is successfully performed. When this happens, the virtual tape cartridge (media) for the virtual library is converted to a D2D media folder, and the physical media where the backup was copied is moved into this folder. A D2D media folder acts as both a piece of media and a media folder. If the D2D media folder is erased or overwritten, this is the signal to Data Protector Express that the associated physical media can be safely erased or overwritten. If you want to retain the backups on the associated physical media indefinitely, then simply move the associated physical media out of the D2D media folder. In this case, the associated physical media will not be erased or overwritten unless you specifically create a backup or media job to do that.

Example 1: Virtual backups of a laptop hard disk while an employee travels

An employee who uses a laptop travels frequently on business. While away from the office he uses Data Protector Express to run daily incremental backups of data files to a local virtual device. These incremental backups are relatively small, but they provide him with access to backups of his work in the event that he deletes his work while away from the office and unable to back up his system on the network. When he returns to the office he connects the computer back to the network, runs a full backup to physical backup devices and copies the incremental backups from virtual to physical media.

In this example, the backups on virtual media have become obsolete since they are now available on physical media.

Example 2: Limited physical backup devices

A small company has a limited number of backup devices. Recently the company has expanded and now has more employees backing up data to these physical devices. Backups are beginning to exceed the physical media capacity. Some backups halt during processing so that an operator can insert additional media into the devices. Backups that could be performed unattended now require an operator to be present.

To ease the burden being placed on both the physical backup devices and the IT support staff, the company instructs the Data Protector Express administrator to create a virtual device on the network. The backup jobs are modified to use this virtual device as the backup destination. If D2D2Any backups are available, you can create rules that transfer the backups from virtual devices to physical media on a staggered schedule. This schedule permits the IT staff to monitor the physical media, swapping out full media as necessary, and keeping the backups running smoothly. In standard D2D backups, you can copy data from virtual media manually.

In this example, a growing company needs the capacity of an expensive library but cannot yet include it in their budget. By creating a virtual library, or a series of them, the company gains the advantages of the larger storage capacity of a library without breaking its budget.

Example 3: Creating redundant backups to ease data restore operations

A large company wants to develop a data protection system that includes full data protection but that also eases the burdens on their IT support staff when minor data restore jobs arise. To do this the company creates a network virtual library and directs all backups to this destination instead of to physical media. Each week these backups are transferred to physical media. Rules are set in Data Protector Express to retain the backup data on the virtual media for a minimum of two weeks before deleting it if the virtual storage is required for current backups.

An employee discovers that a critical data file has been damaged, so she creates a restore job in Data Protector Express. Since Data Protector Express tracks of the location of each backup version in the Data Protector Express catalog, the restore job sees that identical versions of the file exist both on virtual and physical media. The physical media is no longer in a physical device and an IT staff member would have to locate it to do a restore from it. Instead of waiting for another staff member to locate the physical media, Data Protector Express restores the file from the virtual media and the employee can continue her work.

In this example, the company created redundant backups that made it possible for an employee to restore data files without involving support staff.

Devices view and Catalog view

The first time you open Data Protector Express, Data Protector Express recognizes any installed devices — virtual or physical. Data Protector Express provides an intuitive user interface to set up and monitor these devices. From the **Devices** view you perform physical operations with the backup device, such as creating or configuring a device or erasing, formatting and ejecting media. (See *Managing Devices with the Devices View* on page 141.) Using the **Jobs and Media** view, you can create media folders and media in the Data Protector Express catalog and delete them from the catalog as well. (See *Managing Media with the Jobs and Media View* on page 147.) The **Catalog** view displays all of the objects in the Data Protector Express catalog in one location. (See *Catalog View* on page 151.) Many commands can also be executed from this view.

The **Jobs and Media** view displays media folders and media objects. You can use this view to work with these catalog objects. For example, you can create and delete media folders, as well as create and delete media objects, such as tapes. The **Devices** view, on the other hand, is used to perform physical operations with the backup device. For example, media can be erased and formatted from the **Devices** view.

The difference between the **Jobs and Media** view and the **Devices** view is significant: the **Jobs and Media** view is used to make changes to the catalog while the **Devices** view is used to perform operations using the physical or virtual devices themselves (both media and drives). When you want to make changes to the catalog, use the **Jobs and Media** view. When you want to work with the physical media or with the device itself, use the **Devices** view. For example, if you want to change the name of a tape, you make that change on the **Jobs and Media** view because you are making a change to the Data Protector Express catalog. However, if you want to identify a tape by reading its header, you must use the **Devices** view.

The **Catalog** view displays all of the objects in the current catalog. This may be useful, on the one hand, because you will be able to see and work with all the catalog objects at once. On the other hand, because all of the objects are displayed, it may be difficult to work with this view efficiently.

Managing Devices with the Devices view

Data Protector Express recognizes any installed device that is part of the Data Protector Express management domain and displays them on the **Devices** view. You can use the **Devices** view to perform operations on any physical or virtual device in the current Data Protector Express management domain.

Any backup device in the current Data Protector Express management domain can be displayed in the object detail area. Note that this view displays two separate types of objects: controllers and devices. Controllers are usually the physical adapters in your machine that connect Data Protector Express to your physical devices; devices are the actual physical or virtual devices. In the Data Protector Express catalog, controllers work like containers in which multiple devices of the same model and manufacturer are stored.

When you work with devices on the **Devices** view, you select the *device*, not the controller, in the object detail area (or from the hierarchical tree view).

Note that libraries have two or more drivers associated with them: the Library driver and one or more device drivers. In general, many commands on the **Devices** view can be performed with any one of the drivers selected. (Models and manufacturers vary.) However, if your library supports multiple devices (for example, it has more than one tape read/write device) and you want to use a specific device, you must select that device driver to use it. If you select the library driver, Data Protector Express will use the first available device in the library it finds.

Restarting failed devices

Sometimes you will need to restart a device that has, for some reason, failed to initialize properly. A device may have stopped for any number of reasons, such as a power failure or a connecting cable malfunction. Virtual devices on a network appear disabled if the network connection has failed.

When a device is not initialized, it appears with a yellow warning icon. Some devices may take some time to initialize, during which the warning icon will continue to appear. If a device shows the warning icon after it is initialized, press **F5** to refresh the device display.

Devices with a yellow exclamation mark are not initialized

If there is some other problem with the device or the controller, the warning icon will not disappear. You must identify and correct the problem yourself. Then you must restart *both* Data Protector Express and the Data Protector Express service. When Data Protector Express restarts, it will initialize the device driver again. Check the **Devices** view to see that the devices are now properly working and that they no longer display the warning icon. Any duplicate or old devices that are offline can be deleted from the **Catalog** view.

To restart failed devices

1. On the **Administration** desk bar, select the **Devices** view.
2. In the main object detail area, right-click the machine and select **Rescan for New Devices**.
3. Click **Yes** to confirm that you want to scan for devices.

   Once located, new devices or restarted devices appear in the **Devices** view.

Configuring physical devices

Because physical devices are already configured by the manufacturer, they do not need to be configured in Data Protector Express. You can, however, perform other operations for physical devices like enabling auditing and granting or revoking permissions to a device. Open the **General** or **Permissions** property pages to change these settings.

For special issues related to libraries, see *Appendix B: Troubleshooting Guide*.

Viewing diagnostic information

To view diagnostic information for a device

1. Open the **Favorites** desk bar and select **Devices**.
2. Locate the virtual device on the network or local machine.
3. Right-click the device and select **Diagnostics**.
4. The **Diagnostics** property page appears.
5. Review the information and then choose one of these commands:
    - Click **Save** to save the file in one of the supported formats
    - Click **Print** to print the diagnostic information to a printer
    - Click **Email** to email the diagnostic information to the specified email address.

Restoring data from a virtual library

To restore data from virtual media you simply create a restore job. Data Protector Express keeps track of the location of backup versions on virtual and physical media. When you need to restore a file, Data Protector Express locates the most recent version of a file and restores it from the most convenient location.

For example, suppose you backed up a file to virtual media a week ago and Data Protector Express transferred that version to physical media two days ago. Today, when you need to restore the file, Data Protector Express locates these identical versions of the file and determines that no other more current versions exist in the Data Protector Express catalog. Restoring the file from the virtual media is quicker, so Data Protector Express restores that version of the file.

You cannot perform disaster recovery from a virtual library.

Devices view commands

After you have selected a device in the object detail area, you can perform physical operations with this device. Some of these operations affect the device itself, while others affect the current media in the device.

The following commands can be found on the **Commands** task pane. Many of them are also available from the shortcut menu.

NOTE: Check your hardware documentation to determine which of the following commands are supported by your device. If the command is not available, it will not appear on the shortcut menu. Some commands are not required for virtual devices.

For a complete list of available commands, see *Media job wizards*.

Eject Media or Loader Magazine command

You can use this command to eject media from the selected device or eject media magazines from the selected library. If this command is missing, either your device does not support this command or no device is selected. Some device magazines will not be ejectable.

CAUTION: When you eject virtual media, you cannot retrieve it. Be sure that the data contained on the virtual media has been transferred to physical media or is no longer needed before you eject virtual media.

Rewind Media command

You can use this command to manually rewind tapes in the selected device. If this command is missing, your device does not support this command.

NOTE: This command does not apply to virtual media.

Retension Media command

The **Retension Media** command increases the tension of the current tape in the device by fast-forwarding the tape to the end of the tape and then rewinding it to the beginning. This command can be useful in some circumstances. Occasionally when a tape is repeatedly fast-forwarded and rewound for only short distances, tension differences develop in the tape that cause the tape drive to falsely believe it has reached the end or beginning of the tape. By increasing the tension on the tape, you can sometimes make an otherwise unusable tape operational again.

NOTE: If you need to retension tapes regularly to use them, consider servicing your tape drive or replacing your tapes.

NOTE: This command does not apply to virtual media.

Erase Media command

This command erases the media currently loaded in the selected device. It has the following options:

- The **Quick Erase** option erases the first block and then writes an END OF DATA marker to that first block. The other blocks of the tape are not erased, but when that tape is read, Data Protector Express treats it as if it were blank because it encounters the END OF DATA marker in the first block.
- The **Secure Erase** option erases every block on the tape. This operation can be very time consuming, lasting several hours. However, it will physically erase every block on the tape. If you want to destroy sensitive data, use this command.

Some devices support both options; some support only one of the two erase options. If an option is not available, the selected device does not support that option.

Format Media command

You can use this command to format media currently loaded in the selected device.

When you format new media, Data Protector Express opens the **Format Media** dialog box. Use this dialog box to name the media and select a media folder in which to store the media. Data Protector Express will format the media currently loaded in the device you select. If you select a library, select the storage slot that holds the media you want to use. This command also initializes virtual media.

When you format media, you can also assign the media a password. See *Media passwords* on page 150 for more information.

To format media

1. Select **Devices** from the **Favorites** desk bar.
2. Locate and select the device with the media to format. To format all media simultaneously, click **Select All**.
3. Format the new media in one of these ways:
    - Right-click on the selected devices and select **Format** from the shortcut menu
    - Select **Format Media** from the **Commands** task pane
4. Expand the tree and select the device or library and storage slot that holds the media you want to format.
5. If you want to assign a password to the media, click the **Media Password** button and then enter and confirm the password in the **Media Password** dialog box.
6. Click **Finish**. Data Protector Express formats the specified media.

Import Media (into the catalog) command

This command allows you to use data on media that was created in another Data Protector Express management domain or by another software program. To use media that was not created in the current catalog, you must import that media into the current catalog.

You might import media in one the following situations:

- To use media created by an earlier version of Data Protector Express.
- To use media created in a different Data Protector Express management domain.
- To use media created by another backup program.
- To use media accidentally deleted from the catalog.

When you import media, you must supply the media password. No password is required if the media has no password.

NOTE: Previous versions of Data Protector Express automatically assigned PASSWORD as the default media password. If you are having trouble importing media created with an earlier version of Data Protector Express, try using PASSWORD when prompted for the media password.

Data Protector Express will not perform any other operations while it is importing media. Additionally, the process may last several hours. Before you import media, be certain that there is sufficient time to complete this lengthy process. Additionally, you will want to be available to log out of Data Protector Express when the import is complete, in order that the security of the network is not compromised.

To import media

1. Select **Wizards** from the **Favorites** desk bar.
2. Display the **Media** wizards in the list of available media wizards.
3. Select the **Import Media** wizard.
4. Follow the instructions to select the media to be imported and to schedule the job.
5. If you schedule the job to run now, it will start as soon as you click **Finish** on the last screen of the wizard.

Restore Catalog command

The **Restore Catalog…** command provides a quick method of restoring your current catalog, e.g., in case it has been corrupted. Use this command only when your current set of media is intact. For example, you might use this command if the Data Protector Express backup server has crashed.

The **Restore Catalog…** command differs significantly from the **Import Media…** command. The **Restore Catalog…** command *replaces* the current catalog with the last known good catalog on that media. The **Import Media…** command, on the other hand, *does not replace* the current catalog; it only adds additional data to it.

The advantage of the **Restore Catalog…** command is that it provides a quick and easy way to replace a lost or corrupted Data Protector Express catalog. (You could use the **Import Media…** command to restore a corrupted catalog, but this process is very time consuming and, if you have multiple tapes, might require many hours or even days.)

NOTE: All current information in the current Data Protector Express catalog will be lost when you use the Restore Catalog… command. This command does not append data to the current catalog; it replaces the current catalog with the last known good catalog on that media.

To restore a catalog

TIP: Use the **Restore Catalog** wizard to create a job that quickly restores the catalog from available media.

1. Locate the media on which you have backed up the catalog you wish to restore. Normally, this is the last backup job run.

NOTE: If you printed the log from the last backup job, you can identify the media which contains the catalog. To make certain the catalog is regularly backed up, check the Selection tab of the backup job to verify that the catalog for your storage domain is checked.

2. Insert the media into the appropriate backup device and then select it in the object detail area of the **Devices** view.
3. Select **Restore Catalog…** from the **Commands** task pane or the shortcut menu.
4. Select the device or library and storage slot from the tree.
5. In the **Catalog to Restore** field, select from the following restore modes.
    - Select **Any** to restore any catalog version stored on the selected media.
    - Select **Latest** to restore only the most recent catalog stored on the selected media.
6. Click **Start**.
7. Exit Data Protector Express to finish the restore process. When you restart Data Protector Express, the catalog will be restored.

NOTE: If Data Protector Express is running as a service, you must stop and restart the service. Use the Data Protector Express Service Control Manager to start and stop the Data Protector Express service.

Clean Device command

The **Clean Device…** command will run the backup device through a cleaning cycle.

This command is supported only by libraries. If a device in a library provides notification that it needs cleaning and the library has a cleaning cartridge available, a cleaning cycle will be performed automatically at the start of a backup job. If you are using a device that is not a library, you must manually clean the device at the manufacturer's suggested intervals.

To clean a device in a library, highlight the device and select **Clean Device…** from the **Device** menu. Data Protector Express will check to see if one of the slots holds a cleaning cartridge. If it does, the cleaning cycle will be performed in the background; if not, an error message is shown.

If the **Clean Device…** command is missing, it is not available for your backup device. In this case, a cleaning cycle can often be performed by manually inserting a cleaning cartridge into the backup device.

Identify Media command

Use this command to get the name of the media currently loaded in the device. Data Protector Express tries to identify the tape or other media that is currently loaded in the device. If Data Protector Express cannot identify the media, it reads the media header, a process that may take up to several minutes. The name of the media appears on the log file for the media job.

Sort Media command

Use this command to reorganize the media in a library. Data Protector Express can sort the media by name or by bar code in ascending or descending order.

Testing a library or a device

To perform a test on a library, to move or format media contained in a library, or test a device, select a media wizard from the **Wizards** view on the **Favorites** desk bar. For more information about media wizards, see *Media job wizards* on page 27.

Test results

The following test results appears on the status page as you run media jobs.

Element status

Shows information about the current magazine in the library.

Device/Storage: Specifies the device or the storage slot.

- **Dev …:** A tape drive used to read any media contained in a storage slot. The number of available tape devices depends on your library configuration.
- **Storage #:** A slot that holds media that may be used by the Data Protector Express management domain or that is reserved for other purposes.
- **Import/Export #:** A slot that is used to transfer media between storage slots, import/export slots and tape drives.

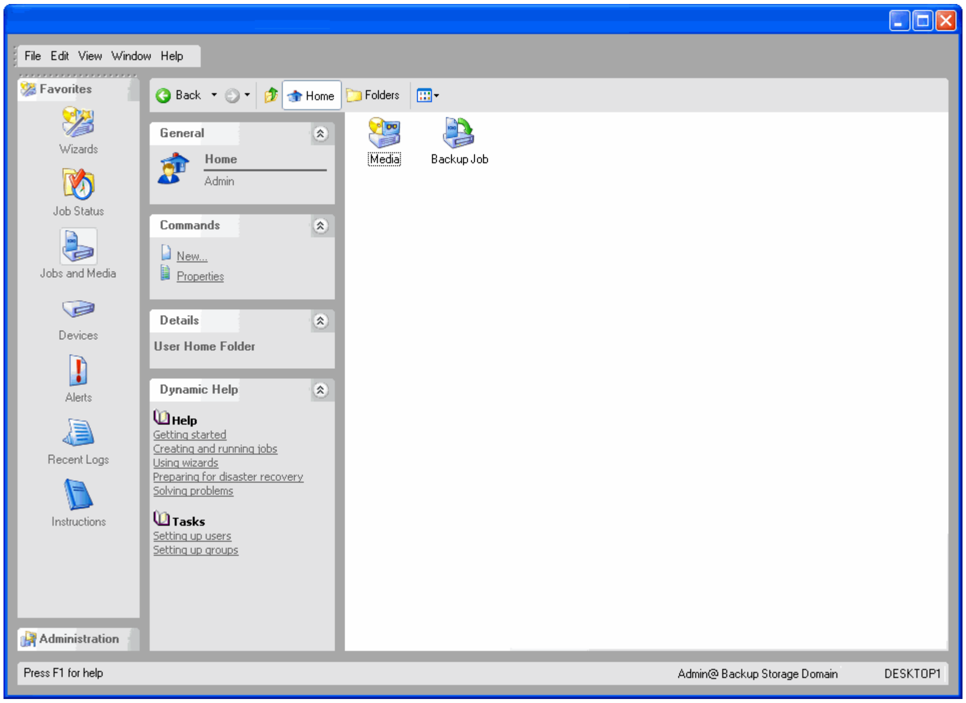
Status: Shows the current or likely status of the device or storage slot.

- **Valid:** The slot is known to hold media that is in the current catalog.
- **Probably Valid:** The slot held valid media previously. Data Protector Express verifies that the media is valid before using it. When you exit and restart Data Protector Express, media marked Valid is reset to Probably Valid.
- **Invalid:** The slot holds media that is definitely not in the current catalog.
- **Probably Invalid:** The slot holds media that may not be in the current catalog. When you exit and restart Data Protector Express, media marked Invalid is reset to Probably Invalid.
- **Empty:** The slot is either known to be empty or a user changed its status to Empty.

- **Probably Empty:** The slot was empty previously. When you exit and restart Data Protector Express, slots marked Empty are reset to Probably Empty.
- **Unknown:** The status of the slot is not known, usually because it has not been used yet.
- **Cleaning Tape:** A user marked the slot as holding a cleaning cartridge. The number of remaining cleaning cycles also appears. Data Protector Express does not verify that a cleaning cartridge was, in fact, inserted into this slot.
- **Probably Cleaning Tape:** The slot previously contained a cleaning tape. When you exit and restart Data Protector Express, slots marked Cleaning Tape are reset to Probably Cleaning Tape.
- **Reserved:** The slot was disabled by a user. Data Protector Express will ignore it during any job. You can only change the status of a reserved slot. Data Protector Express changes the status of all other slots during normal operations.

Managing Media with the Jobs and Media View

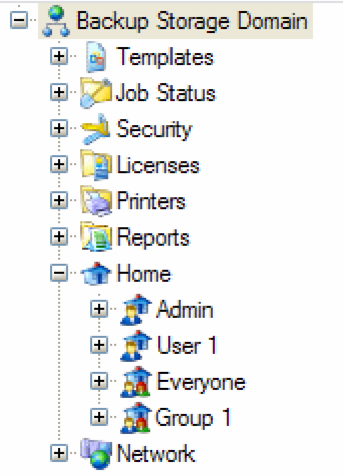
The **Jobs and Media** view displays media folders and media objects in the Data Protector Express catalog. You can use this page to work with these catalog objects. For example, you can create new media folders and media objects on this page, as well as delete media folders and media.



Although you can manipulate media and media folders on the **Jobs and Media** view, many of these operations are normally handled automatically by Data Protector Express. For example, when you run a job that includes media rotation, Data Protector Express will automatically create any new media and media folders needed for that job. As tapes and other media are overwritten and deleted from the catalog, these changes are automatically reflected on the **Jobs and Media** view as well.

Creating media folders

You might wish to create a media folder in which to store media before you create and run a backup job. Note that Data Protector Express automatically creates new media folders when it runs either a job with media rotation. Data Protector Express will create a media folder in the User/Group folder and give it the name of the scheduled backup job. However, if you run a manual job that is not scheduled, you may want to create a new media folder in which to store the new media for that job. For more information on automatically creating media folders, see *Backup options automatically updated* on page 112.



To create a new media folder

1. Select the existing folder in which you want to store the new Media folder. (It cannot be the Home folder.)
2. Create the new media folder in one of these ways:
    - Select **New Object…** from the **File** menu and then select **Folder** from the **New Object** dialog box, or
    - Right-click in the Data Protector Express object detail area and select **New..** and then **Folder** from the shortcut menu, or
    - Click the **New Object** button on the toolbar and then select **Folder** from the **New Object** dialog box.
3. Type in the name of the new folder in the New Object window.

TIP: After creating a new folder, be certain to specify which users have permissions to it. This is the simplest and fastest way to assign permissions to multiple objects stored in the folder.

Deleting media folders

When you delete a media folder, you also delete all of the objects contained within it, including any media folders and media. You might want to delete media folders that were used by jobs you no longer plan to run and that contain media that are no longer in use.

To delete media folders, select the folder and then select **Delete** from either the **Edit** menu or the shortcut (right-click) menu. Alternatively, you can click **Delete** on the **Command** task pane.

Before deleting any media folders, you might want to move any media stored in those folders to another folder. For example, you might create a new folder named **Old Media** and move any currently unused media to this folder before deleting the media folders.

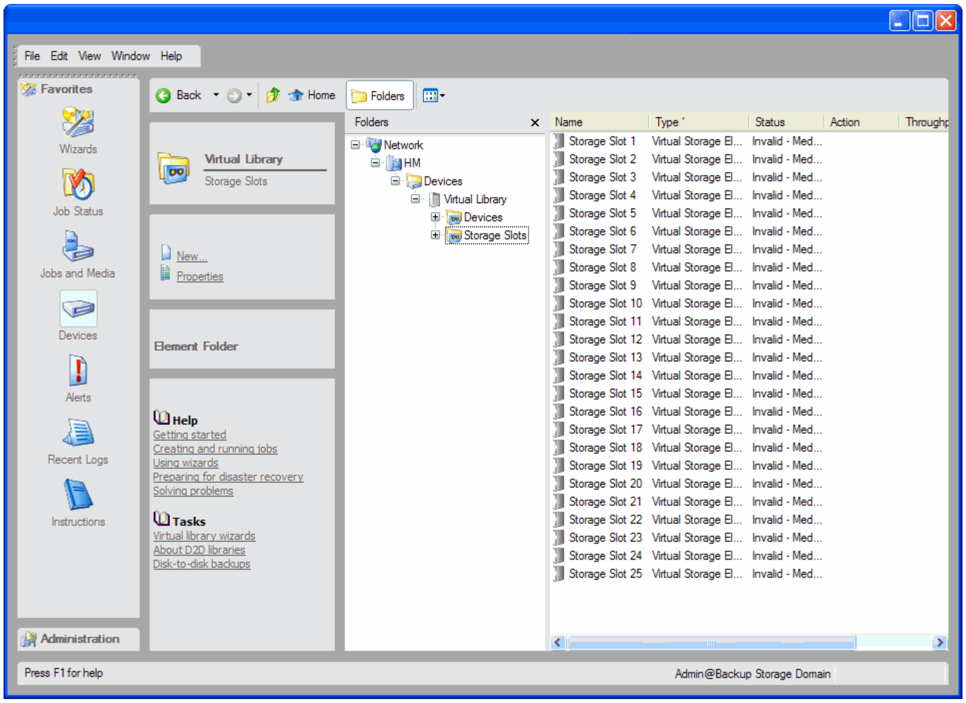
Creating new media

Data Protector Express automatically creates new media when it runs backup jobs that use blank media or any overwrite setting. However, there may be occasions when you may want to manually create new media prior to running the job. For example, you might be recycling old tapes you no longer use. To be certain that the tapes are labeled correctly and that no tapes are inadvertently overwritten, you can manually create new media before running the job.

Note, however, that for jobs that use automatic media rotation, Data Protector Express looks for media with specific names in specific folders. If it does not find the precise media it is looking for, Data Protector Express will display an alert. For this reason, it is best to let Data Protector Express automatically create its own media for automatic rotation jobs than to manually create the media in advance.

When you create new media, Data Protector Express (1) creates a new catalog object and (2) physically formats the current media in the device. This will cause any current data on that media to be erased. When you create new media, be certain that the media Data Protector Express will format is no longer needed.

When you format the new media, Data Protector Express opens the **Format Media** wizard. Use this wizard to name the media and select a media folder in which to store the media. You must also select a device. Data Protector Express will format the media currently loaded in the device you select. If you select a library, select the storage slot that holds the media you want to use.



Name	Type '	Status	Action	Throughp
Storage Slot 1	Virtual Storage El...	Invalid - Med...		
Storage Slot 2	Virtual Storage El...	Invalid - Med...		
Storage Slot 3	Virtual Storage El...	Invalid - Med...		
Storage Slot 4	Virtual Storage El...	Invalid - Med...		
Storage Slot 5	Virtual Storage El...	Invalid - Med...		
Storage Slot 6	Virtual Storage El...	Invalid - Med...		
Storage Slot 7	Virtual Storage El...	Invalid - Med...		
Storage Slot 8	Virtual Storage El...	Invalid - Med...		
Storage Slot 9	Virtual Storage El...	Invalid - Med...		
Storage Slot 10	Virtual Storage El...	Invalid - Med...		
Storage Slot 11	Virtual Storage El...	Invalid - Med...		
Storage Slot 12	Virtual Storage El...	Invalid - Med...		
Storage Slot 13	Virtual Storage El...	Invalid - Med...		
Storage Slot 14	Virtual Storage El...	Invalid - Med...		
Storage Slot 15	Virtual Storage El...	Invalid - Med...		
Storage Slot 16	Virtual Storage El...	Invalid - Med...		
Storage Slot 17	Virtual Storage El...	Invalid - Med...		
Storage Slot 18	Virtual Storage El...	Invalid - Med...		
Storage Slot 19	Virtual Storage El...	Invalid - Med...		
Storage Slot 20	Virtual Storage El...	Invalid - Med...		
Storage Slot 21	Virtual Storage El...	Invalid - Med...		
Storage Slot 22	Virtual Storage El...	Invalid - Med...		
Storage Slot 23	Virtual Storage El...	Invalid - Med...		
Storage Slot 24	Virtual Storage El...	Invalid - Med...		
Storage Slot 25	Virtual Storage El...	Invalid - Med...		

When you format media, you can also assign a password to the media. See *Media Passwords* later in this section for more information.

To create a new media

1. Select the existing folder in which you want to store the new media.
2. Create the new media with one of these ways:
   - Select **New Object…** from the **File** menu and then select **Media** from the **New Object** dialog box, or
   - Right-click in the Data Protector Express object detail area and select **New Media** from the shortcut menu, or
   - Click **New Object** on the **Command** task pane and select **Media** from the **New Object** dialog box.

3. Type in the name of the new media in the **Media name** field of the **Format Media** dialog box.
4. If the device you want to use is not displayed in the **Device** field, click the **Browse…** button and select the proper device from the **Browse** dialog box.
5. If you are using a library, select the library and the storage slot that holds the media you want to use.
6. If you want to assign a password to the media, click the **Media Password** button and then enter and confirm the password in the **Media Password** dialog box.
7. Click **Format**. Data Protector Express formats the specified media.

Media passwords

Whenever you format media, you can assign that media a password. By default, there is no password.

Media passwords are only required on one occasion: when media is *imported* from one catalog to another catalog. For example, you might import media from an earlier version of Data Protector Express to the latest version of Data Protector Express. Or, alternatively, you might want to transfer data from one Data Protector Express management domain to another Data Protector Express management domain. To prevent unauthorized transferring of tapes between secure Data Protector Express management domains, Data Protector Express lets you assign a password to any media you create. That password will be required before that media can be imported into a new catalog.

NOTE: Media passwords are the only security measure that prevents tapes from being imported into another catalog. For sensitive data, be certain that every media is assigned a password.

Whether or not you assign media a password depends on your particular security needs. Media that has no password can be easily imported into any catalog. If you do not assign the media a password, mere possession of the tape or media is enough to compromise the security of your data.

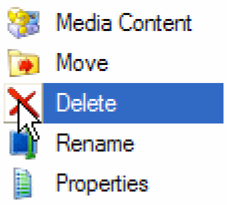
NOTE: Early versions of Data Protector Express automatically assigned **PASSWORD** as the default media password. If you are having trouble importing media created with an early version of Data Protector Express, try using **PASSWORD** when prompted for the media password.

Deleting media

When you delete media, Data Protector Express deletes information about that media from its catalog. This includes any versions of files stored on that tape, which are also deleted from the catalog.

Note however that deleting media does not physically erase the media. The media remains unchanged; only the catalog is changed. This means that you can still import that tape to another catalog or, if necessary, back into the original catalog.

To delete media, select the media you wish to delete and then select **Delete…** from the **Edit** menu or the shortcut (right-click) menu. Alternatively, you can click **Delete** on the **Command** task pane.



Media content

At any time, you can identify media or display the contents of any media in the catalog.

To create an Identify Media job

1. Select **Media** from the **Wizards** view.
2. Select the **Identify Media** wizard.
3. Follow the instructions to select the media to be identified and to schedule the job.
4. If you select Run now, the job will start as soon as you click **Finish**.

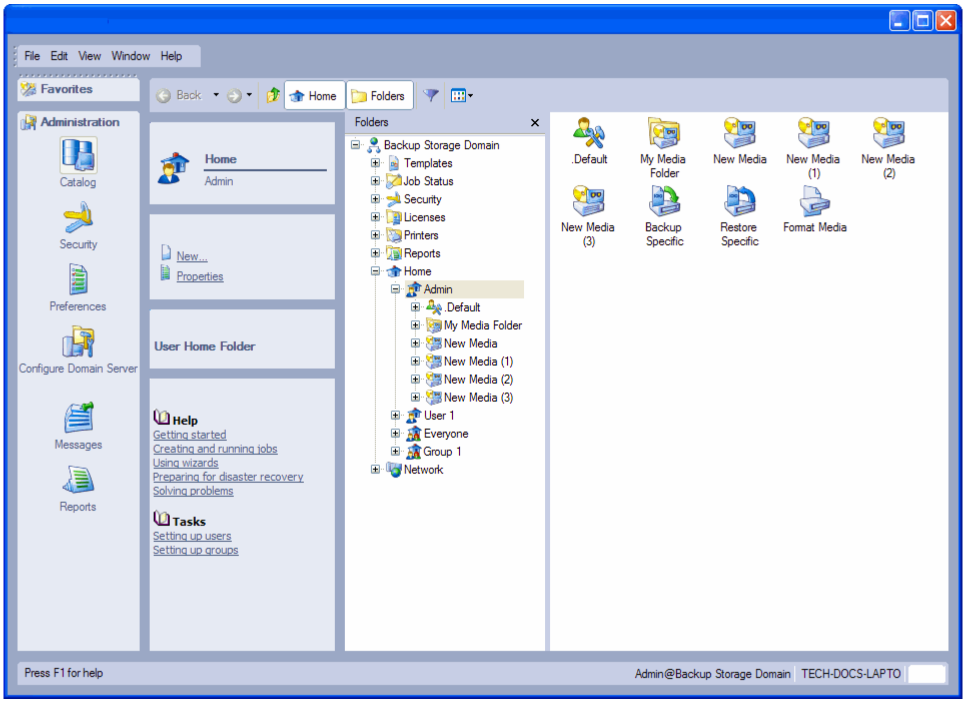
TIP: Use the **Run Repeatedly** schedule type to identify media in a library that changes media frequently throughout the day. This will speed up scheduled jobs and allow Data Protector Express to have current information about the content of media in each slot or device.

To create a Media Contents job

1. Select **Media** from the **Wizards** view.
2. Select the **Media Contents** wizard.
3. Follow the instructions to select the media for which you want to view the contents.

Catalog View

All of the objects in the current Data Protector Express management domain are displayed on the **Catalog** view. (Like other views, you will only be able to see those objects to which you have permissions.)



Many commands can be performed from the **Catalog** view, including all of the commands on the **Devices** view and the **Job Status** view. These commands include running jobs, stopping jobs, formatting media, and so on.

The advantage of the **Catalog** view is that it can display all of the objects in the catalog at once.

TIP: To minimize the number of files that appear in this view on larger systems, click the **Query** button and filter the list to display fewer items based on creation date or other criteria.

Chapter 11: Tips, Techniques and Strategies

This section contains information you can use to work more efficiently with Data Protector Express. The first sections explore managing the catalog and running jobs faster. The last sections of the section cover practical techniques for working with jobs.

In this section

- Tips for Managing the Catalog
- Strategies for Faster Jobs
- Working with Permissions
- Selecting Files for Jobs
- Restoring Tips
- Other Tips

Tips for Managing the Catalog

An important decision when planning a comprehensive backup strategy is where to locate the Data Protector Express catalog. This section explores some considerations you should review before making this decision.

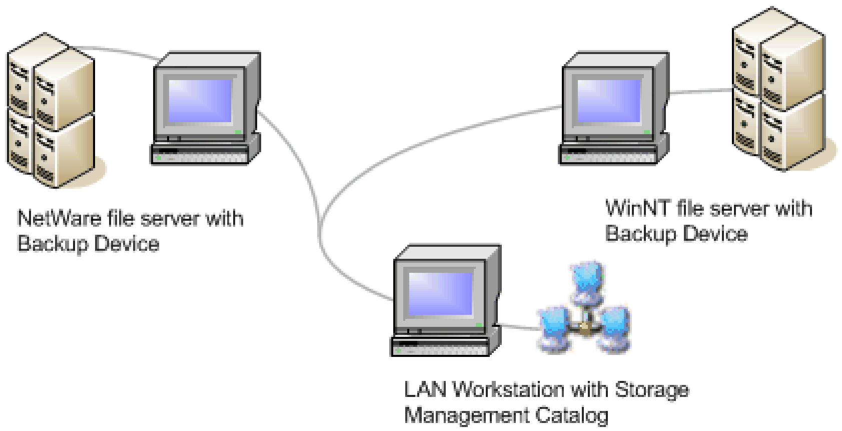
Where to locate the catalog

Consider locating the catalog on a PC desktop or file or application server other than the main file server.

Recall that Data Protector Express keeps track of objects and properties in a catalog that it creates and manages. Where should you store this catalog? That is, which volume and machine should be the storage management server?

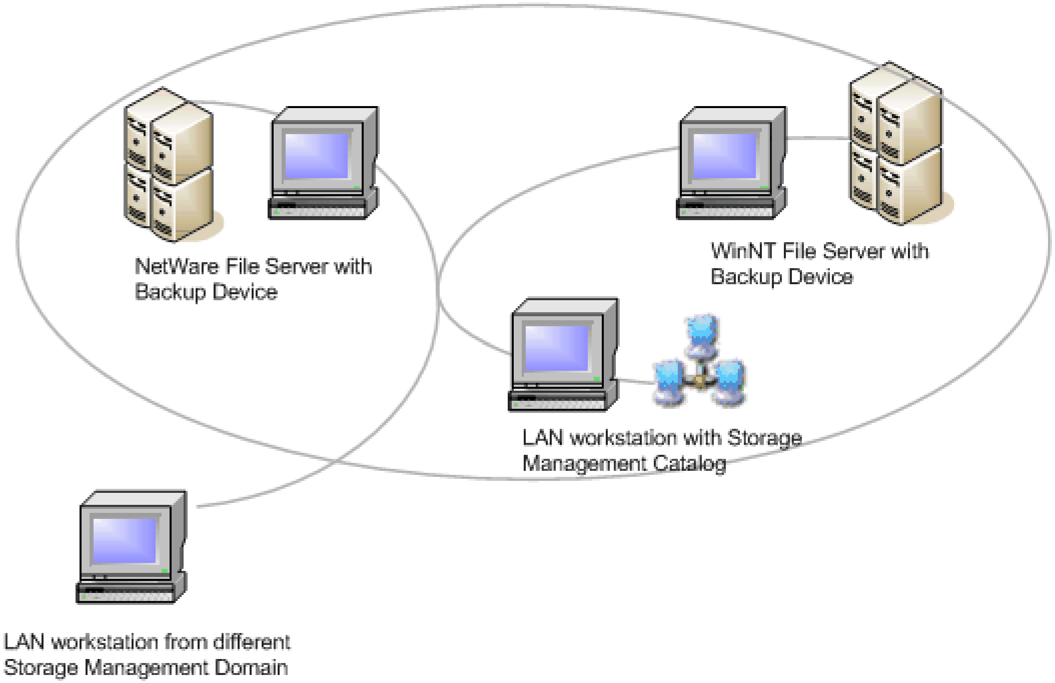
Data Protector Express lets you locate the catalog on any machine (PC desktop or file or application server) or volume in the Data Protector Express management domain. Note that the catalog does not have to be on the same machine to which the backup device is attached. It could be placed on any volume of any machine that is a member of the Data Protector Express management domain.

You can locate the storage management catalog on any machine in the network, including, in this case, a workstation. Attach the backup devices to machines using local buses for the greatest speed.


NetWare file server with Backup Device
WinNT file server with Backup Device
LAN Workstation with Storage Management Catalog

For example, suppose you have a file or application server with a large RAID device attached. Backup jobs using this RAID device will run fastest when the backup device is placed on the same machine as the RAID device. On the other hand, the catalog may be best located on another machine other than the file or application server. This is because if the file or application server were to become inoperable (for example, the drive were to fail), you would still be able to use the catalog to restore the file or application server volumes. Had the catalog been located on the file or application server, however, the catalog must first be restored before other files could be restored. This can be a lengthy, time-consuming process.

A good strategy to consider is to place the backup device on the file or application server for maximum speed, but to locate the catalog on a separate machine. Consider this example. Two file or application servers are connected on an Ethernet network. Each file or application server has its own backup device, which helps the jobs run faster and more efficiently. The storage management server for all three machines is located on a separate machine, which can be called a “storage management server.” Jobs can be run from this storage management server ; additionally, they can also be run from any other machine on the network as well.


NetWare File Server with Backup Device
WinNT File Server with Backup Device
LAN workstation with Storage Management Catalog
LAN workstation from different Storage Management Domain

NOTE: The backup device could have been placed just as easily on any other machine in the network. Data Protector Express does not require that the backup device be physically attached to a file or application server. Additionally, while the term “storage management server” is a convenient label, in fact, Data Protector Express does not require that this machine have a server operating system. It could just as well be a PC desktop.

This arrangement offers several advantages:

1. Jobs run quickly because most of the data is transferred over local buses, instead of over the network. In this arrangement, Data Protector Express will automatically route data from each of the file or application servers over local buses to its own backup device. Whenever there is a choice, Data Protector Express automatically routes data over local connections rather than network connections.
2. Administering jobs is uncomplicated. Jobs can be created and run from any machine on the network. Note that jobs can also be administered from a machine that is a member of a different Data Protector Express management domain. The Data Protector Express administrator or other user can log on to this catalog from another storage domain and then create and run jobs in that storage domain.
3. Suppose a disaster occurs and the RAID device of one of the file or application servers needs to be replaced. Because the catalog is located on another machine, recovery is quick and easy. The catalog contains all of the information necessary to restore the lost data. Had the catalog been stored on the file or application server, recovery would have been much more difficult. Note that the backup device on the other file or application server can be used to help restore the file or application server that failed.
4. Suppose the storage management server fails and the Data Protector Express catalog is lost. While the loss of the storage management server is significant, the file or application servers are not impacted and they can continue to perform their tasks. Backups can still be run from another machine on the network or, if need be, from the file or application servers themselves. Since the catalog was lost, it will have to be imported from existing tapes. This step, however, is not crucial and can be run when convenient, as long as careful backup procedures are followed (that is, no important tapes are overwritten and a full backup job is run immediately).

The advantages of this arrangement extend to any backup strategy or network arrangement. In general, consider placing the Data Protector Express catalog on a machine separate from the most important data. At the very least, consider locating the catalog on a separate volume.

For more information on restoring a corrupted catalog, see *Restore Catalog command* on page 145.

Accounting for catalog size

Before deciding where to locate the catalog, consider how large the Data Protector Express catalog might eventually become.

The size of the catalog is primarily a function of the number of media in the backup set, the number of files backed up and the number of versions of each file on valid media. To a lesser extent, the number of objects in a catalog and the properties of those objects affect the size of the catalog.

In its catalog, Data Protector Express assigns

- 40 bytes for each version of a file,
- 128 bytes for each catalog object, and
- 1024 bytes for the properties associated with objects.

You can use these figures to estimate the size of the catalog. Files are by far the most numerous of the objects in the catalog, so much so that the size of the other objects (such as users and jobs) is negligible. Each file that is backed up is assigned 128 bytes and is made part of the catalog. While this figure can be significant, the *number of versions* for that file in the catalog is more important when predicting the size of the catalog. This is because there might be as many as 20 or 30 versions of a particular file in the catalog. (Files only have properties associated with them when they are assigned permissions or storage streams, but generally, since most files inherit their permissions from other objects, the 1024 bytes assigned for properties can be ignored.)

Consider the following example. Suppose a file or application server which holds 100,000 files is regularly backed up using the GFS-25 automatic rotation schedule. Because there are 25 tapes in this backup set, there are potentially 25 versions of each of these files (although in practice, there will be fewer versions since most of the jobs are incremental). You can predict the size of the catalog as follows:

[(# of files) * (128 bytes)] + [(# of versions) * (# of files) * (40 bytes)], or

[(100,000) * (128 bytes)] + [(25) * (100,000) * (40 bytes)] = ~108 MB.

Backup server and machine platforms

Finally, consider both the operating system and the hardware of the machine that will contain the backup server. For multi-user network installations, we recommend placing the catalog on a high-speed, high-capacity server. For example, in a Windows environment, place the catalog on a Windows NT (or later) server that has a fairly current CPU and adequate RAM.

For single machine installations, Data Protector Express runs adequately under Windows, NetWare, and Linux.

Strategies for Faster Jobs

Data Protector Express is designed to run jobs quickly and efficiently on various network platforms and arrangements. This section will help you plan your backup strategy and network installation to maximize Data Protector Express speed and efficiency.

Organizing machines into workgroups

One strategy for speeding up jobs is to organize machines into workgroups. A workgroup is merely a folder that contains one or more machines. Once included in a workgroup, files and data on these machines can be selected together simultaneously in backup job selection list.

If your Data Protector Express management domain includes many machines on a large network with media servers scattered across subnets, you can speed up jobs by grouping machines on one subnet together in a workgroup and pointing jobs related to these machines to devices also located on the same subnet. Since transferring data across a network from one subnet to another takes longer than data transferred within a single subnet, these jobs will be faster. To set up a workgroup, follow these steps:

To set up a workgroup

1. From the **Administration** desk bar, select **Catalog**.
2. Locate the **Network** in the hierarchical tree view.
3. In the main object detail area of the screen, right-click and select the **New** command.
4. Enter a name for the workgroup and click **OK**.

   The new workgroup will be listed under Network along with any machines in the Data Protector Express management domain.
5. One by one, select each machine that you want to include in the workgroup.

6. Right-click the machine and select the **Move** command.
7. Select a destination under the **Network** and click **OK**.

The next time you set up a backup job (or other job), the workgroup you created will be available on the **Selection** page of the job.

What Slows Down Tape Drives?

Tape drives work most efficiently when they are “streaming,” that is, when the tape itself is constantly moving forward and a steady flow of data is being written to the tape as it passes the write head. In general, tape drives will “stream” if there is a constant flow of data available to write to the tape.

Whenever there is an interruption in the data and the drive must wait for the data, the “stream” breaks off and the tape stops. Additionally, after the tape stops, the drive must reposition the write head and regain the velocity of the tape. To do so, the drive will rewind the tape prior to where it stopped writing and then restart the tape forward again. This can be a time-consuming process, especially if it occurs repeatedly.

For this reason, it is important to keep data constantly flowing to the tape drive. The performance of your job will be maximized when the tape drive constantly has data available to it.

Maintaining the flow of data

There are several steps you can take to make sure that data is constantly available to the backup device.

Local buses compared to network connections: In general, data is transmitted more efficiently over a local bus than over a network connection. Thus, for example, performance increases if the backup device is connected to the file or application server rather than to a different machine on the network, although either arrangement is possible.

Note that the catalog need not be placed on the same machine as the backup device. The location of the catalog does not affect the rate of data transmission. (Other job tasks, such as building backup selection lists and opening and closing files, create network traffic and require CPU calculations. While the location of the catalog will affect these parts of the job, the advantages of a remote location of the catalog often outweigh any speed loss.)

Add a second device controller: A backup device and volume may be on the same machine with a local connection between them. If the backup device and the volume share the same device controller, this limits the speed of data transmission and may cause an error in Data Protector Express. Therefore, you should add a second device controller specifically for the backup device. This can effectively double the rate of data transmission and enhance operation. At the least, you should connect the backup device to a different SCSI chain or IDE channel.

Use a wider data stream: For both network and local connections, the width of the data stream affects the rate at which data can be transferred. Many tape drives are capable of writing data much faster than can be transferred over older device controllers and network connections. By upgrading to more recent technology with wider data streams, there will be fewer interruptions in the stream of data to the backup device. For example, consider using a Wide or Ultra Wide SCSI controller for backup devices that support such an interface. Additionally, for network connections, consider upgrading from 10Base-T Ethernet to 100Base-TX.

Consult your manufacturer’s documentation to see if your backup device would benefit from a wider data stream.

Use the proper number of data streams: Data Protector Express is capable of controlling up to eight data streams per backup device simultaneously. This feature can greatly increase your job speed since multiple devices can simultaneously send data. For example, four backup devices can support up to 32 simultaneous data streams.

You control the data streams of a volume, directory or file from its **Storage page**. Normally, the **Backup stream** field on the **Storage page** of a *volume* is set to **Create new stream**, while the **Backup stream** of a *directory* or file is set to **Use existing stream**. By changing these options, you can change the number of backup streams, thereby affecting the speed at which the job runs. Assigning the proper number of data streams can help speed up the data transmission rate.

In general, you should assign data streams according to the number of streams the *physical* device (e.g., the disk drive) is capable of handling. Usually this number is equal to the number of spindles the drive has. Under most circumstances, you should use this number to determine the number of data streams.

One exception to this general rule is when you are working with very large files. You can increase performance by creating an additional stream for each of these very large files. For example, if you have a very large file with 1.0 GB or more, create a separate stream for this file. Then Data Protector Express will be able to send the file to the tape drive at a higher rate that allows for “streaming.”

Consider these three examples:

1. A RAID device is capable of sustaining multiple data streams at once. By assigning various directories on the RAID device to additional streams, you can increase the rate of data transmission. To do so, assign large directories to their own streams by changing the **Backup stream** field of each directory’s **Storage** page to **Create new stream**. Don’t add any more streams than the RAID device can sustain.
2. On the other hand, a single physical device may have multiple logical volumes. If each volume is assigned a separate stream, this will not result in faster data transmission and may, in fact, result in slower data transmission if it creates additional seeks by the disk drive. To turn off one of the data streams, change the **Backup stream** field on the volume’s **Storage** page to **Use existing stream**.
3. Some file or application servers may have large catalog files on them, perhaps 1.0 GB or larger. These files should be assigned to their own streams. To do so, change the **Backup stream** field on the file’s **Storage page** to **Create new stream**.

In general, when creating or modifying data streams, first use the capacity of the *physical* device to determine the optimum number of data streams and then create separate streams for very large files. Too few or too many data streams will impede maximum performance.

You may experience problems with data streams if you have not dedicated any streams to specific volumes or files. Problems may also occur if you exceed your hardware or operating system capacity.

Other factors that affect job speed

Additional factors that affect job speed include:

File compression: Whether or not files are compressed by the backup unit affects how fast jobs run. When a backup device compresses files, e.g., at a ratio of 2:1, a proportionately greater amount of data needs to be sent to the backup device for it to stream. However, when files are sent across the network already compressed, as NetWare does, further compression by the backup device will be negligible.

NOTE: Compression ratios vary among devices.

Minimize small file size: Large files transfer and are written to the backup device more efficiently than are small files. If you can limit the number of small files you back up, especially those smaller than 64K, your job will run more quickly.

CPU speed: In general, a faster CPU results in faster backups. Take the speed of the CPU into account when deciding where to place the backup device and to locate the catalog.

RAM: In general, additional memory results in faster backups. By default, Data Protector Express allocates 25% of physical memory, up to 32MB per device, for buffering. If you have four devices on one machine, you should install 512MB of memory (32MB x 4 devices x 4) in that machine. If you have eight devices on one machine, install 1GB of memory (32MB x 8 devices x 4) in that machine.

NOTE: Use this as a guideline when attaching devices to each machine.

Working with Permissions

This section provides useful tips for assigning permissions.

Checking the effective permissions of a user

Log on as the user.

On complex installations with multiple users and groups and varying levels of security, a particular user's effective permissions can be difficult to identify. The easiest way to identify a user's effective permissions is to log on as that user.

If you have not yet assigned the user a password, simply log on as the user. Browse the various **General page**s of the objects in the catalog. Verify that the displayed effective permissions match your intended security measures.

If the user has a password and you do not know it, create an "alias" user and make it equivalent to the user whose permissions you wish to check. Then log on as the alias user. Be certain to delete both the alias user and its folder after verifying the effective permissions.

Using groups to handle complex security needs

Set up groups and then make users members of them.

Some security arrangements can be very complex, with multiple users possessing differing levels of effective permissions to different catalog objects. Setting up each user's permissions separately and individually can be a complex and time consuming process.

You can use groups to speed up this process. Consider the following simplified example. Suppose you want some users to have full permissions to a tape drive (that is, the ability to create new tapes, to overwrite old tapes, to write backup tapes and read tapes for restore jobs), but want other users to have limited permissions to the tape drive, for example, only the ability to write to backup tapes, but not overwrite them.

Begin by creating two new groups. Name one group *Users with Full Permission to Tape* and assign this group **Create, Modify, Delete, Write** and **Read** permissions to the tape drive. Name the other group *Users with Write Permission to Tape* and assign this group **Write** permission to the tape drive. Next, delete the corresponding User/Group folders that appear on the job views.

Then when you create new users, rather than individually assigning each user permissions to the tape drive, make them members of the appropriate group.

You create as many groups as necessary, with varying levels of access to catalog objects such as media, machines, volumes and directories. For example, you might create a group named Backup Permission to Volume and another named Backup and Restore Permission to Volume, assigning to each the appropriate permissions.

Selecting Files for Jobs

This section provides useful tips for selecting files.

Selecting files not previously backed up

Set the Version Range filter to At most 0.

Suppose you want to run a backup job that only selects files that have not been backed up previously. You can use the **Version Range** filter to “filter out” any files that have been previously backed up.

Each time Data Protector Express backs up a file, it creates a new version of that file. If a file has not been backed up, Data Protector Express has no versions recorded in the catalog for that file.

To select only files that have not been previously backed up, begin by clicking the **Selection Filters** button on the toolbar of the **Selection** page. The **Selection Filters** dialog box will appear.

Click the **Browse** button next to the **Version Range** field. Set the **Range Type** to **At most** and then set the **Maximum versions** field to **0**. Data Protector Express will only select those files with no versions.

Note that this method does not ensure that you have the latest version of every file. Having a version of a file does not ensure that the version you have reflects the latest changes to the file. It may have been modified after the last time you backed it up and so your latest version may not match the file’s current form.

Selecting deleted files for restoring

*Set the **Delete range** filter to **On or before** some random future date.*

When a file has been deleted from a file or application server or PC desktop and a version of that file exists on valid media, Data Protector Express marks that file in its catalog as having been deleted and assigns it a delete date. Additionally, these files appear with a special icon in the object detail area of the **Selection** page.

Selecting versions from a specific job

Select the appropriate version date for a container object.

When a file is backed up, Data Protector Express creates a version. Each version of a file has a unique version date and every file backed up during the same job has the same version date. (You can view this information for all of the available versions in the **Versions…** dialog box.)

Remember that when you specify the version date for a container, such as a volume or folder, objects in that container are only selected when they have the same version date.

If you want to select only those files backed up during a particular job, begin by checking a container high in the tree hierarchy, such as the machine or network icon. This will cause all of the files below this object to be initially selected. Then open the **Versions…** dialog box by clicking on the **Select Version** button. Select the appropriate date and time version for the job. Now only those files with a matching version date will be selected.

Selecting versions from specific media

*Add the media to the **Media** filter.*

Suppose you want to restore only those files that appear on specific media or want only to verify files from specific media. You can use the **Media** filter on the **Selection Filters** dialog box to only select files that have valid versions on the media you specify.

To do so, open the **Selection Filters** dialog box by clicking on the **Selection Filters** button on the toolbar of the **Selection page** of the job. Then click the **Add...** button to open the **Browse** dialog box. When you add media to the **Media** field, Data Protector Express checks to see if the file selected has a valid version on that **Media**. If so, that file is included in the job. (If you add multiple media to the **Media** field, only files with versions on all the selected media will be included in the job.)

Restoring Tips

This section provides tips for restoring files and volumes.

Restoring volumes for the latest date

If you have used a default schedule and have run backup jobs as scheduled, you can easily and simply restore files as they appeared the last time a backup job was run. Simply select the volumes or files you wish to restore on the **Selection** page of a restore job. The latest version of each file will be automatically restored to the volume. Data Protector Express will prompt you for whatever tapes are needed to complete the restore job.

Restoring volumes for a specific date

You can restore volumes and directories as they appeared on a particular date as long as that date is within the full data recovery period. Recall that the full data recovery period is the number of days prior to the data loss for which any and every file backed up can be recovered. (To restore volumes to the last backup date, refer to *Restoring volumes for the latest date* above.)

Different schedules provide full data recovery periods for varying numbers of days prior to the last backup. For example, a GFS 30-tape job can reconstruct the data for any day of the past three weeks, while a simple 4-tape backup only provides for reconstruction of the past two days.

You can reconstruct the data for any particular day during the full data recovery period. Consider this example. Suppose you want to restore a particular volume as it appeared on Wednesday morning. Providing the date falls within the full data recovery period, there are three possible scenarios for restoring the volume as it appeared at the beginning of business on Wednesday: either (1) restore from a full backup tape; (2) restore from a full backup tape and the most recent *differential* tape; or (3) restore from a full backup tape and all of the *incremental* tapes from the previous full backup and the date in question.

- *If you ran a full backup job the previous evening,* you can run one restore job. Begin by creating a new restore job and selecting the appropriate volume on the selection page of the restore job. Initially, the latest version of these files will be selected. You must select the versions according to the desired date, in this case the Tuesday before the Wednesday. To do so, set the **Backup range** filter to the desired date. Begin by clicking the **Selection Filters** button on the toolbar of the restore job's **Selection** page. The **Selection Filters** dialog box will appear. Then click on the **Browse** button next to the **Backup Range** field. Specify Tuesday's date as the starting and ending date in the **Date Range** dialog box.
- *If you ran a differential job the previous evening,* you need only run two restore jobs. The first restore job must restore all of the files from the previous full backup job; the second restore job must restore files from the previous evening's differential job.

  Suppose in this example that the last full backup was done on Friday evening and that a differential job was run on Tuesday evening. To restore files as they appeared on Wednesday morning, follow these steps.

First, create a restore job, select the appropriate volume and then set the **Backup range** on the **Selection Filters** dialog box to match Friday's date. Name the job with an appropriately identifying name, such as *Restore from Friday's Full Backup*.

Second, copy the first restore job, rename it with an identifying name and change the **Backup range** date to match Tuesday's date.

Run the two jobs, being certain to run them in the proper order.

- *If you ran an incremental job the previous evening,* you will need to run two or more restore jobs. The first job must restore all of the files from the previous full backup job; the other jobs must restore all of the files from all of the previous incremental jobs between the full backup and the date in question.

  Suppose in this example that the last full backup was done on Friday evening and that incremental jobs were run on Monday and Tuesday evenings. To restore the volume as it appeared on Wednesday morning, follow these steps.

  a. Create a restore job, give it an identifying name, select the appropriate volume and then set the Backup range to Friday's date.

  b. Copy the first restore job, rename it with an identifying name and change the Backup range date to match Monday's date. Repeat this step, changing the Backup range date of this third job to Tuesday's date.

  c. Run the three jobs, being certain to run them in the correct order.

Copying a directory structure

Clear the **Allow Children** check box in the **Selection Filters** dialog box.

Suppose you have set up a complex directory that you want to replicate in a new location, for example, on a new PC desktop or file or application server. Data Protector Express provides you an easy way to do this.

If you have not previously backed up the directory, create a backup job that does so. Select the appropriate volume. Then, open the **Selection Filters** dialog box. Clear the **Allow Children** check box, being certain that the **Allow Parents** box is checked. (The job will run faster when the **Allow Children** box is cleared, however it is not necessary to clear this option. You can restore the directory by itself, even when you have previously backed up both the directory and the files in it.)

To copy the directory structure to a new location, create a restore job, selecting the appropriate directory and restore location. Then, open the **Selection Filters** dialog box. Clear the **Allow Children** check box, being certain that the **Allow Parents** box is checked. The job will "copy" that directory to the new location.

Restoring files to a new or different folder

On the **Selection** page, use the ***Move*** command to restore the files to a different folder.

Suppose you want to restore files or folders, but do not want to overwrite files and folders currently existing on the volume. To avoid overwriting (replacing) current files or folders with the versions you are restoring, restore the files or folders to a new or different location.

When you instruct Data Protector Express to restore files and folders in new locations, Data Protector Express creates new files and folders in the specified location.

To restore a file to a different folder, use the **Move** command to restore the file in the tree view area on the **Selection** page of the restore job to the new folder. (If the target folder does not exist, you must create it first.) In the **Select destination for move operation** dialog box, select a target location. Data Protector Express will move the file to the destination you specify.

You can also restore folders and volumes in new locations. The contents of these containers move with them and are restored, along with the folder or volume, in the new location.

Additionally, you can create a new folder and restore files to that new folder. When Data Protector Express restores the files, it creates the new folder and restores the files you specified to that new location. Similarly, you can restore folders and their contents in new folders you create.

To create a new folder in which to restore the file or folder, first highlight the location where you want to create the new folder in the tree view area. Then click on the **New Object** button on the **Selection** page's toolbar. Or use the shortcut (right-click) menu and select **New Directory**. Data Protector Express will create the new folder in the location you specified. Give the folder a new name and then use the **Move** command to restore the files into that folder the files and folders you want restored in it.

Note that when you move a version on the **Selection** page of a restore job, the changes you make are only reflected in the current restore job. Only the current restore job will assign the file or folder the new location. When you create a new restore job, you will see the files and folders in their original locations. Likewise, the **Catalog** view will continue to display files in their original locations.

Restoring files with new names

Rename the file on the **Selection** page of the restore job.

Suppose you want to restore a file with a different name. To do so, you rename the file after you select it. When you rename the file, Data Protector Express restores the file with the new name. This can be useful for not overwriting versions of the file that currently exist on disk.

To rename a file, right-click the file name and select **Rename** from the shortcut menu.

Note that when you rename a version, you are only renaming that file for the purposes of restoring it with this particular restore job. Only the current restore job will assign that file the new name. When you create a new restore job, you will see the file displayed with its original name. Similarly, the **Catalog** view always displays files with the names they had when they were backed up.

Rename the file on the **Selection** page of the restore job. Sometimes it may be necessary to reserve a specific device in a library so that future restore jobs can access that device should the need arise.

1. Create a user in Data Protector Express and log on to Data Protector Express as this user when performing day-to-day backups. Make sure that this user has explicit rights to the library and devices in the library that will be used during these backups. The default permission settings for each added device should be sufficient. *Do not give this user access rights to the device that will be reserved.*
2. To perform a restore job while backup jobs are running, log on to Data Protector Express as Admin. Create a restore job and select the reserved device on the Device page of the restore job.

Other Tips

Here are two additional tips for transferring files between operating systems and for setting up a library for cleaning.

Moving data between operating systems

Clear the **Native data streams** check box in the **Advanced Options** dialog box.

Suppose you want to transfer data (files and folders) from one operating system to another, such as from a NetWare platform to a Windows platform. To do so, you need to back up and restore the data in a generic format.

Different networks transmit data to Data Protector Express in different formats. In particular, Windows, NetWare, and Linux all use different data stream formats. If you intend to share data from one network platform with another, the data should be stored on media in a common data format, not in the native data streams format.

To back up data in a generic format, first create a new backup job and select the data you want to transfer between operating systems. Then open the **Advanced Options** dialog box and clear the **Native data streams format** check box. When Data Protector Express backs up this data, it will convert it to a generic format before writing it to the media.

CAUTION: Security is an issue to consider when checking this option. When this option is checked, Data Protector Express backs up all security information that network software includes in the data stream. If the option is unchecked, Data Protector Express uses a generic format that removes security information.

After the job has completed, create a restore job, selecting the same files to restore. Make certain you have selected the proper versions of these files by selecting the proper version date in the **Versions** dialog box. You can then restore the files to a different operating system.

For more information on native data streams, see *Settings for all platforms*.

Setting up a library for automatic cleaning

Depending on the model and manufacturer, some libraries support automatic cleaning cycles. They will alert Data Protector Express when a cleaning cycle needs to be performed. If Data Protector Express knows that a particular storage slot on a library magazine holds a cleaning cartridge, Data Protector Express will automatically run a cleaning cycle before running a backup job whenever a cleaning cycle is required.

NOTE: If you are using a device that is not a library, you must manually clean the device at the manufacturer’s suggested intervals.

For more information on setting up a cleaning cartridge on a library, see *Status page*.

To set up a library for automatic cleaning

1. Insert a cleaning cartridge into the library and then change the status of the storage slot.

   To change the status of the storage slot to cleaning do the following:

   a. From the **Favorites** desk bar, open the **Devices** view and select the library.

   b. Expand the library until you locate and select the storage slot in which you inserted the cleaning cartridge.

   c. Right-click the storage and select **Element Status**.

   d. Change the status from its current setting to **Cleaning** and click **OK**.

2. Set up a media job to clean the device as follows.

   Some libraries have more than one device. Be sure to select the device that you want to clean and not just the library.

   a. From the Favorites desk bar, open the Wizards view and select Media.

   b. Select the Clean Device wizard.

   c. Follow the instructions on the screen to select the library device that you want to clean.

   d. Set up a schedule for the job to run repeatedly in the future.

When you finish setting up the job, the device will be cleaned automatically on the scheduled days and times.

Data Protector Express will automatically use the cartridge in this slot when performing a cleaning cycle.

To manually clean a library device

1. From the **Device** view on the **Favorites** desk bar, select the library to be cleaned.
2. Expand the view of the library and select a device to clean.
3. Right-click the device and select **Clean Device…** from the shortcut menu.
4. Follow the instructions on screen to set up a **Clean Device** job.
5. On the **Schedule** page, select **Run now** for the schedule type.
6. Once you finish setting up the job, Data Protector Express will clean the device.
7. To clean this same device manually in the future, locate the job in your **Home** folder or from the **Jobs and Media** view and rerun the job.

Chapter 12: Advanced Permissions and Security

This section provides a detailed summary of Data Protector Express's extensive security system. If it is your responsibility to manage the security of your Data Protector Express catalog and you are working with sensitive data, this section can help you set up a complex security system that meets your particular security needs.

In this section

- Adding New Users and Groups
- Effective Permissions
- Permissions Reference

Overview

Permissions control what actions a user is allowed to perform within a given Data Protector Express management domain. Users can be given extensive or limited permissions, allowing the Data Protector Express administrator to distribute backup duties to various users and groups. This allows for a flexible, non-centralized backup system while providing the highest degree of security for the network.

How your security is arranged depends on your unique security needs. Before setting up your security system, consider the following questions:

- *Is more than one Data Protector Express management domain required?*

  Setting up separate Data Protector Express management domains can provide a high level of security. If your security needs require that access to some data be strictly limited, setting up a separate catalog is often the simplest way to achieve this.

  Data cannot be shared between storage domains without using advanced procedures. Media from one catalog must be imported into a new catalog before the data on it can be read or used. When it is imported, Data Protector Express requires the media password, if set. If you assigned the media a password when it was created, the media cannot be imported without that password.

  If you do not assign the media a password, the media can be easily imported into any catalog. As a result, the data is actually less secure when there are two or more catalogs than it would be with just one catalog. If you are relying on multiple catalogs for security purposes, make sure that each created media is assigned a password.

There may be, however, some limitations on the number of catalogs you can set up. In particular, machines (file or application servers and PC desktops) can only be an object in one catalog. Similarly, volumes can only belong to one Data Protector Express management domain. Files in one Data Protector Express management domain cannot, without importing the media, be shared with catalog objects in other Data Protector Express management domains.

Thus your ability to set up separate Data Protector Express management domains is limited by the number of backup devices you have and their respective locations on separate machines. For example, to set up two catalogs, you would require at least two separate PC desktops or file or application servers, each with at least one backup device.

- *Within a single Data Protector Express management domain, must some users be prevented access to some data?*

  Multiple groups may share a single tape drive or backup device and thus are members of the same Data Protector Express management domain. However, there may be reasons to allow these groups to work with only their own data. For example, an accounting group may share a common tape drive with a personnel group, although neither can be allowed access to the files and directories of the other group.

  The security needs of these situations can be addressed by carefully assigning permissions, particularly to the machines, backup devices, media, volumes and directories.

- *Should access to certain functions be limited?*

  You may wish to distribute certain backup tasks to various users or groups. For example, each group might be responsible for its own daily backup jobs and archive jobs. On the other hand, access to certain Data Protector Express features may need to be limited. Users might be able to *create* tapes, for example, but not *restore* files to disk or *delete* files on disk. Alternatively, you may want users to *run* jobs you create, but not *create* their own jobs.

  The security needs of these situations can be addressed by carefully assigning users select permissions to various objects in the catalog. For example, you might assign permission to write files to tapes, but not to volumes, thus preventing restore jobs from running.

About administrator permissions

CAUTION: Data Protector Express administrators have unlimited access to all of the objects in the catalog. Any user who logs on as the Data Protector Express administrator will have complete access to all of the files and machines on the catalog.

The most powerful user in any catalog is the Data Protector Express administrator. Because Data Protector Express administrators are granted supervisor rights to the System Container, they have unlimited access to all of the objects in the catalog. Any user who logs on as the Data Protector Express administrator will have complete access to all of the files and machines on the catalog.

Your first security step should be to change the Data Protector Express administrator’s password. Click on the **Security** page. Select the **Admin** user. Select **Change Password…** from the **Security** menu. Type in the new administrator’s password, enter it again to confirm and click **OK**. Do not continue until you have changed this password.

The only difference between the Data Protector Express administrator (**Admin**) and other users is that the Data Protector Express administrator has **Supervisor** rights to the root object in the Data Protector Express hierarchy, that is, the System Container. You may also create additional Data Protector Express administrators as well as rename the **Admin** user.

CAUTION: Do NOT delete **Admin** unless you assign **Supervisor** or **Access** permission to the System Container to another user.

Adding New Users and Groups

Generally, the first step to arranging the security system is to set up users and groups. You create new users and groups on the **Security** page of the main Data Protector Express window. Use the **New Object…** option from the **File** menu, the **New Object** button or the shortcut (right-click) menu to create new users and groups.

New user or group folders

Each time you add a new user or group to the **Security page**, Data Protector Express automatically creates a new User/Group folder in the **Home** folder with the same name as the new user or group. For example, if you create a new user, Data Protector Express creates a new User/Group folder **My Folder**.

The user or group is automatically assigned six permissions to their User/Group folder: **Access, Create**, **Modify**, **Delete**, **Write** and **Read**. You can modify these permissions at any time using the **Permissions** page of the new user or group property page.

Setting up users

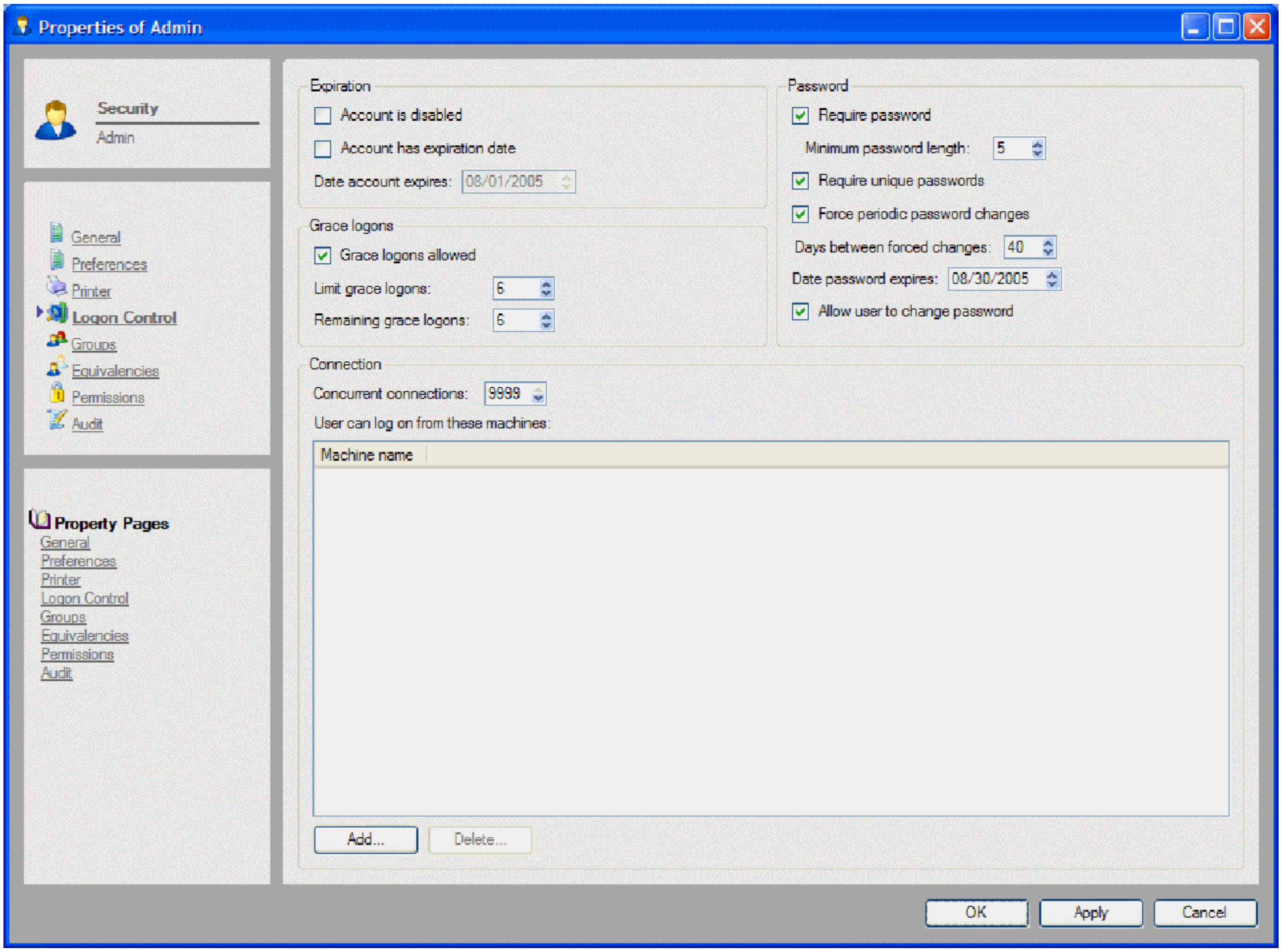
As you create new users, Data Protector Express automatically opens the property page of the new user. Use the property pages to control the user's password, account activity, group membership, equivalencies and permissions.

To create a new user

1. Open the **Administration** desk bar and select **Security**.
2. Create the new user by either
   - Selecting **New Object** from the File menu and then selecting **User** from the **New Object** dialog box, or
   - Right-clicking in the Data Protector Express object detail area and selecting **New User** from the shortcut menu, or
   - Clicking the **New Object** button on the toolbar and then selecting **User** from the New Object dialog box.
3. Type in the new user's name in the **Name** field on the **General** property page.

Logon Control page for users

The **Logon Control** page controls whether passwords are required, whether and when the password must be changed, whether an account has expired and the number of connections a user can have to the network.



Expiration

□ Account is disabled

□ Account has expiration date

Date account expires: 08/01/2005

Grace logons

☑ Grace logons allowed

Limit grace logons: 6

Remaining grace logons: 6

Password

☑ Require password

Minimum password length: 5

☑ Require unique passwords

☑ Force periodic password changes

Days between forced changes: 40

Date password expires: 08/30/2005

☑ Allow user to change password

Connection

Concurrent connections: 9999

User can log on from these machines:

Expiration: A user account can expire on a given date. When the account expires, Data Protector Express disables the account and checks the **Account is disabled** box. This user will be unable to log on until the **Account is disabled** box is cleared.

You can manually disable an account by checking the **Account is disabled** box.

To make a disabled account active again, clear the **Account is disabled** box and change the **Date account expires**.

Grace logons: When **Grace logons** is checked, a user can log on to Data Protector Express a set number of times after their old password has expired. For example, if the **Grace logons allowed** box is checked and **Remaining grace logons** is set to **2**, the user will be allowed to log on two times after their old password has expired. On the third logon attempt, the user must change their password. You can also limit the number of grace logons that are permitted.

NOTE: Grace logons do not function when passwords are not required, that is, when the **Require password** check box is cleared.

Connection: These settings control the allowable machines and simultaneous logons for a user.

The **Concurrent connections** setting controls how many different logons a user may have simultaneously from different machines. For example, if **Concurrent connections** is set to **5**, this user can log on to Data Protector Express from up to five separate machines at the same time.

The user can only log on to Data Protector Express on the machines listed in the **User can log on from these machines** field. To add a machine, click **Add…** and select the machine from the **Browse** dialog box. To remove a machine, select it and click **Delete**.

NOTE: If no machine is listed, a user can log on from any machine.

Password: When **Require password** is checked, Data Protector Express requires the user to have a password.

The minimum length of the password is determined by the **Minimum password length** setting.

NOTE: If you clear the **Require password** box and the user has a password, Data Protector Express will continue to require that user to input their password.

If you check the **Require unique passwords** box, Data Protector Express only accepts the new password if you have never used it.

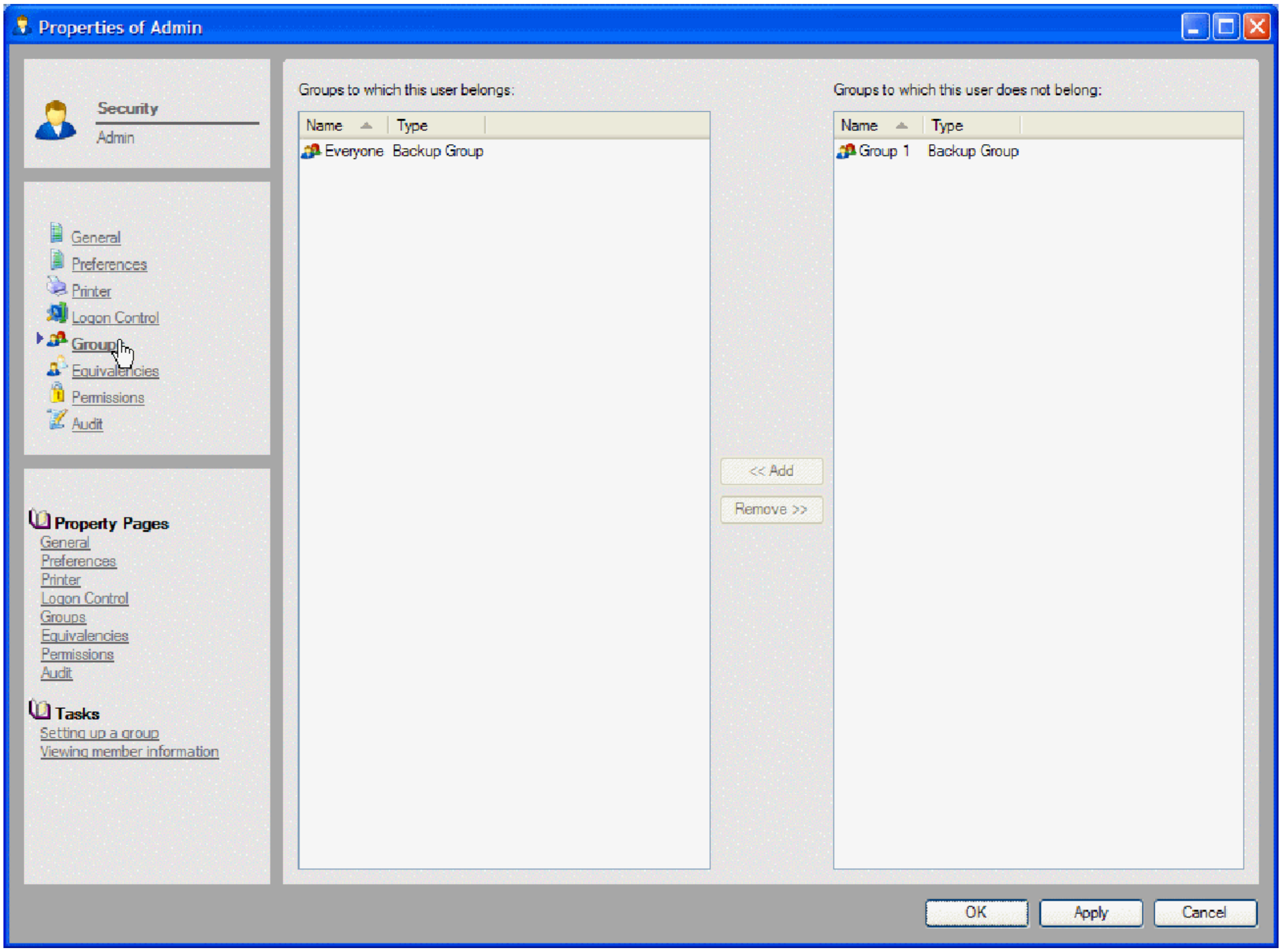
If you check the **Force periodic password changes** box, either the user or the Data Protector Express administrator must change the password per the **Days between forced changes** and **Date password expires** settings.

If you check the **Allow user to change password** box, the user can change their password on their own.

TIP: The Data Protector Express administrator can change a user's password without knowing the user's current password. Data Protector Express does not even ask you to enter the old password. This is useful when the user has forgotten his or her password.

Groups page for users

Use this page to add or remove a user from a group. To add a user to a new group, select the group in the right window pane and click the **Add** button; the group is moved to the left window pane. Similarly, to remove a user from a group, select the group in the left window pane and then click the **Remove** button.



Groups to which this user belongs:

Name	Type
Everyone	Backup Group

Groups to which this user does not belong:

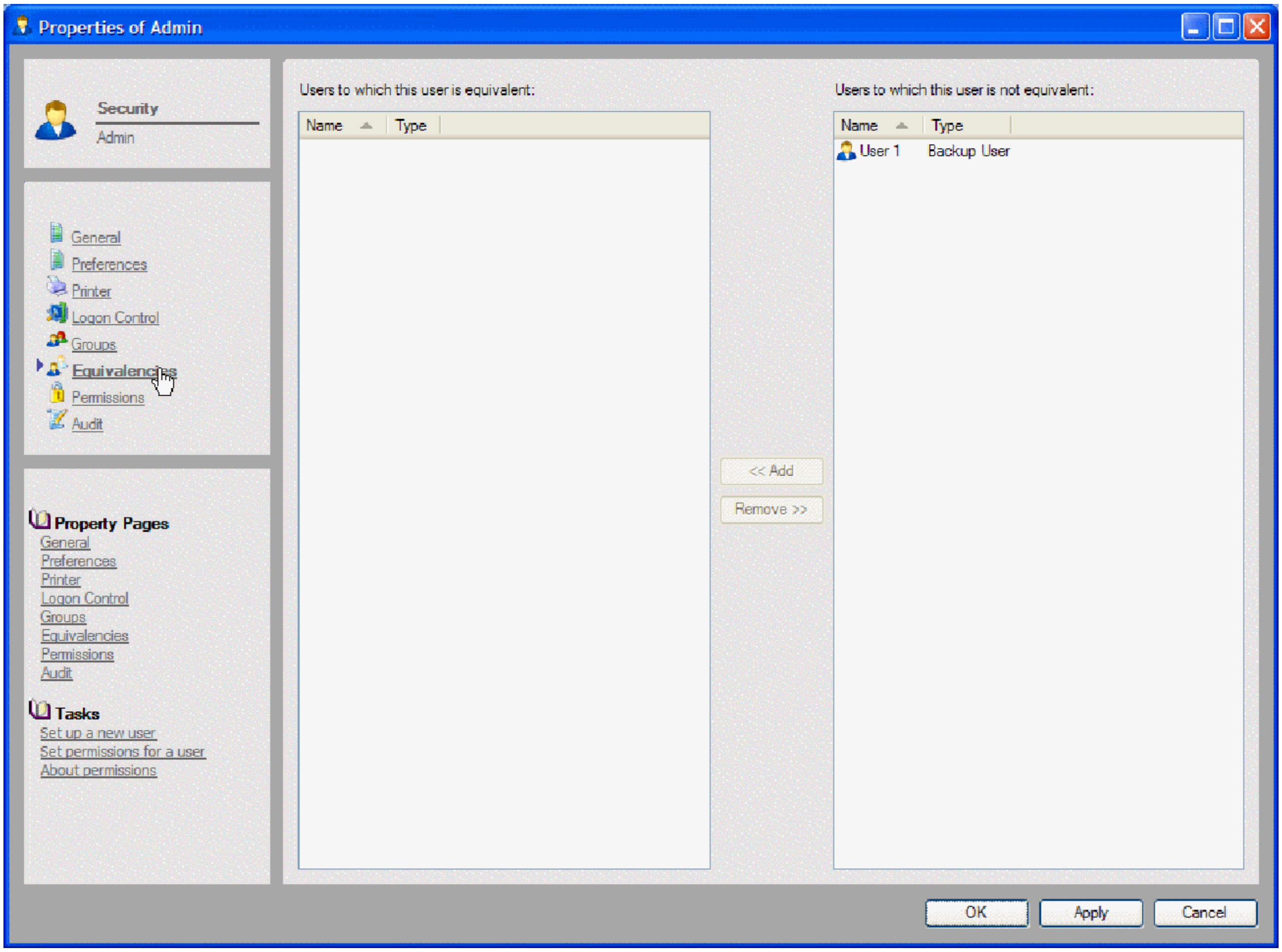
Name	Type
Group 1	Backup Group

Everyone group: When a new user is created, they are automatically added to the **Everyone group**. Members of this group have **Modify**, **Delete**, **Create**, **Write** and **Read** permissions to the **Everyone Folder**. You can modify these permissions at any time, including from the **Permissions** page of the new user's property page.

Equivalencies

One quick way to assign user permissions is to make the current user equivalent to another user. This can be very useful for managing complex Data Protector Express installations with multiple users and varying security or for making temporary changes to a user's permissions.

Use this page to make the current user equivalent to another user. To make the current user equivalent to another user, select the other user in the right window pane and click the **Add** button; the user is moved to the left window pane. Similarly, to end an equivalency, select the other user in the right window pane and then click the **Remove** button.



Users to which this user is equivalent:

Name	Type

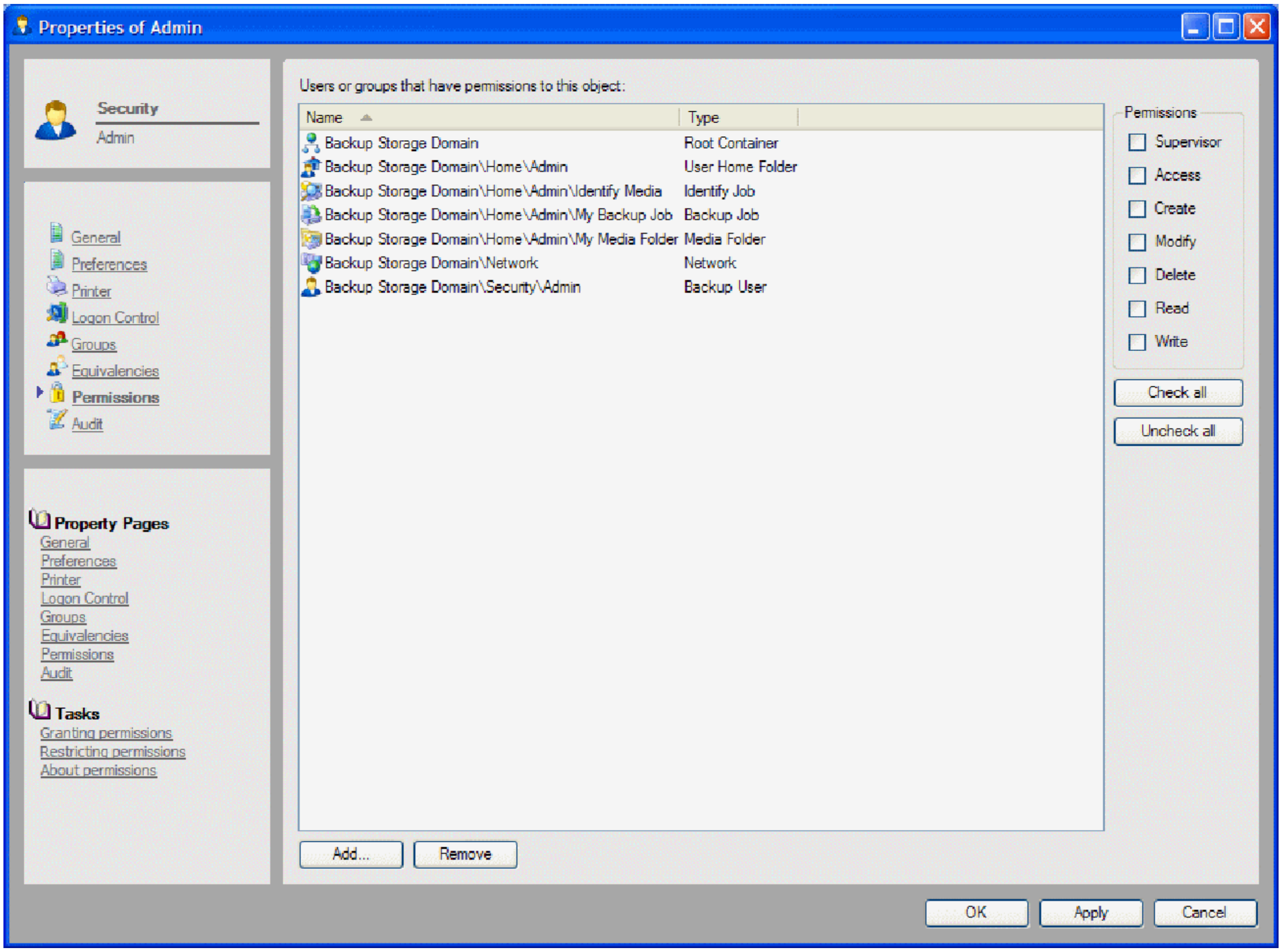
Users to which this user is not equivalent:

Name	Type
User 1	Backup User

Note that equivalencies only work in one direction; they are not reciprocal. The current effective permissions of the user whose property page is open will be calculated using the direct and inherited permissions of the user they are made equivalent to. For example, if User 1 is made equivalent to User 2, the effective permissions for are calculated using *both* of their direct permissions. However, the effective permissions for User 2 remain unchanged.

Permissions page for users

Use this page to grant users permissions to objects in the catalog. The **Permissions** check boxes show the permissions of whatever object is selected in the **Objects to which this user or group has permissions** list. Select another object to see the user's permissions to that object.



Users or groups that have permissions to this object:

Name	Type
Backup Storage Domain	Root Container
Backup Storage Domain\Home\Admin	User Home Folder
Backup Storage Domain\Home\Admin\Identify Media	Identify Job
Backup Storage Domain\Home\Admin\My Backup Job	Backup Job
Backup Storage Domain\Home\Admin\My Media Folder	Media Folder
Backup Storage Domain\Network	Network
Backup Storage Domain\Security\Admin	Backup User

☐ Supervisor
☐ Access
☐ Create
☐ Modify
☐ Delete
☐ Read
☐ Write

Note that permissions can be granted from either the property page of the catalog object or the property page of the user. Either way, the permissions appear on the appropriate corresponding object's **Permissions** page. For example, if Admin user is granted permissions to the **C:** volume from the **Permissions** page on his property page, the **Permissions** page on the property page of the **C:** volume will list Admin as a user who has permissions. Alternatively, if the Admin user is granted permissions from the property page of the **C:** volume, the appropriate permissions will appear on the Admin user's **Permissions** page.

Note additionally that a user has direct permissions only to those objects listed on that user's **Permissions** page. Any and all other effective permissions to other objects are calculated through inherited permissions, through equivalencies or through groups.

Setting up groups

As you create new groups, Data Protector Express automatically opens the property page of the new group. Use the property pages to assign members to the group and assign permissions to the group.

To create a new group

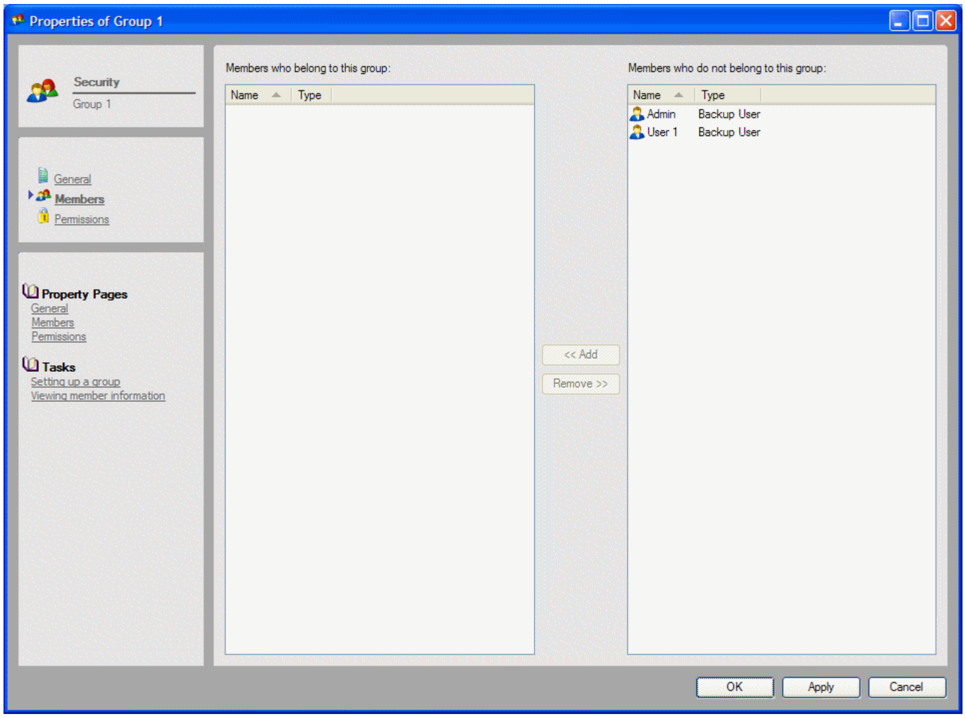
1. From the **Administration** desk bar, select **Security**.
2. Create the new group by either
   - Selecting **New …** from the **File** menu and then selecting **Group** from the **New Object** dialog box, or

- Right-clicking in the Data Protector Express object detail area and selecting **New …** from the shortcut menu.

3. Type in the new group's name in the **Name** field on the **General** property page.

Members page

Use the **Members** page of the group's property page to add and remove users from the group. To add a user to the group, select the user in the right window pane and click the **Add** button; the user is moved to the left window pane, under **Members who belong to this group**. To remove a user from a group, select the user in the left window pane and click the **Remove** button; the user is moved to the right window pane, under **Members who do not belong to this group**.



Members who belong to this group:

Name	Type

Members who do not belong to this group:

Name	Type
Admin	Backup User
User 1	Backup User

Permissions page for groups

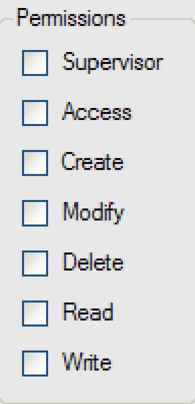
If a user is a member of a group, that user's effective permissions are determined using the direct permissions that group has to objects in the catalog. Use this page to assign the group permissions to objects. The **Permissions** check boxes show the permissions of whatever object is selected in the **Objects to which this user or group has permissions** list. Select another object to see the group's permissions to that object.

Note that the permissions granted from this page, like all permissions, are reciprocal. Changes made on this page appear on the property pages of the corresponding object. For example, if you grant permission to a folder to a group, the **Permissions** page of that folder will list the group, along with the appropriate corresponding permissions.

Effective Permissions

Data Protector Express ensures the security of the catalog and network by calculating the **effective permissions** a user has to an object and using these permissions to determine what actions that user can perform.

The current user's effective permissions to an object are displayed on the **General** page of the object's property page. The **Effective permissions** box shows the current user's effective permissions to the object.



Permissions

□ Supervisor
□ Access
□ Create
□ Modify
□ Delete
□ Read
□ Write

Calculating effective permissions

A user is assigned effective permissions to an object in one of two ways, either through **direct permissions** or through **inherited permissions**.

A user has *direct permissions* to an object if they are listed on the **Permissions** page of the object, if they are equivalent to a user who has direct permissions to the object; or if they are a member of a group that is listed on the Permissions page of that object. Note that a user can gain permissions from any combination of these.

A user has *inherited permissions* to an object if (1) they do not have direct permission and (2) they have effective permissions to the container that contains the object. This means that, if you do not have direct permissions to an object, you must have effective permissions to the container in which the object is stored.

NOTE: Your effective permissions to the container object can be either direct or inherited permissions. All that matters is that you have effective permissions to the container.

When Data Protector Express determines the effective permissions a user has to an object, it first looks to see if the user has direct permission; if not, Data Protector Express then checks to see if the user has inherited permission.

Effective permissions algorithm

Data Protector Express uses the following algorithm to determine effective permissions:

- Does the user have direct permissions to the object? If yes, these are used to calculate the effective permissions. Data Protector Express does not check to see if the user has inherited permissions.
- Does the user have effective permissions to the container that contains the current object (inherited permissions)? If yes, these permissions are used to calculate the effective permissions. If not, then the user does not have effective permissions to the object.

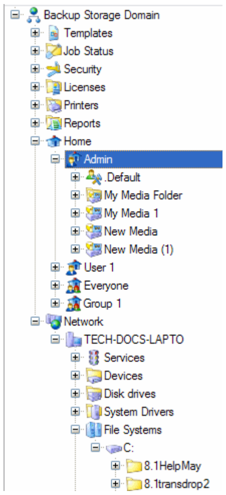
Permissions from multiple sources

Users can gain *direct* permissions to objects either as users, as a result of equivalencies or as members of a group. When the direct permissions result from multiple sources, Data Protector Express uses all of the sources to determine the permissions.

Consider the following example: The Admin user has direct permissions to **Read** and **Write** to a folder called **My Backup Folder**; Admin is also a member of a group that has direct permissions to **Modify** to the folder. As a result, his effective permissions are **Read**, **Write** and **Modify**.

Examples of effective permissions

The following six examples illustrate how effective permissions are calculated. The diagram below illustrates these six examples.



1. The Data Protector Express administrator has direct permissions to the **System Container**, the object at the very top of the catalog hierarchy. These determine his or her effective permissions to this object. Because it is a container, the objects below it in the catalog all have inherited permissions because the object directly above them has effective permissions. So, for example, the Data Protector Express administrator has effective permissions to the **Home Folder** because it inherits its permissions from the object that contains it, the **System Container**. Thus, the Data Protector Express administrator has effective permissions to all of the objects in the catalog.

2. A user (called User 1) has direct permissions to his User/Group folder, named **My Folder.** As a result, by inherited permission, this user has effective permissions to the objects stored in this folder, including any jobs, media or job folders stored in this folder. This user does not, however, have effective permissions to the **Home Folder** or to the **System Container**—these objects are *above* his User/Group folder and thus do not inherit permissions.

3. A second user (called User 2) has direct permissions to a **Machine**, in this case a file or application server with an attached backup drive and several associated disk drives. The direct permissions to the file or application server mean that this second user also has effective permissions (by inheritance) to the backup drive. So, for example, this user might be given read and write permissions to the file or application server and thus to the backup drive.

   However, he is prevented from having permissions to the volumes on the file or application server. He is listed on the **Permissions** page of the volume and these direct permissions are used to deny him access to the volume. In this example, he is granted **Read** permission by checking that box, but denied **Write** permissions by clearing the appropriate box.

Thus even though this user has effective permissions to the container that contains the volume, his effective permissions to the volume are determined *only* by his direct permissions to the volume. Because he has direct permissions, Data Protector Express does not check to see if he has inherited permissions.

4. The following example is more complex, but illustrates an important concept: that Data Protector Express does not check for inherited permissions when there are direct permissions.

   This user is a member of the **Marketing** group, which has five direct permissions to the **Marketing Folder**: *Create*, *Modify*, *Delete*, *Write*, and *Read* permissions. This user also has direct permissions to the **Marketing Media Folder**, but only **Write** permission.

   This user has five effective permissions to objects contained in the **Marketing Folder**, but not to the **Marketing Media Folder**, where he has only one (Write permission). Data Protector Express does not look to see if this user has effective permissions to the container that contains the **Marketing Media Folder** because this user has direct permissions to that object. Thus even though other members of the **Marketing** group have effective permissions to the **Marketing Media Folder** through inherited permissions, this user will not. This user will have only **Write** permissions to this folder.

5. The following example shows how equivalencies and group membership work together to determine effective permissions.

   Suppose that User 1 is a member of the **Marketing** group *and* that he is made equivalent to User 2. What permissions will the user have?

   User 1 has permissions to all of the User/Group folders, except the **Admin Folder**. For example, he has permissions to User 2's **Folder** because he is equivalent to User 2. (Note that this equivalency does not give User 2 permission to User 1's **Folder**.) User 1 also has the same permissions to the **Machine** and **Tape Drive** that User 2 has.

   However, User 1's permissions to the **Volume** are different from those of User 2. User 1 has direct permission to the **Volume** in three ways: as a user, as a member of the **Marketing** group and as a result of his equivalency to User 2. When Data Protector Express calculates his effective permissions, it uses these direct permissions from all three sources. In this case, will have five permissions (Create, Modify, Delete, Write and Read).

   Note that it does not matter that User 1's own direct permissions as a user do not include Create and Modify permissions. Data Protector Express uses all three sources to determine User 1's effective permissions to the volume. In this case, User 1's membership in the **Marketing** group grants him Create and Modify permissions.

6. Given the above example, suppose we wanted to deny *all* permissions to the **Volume**. How could this be accomplished?

   To deny all permissions to the **Volume**, three things must happen: his equivalency to User 2 must end; his membership in the Marketing group must end; and his direct permissions must be changed so that is listed on the **Permissions** page of the **Volume** but no permission boxes are checked.

   Note that listing User 1 on the **Permissions** page and clearing the permissions check boxes is not enough to deny his permissions to the property page. User 1 must no longer be equivalent to User 2 and User 1 must no longer be a member of the Marketing group.

Checking effective permissions

On complex installations with multiple users and groups and varying levels of security, a particular user's effective permissions can be difficult to identify. The easiest way to identify a user's effective permissions is to log on as that user.

If you have not yet assigned the user a password, simply log on as the user. Browse the various **General** property pages of the objects in the catalog. Verify that the displayed effective permissions match your intended security measures.

If the user has a password and you do not know it, create an “alias” user and make it equivalent to the user whose permissions you wish to check. Then log on as the alias user. Be certain to delete both the alias user and its folder after verifying the effective permissions.

Permissions Reference

There are seven permissions: **Read**, **Write**, **Delete**, **Modify**, **Create**, **Access** and **Supervisor**. These permissions affect different objects in the Data Protector Express catalog differently. Even though a particular permission may not apply directly to that object, objects below it in the catalog hierarchy can still inherit permissions from that object.

Read permission

Affected objects: Media, controller, device, library, volume, directory, file, catalog.

Description: Controls whether a user can read from a given catalog object.

In the case of physical peripherals that perform read functions, such as controllers, devices, libraries and volumes, **Read** permission to the peripheral is required in order for Data Protector Express to instruct the peripheral to read files or directories.

In case of catalog objects that hold data, such as media, volumes, directories and files, **Read** permission is required to read the data these objects contain.

Affected commands: Copy, Run (job type), Rewind, Start, Eject Media, Eject Magazine, Retension, Restore Catalog, Clean Device, Identify Media, Import Media, Restore Catalog.

This permission enables **Copy** (but not **Paste**), allowing the user to copy objects in the catalog.

Read permission is also required to run jobs. Backup jobs require **Read** permission to the appropriate volumes, directories and files. Restore jobs require **Read** permission to the appropriate devices, libraries and media. Verify jobs require **Read** permission to all of these objects.

Many commands that perform utility functions, such as **Clean Device** or **Eject Media** on a device, require **Read** permission. Device commands that also read media in backup devices require this permission.

Write permission

Affected objects: Media, device, library, volume, directory, file, catalog.

Description: Controls whether a user can write to a given catalog object.

In the case of physical peripherals that perform write functions, such as controllers, devices, libraries and volumes, **Write** permission to the peripheral is required in order for Data Protector Express to instruct the peripheral to write files or directories.

In the case of catalog objects that hold data, such as media, volumes, directories and files, **Write** permission is required to write data to these objects.

Affected Commands: *Run.*

Write permission is also required to run jobs. Backup jobs require **Write** permission to the appropriate devices, libraries and media. Restore jobs require **Write** permission to the appropriate volumes, directories and files.

Delete permission

Affected objects: Media, device, library, volume, directory, file, catalog.

Description: Controls whether a user can delete catalog objects or perform delete functions.

In the case of physical peripherals that perform delete functions *including overwrite functions*, such as controllers, devices, libraries and volumes, **Delete** permission to the peripheral is required in order for Data Protector Express to instruct the peripheral to delete or overwrite files or directories.

In case of catalog objects that hold data, such as media, volumes, directories and files, **Delete** permission is required to delete or overwrite the data contained in these objects.

Affected commands: *Delete, Run*.

This permission enables **Delete**, allowing the user to delete objects in the catalog.

Delete permission is also required for some types of jobs. Backup jobs require **Delete** permission to the appropriate devices, libraries and media whenever files are overwritten or media are formatted. Restore jobs require **Delete** permission to the appropriate volumes, directories and files whenever the files are overwritten.

Modify permission

Affected objects: All catalog objects.

Affected property pages: General, Selection, Options, Schedule, Logs, Storage, machine diagnostic pages.

Description: Controls whether a user can change the name of an object, modify the specified property pages of an object or move an object to a new location in the catalog.

For any object, **Modify** permission allows the user to change the object's **General page**. (This affects only the name of the object.)

For backup, restore and verify jobs, **Modify** permission *to the job* allows the user to change the job's **Selection**, **Options**, **Schedule** and **Logs** pages. Note that **Read** permission to the volume is required in order to select the volume's files and directories on the **Selection** page.

For machines, controllers and volumes, **Modify** permission allows the user to modify the diagnostic pages, such as **Communication Test** and **Ping Test**.

Affected commands: *Move…, Rename.*

This permission enables **Move…** and **Rename**, allowing users to move objects in the catalog and rename them.

Create permission

Affected objects: Home folder, user/group folder, job folder, media folder, restore job.

Description: Controls whether a user can create new objects within a container object.

For the Home folder, **Create** permission is required in order to create new User/Group folders.

For User/Group folders, **Create** permission is required in order to create new job folders, to create backup jobs, restore jobs, verify jobs, and to create media folders and media.

For Job folders, **Create** permission is required in order to create new job folders, backup jobs, restore jobs and verify jobs.

For Media folders, **Create** permission is required in order to create new Media folders and media.

For Restore Jobs, jobs that restore files in new locations or with new names require **Create** permission to the appropriate machines, volumes and directories.

Affected commands: *New…Job, New…Folder, New Object…, Paste.*

This permission enables the **New…Job** and **New…Folder** commands, for each type of job and folder. This permission also enables the **New Object…** command on the **File** menu.

This permission enables **Paste**, allowing the user to paste objects in the catalog.

Access permission

Affected Objects: All catalog objects, except Security Container, User and Group.

Affected property pages: *Permissions.*

Description: Controls whether a user can see and modify the **Permissions** page of an object.

For any object, **Access** permission allows the user to change the permissions to the object. To add a new user to the **Permissions page**, **Modify** permission is also required. A user listed on the **Permissions** page can be deleted with **Access** permission alone.

Note that **Access** permission does not allow the user to change the **Permissions** page on the Security Container, a User or a Group.

Supervisor permission

Affected objects: All catalog objects.

Affected property pages: Logon Control, Equivalencies, Groups, Members, Permissions.

Description: This permission gives the user unlimited permissions to the object and all objects below it in the catalog. Additionally, only a user with **Supervisor** permission to the Security Container can create new users and groups.

When a user has **Supervisor** permission to an object, the user is automatically granted all seven permissions to the object. Furthermore, the user cannot be denied any permission to any object below it in the hierarchy, even by assigning that user direct permission. As a result, a user with **Supervisor** permission to an object will have *all* permissions to the object and *every* object below it in the catalog tree.

Supervisor permission to the Security Container is required to create new users and groups. Additionally, the **Logon Control**, **Groups**, **Equivalencies**, **Email**, **Autoprint** and **Members page**s are only available to users with **Supervisor** permission to the Security Container.

Normally, only the Data Protector Express administrator has **Supervisor** permission to the System Container.

Affected commands: *New User, New Group*

This permission enables the **New User** and **New Group** commands, allowing the user to create new users and groups.

Chapter 13: Objects and Properties Reference

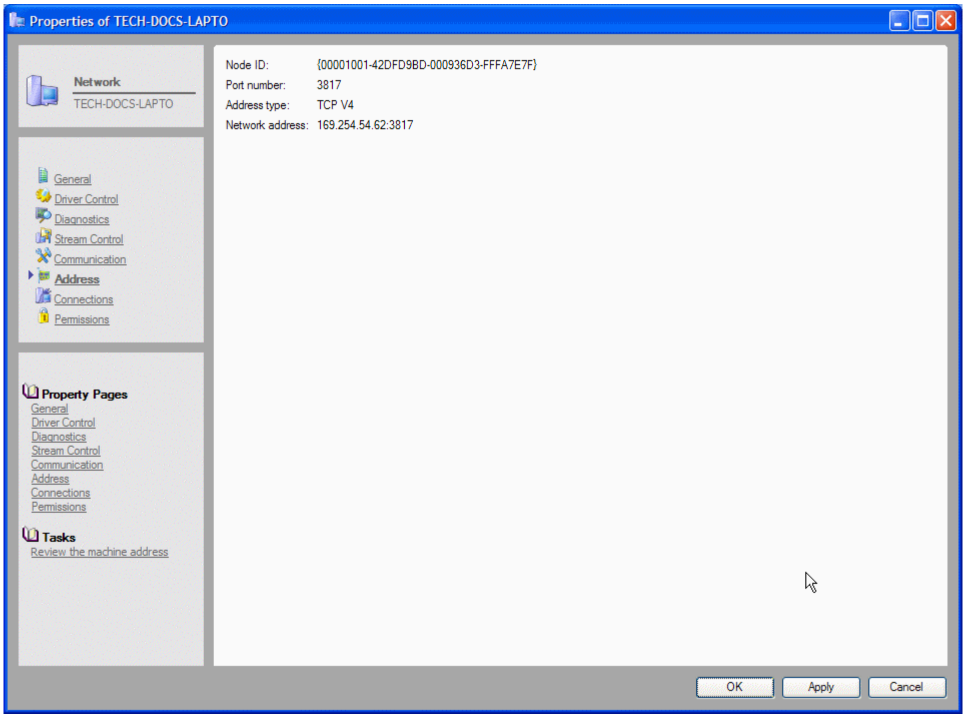
This section provides reference details for every object and property in the Data Protector Express catalog. It is organized alphabetically according to the name of each property page. The applicable objects for each property page are listed under the *Applicable Objects* heading. Various fields and settings on each property page are indicated by bold headings, followed by a short description. List box choices and field settings are indicated by bold in-line headings.

In addition to the property pages, this section provides reference information for the **Versions**, **Preferences**, **Query** and **Selection Filters** dialog boxes and the **Wizards** view.

Address page

Applicable objects: *Machine*

The **Address page** shows the machine's network address and other information.



Node ID: {00001001-42DFD9BD-000936D3-FFFA7E7F}
Port number: 3817
Address type: TCP V4
Network address: 169.254.54.62:3817

Node ID: The identification number for this machine. Data Protector Express assigns a node ID to each machine.

Port: The port number registered with IANA (Internet Assigned Numbers Authority) that is used by Data Protector Express to communicate across the network with other machines in the Data Protector Express management domain.

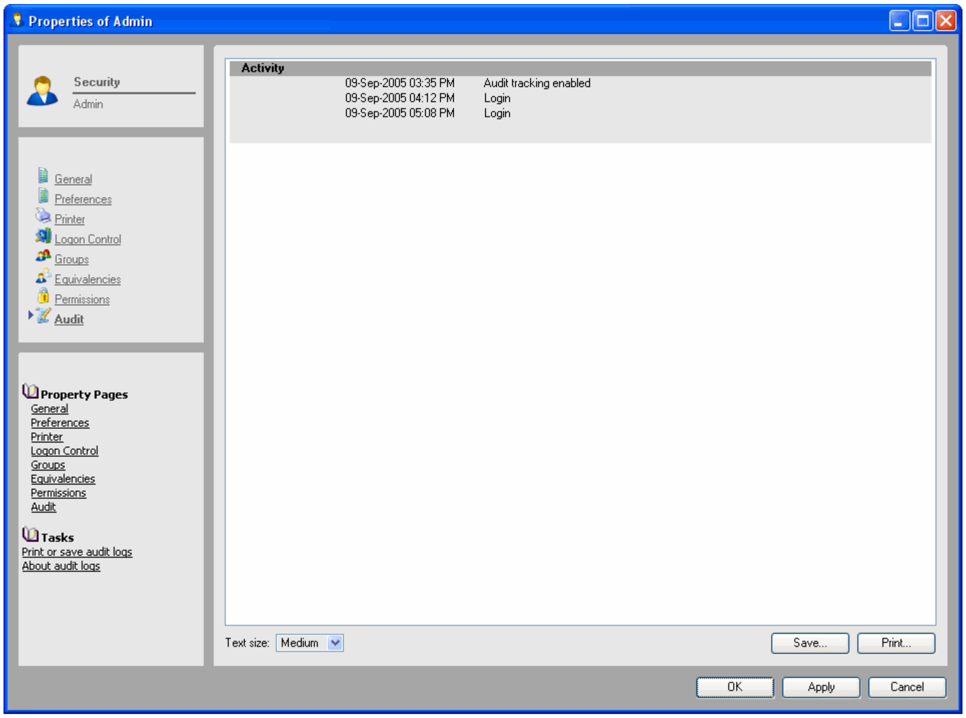
Address type: This field shows the address type that is in use to communicate with this machine, for example, TCP version 4

Network address: This field shows the IP address for this machine.

Audit page

Applicable objects: *File, Directory, Volume*

The **Audit page** shows the audit log for the object. It appears on the property page of an object for which auditing has been enabled.



```
Activity
09-Sep-2005 03:35 PM    Audit tracking enabled
09-Sep-2005 04:12 PM    Login
09-Sep-2005 05:08 PM    Login
```

To enable an object's audit log, open the **General** page of the object and check the **Enable audit** box.

When audit is enabled, Data Protector Express enters into that object's log a record every action performed on that object. For example, there will be an entry each time the object is backed up or restored. Additionally, the audit log will show the media on which versions of the object are stored.

Print: Click to print the audit log. Note that some logs can be quite long; check the length of the document before printing it.

Save: Click to save the audit log in one of the support file types.

Save your changes by clicking **Apply** or **OK**.

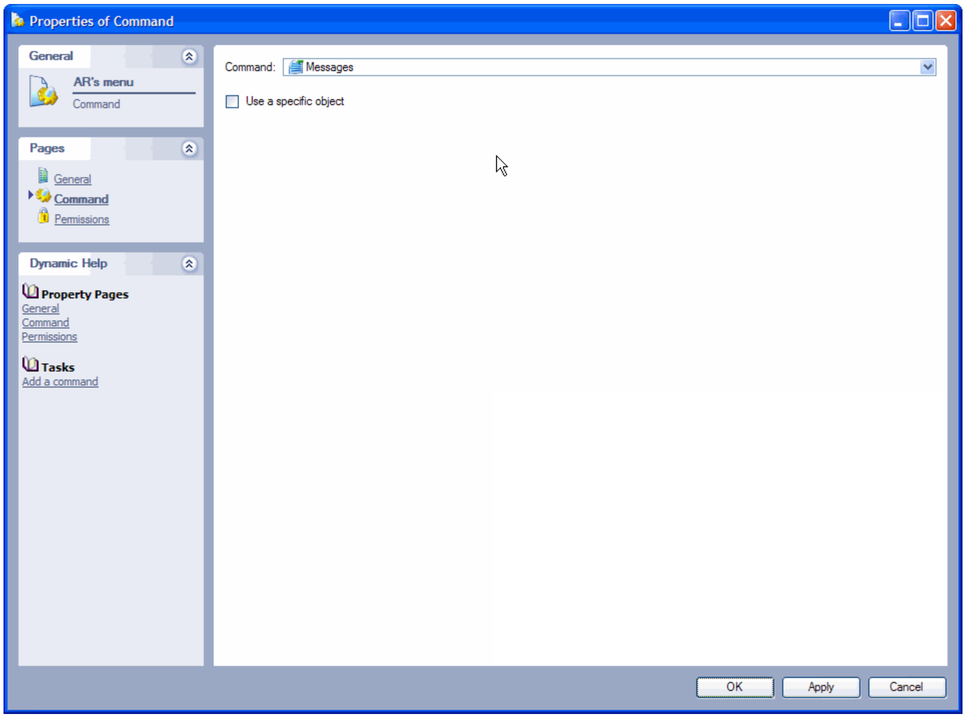
Related topics

For more information about using audit logs, see *Audit Logs* on page 131.

Command page

Applicable objects: Data Protector Express *commands*

Use the **Command** page to assign a function to a custom Data Protector Express command. Custom commands can execute any function available in Data Protector Express.



Command: Messages

☐ Use a specific object

For example, you may create a new backup command and assign the backup specific command to it. Each time you run your custom command, it performs the Data Protector Express command assigned to it. You can also associate the command with any object in the Data Protector Express management domain.

Command: Data Protector Express executes this command each time you run your custom command.

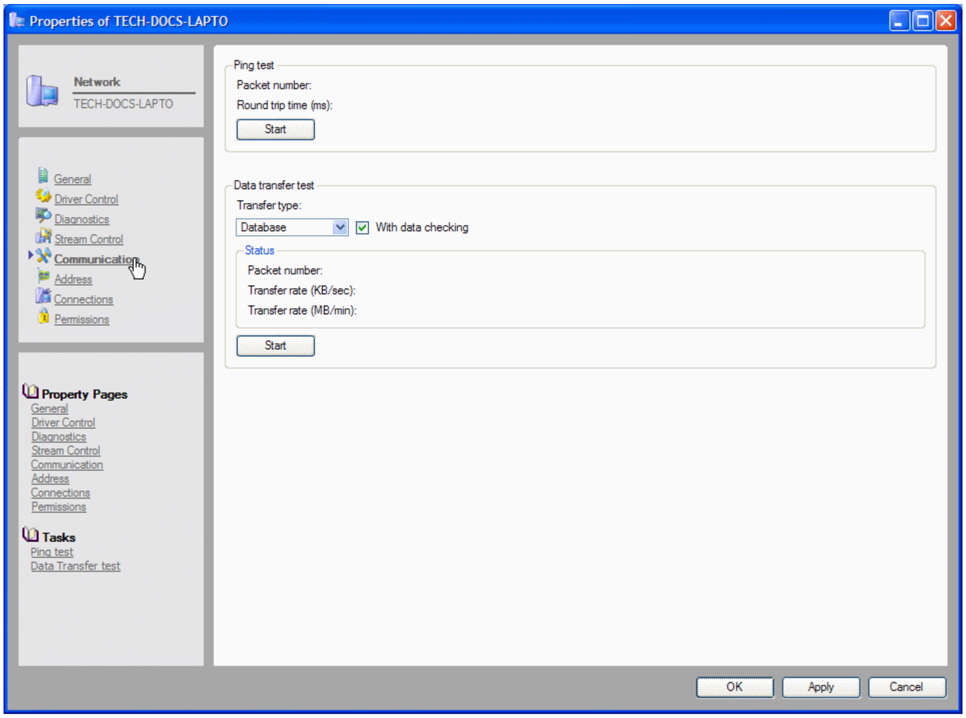
Use a specific object: Check this box if you want to limit the custom command to use only a specific object in the Data Protector Express management domain.

Object: Data Protector Express executes this command and uses the selected object as a starting point for the command. For example, select a specific file or folder and you can execute a specific command each time the file or folder is backed up. You might also set up a command that always opens your home folder with a list of its contents. Use the **Browse** button to select the object that you want to associate with this command. For example, you might decide to run this command with a specific data file on your local hard disk.

Communication page

Applicable objects: *Machine*

Use the **Communication Test page** to test the communication performance of the network. You can perform a ping test to determine how long it takes an echo packet to travel back and forth on the network. The packet is sent from the machine on which Data Protector Express is currently running to the machine whose property page is open. This page can also be used to evaluate the ability to transfer data under optimum circumstances.



Properties of TECH-DOCS-LAPTO

Ping test

Packet number:

Round trip time (ms):

Data transfer test

Transfer type: Database ☑ With data checking

Status

Packet number:

Transfer rate (KB/sec):

Transfer rate (MB/min):

Use the **Ping Test** page for a machine to measure how long it takes an echo packet to travel back and forth on the network.

Click **Start** to begin a test. Click **Stop** to end a test.

Ping test

Performing a ping test displays the following test results:

Packet No.: Shows the number of data packets sent from one machine to another up to this point in the test.

Round trip time (ms): Shows the average time for the echo packet to travel between the two machines. The time is expressed in milliseconds.

Data Transfer test

NOTE: To accurately test network performance, stop the Data Protector Express service on the machine to be tested (see *Appendix E* — Data Protector Express *Service* in the Data Protector Express *Installation Guide*). Then start Data Protector Express and access the **Communication Test page**.

Select the data transfer type you want to test:

Database: Simulates data transfer during a backup job of a database. The local machine sends a large packet; the remote machine sends small replies acknowledging receipt of the data.

Backup: Simulates data transfer during a backup job. The local machine sends a large packet; the remote machine sends small replies acknowledging receipt of the data.

Restore: Simulates data transfer during a restore job. The remote machine sends a large packet; the local machine sends small replies acknowledging receipt of data.

Full (large packet): Send a large-sized packet of data between remote and local machine.

Select **With data checking** to send a known byte pattern between machines. The receiving machine will verify the pattern.

Click **Start** to begin the test. As the test runs, the **Communication status** fields reflect the results of the test.

Click **Stop** to end the test. The final results appear in the **Communication status** fields.

Status

The following communication status information is displayed on this page:

Packet number: This is the number of data packets sent from one machine to another up to this point in the test.

Transfer rate (KB/sec): The rate at which the test data packets are being transferred in kilobytes per second.

Transfer rate (MB/min): The rate at which the test data packets are being transferred in megabytes per minute.

NOTE: Use this information to identify current transfer rates between machines. If the rates are less than expected, try one or more Data Protector Express optimization strategies.

Related topics

For information about optimizing backup jobs by increasing data transfer rates, see *Strategies for Faster Jobs* on page *156*.

Configuration page

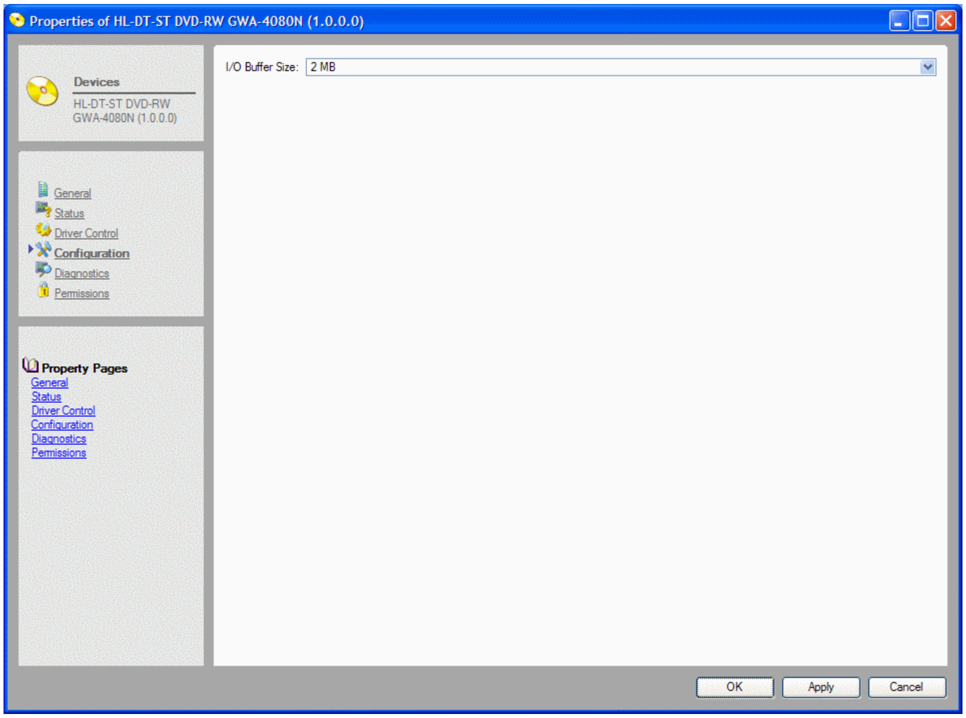
Applicable objects: *Devices, Storage folder, selected objects*

The **Configuration** page presents the settings that can be configured for the selected device or other object. For example, if you are configuring a virtual library, only settings related to virtual libraries appear on this page. You can configure the following devices in Data Protector Express:

- *Devices*
- *Virtual libraries*
- *Storage slots*
- *Email*
- *File system stream*
- *Microsoft Exchange Server*
- *Microsoft SQL Server*
- *Certificate Services*

Device configuration

This page applies to devices such as CDs, DVDs, tapes, Iomega REV devices, virtual devices, and other storage devices.

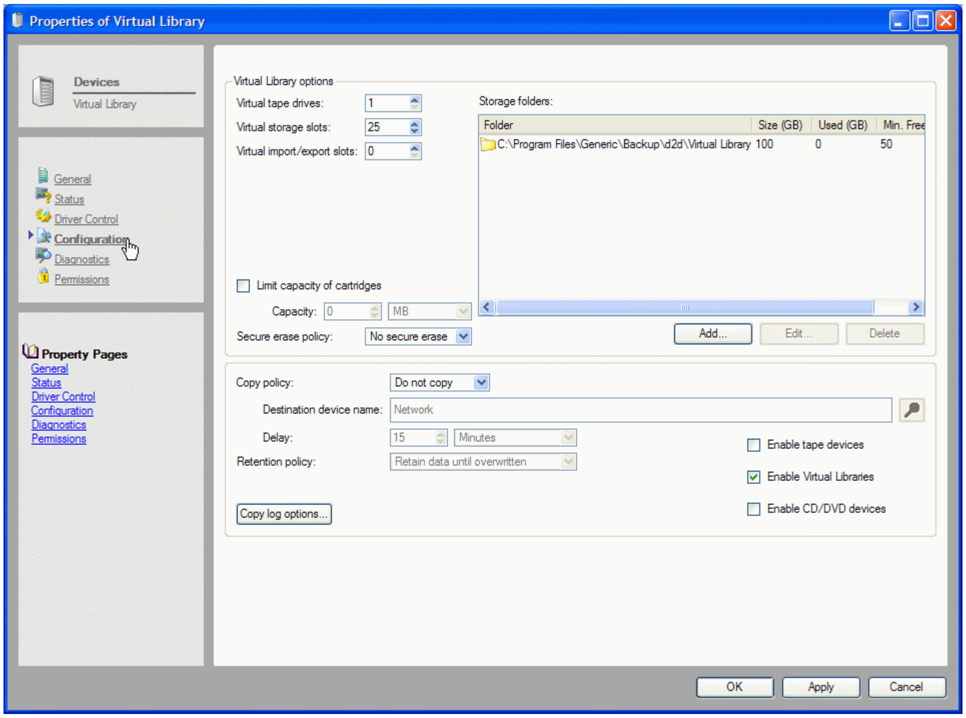


Properties of HL-DT-ST DVD-RW GWA-4080N (1.0.0.0)

I/O Buffer Size: 2 MB

I/O buffer size: The size of the input/output temporary memory space on the device that holds data until it can be written to the DVD or CD (e.g., 256 KB, 256 MB, etc.).

Virtual library configuration



Properties of Virtual Library

Devices
Virtual Library

Virtual Library options

Virtual tape drives: 1

Virtual storage slots: 25

Virtual import/export slots: 0

Storage folders:

Folder	Size (GB)	Used (GB)	Min. Free
C:\Program Files\Generic\Backup\d2d\Virtual Library	100	0	50

□ Limit capacity of cartridges

Capacity: 0 MB

Secure erase policy: No secure erase

Copy policy: Do not copy

Destination device name: Network

Delay: 15 Minutes

Retention policy: Retain data until overwritten

□ Enable tape devices

☑ Enable Virtual Libraries

□ Enable CD/DVD devices

Virtual library options

Virtual tape drives: The number of virtual tape drives you set up for the current virtual library. The default is 1 (one).

Virtual storage slots: The number of storage slots for the virtual library. The default is 25.

Storage folder: The storage folder to which the virtual library belongs. The default storage folder is selected. Click the **Add** or **Delete** buttons to add or remove storage folders.

Secure erase policy: Determines whether or not virtual media is erased with a secure erase or quick erase command of the backup job. You can determine the erase policy for each backup job. For virtual devices, you can set a secure erase policy that overrides the policy set for the backup job. Choices are:

- **No secure erase:** Select this option if you do not want to erase virtual media after it has been copied to a physical device.
- **Secure erase:** Select this option to perform a secure erase command on virtual media once it has been removed from the virtual library.

D2D2T options

If available in your installation, you can set up policies to copy backups stored in this virtual library to other devices.

Copy policy: Determines whether or not files backed up to the virtual device are copied to alternate media.

Destination device name: The device in the Data Protector Express management domain to which virtual backups will be copied. Note that you can copy your backups to either a physical or virtual device. You can also include or exclude specific types of devices. Check boxes are available to enable all tape devices, all virtual devices, or all CD/DVD devices.

Delay: Determines the length of time Data Protector Express waits before copying virtual backups to another device.

Retention policy: Determines how long backups are stored on virtual media before they are overwritten by subsequent jobs. Choices are:

- **Retain data until overwritten:** Select this option to keep the data on the virtual device until the data is written to another backup device; that is, there are newer versions of the data in other backup jobs.
- **Retain data until copied:** Select this option to keep the data on the virtual device until it is copied to a physical device.
- **Retain data until space is needed:** Select this option to keep the data on the virtual device indefinitely. With this policy, Data Protector Express retains the data in the virtual library until the space is needed by subsequent virtual backups.

Copy log options: Click this button to set up logs for the copy jobs. It is recommended that you establish a procedure for reviewing the logs for copy jobs to help you ensure that your data is available on alternate media.

Enable tape devices: Select this checkbox to use any available tape device.

Enable Virtual Libraries: Select this checkbox to use any available virtual library.

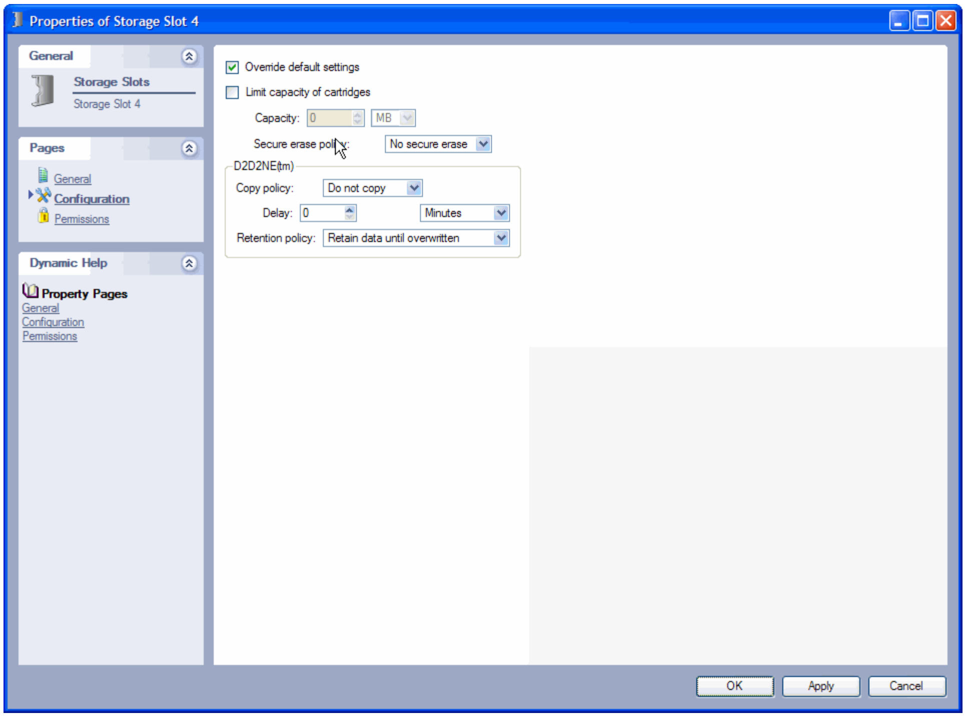
Enable CD/DVD devices: Select this checkbox to use any available CD or DVD device.

Enable CD/DVD devices: Select this checkbox to use any available CD or DVD device.

Enable removable drives: Select this checkbox to use any available removable drive.

Storage slot configuration

Use this page to manage the virtual media represented by the storage slot.



☑ Override default settings

☐ Limit capacity of cartridges

Capacity: 0 MB

Secure erase policy: No secure erase

D2D2NE(tm)

Copy policy: Do not copy

Delay: 0 Minutes

Retention policy: Retain data until overwritten

Override default settings: Select this checkbox to edit the following options.

Limit the capacity of cartridges: Select this checkbox to set a limit on the capacity of cartridges.

Capacity: Specify the capacity in megabytes or gigabytes.

Secure erase policy: Determines whether or not virtual media is erased with a secure erase or quick erase command of the backup job. You can determine the erase policy for each backup job. For virtual devices, you can set a secure erase policy that overrides the policy set for the backup job. Choices are:

- **No secure erase:** Select this option if you do not want to erase virtual media after it has been copied to a physical device.
- **Secure erase on removal:** Select this option to perform a secure erase command on virtual media once it has been removed from the virtual library.

D2D2T options

If available in your installation, you can set up policies to copy backups stored in this virtual library to other devices.

Copy policy: Determines whether or not files backed up to the virtual device are copied to alternate media.

Delay: Determines the length of time Data Protector Express waits before copying virtual backups to another device.

Retention policy: Determines how long backups are stored on virtual media before they are overwritten by subsequent jobs. Choices are:

- **Retain data until overwritten:** Select this option to keep the data on the virtual device until the data is written to another backup device; that is, there are newer versions of the data in other backup jobs.
- **Retain data until copied:** Select this option to keep the data on the virtual device until it is copied to a physical device.
- **Retain data until space is needed:** Select this option to keep the data on the virtual device indefinitely. With this policy, Data Protector Express retains the data in the virtual library until the space is needed by subsequent virtual backups.

Email settings

SMTP email settings can be configured for the Data Protector Express Data Protector Express management domain.

For SMTP email settings provide the following:

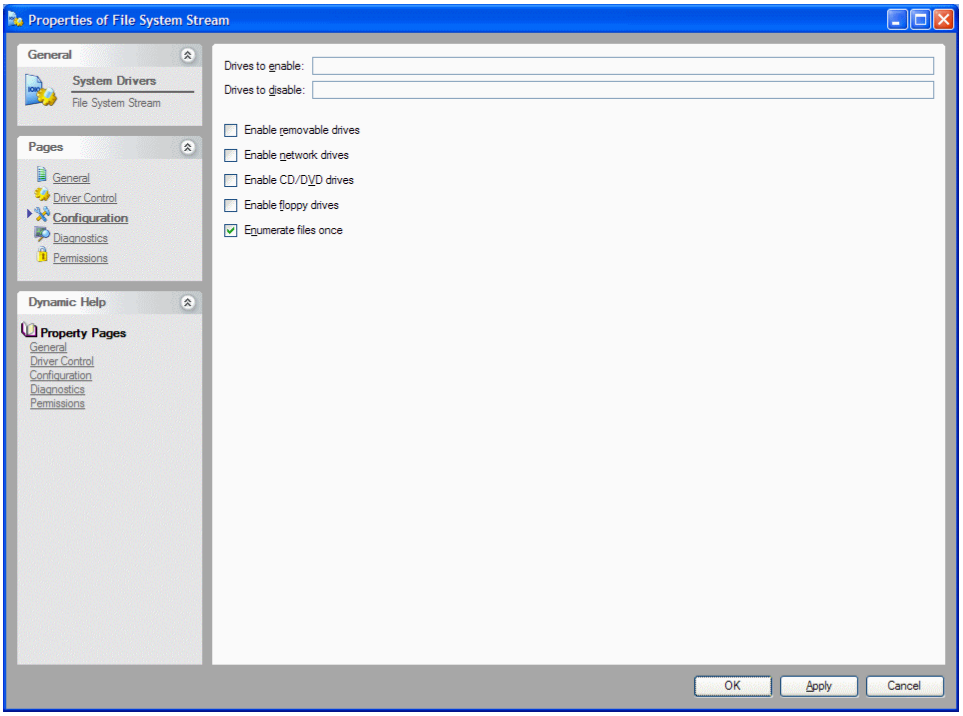
Server address: Enter the name of the mail server.

Server port: Enter the appropriate SMTP port. The **Server port** default is **25**, which is usually the correct value. If you are using a proxy server, you may have to enter a different **Server port**.

From address: Enter the email address to be entered in the *From* field for each job log email. This email address must be valid.

File system stream configuration

Use the **Configuration** page for file system drivers to enable or disable mapped drives for backups. Data Protector Express uses these settings while creating a list of files or folders for inclusion in backup jobs.



Drives to enable:

Drives to disable:

□ Enable removable drives

□ Enable network drives

□ Enable CD/DVD drives

□ Enable floppy drives

☑ Enumerate files once

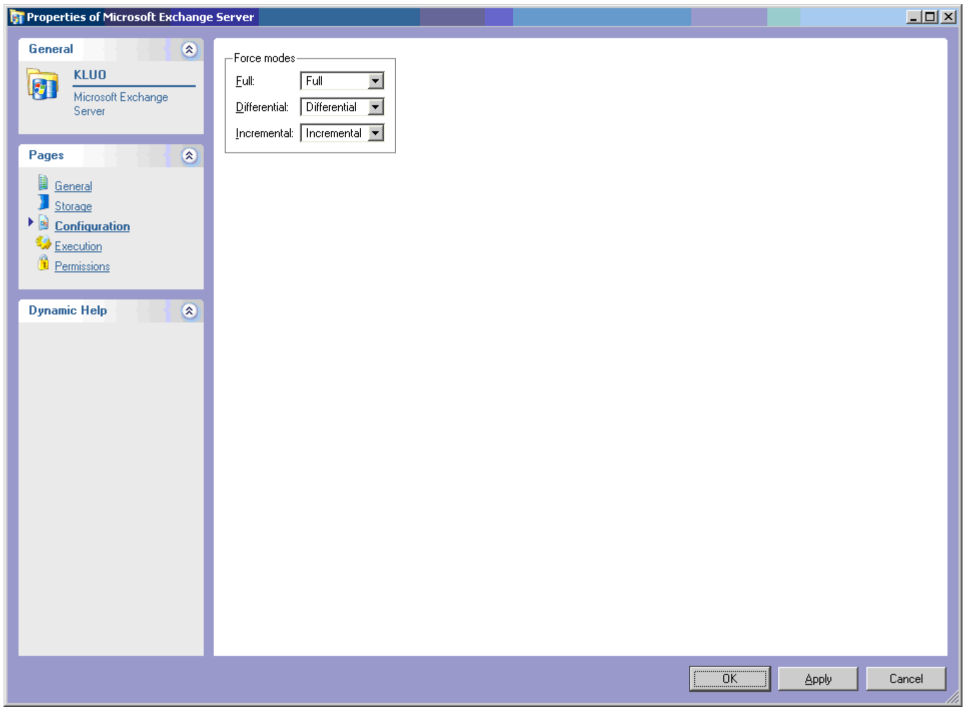
Drives to enable: Enter the list of drives that you want to enable for backups for the current machine. Include in the list each drive that has been mapped on the machine. Enter the list of drives as a single string of letters (e.g., GHIJKLMNO).

Drives to disable: Enter each drive in this list that you do not want to be included in backups. Data Protector Express will ignore any files or folders on these drives during backups. Enter the list of drives as a single string of letters (e.g., GHIJKLMNO).

Check the following settings to create a list of drives for inclusion in backup jobs:

- **Enable removable drives:** Select this setting to include files located on removable drives in backups.
- **Enable network drives:** Select this setting to include files located on network drives in backups.
- **Enable CD/DVD drives:** Select this setting to include files located on CD or DVD drives in backups.
- **Enable floppy drives:** Select this setting to include files located on located on floppy drives in backups.
- **Enumerate files once:** Select this setting to include files only once in backups. Data Protector Express uses this setting to limit the number of duplicate files that are included in any backup job.

Microsoft Exchange Server configuration



Force modes

Full: Full

Differential: Differential

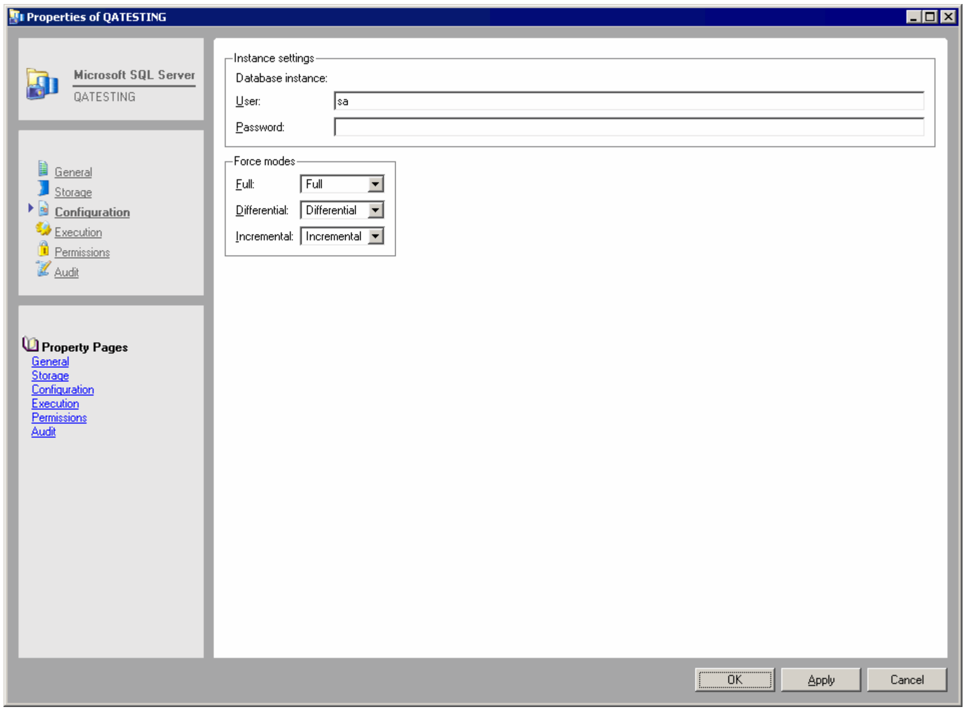
Incremental: Incremental

Force modes: The **Force modes** settings control how Data Protector Express backs up the Microsoft Exchange Server storage group files. This setting overrides the backup mode setting for a backup job when an Exchange Server database is selected along with other files.

NOTE: There is no user name configuration requirement for a Microsoft Exchange Server. Data Protector Express logs on to the Exchange Server with the administrator settings that were provided in Windows when the server was set up. Since no other user could modify the server, there is no need to provide additional user name information in Data Protector Express. Consequently, only a Microsoft Exchange Server administrator will be able to perform backups of an Exchange Server with Data Protector Express.

For additional information, see *Appendix F - Working with Microsoft Exchange Server* on page 268.

Microsoft SQL Server configuration



Instance settings

Database instance:

User: sa

Password:

Force modes

Full: Full

Differential: Differential

Incremental: Incremental

User name: The name of the Microsoft SQL Server administrator who has permissions to back up the server.

Password: The password of the SQL Server administrator who may perform backups of the server.

Force modes: The **Force modes** settings control how Data Protector Express backs up the Microsoft SQL Server database instances. This setting overrides the backup mode setting for a backup job when a Microsoft SQL Server database instance database is selected along with other files.

For additional information, see *Appendix G - Working with Microsoft SQL Server* on page 275.

Certificate services configuration page

Use this page to override the backup modes that jobs specify.

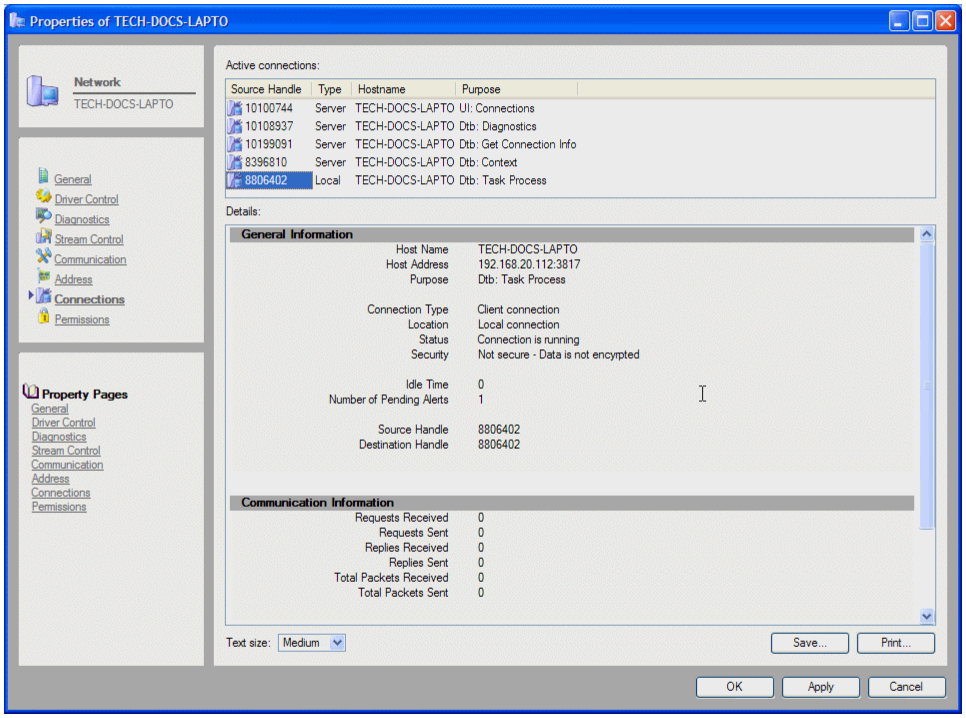
Force modes: Set the modes to use when a job specifies **Full**, **Differential**, and **Incremental** modes For example, if you specify Full for the **Incremental** mode, Data Protector Express will run a full backup even though a backup job specifies an incremental mode.

Connections page

Applicable objects: *Machine*

The **Connections** page shows the active connections for this machine. It is for information purposes only.

Connections are established for varying purposes and are automatically opened and closed as necessary.



Active connections:

Source Handle	Type	Hostname	Purpose
10100744	Server	TECH-DOCS-LAPTO	UI: Connections
10108937	Server	TECH-DOCS-LAPTO	Dtb: Diagnostics
10199091	Server	TECH-DOCS-LAPTO	Dtb: Get Connection Info
8396810	Server	TECH-DOCS-LAPTO	Dtb: Context
8806402	Local	TECH-DOCS-LAPTO	Dtb: Task Process

Details:

General Information

Host Name	TECH-DOCS-LAPTO
Host Address	192.168.20.112:3817
Purpose	Dtb: Task Process
Connection Type	Client connection
Location	Local connection
Status	Connection is running
Security	Not secure - Data is not encrypted
Idle Time	0
Number of Pending Alerts	1
Source Handle	8806402
Destination Handle	8806402

Communication Information

Requests Received	0
Requests Sent	0
Replies Received	0
Replies Sent	0
Total Packets Received	0
Total Packets Sent	0

Text size: Medium

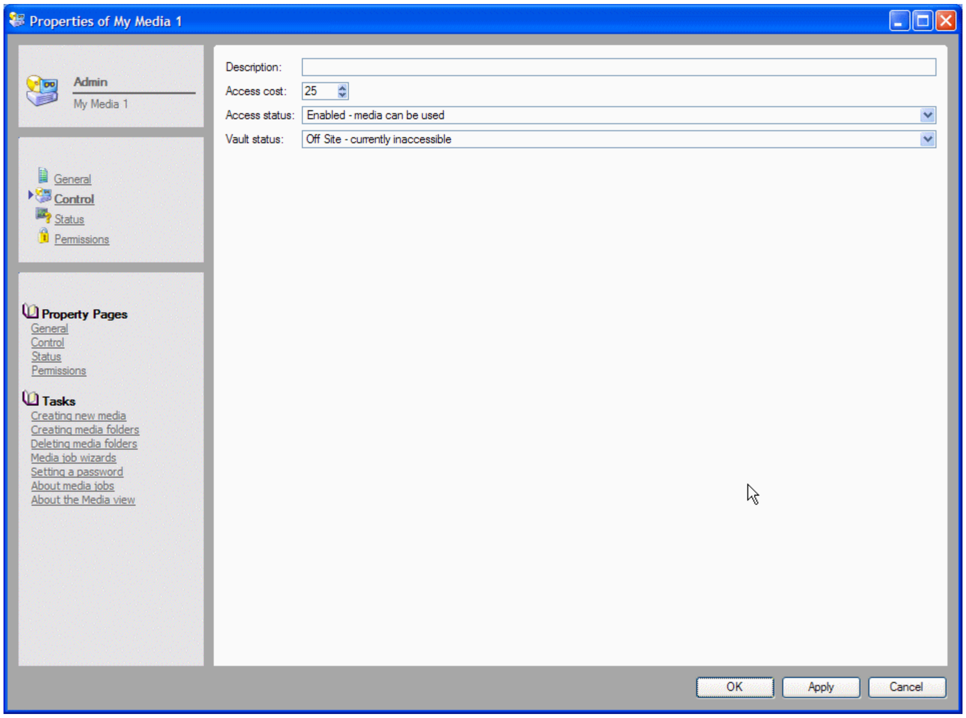
Active connections: Lists the currently active connections for this machine.

Details: Shows detailed information about the selected active connection.

Control page

Applicable objects: *Media*

The **Control** page shows information about the current media that Data Protector Express stores in its catalog and whether or not the media is available for use during restore jobs.



Description:
Access cost: 25
Access status: Enabled - media can be used
Vault status: Off Site - currently inaccessible

Description: Enter a description for the current media. Data Protector Express retains this description so long as the media is in use. Use the **Apply** command to save the description.

Access cost: Used during restore jobs, this information determines whether the media would result in a faster restore operation than other media. If Data Protector Express finds two or more copies of the same version of a file or object, Data Protector Express restores the version with the lowest cost. For example, if there is one version of a file on a virtual library and one on physical media, Data Protector Express will decide that it is "cheaper" and faster to restore from the virtual library.

Access status: Shows whether or not Data Protector Express will try to find or request a particular media even if it is still in the catalog. When access status is enabled, the media can be used. When access status is disabled, the media cannot be used. For example, if you take media offsite and you do not want Data Protector Express to access it during restore jobs, set the access status to disabled.

Vault status: Shows the location of the media - offsite or on site. Data Protector Express uses this status to determine whether or not the media can be used during a restore job. When set to on site, the media is considered to be accessible for restore jobs. When set to offsite, the media is not accessible.

Related topics

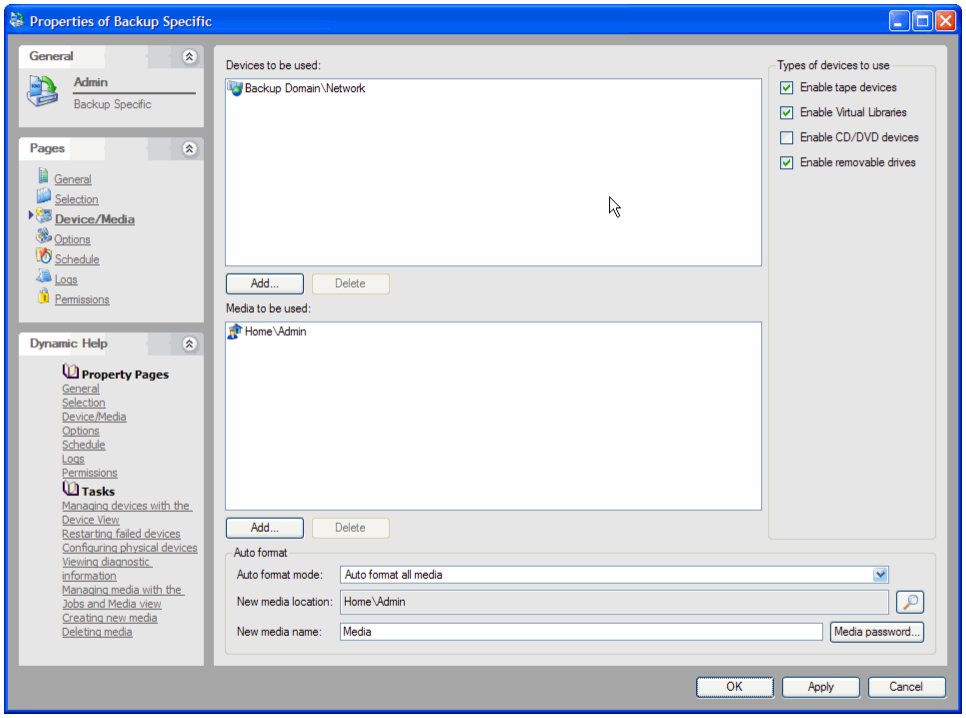
For information about how to format media, see *Creating new media* on page 148.

Device/Media page

Applicable objects: *Backup Job, Verify Job, Restore Job, Media Job*

The **Device/Media** page shows the devices and media that will be used by the current job. For backup jobs, devices and media listed here are the destination. For restore jobs, they are the source for locating files to be retrieved. For media jobs, these are the devices and media that will be formatted, identified, moved, and so on.

You can add more devices and media to be used during jobs, or you can remove them. By default, Data Protector Express uses any available device or media on the network.



Properties of Backup Specific

Devices to be used:
Backup Domain\Network

Media to be used:
Home\Admin

Types of devices to use
☑ Enable tape devices
☑ Enable Virtual Libraries
☐ Enable CD/DVD devices
☑ Enable removable drives

Auto format
Auto format mode: Auto format all media
New media location: Home\Admin
New media name: Media

Device to be used

Specifies which tape drive or other removable media device Data Protector Express will use to run the backup, restore or verify job.

By default, Data Protector Express sets this setting to the network container. When running the job, Data Protector Express will use whatever device it finds on the network. If there is only one device in your Data Protector Express management domain or if you only have permissions to one device, there is no reason to change this setting.

However, if there are several devices on your network and you need to select a specific device, specify which device the job should use by selecting it from the **Device** list. (If a machine has only one device, you can just select the machine and not the device.)

To use a device that is not shown in the **Device** list, click the **Add…** button and select the new device from the **Browse** dialog box. Then select the undesired network container from the **Device** list, click **Delete** and confirm the deletion.

Types of devices to use

You can select the types of devices you want Data Protector Express to use during a job. For example, you can enable or disable tape devices, virtual libraries, or CD/DVD devices. By default, CD and DVD devices are disabled.

Media to be used

(Backup jobs only)

Specifies the media folder in which the tape or other removable media are stored. Data Protector Express will look here for media to use with this job.

The default folder is the current User/Group folder. If you wish to use media from another folder, specify which folder by selecting it from the **Media** list.

If you wish to use a folder that is not shown in the **Media** list, click the **Add…** button and select the new folder from the **Browse** dialog box.

Auto format information

Auto format mode

(Backup jobs only)

Determines whether or not Data Protector Express will format media automatically.

Before data can be written to media, the media must be formatted. When media is formatted, any data on it is lost. Tapes and other media are formatted when Data Protector Express does not recognize the media, that is, when it has no information in its catalog about that particular media. This will occur when the media is blank, it has been erased, it is first used or it has been deleted from the catalog.

The Auto format mode is either No auto format, Auto format blank media or Auto format all media.

No auto format: Instructs Data Protector Express to send an alert to the alert window if it encounters media that needs to be formatted (either blank or unrecognized media). While waiting for a user reply, Data Protector Express scans the network for devices with the media it was expecting. When selected, Data Protector Express waits for a reply to the alert before formatting unrecognized media.

Auto format blank media only: Instructs Data Protector Express to automatically format all new or blank media. However, if Data Protector Express encounters unrecognized media, it sends an alert to the alert window and then scans the network for the media it was expecting. This setting can help prevent data from being accidentally destroyed by formatting, while not needlessly querying the user before formatting a blank media.

Auto format all media: Instructs Data Protector Express to automatically format all of the media inserted into the tape drive which require formatting. With this setting selected, Data Protector Express will automatically format all new (or blank) media and all unrecognized media.

New media location

(Backup jobs only)

Specifies the folder in which Data Protector Express will store any new media created while the job is run. By default, Data Protector Express stores media in the current User/Group folder; the media will appear there on the **Media** and **Catalog** views. You can also store the media in a separate media folder inside the User/Group folder.

Select the folder in which to store any new media by clicking the **Browse** button. Then select the folder from the **Browse** dialog box. If the folder does not exist, use the **Jobs and Media** view to create it first. Then you can select **New media locations**.

When Data Protector Express runs any scheduled automatic rotation job, it automatically creates new media folders for the job. The folders are organized by the name of the job and the various rotation sets in that job. There is no reason to create these folders manually. Data Protector Express will automatically create these folders for you.

NOTE: Data Protector Express does not automatically create new media folders for manual jobs.

New Media Name

(Backup jobs only)

Specifies the name Data Protector Express gives to any new media it creates while running the job. For scheduled automatic rotation jobs, Data Protector Express automatically updates this setting to match the media's place in the rotation schedule.

For manual rotation and unscheduled jobs, Data Protector Express assigns any new media it creates the name listed in this field. This is also true for automatic rotation jobs that are "forced" to run.

Media Password…

(Backup jobs only)

When a job creates new media, you can assign that media a password. A password prevents the media from being imported into another Data Protector Express catalog and can be an important part of your overall security plan.

To have the job assign a password to the new media, click the **Media Password…** button and type and confirm your password.

Note that passwords can only be assigned when media is formatted. Additionally, media passwords are only required when importing media.

Media options automatically updated

Some settings shown on the **Device/Media** page are automatically updated as a Data Protector Express runs a job. These updated settings fall into two categories: (1) settings that are updated automatically when Data Protector Express runs a scheduled *automatic media rotation* job (default or custom), but specified manually in *unscheduled* and *manual media rotation* jobs; and (2) settings that are always specified manually by the user. For more information, see *Forcing scheduled jobs to run* on page 125. For more information on scheduling a job, see *Choosing a Schedule Type* on page 90.

When an automatic media rotation job is scheduled, the job appears on the **Job Status** view with an indication of the date and time the job is scheduled to run. When Data Protector Express runs the scheduled jobs listed on the **Job Status** view, it automatically updates several settings on the **Device/Media** page: **New media location** and **New media name**.

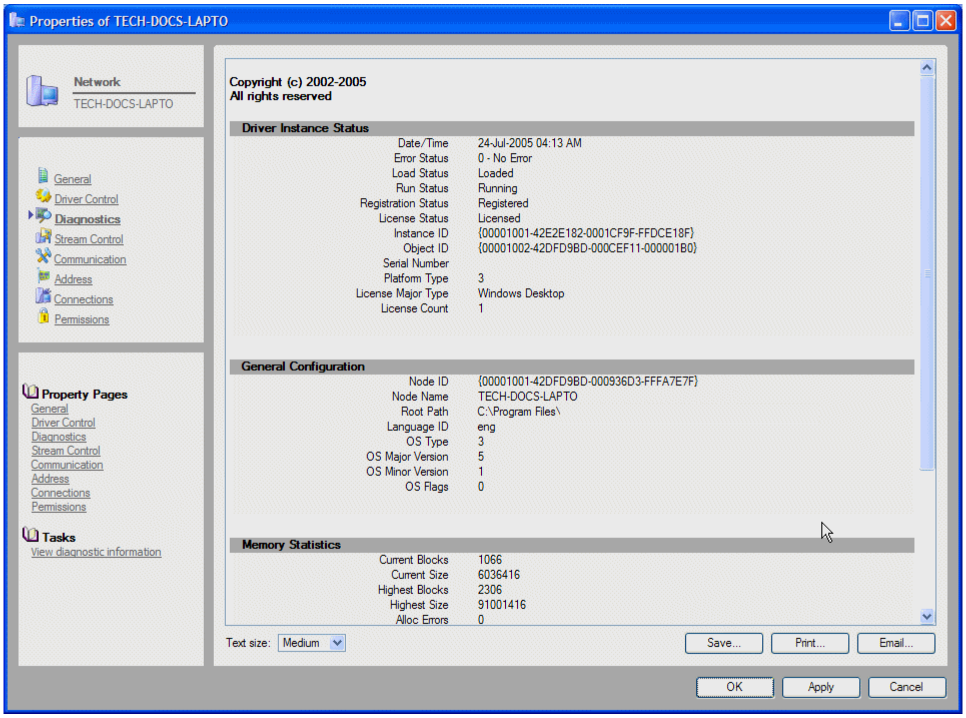
When you run an unscheduled or manual rotation job, Data Protector Express always uses the settings selected by the user.

Diagnostics page

Applicable objects: *Machine, Drivers, and Devices*

The **Diagnostics** page provides detailed information about the current machine or driver object. It is available for all active machines, drivers and devices, including controllers, logical tape formats, services and virtual libraries.

You can print a diagnostics report, save it to a file, or email it to a specified address. Click the **Save** button and choose a file type. Support file types are HTML, text, Comma separated, and XML. To save your changes, click **Apply** or **OK**.



Copyright (c) 2002-2005
All rights reserved

Driver Instance Status

Date/Time	24-Jul-2005 04:13 AM
Error Status	0 - No Error
Load Status	Loaded
Run Status	Running
Registration Status	Registered
License Status	Licensed
Instance ID	{00001001-42E2E182-0001CF9F-FFDCE18F}
Object ID	{00001002-42DFD9BD-000CEF11-000001B0}
Serial Number	
Platform Type	3
License Major Type	Windows Desktop
License Count	1

General Configuration

Node ID	{00001001-42DFD9BD-000936D3-FFFA7E7F}
Node Name	TECH-DOCS-LAPTO
Root Path	C:\Program Files\
Language ID	eng
OS Type	3
OS Major Version	5
OS Minor Version	1
OS Flags	0

Memory Statistics

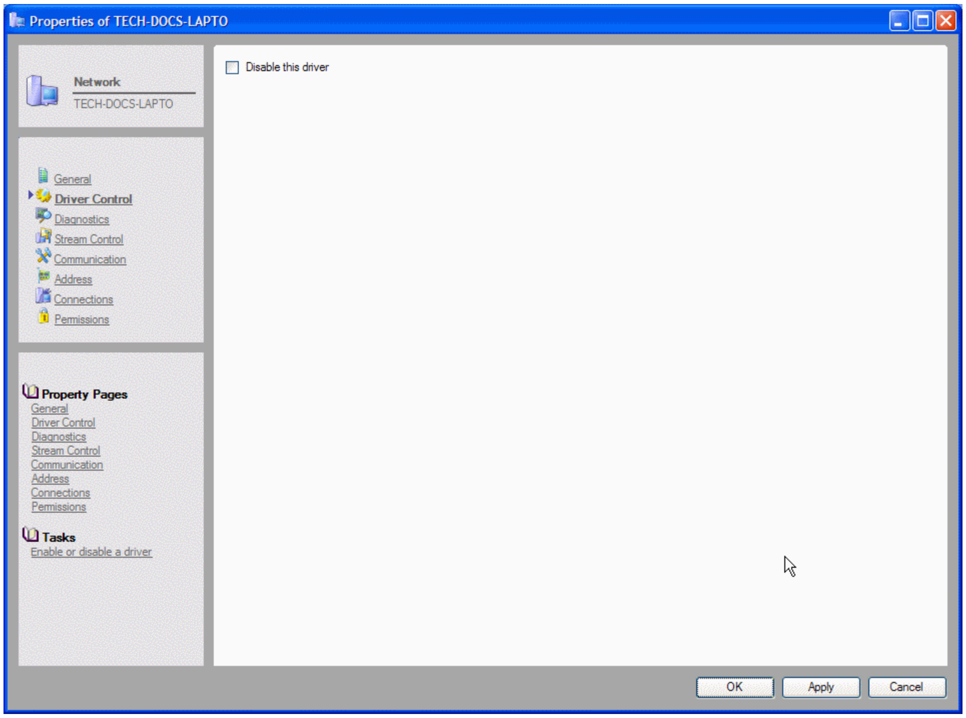
Current Blocks	1066
Current Size	6036416
Highest Blocks	2306
Highest Size	91001416
Alloc Errors	0

Text size: Medium

Driver control page

Applicable objects: *Machine*

The **Driver control** page shows the available drivers for the selected machine. It provides users with a single view of all drivers associated with the machine. (The **Driver control** page also appears on the **Catalog** view in various locations.) It is for information purposes only.



□ Disable this driver

Drivers are used by Data Protector Express for differing purposes. The name of each folder on this page indicates the purpose of the drivers in that folder. To disable a driver, check its box, then click **Apply** or **OK** to save your changes.

Drivers that are marked with a yellow exclamation point are currently unavailable for some reason. The device could be initializing or there may be an actual failure. For example, a controller driver may be marked with this icon during device initialization. Once initialized, the exclamation disappears when you press **F5**. When there is an actual failure, you must correct the problem and restart the driver. You must exit and restart Data Protector Express and the Data Protector Express service. When Data Protector Express restarts, it will reinitialize these devices.

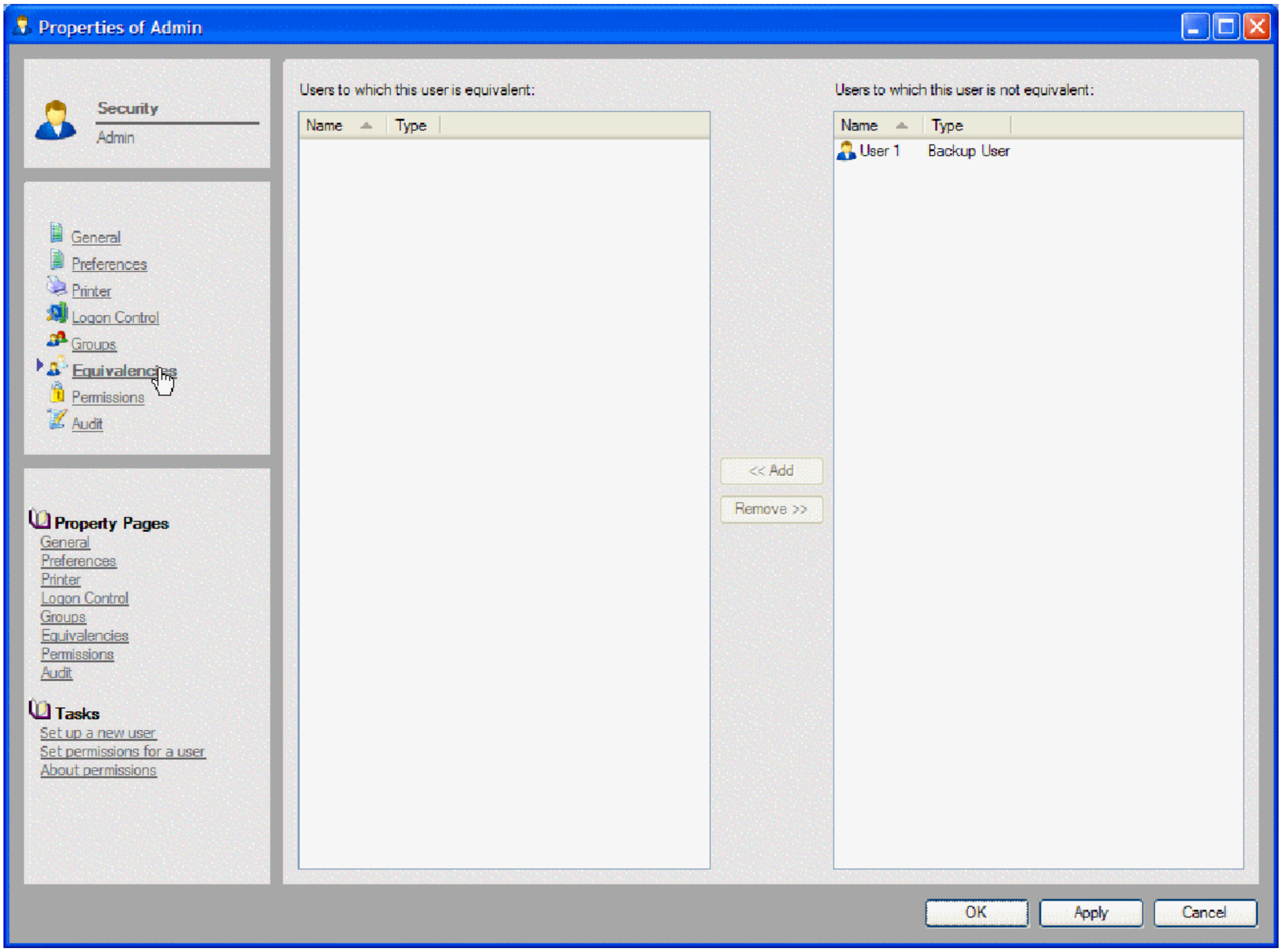
Equivalencies page

Applicable objects: *User*

The **Equivalencies** page is used to assign an individual user effective permissions equivalent to the effective permissions of another user.

Note that equivalencies only work in one direction; they are not reciprocal. The current user's effective permissions (the effective permissions of the user whose property page is open) will be calculated using the direct and inherited permissions of the user they are made equivalent to. For example, if User 1 is made equivalent to User 2, the effective permissions of are calculated using *both* of their direct permissions. However, the effective permissions of User 2 remained unchanged.

Additionally, note that users can gain *direct* permissions to objects either as users, as a result of equivalencies or as members of a group. When the direct permissions result from multiple sources, Data Protector Express uses all of the sources to determine the permissions.



Users to which this user is equivalent:

Name	Type

Users to which this user is not equivalent:

Name	Type
User 1	Backup User

Users to which this user is equivalent: Lists those users to whom the current user (whose property page is open) is equivalent.

Users to which this user is not equivalent: Lists those users to whom the current user (whose property page is open) is *not* equivalent.

Add: To add a user to the equivalent list, select the user from the right window pane and click **Add**. The user is moved to the left window pane.

Remove: To remove a user from the equivalent list, select the user from the left window pane and click **Remove**. The user is moved to the right window pane.

Related topics

For information about related features, refer to the following documentation:

- *Effective Permissions* on page 44
- *Examples of determining effective permissions* on page 44

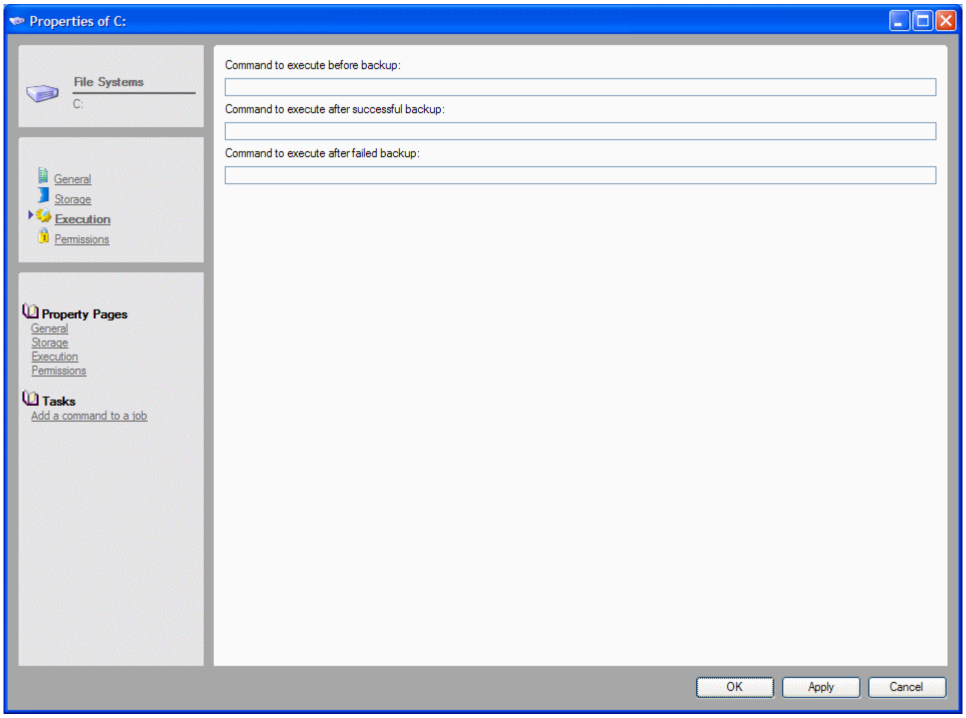
Execution page

Applicable objects: *Volume, Directory, File, and Media*

Use the **Execution** page to execute operating system commands before and after backup jobs. These commands can execute programs, batch files or scripts.

The default path for these programs, batch files or scripts is the same as the path of the current object (e.g., the volume, directory or file whose property page is open). You can specify another path if necessary.

You must enter commands that are appropriate to the operating system. On Windows systems, you can specify **.exe** and **.bat** files, such as **c:\mybatch.bat**. On NetWare systems, you can specify **.ncf** files, such as **mybatch.ncf**. On Linux systems, you can specify shell scripts, such as **myscript.sh**. You can also specify any settings with these commands, according to the operating system.



For example, you may want to temporarily close certain files before backing them up. You could prepare one batch file to close these files and one to open these files after a successful backup. You could also prepare a batch file to execute if the backup job fails. Then you would enter these commands in the appropriate fields.

NOTE: If a command takes more than 15 seconds to execute, Data Protector Express continues the job. This is a precaution in case the command fails in some way, which would prevent Data Protector Express from continuing. If the command must be run, we recommend that you assign it to the next object up in the tree view.

Command to execute before backup: Data Protector Express executes this command before it opens the current object for backup. Enter the command with its path (if necessary) and any settings.

Command to execute after successful backup: Data Protector Express executes this command after it has successfully backed up and closed the current object. Enter the command with its path (if necessary) and any settings.

NOTE: If the backup job includes a verify step, Data Protector Express executes this command if the current object was backed up successfully. Data Protector Express closes the object and executes this command. Then it performs the verify step.

Command to execute after failed backup: Data Protector Express executes this command after it closes the current object if the backup fails. Enter the command with its path (if necessary) and any settings.

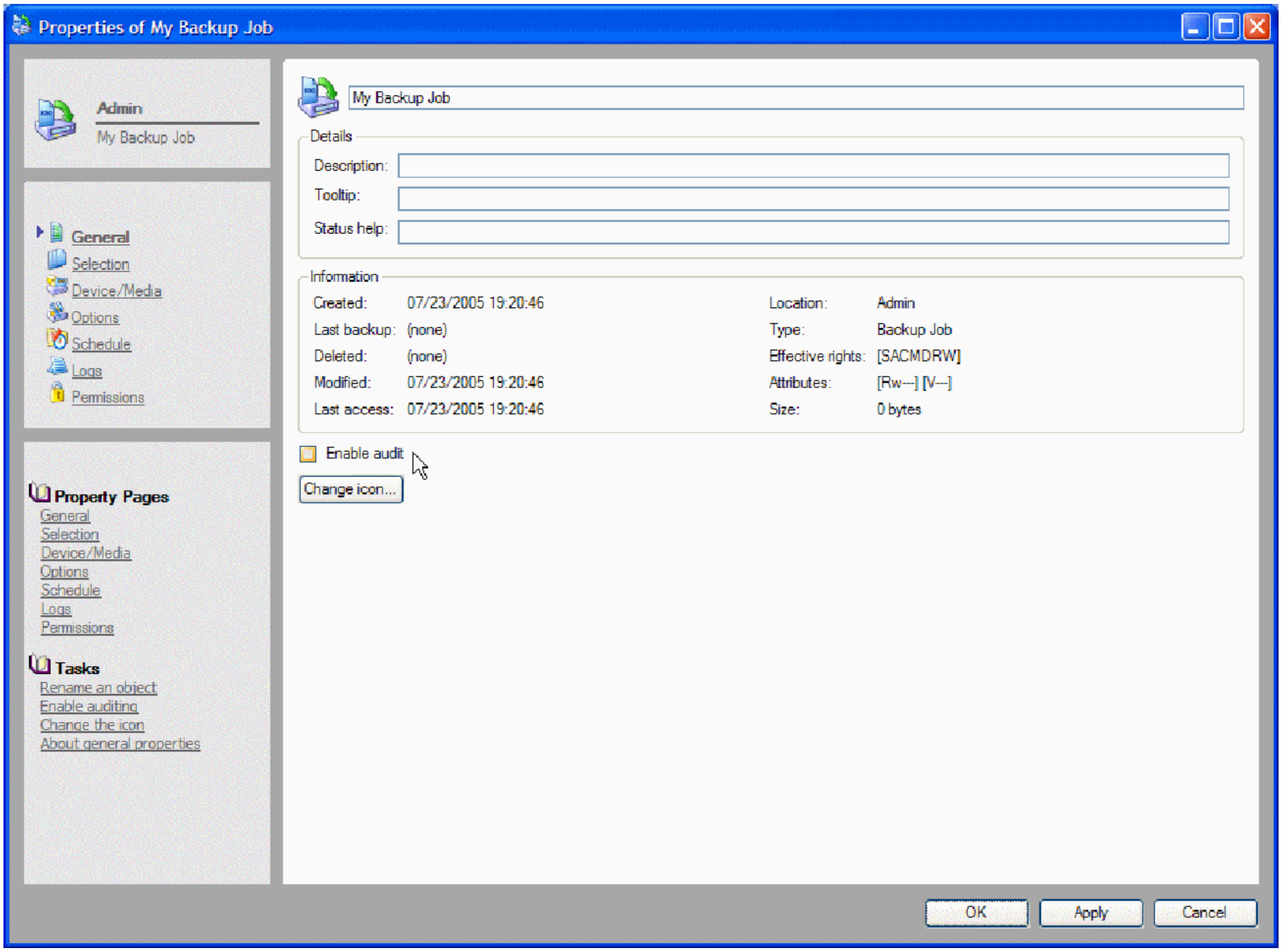
NOTE: If the backup job includes a verify step, Data Protector Express executes this command if the backup of the current object fails. Data Protector Express closes the object and executes this command. Then it performs the verify step.

General page

Applicable objects: *All objects*

The **General** page shows information and object attributes stored in the Data Protector Express catalog for the current object.

The data on this page is taken from the Data Protector Express catalog. For files, directories and volumes, this data is regularly updated. Each time Data Protector Express opens a directory or volume, it updates it catalog with any new information about these files and directories.



My Backup Job

Details

Description:

Tooltip:

Status help:

Information

Created:	07/23/2005 19:20:46	Location:	Admin
Last backup:	(none)	Type:	Backup Job
Deleted:	(none)	Effective rights:	[SACMDRW]
Modified:	07/23/2005 19:20:46	Attributes:	[Rw---] [V---]
Last access:	07/23/2005 19:20:46	Size:	0 bytes

□ Enable audit

From this property page you can rename the object, change the icon associated with it, add a description, tooltip, or status help message and enable or disable auditing. Instructions to update general information about an object appear below.

Name: Shows the name of the current object. To change the name, select it and type in a new name. An object name can be up to 256 characters long.

Description: Use this field to enter a description of the object. This description appears in under the name of the object when you use the **Tiles** view.

Tooltip: If you have included this object in a custom menu, use this field to enter helpful information about the object that you want to see when you scroll your mouse over the object.

Status help: If you have included this object in a custom menu, use this field to enter information about the object that you want to see in the Status bar each time you select the object.

Information about each object:

Created: Shows operating system information about date file or directory created. The create date is taken from the operating system and is updated each time the directory that contains the file is opened. You can use this information to sort files with filters.

Last backup: Shows the date and time when this object was last backed up. You can use this information to sort files with filters.

Deleted: When a file that was previously backed up is deleted, Data Protector Express assigns it a delete date. When Data Protector Express opens a directory, it compares the files it finds with information about versions of files in its catalog. When a version of the file is found in the catalog, but not in the directory, Data Protector Express assigns that version a delete date.

Modified: Shows operating system information about date file or directory last modified. The modify date is taken from the operating system and is updated each time the directory that contains the file is opened. You can use this information to sort files with filters.

Last access: Shows operating system information about the date the file or directory last accessed. The access date is taken from the operating system and is updated each time the directory that contains the file is opened. You can use this information to sort files with filters.

Location: Shows the full path to the object in the Data Protector Express catalog.

Type: Shows the type or category of object.

Effective rights: Shows the effective permissions (or rights) the current user has to this object. Note that these are the *effective* permissions, not the *direct* permissions. There are seven possible permissions, abbreviated as follows:

S	Supervisor
A	Access
C	Create
M	Modify
D	Delete
R	Read
W	Write

Attributes: Shows operating system attribute information about file or directory. The attribute information is taken from the operating system and is updated each time the directory that contains the file is opened. You can use this information to sort files with filters.

The attribute abbreviations are grouped as follows:

Ro	Read only
Rw	Read and write
H	Hidden
Sy	System
X	Execute only
D	Directory
A	Archive
I	Incremental
D	Differential
E	Encrypted

Sh	Share
Tm	Temporary
T	Transaction
Ra	Read audit
Wa	Write audit
P	Immediate purge
Ri	Rename inhibit
Di	Delete inhibit
Ci	Copy inhibit
Dm	Migrate inhibit
Ds	Sub-allocation inhibit
Ic	Immediate compression
Dc	Do not compress
Co	Compressed
Cc	Cannot compress
Mg	Migrated

Size: Shows operating system information about file or directory size. Information about the size of the file or directory is taken from the operating system and is updated each time the directory that contains the file is opened. You can use this information to sort files with filters.

Enable audit: Check this box to create logs for the current object. Information about this object will appear in log files as Data Protector Express performs operations (e.g., backups, restores, etc.) on the file.

Change icon: Use this command to change the icon associated with the object. Clicking this button opens an Icon browser from which you can select any icon available in Data Protector Express.

To rename an object

You can rename any object in the Data Protector Express catalog.

1. Select the object you want to rename and display its General property page
2. Enter a new name in the Name field and select Apply or OK.
3. If the name does not update immediately, press **F5** to refresh the display.

To add a description, tooltip or status help

1. Select the object for which you want to add a description or other information and display its **General** property page.
2. Enter information in the Description, Tooltip or Status help fields.
3. Click **Apply** or **OK** when you are finished.

To enable auditing

1. With the **General** property page open, check the **Enable Audit** box.
2. A check mark appears in the box if auditing is enabled.
3. Select **Apply** or **OK** to save your changes.

If **Enable Audit** does not appear on the **General** page, the option is not available for the selected object.

To change the icon associated with an object

You can change the icon associated with any object in Data Protector Express.

1. With the **General** property page open for an object, click **Change Icon**.
2. Select a new icon in the **Icon** browser, and click **OK**.
3. Select **Apply** or **OK** on the **General** property page to save the changes.

Related topics

For information about related features, refer to the following documentation:

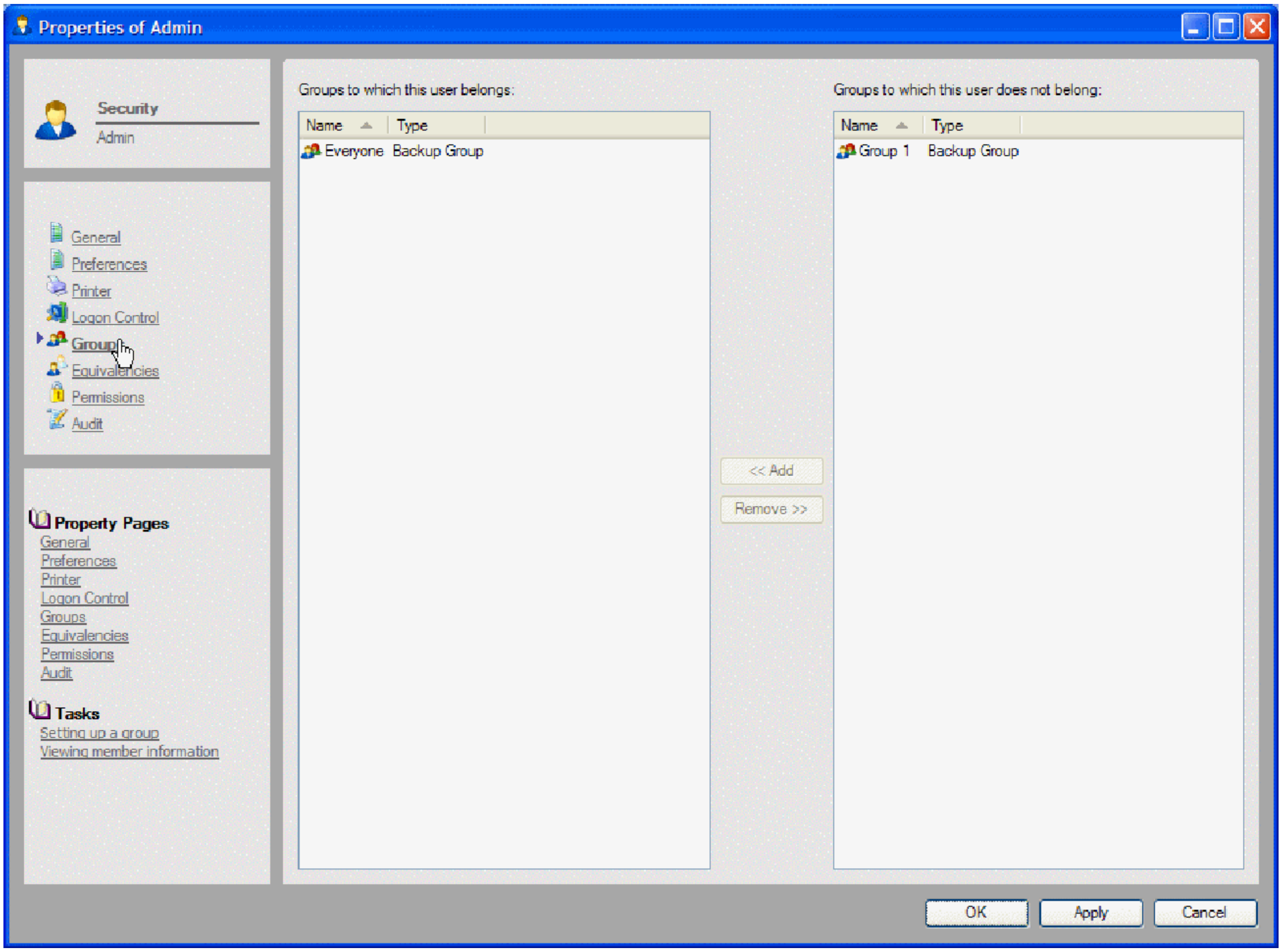
- *Effective Permissions* on page 44
- *Filter selection criteria* on page 63

Groups page or Members page

Applicable objects: *User, Group*

The **Groups** pages shows the groups to which the current user belongs. Use this page to add or remove a user from a group. The **Members** page shows the users that are members of the group. Use it to add and remove members from a group. A user's group membership is used to calculate their effective permissions.

Click **Apply** or **OK** to save any changes you make.



Groups to which this user belongs:

Name	Type
Everyone	Backup Group

Groups to which this user does not belong:

Name	Type
Group 1	Backup Group

Fields on the Groups page

Groups to which this user belongs: Shows the groups to which the current user belongs. To add the user to a new group, select the group in the right window pane and click the **Add** button; the group is moved to the left window pane. Similarly, to remove a user from a group, select the group from the left window pane and then click the **Remove** button.

Everyone group: Normally, this group will be listed in this field. As they are created, new users are automatically added to the **Everyone** group. Members of this group have **Modify**, **Delete**, **Create**, **Write** and **Read** permissions to the **Everyone Folder**. You can remove a user from this group by selecting the **Everyone** group and then clicking remove.

Groups to which this user does not belong: Shows the groups to which this user does *not* belong.

Fields on the Members page

Members who belong to this group: This list shows the users that are members of the group.

Members who do not belong to this group: This list shows the users that are not members of the group.

Add: To add a user to the group, select the user in the right list and click **Add**. The user is moved to the left list.

Remove: To remove a user from the group, select the user in the left list and click **Remove**. The user is moved to the right list.

Related topics

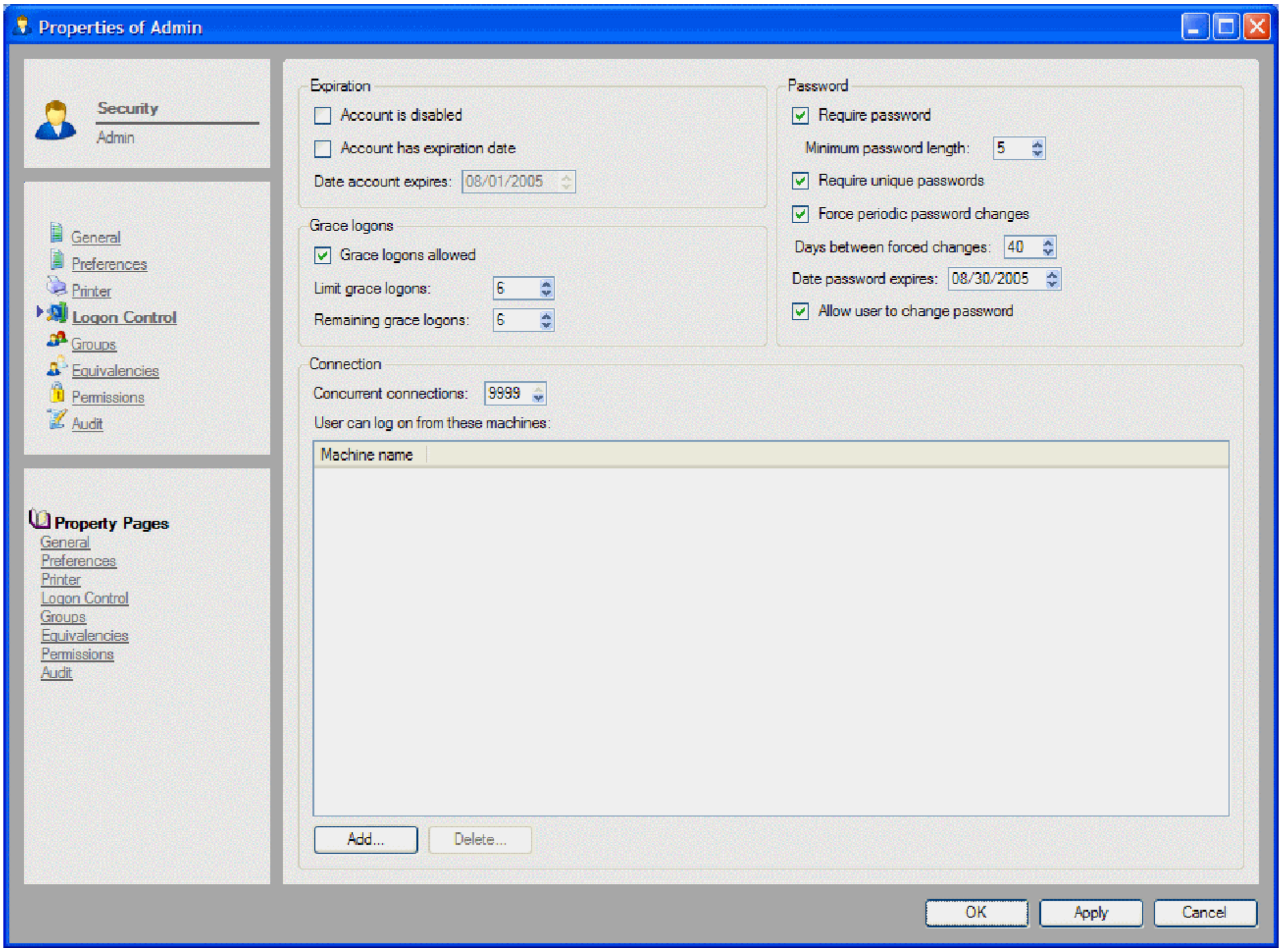
For information about related features, refer to the following documentation:

- *Effective Permissions* on page 44
- *Setting up users* on page 168

Logon Control page

Applicable objects: *User*

The **Logon Control** page controls the ability of a user to log on to the current Data Protector Express storage domain. Controls whether passwords are required, whether and when the password must be changed, whether an account has expired and the number of connections a user can have to the network.



Properties of Admin

Security
Admin

Expiration
☐ Account is disabled
☐ Account has expiration date
Date account expires: 08/01/2005

Grace logons
☑ Grace logons allowed
Limit grace logons: 6
Remaining grace logons: 6

Password
☑ Require password
Minimum password length: 5
☑ Require unique passwords
☑ Force periodic password changes
Days between forced changes: 40
Date password expires: 08/30/2005
☑ Allow user to change password

Connection
Concurrent connections: 9999
User can log on from these machines:

Machine name

Expiration

Controls when the current account will expire. A user account can expire on a given date or can be disabled manually.

Account is disabled: Checked when the account has expired. To make a disabled account active again, clear the checkbox.

Account has expiration date: Check this box to set an expiration date for the user account.

Date account expires: Specifies a date when the account will no longer be active. When the account expires, Data Protector Express disables the account and checks the **Account is disabled** box. This user will be unable to log on until the **Account is disabled** box is cleared.

Grace logons

Controls how many times a user can log on to Data Protector Express after their password has expired. For example, if the **Allow grace logons** box is checked and the **Remaining grace logons** is set to **2**, the user will be allowed to log on two times after their old password has expired. On the third logon attempt, the user must change their password.

NOTE: Grace logons do not function when passwords are not required, that is, when the **Require password** check box is cleared.

Grace logons allowed: If checked, a user can log on after their old password has expired.

Limit grace logons: Shows the maximum number of grace logons allowed. For example, if it is set to **2**, the user can log on with an expired password two times.

Remaining grace logons: Shows the number of remaining grace logons. Data Protector Express automatically adjusts this number each time the user logs on with expired password. You can also set this manually.

Password

Controls whether a user must have a password to log on.

Require password: When checked, Data Protector Express requires the user to have a password.

NOTE: If you clear the **Require password** box and the user has a password, Data Protector Express will continue to require that user to input their password.

Minimum password length: Specifies the minimum length of the password.

Require unique passwords: If checked, Data Protector Express only accepts the new password if the user has not used it before.

Force periodic password changes: If checked, either the user or the Data Protector Express administrator must change the password per the **Days between forced changes** and **Date password expires** settings.

Days between forced changes: Specifies the interval between forced password changes.

Date password expires: Calculated date of next password expiration, based on **Days between forced changes** setting.

Allow user to change password: If checked, the user can change their password on their own.

TIP: The Data Protector Express administrator can change a user’s password without knowing the user’s current password. Data Protector Express does not even ask you to enter the old password. This is useful when the user has forgotten his or her password.

Connection

Controls the allowable machines and simultaneous logons for a user.

Concurrent connections: Controls how many different logons a user may have simultaneously from different machines. For example, if the **Number of concurrent connections** is set to **5**, this user can log on to Data Protector Express from up to five separate machines at the same time.

User can log on from these machines: Lists the machines from which a user can log on to Data Protector Express. The user cannot log on to Data Protector Express from any machine unless it is listed. To add machines, click **Add…** and select the appropriate machine from the **Browse** dialog box. To remove machines, select the machine and click **Delete**.

NOTE: If no machine is listed, a user can log on from any machine.

Related topics

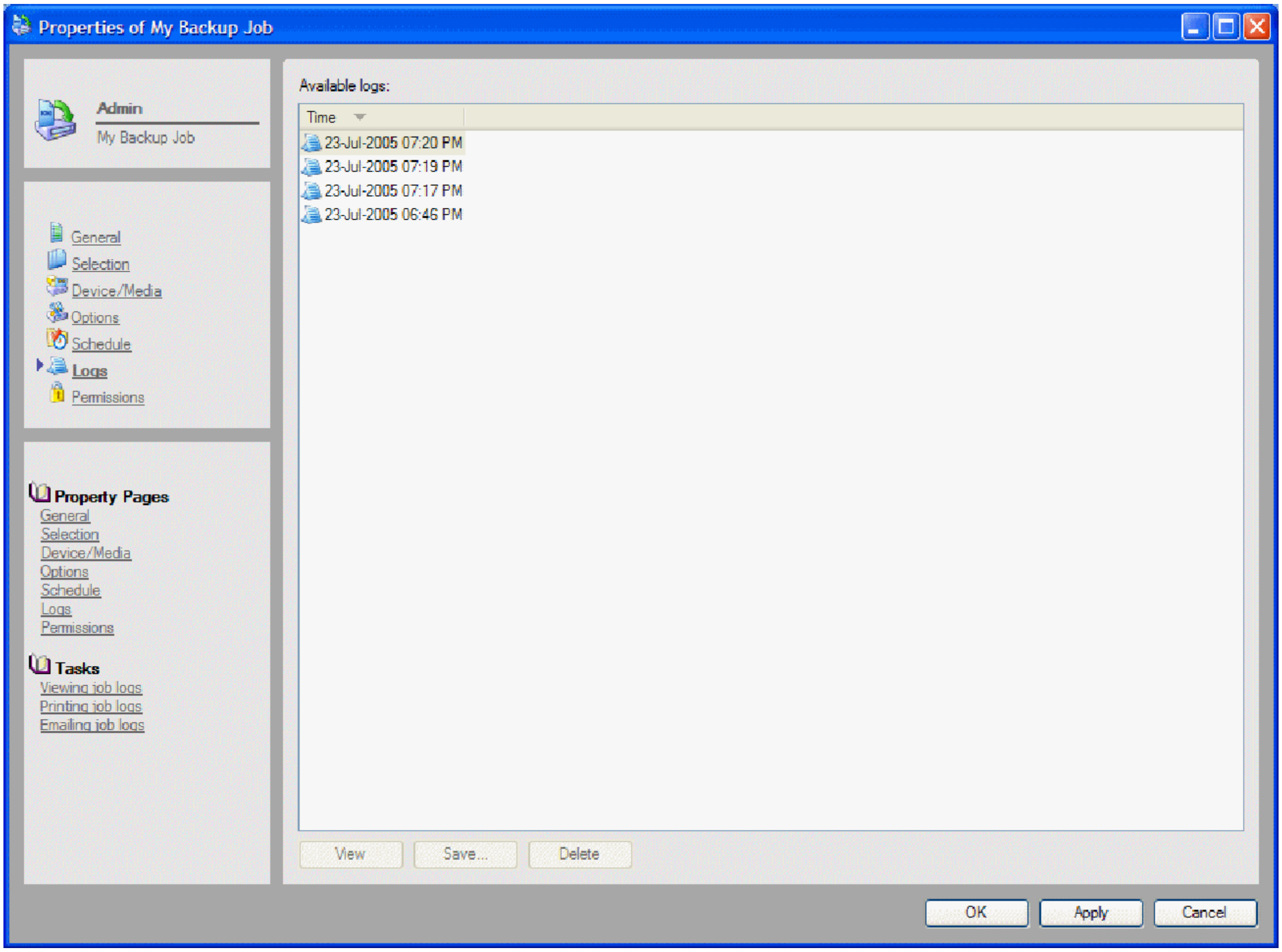
For information about how to set up new users, see *Setting up users* on page 168.

Logs page

Applicable objects: *Backup Job, Restore Job, Verify Job*

The **Logs** page shows the available logs for the current job.

Data Protector Express creates a log for each job, according the **Log option** on the job's **Options page** After the job runs, you can view or print this log to see the files that were successfully or unsuccessfully backed up, restored or verified. Once you open a log, you can print it or save it to one of several file types.



Available logs:

Time
23-Jul-2005 07:20 PM
23-Jul-2005 07:19 PM
23-Jul-2005 07:17 PM
23-Jul-2005 06:46 PM

Available logs: Lists the available logs for this job.

View: Select a log and click to open the file in the specified text editor. You can print or save the log. Note that some logs can be quite long; check the length of the document before printing it.

Save: Select one or more logs and click to save them. Logs can be saved as the following file types: HTML, text, comma-separated files (CSV), or XML.

Delete: Select one or more logs and click to delete them.

NOTE: The maximum number of logs per job is 250. Data Protector Express will overwrite the oldest log when you reach this maximum.

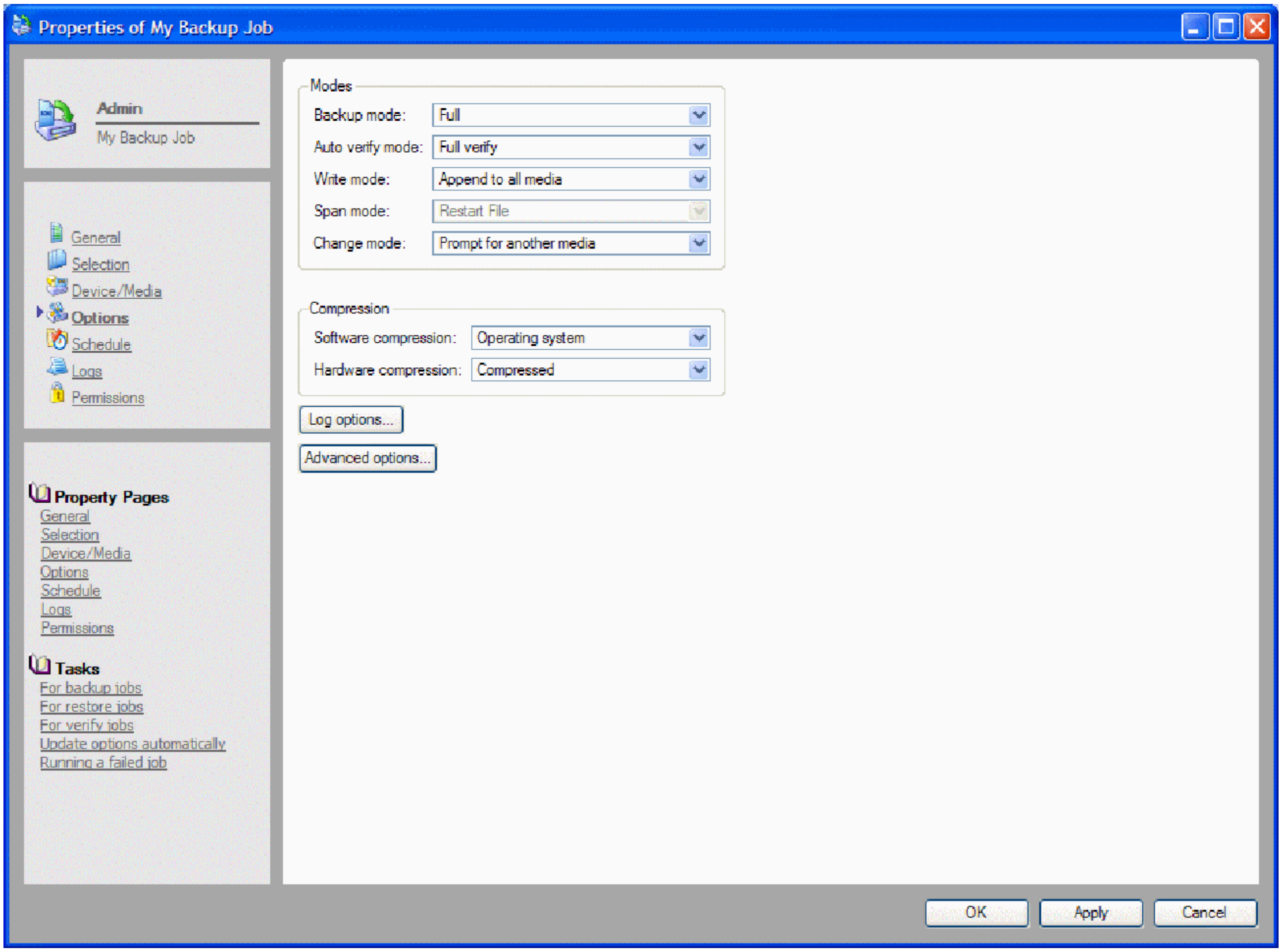
Related topics

For information about related topics, refer to the following documentation:

- *Log options* on page 108
- *Job Logs* on page 129
- *Preferences* on page 227

Options page

Applicable objects: *Backup Job, Restore Job, Verify Job*
To learn more about the options for a job group, see *Job Group options* on page 222. For additional information about options for media jobs, see *Media job options* on page 223.



Modes

Backup mode: Full
Auto verify mode: Full verify
Write mode: Append to all media
Span mode: Restart File
Change mode: Prompt for another media

Compression

Software compression: Operating system
Hardware compression: Compressed

The **Options** page on the property page of a job controls various settings important to how Data Protector Express runs backup, restore and verify jobs. For options related to a Job Group, see *Job Group options* on page 222.

Backup Mode

(Backup jobs only)

Determines whether all files or only changed files are backed up. For scheduled automatic rotation jobs, Data Protector Express uses the backup mode for each backup set as indicated on the **Schedule** page; for unscheduled or manual jobs, Data Protector Express uses the settings set by the user.

The Backup mode is either Full, Incremental, Differential or Copy.

Full: Instructs Data Protector Express to back up all selected files. For each file, Data Protector Express resets the incremental bit in the catalog and the archive bit on disk.

Differential: Instructs Data Protector Express to back up all selected files that have changed since the last full backup. When a file changes, its differential bit has been set. Data Protector Express does not reset any bits.

Incremental: Instructs Data Protector Express to back up all selected files that have changed since the last backup. For each file, Data Protector Express resets the incremental bit in the storage management and the archive bit on disk.

Copy: Instructs Data Protector Express to back up all selected files. It has no effect on any future scheduled job. After backing up each file, the archive bit is left unchanged.

Auto Verify Mode

(Backup and verify jobs)

Verifies that a file was backed up correctly. Data Protector Express compares the file to the original file.

The Auto verify mode is either No verify, Full verify or Quick verify.

No verify: Instructs Data Protector Express to skip the verification step. It is not recommended.

Full verify: Instructs Data Protector Express to compare every selected file stored on media with the original file from the PC desktop or file or application server. This default option is strongly recommended.

Quick verify: Instructs Data Protector Express to be certain that every file backed up onto the tape is in readable condition. It does not verify that the data is correct, only that the data stored on the media (incorrect or not) can be read. While selecting this option can save time, it is nonetheless not recommended.

Write Mode

(Backup jobs only)

Determines whether the old data on the media is overwritten with new data or whether the new data is appended to the end of the old data. When media is overwritten, all of the data previously stored on it is lost. Appending data will preserve the old data.

For scheduled automatic rotation jobs, Data Protector Express defaults to **Overwrite all media**; for unscheduled and manual jobs, Data Protector Express uses the settings set by the user.

Append to all media: Instructs Data Protector Express to append all data to the end of the media. No data is overwritten. Select this setting for permanent storage.

Append to first media, overwrite others: Instructs Data Protector Express to append data to the end of the first media, but to overwrite all media that follows. For example, Data Protector Express will not overwrite the first tape inserted, but will overwrite the second, third and later tapes. This setting is useful if you have a set of media with old data you no longer need. By selecting this option, Data Protector Express preserves your most recent data on the first media, but overwrites older, unneeded media.

Overwrite all media: Instructs Data Protector Express to overwrite all media. All data on media that is overwritten is lost. Use this option for media that you want to recycle.

Span Mode

(Backup jobs only)

This option is active when you select **Append to first media, overwrite others** or **Overwrite all media**. Determines whether Data Protector Express splits files across more than one media during the backup job. Choices are **Restart File** and **Split File**.

Restart File: Instructs Data Protector Express to back up the file to additional media if the file will not fit on the current media. Select this option of you *do not* want to split files across media.

Split File: Instructs Data Protector Express to begin backing up the file on the current media and to continue the backup on additional media as needed. Select this option of you *want* to split files across media.

Change Mode

(Backup jobs only)

Determines what action Data Protector Express will perform when it fails to find the media it was expecting to use for a job. When Data Protector Express runs a job, if the job uses specific media, Data Protector Express scans the network for devices with that media. If it does not find the media it expects, its response is determined by the **Change mode** setting.

The Change mode is either Force to append to end of media or Prompt for another media.

Force to append to end of media: Instructs Data Protector Express to append data to whatever media it finds in the designated backup device. If it cannot find the correct media, Data Protector Express appends data to whatever media is available. This option will ensure that the job runs, if the media contains enough room to complete the job.

Prompt for another media: Instructs Data Protector Express to continue to scan for the expected media and to send an alert warning that the proper media has not been found. This option will not allow a job to run with any other media except with the expected media. Additionally, this option will not search for another device that might contain the proper media.

Compression

(Backup jobs only)

Controls how Data Protector Express compresses or maintains the compression of files and directories for both Software and Hardware.

The Software Compression types are either **None**, **Software**, **Operating System** or **Both**.

None: Instructs Data Protector Express to write all data to the tape in a decompressed format. If the file is stored on disk in a compressed format, the file will be decompressed before writing. This option is useful if the device supports hardware data compression and the files are to be restored to a different operating system.

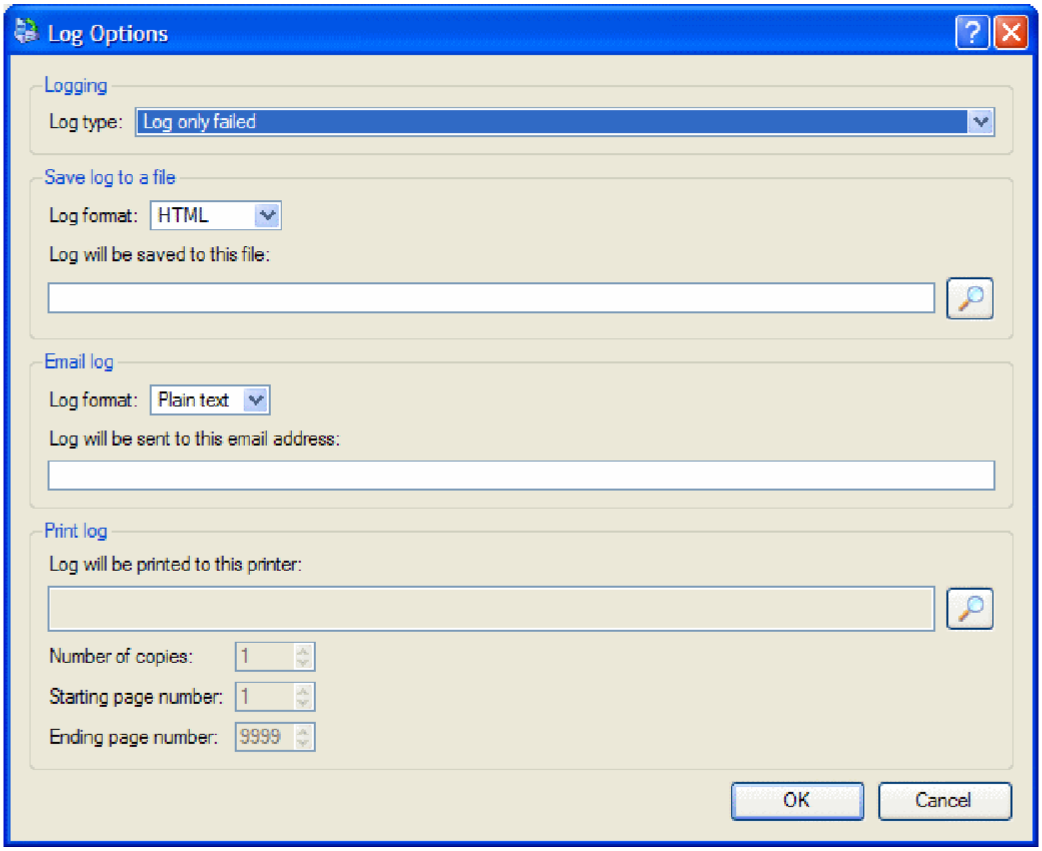
Software: Instructs Data Protector Express to write all data to tape in the Data Protector Express compression format. If the file is stored on disk in a compressed format, the file will be decompressed before being re-compressed by Data Protector Express. This option is useful if the tape device does not support hardware data compression and the files are to be restored to a different operating system.

Operating System: Instructs Data Protector Express to write all data to tape in the same mode it is stored on disk. If the file is stored on disk in compressed format, Data Protector Express will write the data in the host operating system’s compressed format. If the file is not compressed on disk, Data Protector Express will store the file on tape in a non-compressed format. This option is useful if the hardware supports data compression and the files are to be restored to the same operating system. This option also gives better performance.

Both: Instructs Data Protector Express to write all compressed data in its compressed format. Any uncompressed files will be stored in the Data Protector Express compression format. This option is useful if the hardware does not support data compression and the files are to be restored to the same operating system.

The Hardware Compression types are either **None** or **Compressed**. If the backup device supports hardware compression, be sure to select **Compressed**.

Logging options



Log Options

Logging

Log type: Log only failed

Save log to a file

Log format: HTML

Log will be saved to this file:

Email log

Log format: Plain text

Log will be sent to this email address:

Print log

Log will be printed to this printer:

Number of copies: 1

Starting page number: 1

Ending page number: 9999

Determines the kind of log that Data Protector Express keeps of the current job. The **Log type** is either **None**, **Log only failed**, **Log only completed** or **Log all.**

After a job is run, you can view or print the log to see which files were successfully or unsuccessfully backed up, restored or verified. The default value is **Log only failed**, which writes to the log any files that were not successfully backed up, restored or verified.

None: Instructs Data Protector Express to not keep a log of the backup job as it runs.

Log only failed: Instructs Data Protector Express to log the name of any selected file that was not successfully backed up, restored or verified.

Log only completed: Instructs Data Protector Express to log the name of any file selected for and successfully backed up, restored or verified.

Log all: Instructs Data Protector Express to log the name of every file selected and whether or not that file was successfully backed up, restored or verified.

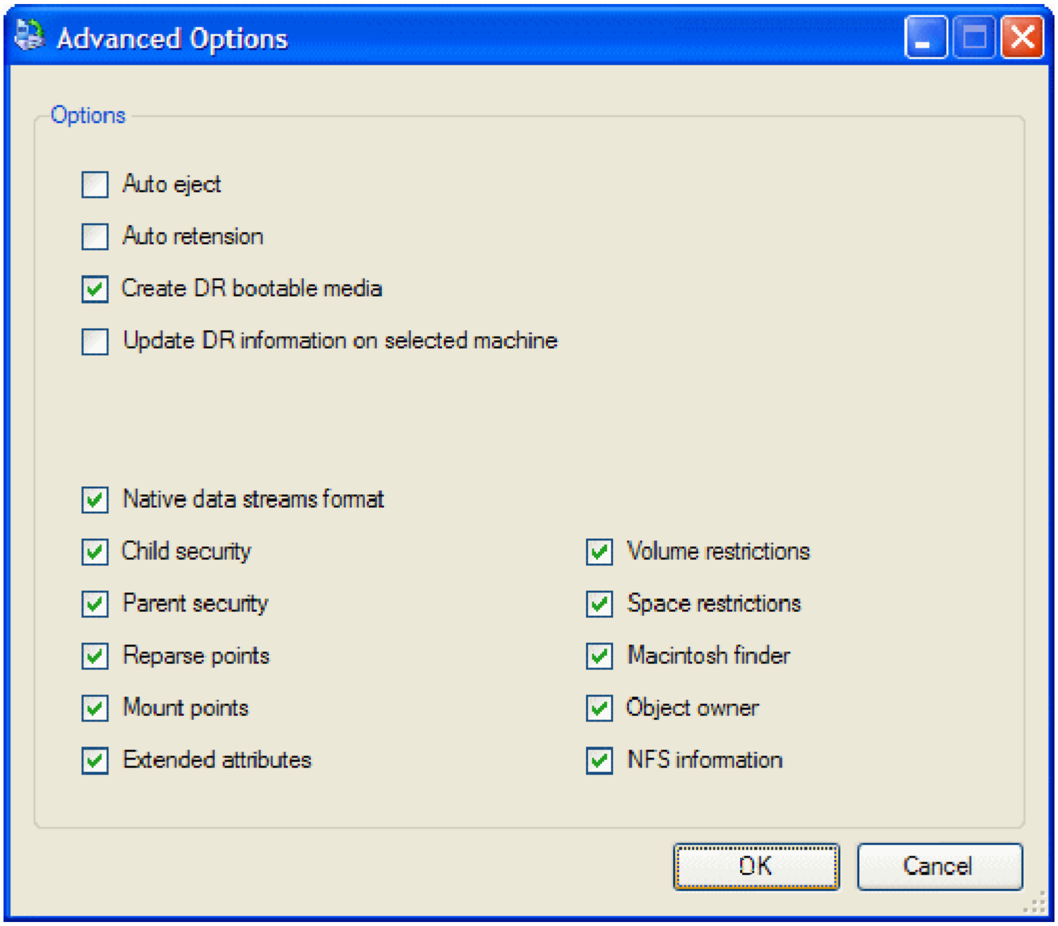
NOTE: If you choose the Log All setting under the Log options for a job, your log files might be very large. Creating and viewing very large log files can slow performance. HP recommends that you choose a setting that creates a smaller log file (e.g., Log only failed, Log only completed) if you intend to view log files while running Data Protector Express. If you need to create verbose log files, HP recommends that you save them and view them with an Internet browser or word processor.

Save log to a file: The Log format can be one of the following types: HTML, XML, Excel CSV, or plain text. Specify the path and filename for the log file.

Email log: The **Log Format** can be one of the following types: plain text or HTML.

Print log: Click **Browse** to select a printer. You can select the number of copies and a page range of pages to print.

Advanced options



☐ Auto eject

☐ Auto retension

☑ Create DR bootable media

☐ Update DR information on selected machine

☑ Native data streams format

☑ Child security

☑ Parent security

☑ Reparse points

☑ Mount points

☑ Extended attributes

☑ Volume restrictions

☑ Space restrictions

☑ Macintosh finder

☑ Object owner

☑ NFS information

For information about these options, see:

Advanced options for backup jobs on page 113.

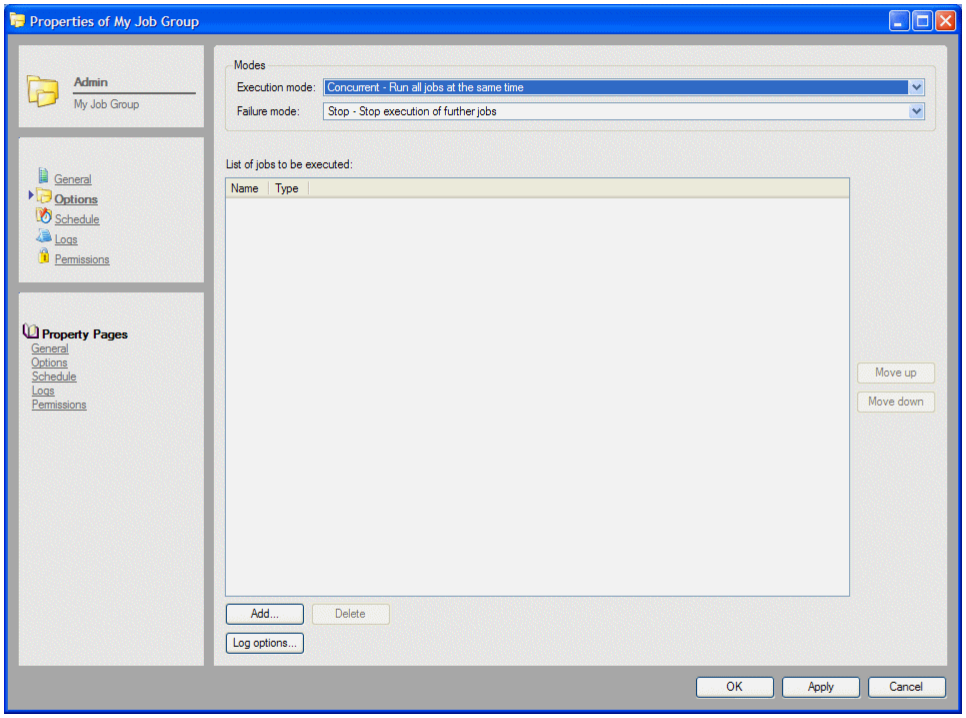
Advanced options for restore jobs on page 116.

Advanced options for verify jobs on page 119.

Job Group options

Applicable objects: *Job Group*

The **Options** page presents different options for a job group.



Execution mode: Concurrent - Run all jobs at the same time

Failure mode: Stop - Stop execution of further jobs

Modes

You can configure how Data Protector Express handles jobs in a job group as they run and if they encounter any failures.

Execution mode: Determines how Data Protector Express will execute the jobs, sequentially or concurrently.

Failure mode: Determines whether Data Protector Express will continue with subsequent jobs when one fails or if the remaining jobs will be stopped.

List of jobs to be executed

The list of jobs to be executed contains all of the jobs that have been included in this job group. To move a job, select it and use the **Move up** or **Move down** commands to reorganize the jobs in the list. Use the **Add** command to add more jobs to the list. Use the **Delete** command to remove a selected job from the list. Deleting a job from a job group does not remove the job from Data Protector Express.

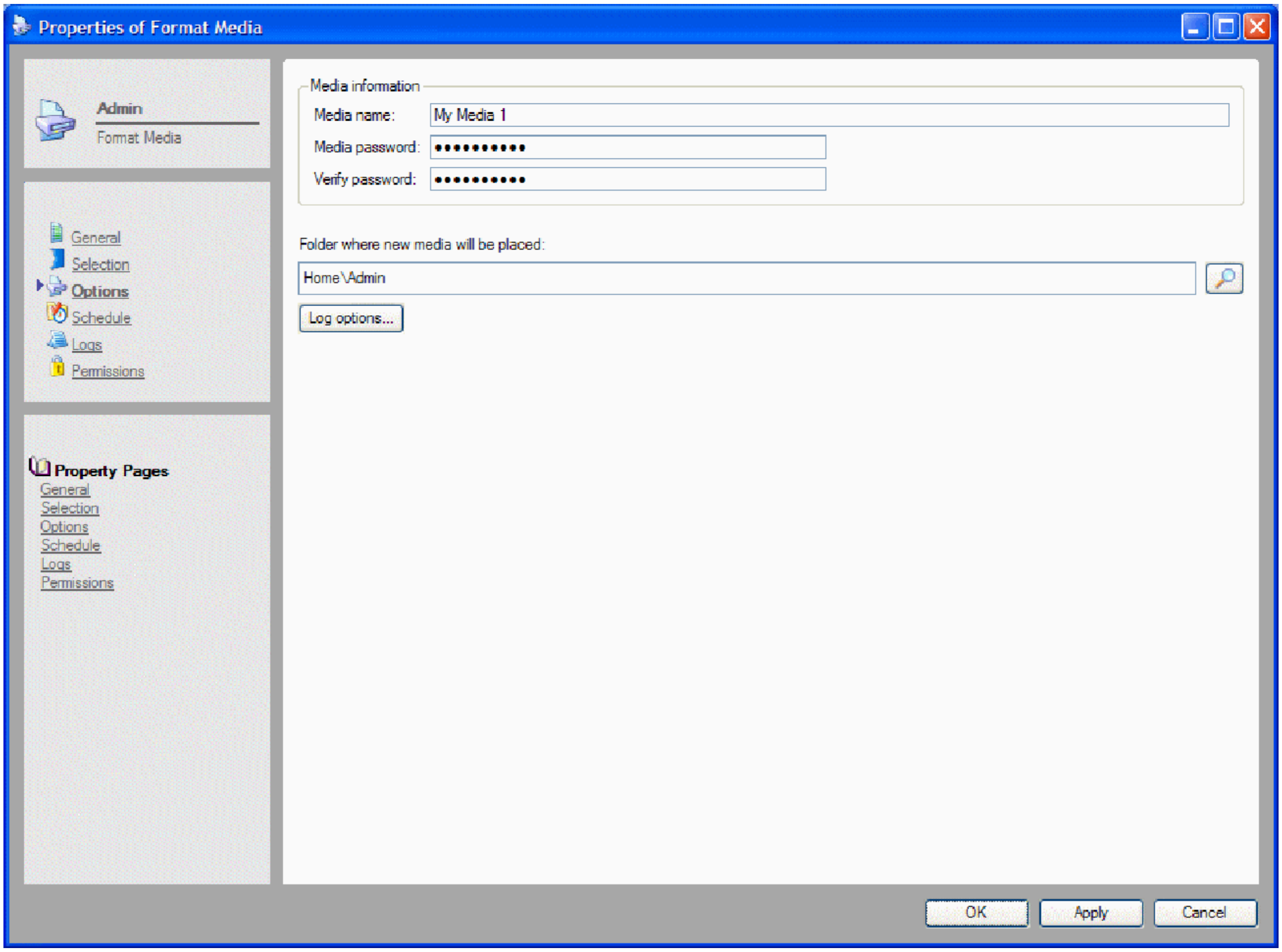
Log options

Use this command to set up log options for the jobs included in this group. For more information about log options for jobs, see *Log options* on page 108.

Media job options

Applicable objects: *Selected Media jobs*

The **Options** page presents different options for selected media jobs. Each media job type presents a slightly different set of options.



Media information

Media name: My Media 1

Media password: ••••••••••

Verify password: ••••••••••

Folder where new media will be placed:

Home\Admin

Log options: Click this button to determine how much information Data Protector Express will write to job logs.

Media information: Enter the media name and password that Data Protector Express should assign to media when formatting media.

Folder information: Depending on the media job type, you can specify where Data Protector Express should store media once a job is completed or where to locate media required for a job that is about to begin.

Erase options: Select the preferred method to erase media: secure erase or quick erase.

Sort jobs: For sort media jobs, you select whether to sort media in ascending or descending order. Media is sorted alphabetically by name. You can also select a sort key: either media name or media tag.

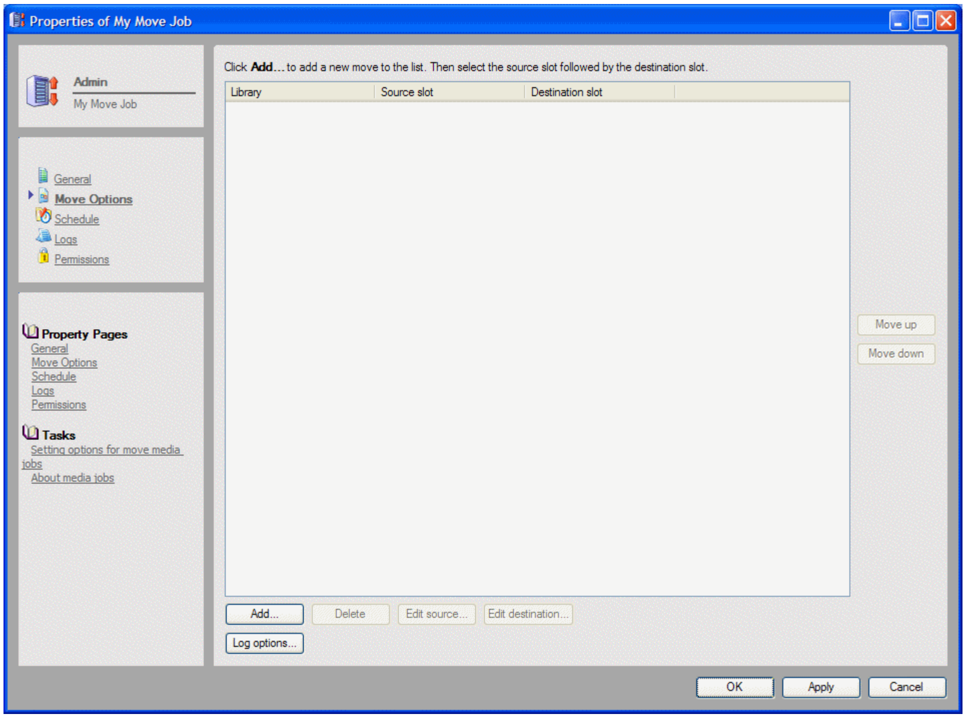
For information about related topics, refer to *Job Options* on page 107.

Move Options page

Applicable objects: *Move media jobs*

For move media jobs, the **Move Options** page lists each library source and destination location for the media that Data Protector Express will move in this job. Use this page to reorganize the media in a library. For added convenience, set up the job to run unattended by scheduling it for a time when demands on the library are low. See *Scheduling Jobs* on page 90 for information on automating jobs with schedules.

Click the **Add** button to include more media in the job. Click the **Delete** button to exclude media from the job. Use the **Edit source** and **Edit destination** buttons to modify source or destination information for media that is already included in the list.



Click **Add**... to add a new move to the list. Then select the source slot followed by the destination slot.

Log options: Click this button to determine how much information Data Protector Express will write to job logs.

Library: For move media jobs, you select the library whose media you want to move and the source and destination slots for the media to be moved.

Source slot: The current location of the media to be moved.

Destination slot: The location in the library to where you want to media to be moved.

Move up or down: Use these buttons to reorganize the media within the job. Move media up in the list to process it sooner in the job. Move media down in the list to process it later.

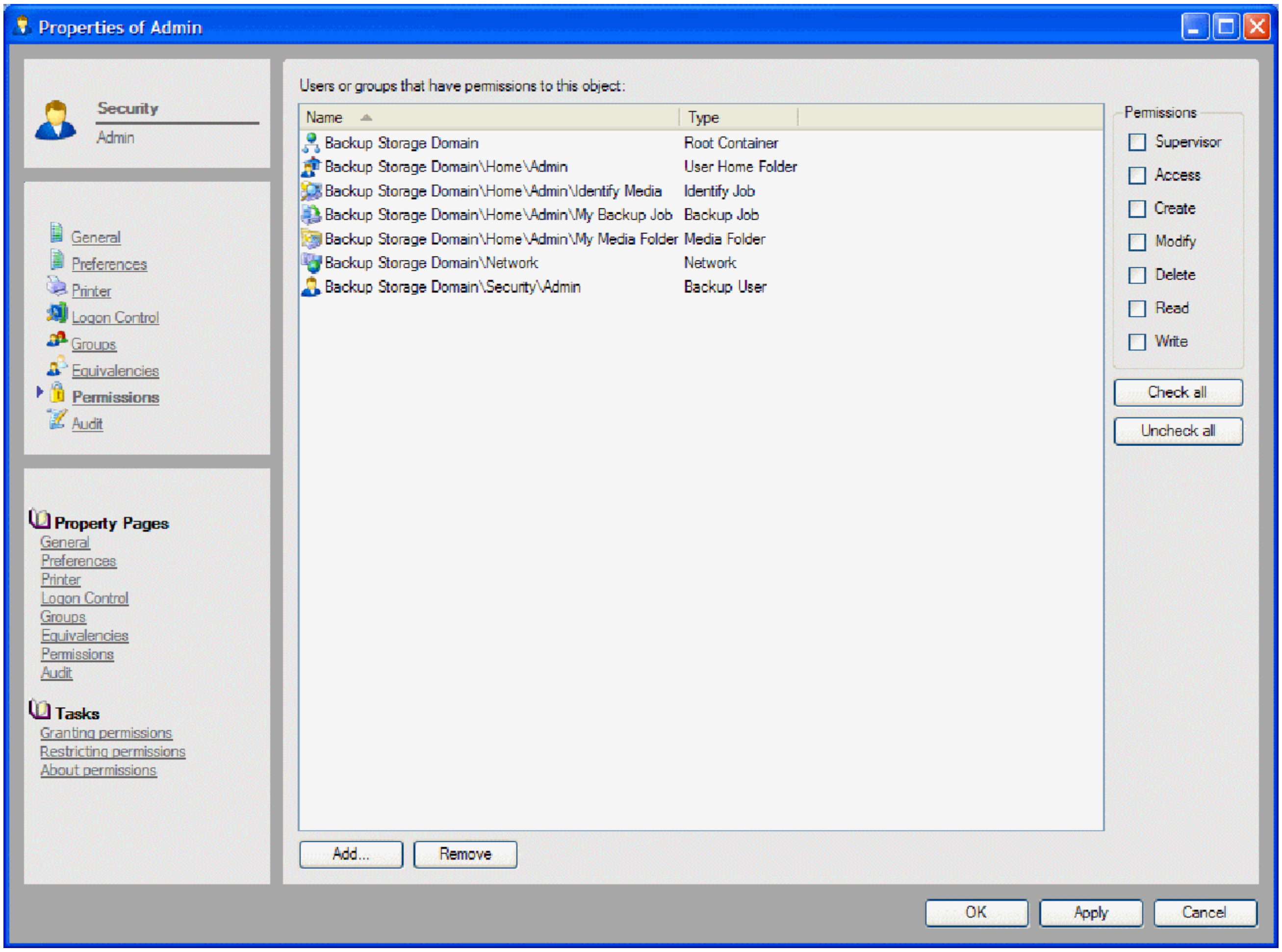
Permissions page

Applicable objects: *All catalog objects*

For users and groups, the **Permissions page** lists the objects to which the current user or group has permissions. For all other objects, it shows the users or groups that have permissions to the current object.

Use this page to grant users or groups permissions to objects. Note that permissions can be granted from either the property page of the catalog object or the property page of the user or group. Either way, the permissions appear on the appropriate corresponding object's **Permissions** page. For example, if a user is granted permissions to the **C:** volume from the **Permissions page** on his property page, the **Permissions** page on the property page of the **C:** volume will list this user as a user who has permissions. Alternatively, if this user is granted permissions from the property page of the **C:** volume, the appropriate permissions will appear on his **Permissions** page.

Note additionally that a user has direct permissions only to those objects listed on that user's **Permissions** page. Any and all other effective permissions to other objects are calculated through inherited permissions, through equivalencies or through groups.



Users or groups that have permissions to this object:

Name	Type
Backup Storage Domain	Root Container
Backup Storage Domain\Home\Admin	User Home Folder
Backup Storage Domain\Home\Admin\Identify Media	Identify Job
Backup Storage Domain\Home\Admin\My Backup Job	Backup Job
Backup Storage Domain\Home\Admin\My Media Folder	Media Folder
Backup Storage Domain\Network	Network
Backup Storage Domain\Security\Admin	Backup User

Permissions

□ Supervisor
□ Access
□ Create
□ Modify
□ Delete
□ Read
□ Write

Users or groups that have permissions to this object: Lists the users or groups which have permissions to the current object (does not apply to either group or users).

To display the permissions for a user or group, select the user or group; the permissions appear in the **Permissions** fields.

To add a user or group, click **Add**. To remove a user or group, select it and click **Remove**.

Objects to which this user or group has permissions: Lists the objects to which the current user or group has permissions (only applies to group and users).

To see the permissions each user or group has to a particular object, select the object; the permissions to that object appear in the **Permissions** fields.

To grant a user or group permissions to a new object, click **Add** and select the appropriate permissions. To end permissions to an object, select the object and click **Remove**.

Permissions: Shows the permissions granted to the currently highlighted object, user or group. Check or uncheck the appropriate boxes to grant or restrict permissions.

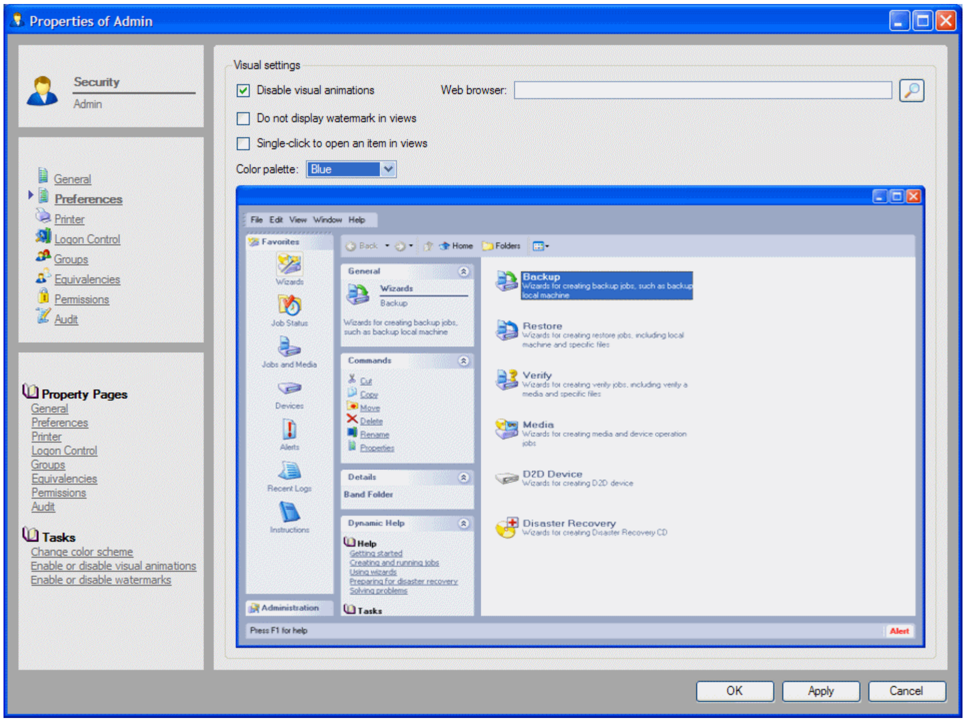
Related topics

For information about related topics, refer to the following sections:

- *Effective Permissions* on page 44
- *Permissions page for users* on page 172
- *Permissions page for group* on page 174
- *Permissions Reference* on page 178

Preferences page

Use the **Preferences** page to control the user interface. Changes are user-specific and are used each time you log on to Data Protector Express until you modify them.



Visual settings

☑ Disable visual animations

Web browser:

☐ Do not display watermark in views

☐ Single-click to open an item in views

Color palette: Blue

Disable visual animations

Check this option to enable or disable visual animations in Data Protector Express. Visual animations are used to notify you when a matter requires your attention. For example, an alert will flash in the lower right corner of the Status bar when Data Protector Express has a message for you to review.

Web browser

Use the **Browse** button at the right of this field to select a default web browser for the user. This web browser is used to open links to Internet web sites that are contained in alerts or other messages in Data Protector Express.

Do not display watermark in views

Check this option to remove the watermark from the Data Protector Express main object detail area. This watermark indicates which edition of Data Protector Express you are running.

Single-click to open an item in views

Check this option to force Data Protector Express to open a command or display a link each time this user clicks on an object in Data Protector Express. By default, users must double-click an item to open it.

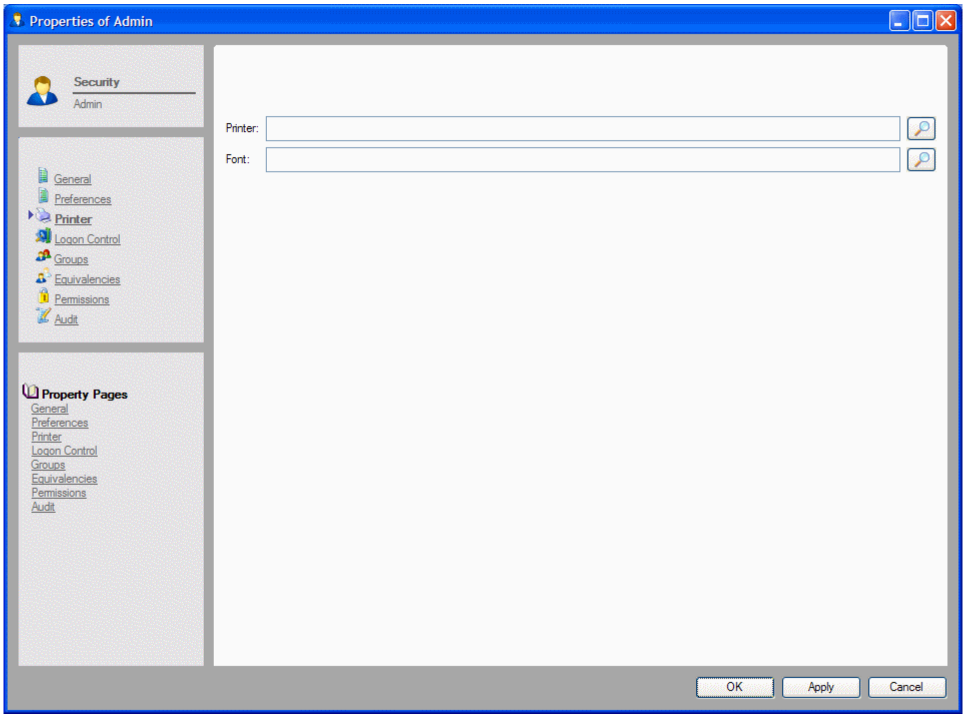
Color palette

Sets the color scheme for the Data Protector Express user interface. As you select a color the sample screen shows the results.

Printer page

Applicable objects: *User, Group*

The **Printer page** shows the print settings to use when automatically printing a job log for the selected user or group.



The **Printer page** appears on the property page of a user or group in the Security view. When the **Print log** option is selected on the **Options** property page for a job, the job log prints automatically as soon as the job is complete. It prints to the printer specified on the **Printer page** for the job owner.

Click the **Browse** buttons to select a printer and font.

Related topics

For information about related features, refer to the following documentation:

- *Job Logs* on page 129
- *Automatically printing job logs* on page 130

Query window and Selection Filters window

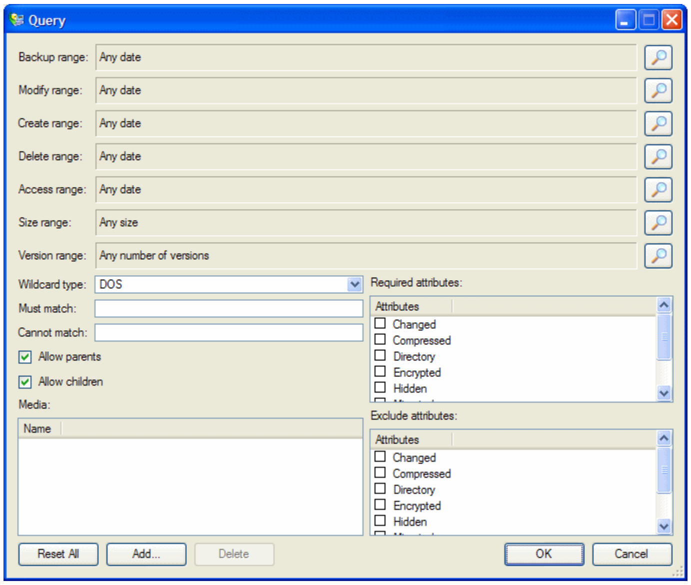
Applicable Objects: All catalog objects, Backup, Restore and Verify jobs

Use the **Query** window to sort files for displaying on **Catalog** view. Use it to exclude or "filter out" files that do not meet the specified selection criteria.

Query filters are applied to all of the volumes, folders and files ordinarily displayed on the **Catalog** view. *You cannot apply different filters to different machines or volumes.* Data Protector Express uses the selection filters to sort the files and only displays the files that meet the selection criteria.

Use the **Selection Filters** window to specify the selection criteria for a job. It excludes or "filters out" files that do not match the selection criteria.

The filter criteria are applied to all marked files, regardless if they were marked before or after the filter criteria were specified. After specifying the selection filter criteria, you can then mark or unmark files, folders and volumes for backup. You can also change the filter criteria at any time; Data Protector Express will automatically reapply the new selection filter criteria to the marked folders and files.



Backup range: Any date

Modify range: Any date

Create range: Any date

Delete range: Any date

Access range: Any date

Size range: Any size

Version range: Any number of versions

Wildcard type: DOS

Must match:

Cannot match:

☑ Allow parents

☑ Allow children

Required attributes:

□ Changed
□ Compressed
□ Directory
□ Encrypted
□ Hidden

Exclude attributes:

□ Changed
□ Compressed
□ Directory
□ Encrypted
□ Hidden

Backup range: Displays files according to their backup date. The backup date is assigned to a file each time it is backed up. The backup date for a file is the same as the *last* time it was backed up.

Modify range: Displays files according to their modify date. Each time a file is modified, its modified date is updated. You can use this filter to display files whose modified date matches your criteria. Data Protector Express checks the directory information on the volume to see if the file should be included in the job.

Create range: Displays files according to their create date. When a file is first created, it is assigned a create date. You can use this filter to display only those files which match your criteria. Data Protector Express checks the created date for each file stored in the directory of the volume and uses this to sort files.

Delete range: Displays files according to their delete date.

When files have been backed up and are later deleted, Data Protector Express marks the file as having been deleted and assigns it a delete date. This filter instructs Data Protector Express to display only files which have a delete date that matches the selection criteria. If a file has not been deleted, it will not have a delete date and will not be displayed.

Access range: Displays files according to their access date. Each time a file is read, whether or not it is modified, its access date is updated by the operating system. You can use this information to select and filter files.

Size range: Displays files according to their size.

Version range: Displays files according to their version date. Each time Data Protector Express backs up a file, it creates a new version of that file and assigns it a version date.

Wildcard type: Displays the wildcard format used by the **Must match** and **Cannot match** filters. Select one of these types of wildcard formats: **DOS** or **Long**.

Must match: Displays files that match specified wildcards. Only files that match the wildcard indicated in this field are selected.

Specify multiple wildcards by separating each with a semicolon (no spaces). Data Protector Express displays any file that matches any one of the wildcards. For example, if you enter ***.exe;*.doc** in the **Must match** field, Data Protector Express displays all files that have *either* the .exe extension *or* the .doc extension.

Cannot match: Files that match the specified wildcard are not displayed; they are excluded. You can specify multiple wildcards by separating them with a semicolon (no spaces); if you specify multiple wildcards, Data Protector Express excludes any file that matches any one of the wildcards you specify.

Required attributes: Displays files according to attributes controlled by the operation system.

Operating systems track certain features of files called attributes that they use to manage these files. In this field, if an attribute is checked, Data Protector Express only displays those files which have these attributes.

You can select multiple attributes. In this case, Data Protector Express only displays those files that meet *all* of the required attributes.

Note that some of these attributes are only supported by certain operating systems. If you specify an attribute that is specific to a particular operating system, then only files created under that operating system will be displayed.

Exclude attributes: Files with specified operating system attributes are not displayed.

This field works like the **Required attributes** field except that Data Protector Express excludes files that match these attributes.

You can select multiple attributes. Data Protector Express excludes any file that has *any one* of the attributes. For example, if you the **Hidden** and **System** attributes, a file will be excluded if it has *either* the **Hidden** attribute *or* the **System** attribute.

Allow Parents: Determines whether or not the directories are displayed.

When this option is checked, Data Protector Express displays the directories for any object that meets the other display criteria.

Allow Children: When this option is checked, Data Protector Express backs up and restores the selected files. If you want only to back up or restored the marked *directories*, uncheck this option. When the **Children** box is unchecked and the **Parents** box is checked, Data Protector Express backs up the directory structure, but not the files stored in the directories (that is, in the folders).

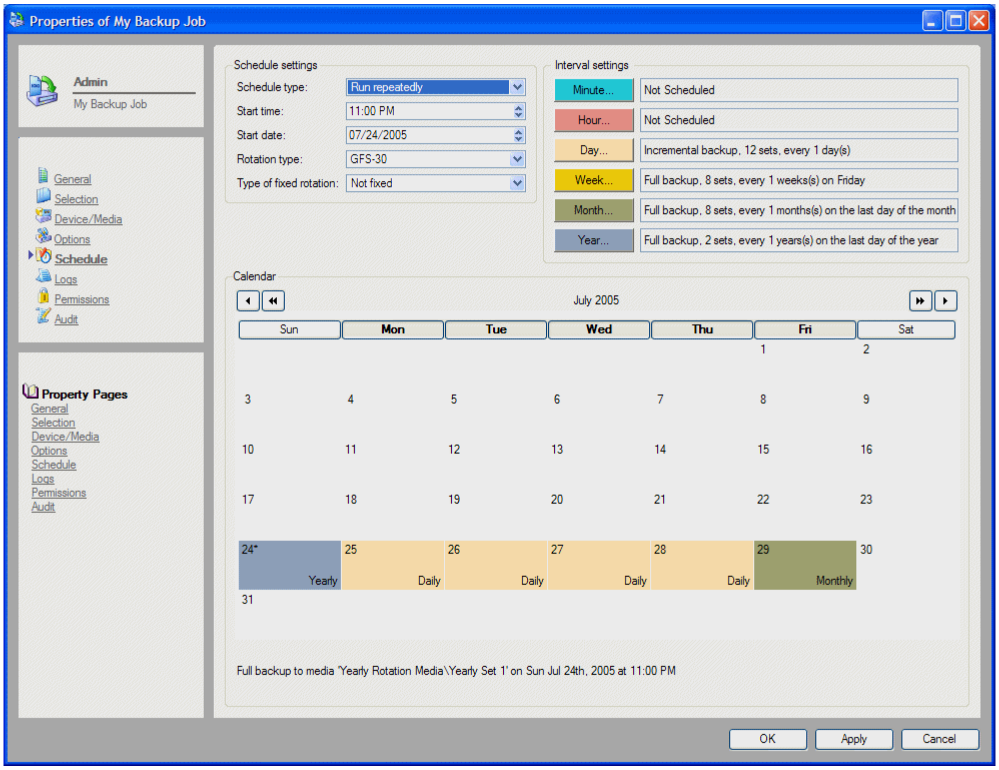
Media: Displays files which have a valid version on the media listed in this field.

Data Protector Express tracks versions of files and the media on which those versions are stored. You can use this information to sort files according to the media on which they appear. Only files with versions on the media in the **Media** field will be displayed. If there are multiple media shown in the **Media** filter field, only files which have a valid version on *all* the media listed will be displayed.

Schedule page

Applicable objects: *Backup Job, Verify Job, Restore Job*

The **Schedule page** controls when and how often a job is run.



Schedule settings

Schedule type: Run repeatedly
Start time: 11:00 PM
Start date: 07/24/2005
Rotation type: GFS-30
Type of fixed rotation: Not fixed

Interval settings

Minute...	Not Scheduled
Hour...	Not Scheduled
Day...	Incremental backup, 12 sets, every 1 day(s)
Week...	Full backup, 8 sets, every 1 weeks(s) on Friday
Month...	Full backup, 8 sets, every 1 months(s) on the last day of the month
Year...	Full backup, 2 sets, every 1 years(s) on the last day of the year

Calendar

July 2005

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24* Yearly	25 Daily	26 Daily	27 Daily	28 Daily	29 Monthly	30
31						

Full backup to media 'Yearly Rotation Media\Yearly Set 1' on Sun Jul 24th, 2005 at 11:00 PM

Schedule settings

A job schedule can contain any of the following schedule settings. The available options change as you select a different schedule.

Schedule type

Not scheduled: The job will run only when instructed to do so. Uses settings set on job’s **Options page**.

Run now: The job will run as soon as you finish setting up the job. Uses the settings set on the job’s **Options page**.

Run once: The job will run only at the selected **Start Date** and **Start Time**. Uses the settings set on the job’s **Options page**.

Run on selected days: Turns on scheduling calendar, allowing job to be scheduled to run repeatedly. Job will run every day as scheduled on the calendar. Uses settings set on job’s **Options** page. User manually controls set count, media rotation, media name and backup mode.

Run hourly: Turns on scheduling calendar, allowing job to be scheduled to run repeatedly. Job will run hourly every day as scheduled on the calendar. Enables the Rotation Type feature which lets users controls set count, media rotation, media name and backup mode. Data Protector Express will automatically update the **Backup mode**, **Write mode**, **New media location** and **New media name** settings on the **Options** page of the job when it runs the job as scheduled. (These settings are not updated if the job is manually "forced" to run by a user.) Allows the user to determine the set count for each set type; however, Data Protector Express will automatically control the implementation of these features.

Run daily, weekly, monthly, yearly: Turns on scheduling calendar, allowing jobs to be scheduled to run repeatedly. Jobs will run daily on every day as scheduled on the calendar. Enables the **Rotation type** feature which lets users control set count, media rotation, media name and backup mode. Data Protector Express will automatically update the **Backup mode**, **Write mode**, **New media location** and **New media name** settings on the **Options** page of the job when it runs the job as scheduled. (These settings are not updated if the job is manually "forced" to run by a user.) Allows the user to determine the set count for each set type; however, Data Protector Express will automatically control the implementation of these features.

Run at Custom Interval: Turns on automatic rotation schedule. Applies to backup jobs only. Job will run every day as scheduled in the calendar. Data Protector Express will automatically update the **Backup mode**, **Write mode**, **New media location** and **New media name** settings on the **Options** page of the job when it runs the job as scheduled. (These settings are not updated if the job is manually "forced" to run by a user.) Allows the user to determine the set count for each set type and Data Protector Express will automatically control the implementation of these features. When first selected, initially defaults to GFS–25 schedule.

Start Time

Specifies the time of day the job will run. Note that jobs can run concurrently. The default start time is 11:00 PM.

Start Date

Specifies the first date the job will run. Data Protector Express defaults to start a job on the current date.

Add Minutes, Hours, Days

Specifies the number of minutes, hours or days that you want to add to the time at which the job will run. Adding more time accumulates each time the job is run. A job starting at 11:00 PM that has 25 minutes added to its schedule will eventually skip a day. Note that all job schedules for which this field applies default to adding a day to the schedule.

Rotation Settings

Many schedule types can include media rotation settings. Not all settings apply to all schedule types.

Rotation Type

Sets the tape rotation schedule. There are thirteen automatic rotation types:

- GFS-62 tape, GFS-54 tape, GFS 30-tape, GFS 25-tape, GFS 20-tape
- Fixed by Day of Week, Fixed by Day of Month, Fixed by Day of Year
- Simple 12-tape, Simple 11-tape, Simple 10-tape, Simple 6-tape, Simple 4-tape.

Applies to job types, that is, *backup*, *restore* and *verify* jobs. Jobs will run every day as scheduled on the calendar. Data Protector Express will automatically update the **Backup mode**, **Write mode**, **New media location** and **New media name** settings on the **Options** page of the job when it runs the job as scheduled. (These settings are not updated if the job is manually "forced" to run by a user.) Group or Set count for each set type have default values that you can reset and Data Protector Express automatically controls media rotation.

End of Week

Indicates the day of the week that Data Protector Express will use to schedule **Weekly** backup jobs. Change the list box to match whatever day of the week Data Protector Express should run weekly jobs.

End of Quarter

Indicates the ending month of the current quarter that Data Protector Express will use to schedule **Quarterly** backup jobs. Change the list box to the month Data Protector Express should run quarterly jobs. Data Protector Express defaults to running the quarterly backup on the last business day of the quarter in the selected month.

Rotation Details

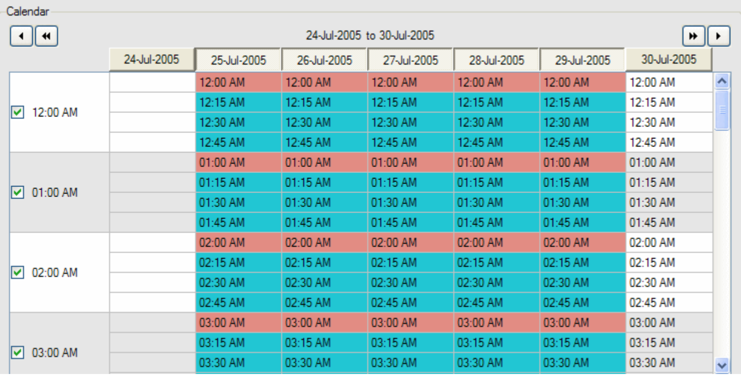
Many rotation types require more information. You can set the following details about rotation types.

Set Type for Daily, Weekly, Monthly, Yearly

Indicates the backup mode and set count for the **Daily**, **Weekly**, **Monthly,** and **Yearly** media sets respectively. **Backup mode** and **Set** or **Group** can be set by the user; Data Protector Express determines the next set in the rotation based on the **Set** or **Group** number.

View a sample rotation

Depending on which schedule type and media rotation plan that you select, you can view a sample rotation schedule. This schedule sample displays the days on which the job will run and the media that Data Protector Express will use. You can print the schedule or save it for later reference. As you modify the schedule, the sample schedule displays updated information based on your schedule modifications.



Calendar

24-Jul-2005 to 30-Jul-2005

	24-Jul-2005	25-Jul-2005	26-Jul-2005	27-Jul-2005	28-Jul-2005	29-Jul-2005	30-Jul-2005
☑ 12:00 AM		12:00 AM	12:00 AM	12:00 AM	12:00 AM	12:00 AM	12:00 AM
		12:15 AM	12:15 AM	12:15 AM	12:15 AM	12:15 AM	12:15 AM
		12:30 AM	12:30 AM	12:30 AM	12:30 AM	12:30 AM	12:30 AM
		12:45 AM	12:45 AM	12:45 AM	12:45 AM	12:45 AM	12:45 AM
☑ 01:00 AM		01:00 AM	01:00 AM	01:00 AM	01:00 AM	01:00 AM	01:00 AM
		01:15 AM	01:15 AM	01:15 AM	01:15 AM	01:15 AM	01:15 AM
		01:30 AM	01:30 AM	01:30 AM	01:30 AM	01:30 AM	01:30 AM
		01:45 AM	01:45 AM	01:45 AM	01:45 AM	01:45 AM	01:45 AM
☑ 02:00 AM		02:00 AM	02:00 AM	02:00 AM	02:00 AM	02:00 AM	02:00 AM
		02:15 AM	02:15 AM	02:15 AM	02:15 AM	02:15 AM	02:15 AM
		02:30 AM	02:30 AM	02:30 AM	02:30 AM	02:30 AM	02:30 AM
		02:45 AM	02:45 AM	02:45 AM	02:45 AM	02:45 AM	02:45 AM
☑ 03:00 AM		03:00 AM	03:00 AM	03:00 AM	03:00 AM	03:00 AM	03:00 AM
		03:15 AM	03:15 AM	03:15 AM	03:15 AM	03:15 AM	03:15 AM
		03:30 AM	03:30 AM	03:30 AM	03:30 AM	03:30 AM	03:30 AM

Related topics

For information about related topics, refer to the following documentation:

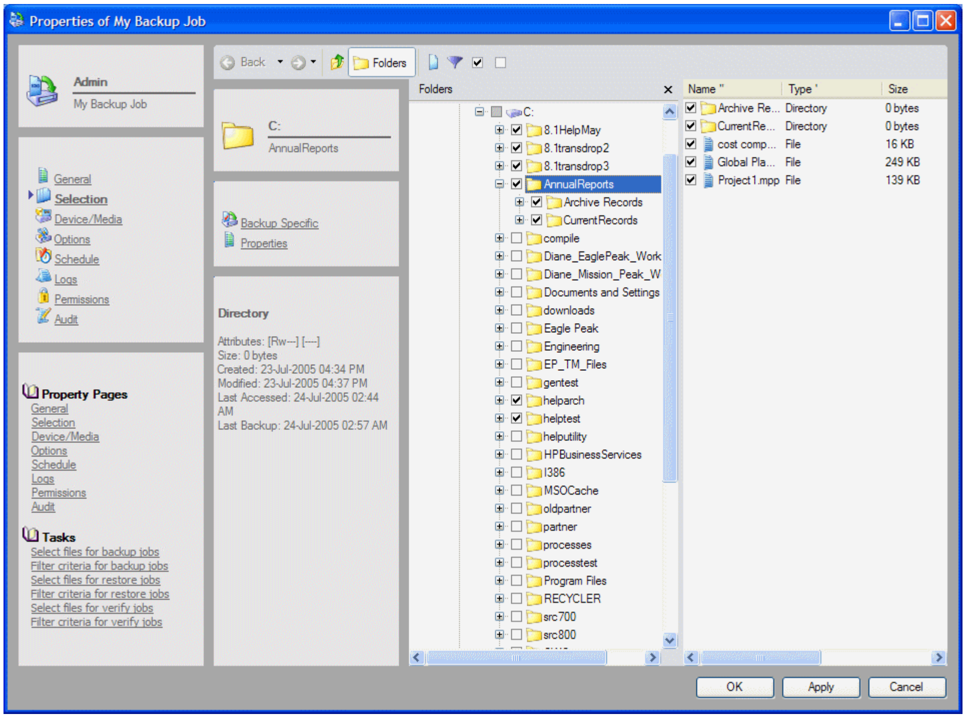
- *Scheduling Jobs* on page 90

Selection page

File Selection Page

Applicable objects: *Backup Job, Restore Job, Verify Job*

Use the **Selection** page to select the files and object versions for use by the current job.



Directory

Attributes: [Rw--] [---]
Size: 0 bytes
Created: 23-Jul-2005 04:34 PM
Modified: 23-Jul-2005 04:37 PM
Last Accessed: 24-Jul-2005 02:44 AM
Last Backup: 24-Jul-2005 02:57 AM

	Name	Type	Size
☑	Archive Re...	Directory	0 bytes
☑	CurrentRe...	Directory	0 bytes
☑	cost comp...	File	16 KB
☑	Global Pla...	File	249 KB
☑	Project1.mpp	File	139 KB

Data Protector Express uses the following to identify selected objects for all job types:

- The box is checked for each selected object.
- The box is shaded for each container (folder, volume, machine and network) that has one or more selected objects.

If you select a container, all objects within that container are selected. If you add new objects to a marked container, those objects will also be selected when the job is run.

If a container is both unmarked and not gray, it contains no selected objects and it is not itself selected.

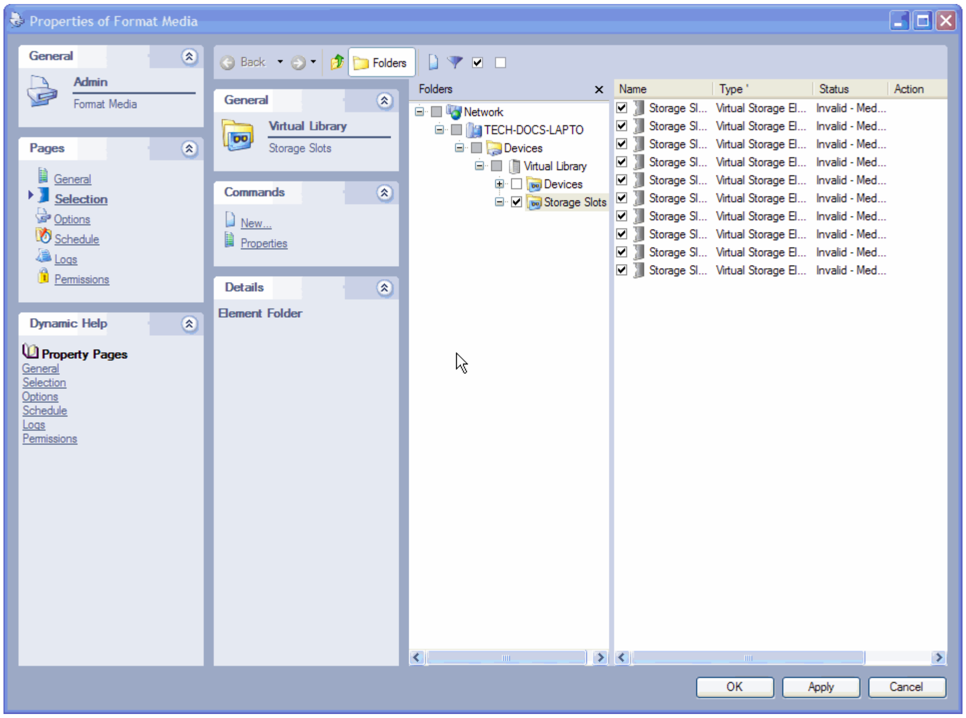
Related topics

For more information about filtering and selecting files for jobs, see *Selecting Files and File Versions* on page 54.

Device or Media Selection Page

Applicable objects: *Media Jobs*

Use the **Selection** page to select a device or media on which to perform an action.



Name	Type	Status	Action
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	
☑ Storage Sl...	Virtual Storage El...	Invalid - Med...	

Data Protector Express uses the following to identify selected objects for all job types:

- The box is checked for each selected object.
- The box is shaded for each container (folder, volume, machine and network) that has one or more selected objects.

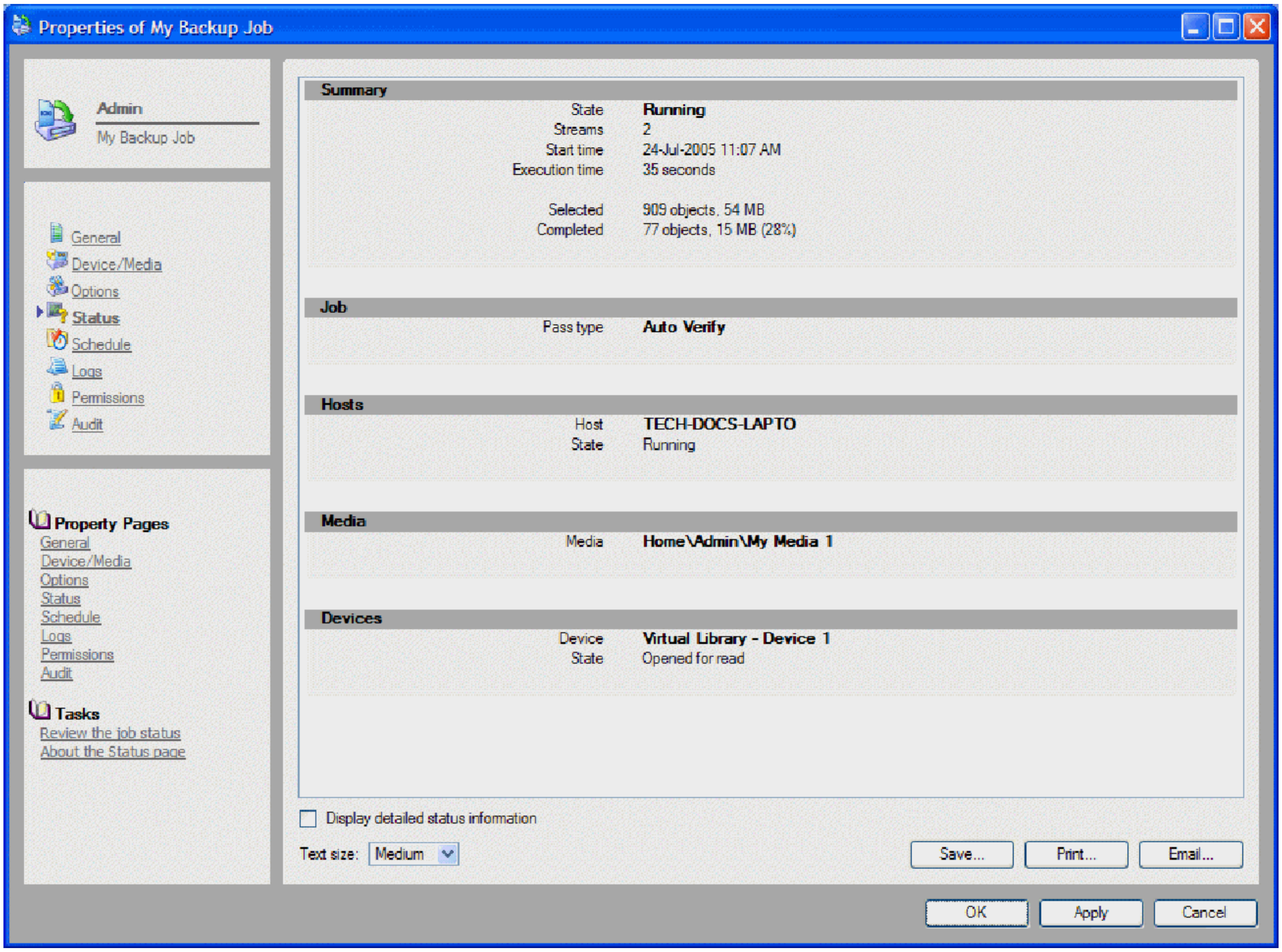
If you select a container, all objects within that container are selected. If you add new objects to a marked container, those objects will also be selected when the job is run.

If a container is both unmarked and not gray, it contains no selected objects and it is not itself selected.

Status page

Applicable objects: *All jobs, Library*

The **Status** page shows the status of a job. It also displays the status of a device or storage slot that is associated with a library. Use it to review the status of your job as it progresses or of storage slots and media as various functions or tests are run on the media in the library. Once you review the status of a completed job or test, the **Status** page will no longer be available until another job or test is run.



Summary

State	Running
Streams	2
Start time	24-Jul-2005 11:07 AM
Execution time	35 seconds
Selected	909 objects, 54 MB
Completed	77 objects, 15 MB (28%)

Job

Pass type	Auto Verify

Hosts

Host	TECH-DOCS-LAPTO
State	Running

Media

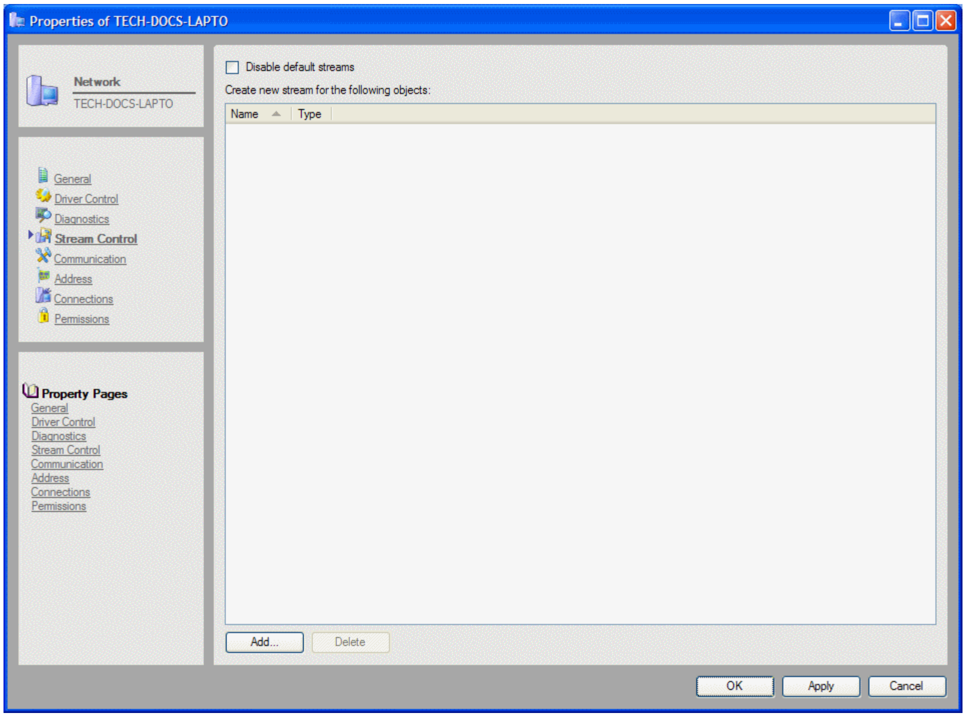
Media	Home\Admin\My Media 1

Devices

Device	Virtual Library - Device 1
State	Opened for read

Stream Control page

Applicable objects: *Machine*



☐ Disable default streams

Create new stream for the following objects:

Use the **Stream Control** page to configure the **Backup stream** setting for all objects found in a machine.

Data Protector Express is capable of controlling multiple concurrent data streams simultaneously (up to eight streams per device). Data streams are automatically created for each machine object. To view this setting for a specific file, directory or volume, open the **Stream Control** page for the file, directory or volume.

NOTE: The number of concurrent data streams that you can create is controlled by your Data Protector Express license. If your data storage needs have increased, consider upgrading your product edition to accommodate more data streams.

To disable the default stream

The default data stream setting determines whether or not a new data stream is created for each object in the machine. To disable it, check **Disable default stream** then save your changes by clicking **Apply** or **OK**.

To create a new stream

You can create a new data stream for selected objects. Creating a new data stream for some objects can improve throughput between the machine and the backup device especially if an object is rather large. For example, you might decide to create a new data stream whenever Data Protector Express backs up a database (such as Microsoft SQL Server databases).

1. On the Stream Control page, click **Add**.
2. Select an object from the selection tree

3. Click **Apply** or **OK** to save your selections.

Storage page

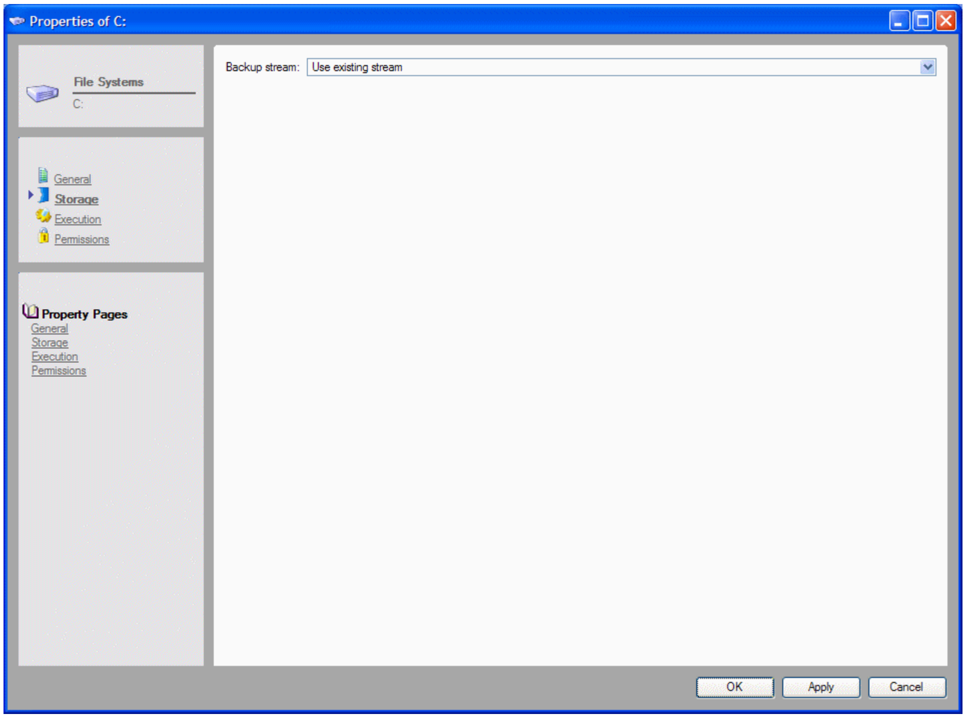
Applicable objects: *File, Directory, and Volume*

Use the **Storage** page to configure the **Backup stream** for this object.

Data Protector Express is capable of controlling multiple concurrent data streams simultaneously (up to eight streams per device). Data streams are automatically created for each machine object. To view this setting for a machine, open the **Stream Control** page for the machine.

NOTE: The number of concurrent data streams that you can create is controlled by your Data Protector Express license. If your data storage needs have increased, consider upgrading your license to accommodate more data streams.

By default, new data streams are created for each volume, while files and directories use the data stream of their parent volume by default. For files, directories and volumes, these settings can be modified.



Backup stream: Use existing stream

Backup Stream

Determines whether or not a new data stream is created for the current object.

Use existing stream: Data Protector Express does not create a new stream for this object. This is the default value for directories and files.

Select this setting for a volume when you do not want to create a new stream for that volume. For example, you may wish to not create an additional stream when the volume is only a logical partition—not a physically separate device.

Create new stream: Data Protector Express will create a new stream for this object when running a backup job. This is the default value for volumes.

Select this setting for directories and files when you want to create a new stream for these objects. For example, to speed up a backup job, you may wish to create an additional stream for a very large file or for a RAID device.

Related topics

For more information about related topics, refer to the following documentation:

- *Strategies for Faster Jobs* on page 156
- *Audit Logs* on page 131

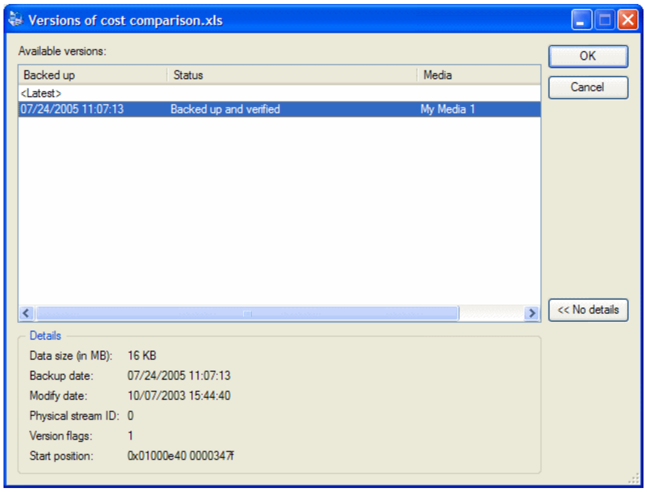
Versions window

Open the **Versions of…** window by clicking the **Check** button on the toolbar of the **Selection** page of either a restore or verify job. This window is used to select a version of the object targeted on the **Selection** page.

Each time an object is backed up, a *version* of that object is created. There may be multiple versions of objects stored on different media created by different backup jobs. Data Protector Express keeps track of all the versions of each object in its catalog and the media on which each version is stored. When media is overwritten or deleted, Data Protector Express deletes those versions from its catalog as well.

When you select an object for restoring, Data Protector Express initially selects the latest version. To select a different version, use the **Versions of…** window.

The latest version is a wildcard and automatically selects the most recent version. Which version is selected is updated as the *restore* or *verify* job is run.



Versions of cost comparison.xls

Available versions:

Backed up	Status	Media
<Latest>		
07/24/2005 11:07:13	Backed up and verified	My Media 1

Details

Data size (in MB):	16 KB
Backup date:	07/24/2005 11:07:13
Modify date:	10/07/2003 15:44:40
Physical stream ID:	0
Version flags:	1
Start position:	0x01000e40 0000347f

Available Versions

Shows a list of the versions of the object and the media on which those versions are stored.

Backed up: Shows the date and time the job was run. All objects backed up during a single job will be listed with the same date and time.

Status: Shows whether or not the object was verified when the job was run. It is either Backed up and verified; Backed up but verify failed; Backed up, possibly corrupted; Backed up, probably corrupted; or Backed up, not verified.

Media: Shows the media on which the version is stored.

Select the version to restore and click **OK**.

Details

Shows more information about whatever version of an object is highlighted. When you click **Details**, Data Protector Express displays the following information about the object. Click **No Details** to close the **Details** window.

Data size: Shows the size of the data fork for the selected object: 0 bytes for folders and directories; the size of each file.

Backup date: The date and time this version was created.

Modify date: The last time the object was modified. This information is recorded from the operating system when the object is backed up.

Physical Stream ID: Shows internal data used by Data Protector Express to manage the version.

Version flags: Shows internal data used by Data Protector Express to manage the version.

Appendix A - Configuring Email

You can configure email information for the Data Protector Express management domain. You can also configure Data Protector Express to automatically email the job log to the job owner as soon as the job has run.

Configuring Email for the Data Protector Express management domain

1. From the **Administration** desk bar, select **Configure Domain Server**.
2. Enter SMTP email settings for your storage domain as follows:

   Server address: Enter the address of the mail server.

   Server port: Enter the appropriate SMTP port. The **Server Port** default is **25**, which is usually the correct value. If you are using a proxy server, you may have to enter a different **Server Port**.

   From address: Enter the email address to be entered in the *From* field for each job log email. This email address must be valid.

   NOTE: Some SMTP mail servers require that the **From address** be a valid *user@host* address; other SMTP mail servers ignore this field.

Configuring Email for a Job

1. Select a job and open its **Options** property page.
2. Click the **Log Options** button. The Log Options screen appears.
3. Under Email logs, select the log format and enter an email address for the recipient.
4. Click **OK** to save the log options.
5. Click **OK** or **Apply** to save the changes to the job.

Appendix B - About the Data Protector Express Service

The Data Protector Express Service lets you run backup jobs automatically and unattended. Data Protector Express can be closed, enhancing PC desktop security. The service makes sure your scheduled backup jobs run even when the machine reboots after a power loss.

NOTE: Data Protector Express is available as a service on Windows, and as a daemon on Linux platforms. The Data Protector Express Agent is available for NetWare systems.

In this section

- Microsoft Windows and the Data Protector Express Service
- NetWare and the Data Protector Express Agent
- Linux and the Data Protector Express Daemon

Microsoft Windows and the Data Protector Express Service

You can manage the Data Protector Express service from the Windows **Services** screen.

To display the Data Protector Express Services screen

1. Select **Start → Administrative Tools → Services**.
2. Locate and double-click Data Protector Express in the list of services.
3. Make any changes to the service and click **Apply** or **OK** to save your changes.

WARNING: Changing the Startup type for the Data Protector Express service to Manual or Disabled means that other machines will not have access to this machine to perform backups unless Data Protector Express is actually running. This means that files on this machine will not be backed up during routine backups for this machine. Before disabling the service, you should evaluate the impact that this decision will have on your company's backup and restore policies.

Data Protector Express Service Controls

You can perform the following from the General page of the Microsoft **Services** screen:

Startup type: You can set the method used to start the Data Protector Express service when your computer starts up. The options include the following:

- **Automatic:** Select **Automatic** to start the Data Protector Express service each you restart the computer. HP recommends that you use this setting if you intend to run backup and restore jobs whether or not the application is running.
- **Manual:** Select **Manual** if you intend to start the Data Protector Express service each time you want it to run. You can run it from a command prompt or by starting it on the Windows Services screen.
- **Disabled:** Select **Disabled** if you want to stop the Data Protector Express service indefinitely. Once disabled, all commands are disabled for the service, including the ability to start the service.

Service status: The status of the Data Protector Express service is displayed below the Startup type. To changes the status, use one of the following commands:

- **Start:** Select this command to start the Data Protector Express service. The **Start Pending** message appears, and the status of the service changes to **Started**. Your backup jobs will automatically start as scheduled.
- **Stop:** Select this command to stop the Data Protector Express service. The **Stopping** message appears, and the status of the service changes to blank. Your backup jobs will not automatically start as scheduled. Selecting this option does not affect the **Startup type** option.

NetWare and the Data Protector Express Agent

The Data Protector Express agent extends the basic Data Protector Express service functionality to NetWare. Like the Data Protector Express service, it can be loaded when the system is started and will run in the background.

NOTE: The Data Protector Express agent and Data Protector Express cannot run at the same time. Therefore, you must stop one before you can start the other.

Running the Data Protector Express Agent

To automatically run the Data Protector Express agent each time the system is restarted, add the following line to the end of the `AUTOEXEC.NCF` file:

```
load dpagent
```

To manually run the Data Protector Express agent, type `load dpagent` from the console prompt and press **Enter**.

Once loaded, the Data Protector Express agent status appears on the screen.

Stopping the Data Protector Express Agent

To manually stop the Data Protector Express agent:

1. Use Alt-Esc to display the Data Protector Express **Agent** screen.
2. Press **Esc**.
3. When the Exit Data Protector Express message appears, select **Yes** and press **Enter**.

Linux and the Data Protector Express Daemon

On Linux platforms, the Data Protector Express service, or daemon, is designed to run automatically each time the system is restarted.

The daemon program (`dplinsvc`) is located in the Data Protector Express directory. To access the service in the default installation directory you would type `cd /usr/local/hp/dpx/dplinsvc` and press **Enter**.

If you have disabled this automatic startup of the service, you can use one of the following commands to manage the service:

Install service: Type `./dplinsvc -i` and press **Enter** to start the Data Protector Express service automatically when your computer starts up. Your selection takes effect the next time your computer starts up.

Uninstall service: Type `./dplinsvc -r` and press **Enter** to not start the Data Protector Express service automatically when your computer starts up. In this case, your scheduled backup jobs may not run. Your selection takes effect the next time your computer starts up.

To start or stop the service if it is already installed, use one of the following commands to manage the service:

Start service: Type `./dplinsvc -s` and press **Enter** to start the Data Protector Express service.

Stop service: Type `./dplinsvc -x` and press **Enter** to stop the Data Protector Express service.

Appendix C - Disaster Recovery

Bare Metal Disaster Recovery is a Data Protector Express agent that performs disaster recovery operations as automatically as possible during initial preparation and recovery. Once installed, this optional feature will perform its tasks without any intervention by you.

In this section

- Create the Disaster Recovery Backup
- Testing Disaster Recovery Media
- Recovering From a Disaster
- Using Disaster Recovery with Libraries
- Using Disaster Recovery with Windows Active Directory

Overview

The Data Protector Express disaster recovery agent can be prepared using CD or DVD media and other devices, depending on your computer configuration. You create bootable media which you use to recover your system configuration, software and data following a system or disk failure. You can use this media to boot your system and initiate the recovery process.

To make your disaster recovery process as easy as possible, please note the following:

- Data Protector Express rewrites most system configuration information to the media each time it overwrites the media during backup jobs. Therefore, when making a full backup to be used for disaster recovery, you should select **Overwrite all media** on the backup job's **Options page**.
- Recovering from a disaster works best with full backups, in which all disks on your system fit on a single media. If the total amount of data on your system requires more than one media, Data Protector Express will prompt you to change media during recovery. You can also use incremental and differential jobs for recovery purposes, but you must insert the recovery media in the correct chronological order.
- If you have a library, make sure the most recent backup media is loaded in slot 1. For more information, see *Using Disaster Recovery with Libraries* on page 257.

- When recovering your system, Data Protector Express gives you the option to recover your whole system or just the hard disk that your system boots from. If the volumes on your boot hard disk are split among multiple physical hard disks, you should recover the entire system and not just the boot disk. Otherwise, some system data may not be restored.
- You must install the disaster recovery option and prepare bootable media on each system that will use this feature. Data Protector Express does not support remote disaster recovery. It only saves recovery information for the local system.

  For example, if the tape device is connected to Machine1 and you make a remote backup of Machine2, the media will contain system configuration information for Machine1, not Machine2. You can use the media to boot Machine1, but Data Protector Express only restores system information to Machine1 during recovery. All other files on the media were backed up from Machine2. To perform disaster recovery on Machine2, you must connect a tape device to Machine2.

When performing disaster recovery, Data Protector Express assumes that major changes to your hardware have not occurred. The hardware on the target system must be nearly *identical* to the source system with the following exceptions:

- You may change your video adapter as long as the new video adapter is VGA compatible.
- You may increase the size of your hard disk, but the geometry of the hard disk should remain the same. For example, if your original system had a hard disk with 63 sectors per track and 255 heads, then the new hard disk should be the same. The actual number of cylinders can be larger. If the geometry has changed, Data Protector Express will still use it, but the recovered operating system may not function correctly.
- Your SCSI, ATAPI, Fibre Channel or USB tape drive and adapter *must be the same or use the same driver* as it did when the disaster recovery media was created.
- You may change network cards, USB ports and USB peripherals, *except* tape drives, without restriction.
- *You may not perform disaster recovery to a USB hard drive or to FC devices.*

NOTE: Ideally, you should perform the disaster recovery operation on the same computer after replacing the faulty hardware that caused the system failure.

Create the Disaster Recovery Backup

Preparing for disaster recovery is a three-step process:

1. Install Data Protector Express and the Bare Metal Disaster Recovery option on each computer that will use disaster recovery (see *Chapter 2: Windows Operating Systems* and *Chapter 3: Non-Windows Operating Systems* in the Data Protector Express *Installation Guide*).
2. Create a full backup of your system, according to the instructions in *Create full backup* below.
3. Create the bootable media (see *Create bootable media* on page 251 later in this section). If you have a bootable tape device, you already created bootable media when you ran the full backup.
4. Test the bootable media to make sure you have created it properly (see *Testing Disaster Recovery Media* on page 253).

NOTE: We recommend that you create at least one extra set of bootable media in case the first set fails during disaster recovery.

Create full backup

Data Protector Express automatically creates disaster recovery media whenever you run a full backup with the **Overwrite all media** job option. To create your disaster recovery media:

1. Log in to Data Protector Express.
2. Insert the first disaster recovery media.
3. Create a backup job in the **Admin Folder**.
4. Enter a name for the job, such as **Disaster Recovery Backup**.
5. Click the **Selection page** and select the check box for the local computer.

NOTE: When creating the disaster recovery media, back up the local machine only. Otherwise, disaster recovery may not restore properly.

6. Click the **Options page**. The **Backup mode** should be set to **Full** by default.
7. Select **Overwrite all media** from the **Write mode** drop-down list.
8. Select **Full verify** from the **Auto verify mode** drop-down list.
9. If your backup device does not support compression, select **None** from the **Hardware compression** drop-down list.
10. If your backup device supports automatic eject, you can configure the job to eject the media after the job finishes. Click **Advanced Options**. When the **Advanced Options** window appears, select **Auto eject** and click **OK**.
11. Click **OK**. The job appears in the **Admin Folder** on the **Backup** page.
12. Run the job, inserting additional media as required.

NOTE: If you have a bootable tape device, Data Protector Express makes each media bootable. For example, if the full backup uses three media, all three media are bootable.

13. Once the backup job is complete, we recommend that you test the disaster recovery media on a test computer (see Testing Disaster Recovery Media on page 253).
14. After the test is successful, store the disaster recovery media.

Create bootable media

After you make a full backup of your system, you must create bootable disaster recovery media. Depending on your platform (Windows, NetWare, Linux), Data Protector Express lets you create bootable CD or DVD or REV media.

NOTE: If you have a bootable tape device, Data Protector Express automatically creates bootable media when you create the disaster recovery backup (see *Create full backup* on page 251). However, you should still create a bootable CD or DVD as a precaution.

Windows

Under Windows, you can create bootable CD or DVD. To create the bootable media:

1. Log in to Data Protector Express.
2. Select **Disaster Recovery** from the Data Protector Express **Wizards** view.

3. Select **Make Bootable CD**.
4. Follow the instructions in the wizard to create a bootable CD or DVD for your machine. You can create either a bootable CD or DVD with this wizard.

If you have several machines connected to the Data Protector Express management domain, create a bootable CD or DVD for each machine.

TIP: Consider making duplicate bootable media for use in case the primary bootable media is unavailable or damaged.

NetWare

On NetWare systems, you can create a bootable CD or DVD. To create the bootable media:

1. Log in to Data Protector Express.
2. Open the **Wizards** view and select **Disaster Recovery**.
3. Select **Create bootable CD** and follow the on-screen steps to create your bootable media.
4. When you are done, press **Esc** twice to return to the main menu.

This procedure creates a bootable CD or DVD media, which contains the entire ISO-9660 bootable image required to boot your system and initiate the recovery process.

As soon as you create the bootable media, we recommend that you test the it on a test computer (see Testing Disaster Recovery Media on page 253). After the test is successful, store the CD or DVD media.

Linux

This procedure creates a bootable CD or DVD that can be used to recreate the operating system for the machine on which it was generated.

TIP: Consider making duplicate bootable media for use in case the primary bootable media is unavailable or damaged.

Console Interface

To create a bootable CD or DVD from the console version of Data Protector Express:

1. Log in to Data Protector Express.
2. Select **Other** from the **Available Options** menu.
3. Select **Disaster Recovery** from the **Other Options** menu.
4. Select **Create bootable CD**. Data Protector Express prepares the system information and copies it to the CD or DVD.
5. When the **Available Options** menu appears again, press **Esc** twice to return to the main **Available Options** menu.

X Window Interface

To create a bootable CD or DVD from the X Window version of Data Protector Express:

1. Log in to Data Protector Express.
2. Select **Disaster Recovery** from the Data Protector Express **Wizards** view. The **Disaster Recovery** window appears.

3. Select **Create bootable CD** and follow the on-screen steps to create your bootable media.
4. As soon as you create the media, we recommend that you test the disaster recovery media on a test computer (see Testing Disaster Recovery Media on page 253). After the test is successful, store the CD or DVD.

Troubleshooting disaster recovery backups

When creating disaster recovery backups, any of the following problems may occur:

- Unable to find files

  Open the **Logs** view and examine the log file for the disaster recovery wizard that you ran. This will list the file that was not found. All files must reside in "standard" directory locations provided by the operating system, that is, \WINNT\SYSTEM32\DRIVERS subdirectory under Windows NT and SYS:SYSTEM or C:\NWSERVER under NetWare. If the file is not a driver file for your hardware, visit www.hp.com/go/dataprotectorexpress to review knowledge base articles on this topic.

- Unable to open the Microsoft Windows registry

  Data Protector Express requires full access to the Windows registry to create disaster recovery information. Make sure you are starting Data Protector Express from an account with full administration privileges.

- Failures getting or setting server information

  An error might occur while retrieving the disk configuration information. Open the **Logs** view and examine the log file for the disaster recovery wizard that you ran. This error usually occurs if a hard drive is not turned on or if a user does not have adequate system administration privileges to the hard disk.

When to create new bootable media

Your bootable media may become *obsolete* whenever any of the following occurs:

- You update your operating system by installing a service pack or other software.
- You add or remove hardware from your computer.
- You change the configuration of your disk drives, e.g., adding or removing volumes or partitions.
- You change your Data Protector Express environment information, including changes to the dpconfig.ini file.

Therefore, we recommend that you create new bootable media anytime you change the environment.

Testing Disaster Recovery Media

We recommend that you test your disaster recovery media before you have to rely on it following a disaster. We also recommend that you create additional bootable media in case your new hardware configuration does not support your original bootable media. For example, if you create a bootable CD or DVD, but your new hardware does not support booting from CD or DVD, you should also create an alternate set of bootable media like a REV storage device or other media.

WARNING: Before relying on any disaster recovery media, you should verify that your system can boot from the bootable device as described below.

To test your disaster recovery media, perform the following steps. You will not lose any data on your system. This procedure is completely safe.

1. Make a full backup of your system and create bootable media as directed in *Create the Disaster Recovery Backup* on page 250.
2. Shut down your system as normal.
3. If you are using a bootable CD or DVD:
   a. Insert the disaster recovery CD or DVD into your computer.
   b. Turn on your computer.
   c. Perform any special steps for booting your computer from CD or DVD (refer to your system documentation).
   d. The system boots from the CD or DVD.
4. If you are using an alternate set of bootable media:
   a. Insert the first media into your backup device.
   b. Turn on your computer.
   c. The system boots from the media.
   d. Data Protector Express prompts you to insert additional media as necessary.
5. If you are using a bootable tape:
   a. Remove all media from all tape drives and/or library magazine slots.
   b. Insert the first bootable media:
      - If you are using a single tape drive, insert the first bootable media into the drive.
      - If you are using a library, insert the first (or only) bootable media into slot 1 of the magazine. If the full backup used two or more media, insert the rest of the full backup media into the library magazine in their proper order.

NOTE: Slot 1 must contain the first (or only) bootable media from the most recent full backup.

   c. Perform any special steps for booting your computer from the tape drive (refer to your system documentation). Most bootable drives use a combination of power cycling and pressing the Eject button on the front panel. Many also require that you update the computer BIOS.
   d. The system boots from the tape.
6. If your system boots and displays the Disaster Recovery (Phase 2) screen, your bootable media should function correctly during disaster recovery.
7. If you are using a bootable tape, the **Disaster Recovery (Phase 2)** screen may not appear. Your system may hang during startup or your operating system may not boot from the tape. If either case, you must use a bootable CD or DVD to perform disaster recovery. Your tape device is not compatible with bootable tape.
8. Select **Exit from Disaster Recovery** and press **Enter**.
9. Remove the bootable media and restart your computer. This ends the disaster recovery test.

Recovering From a Disaster

If disaster strikes and you are unable to boot your system using your normal boot procedure, use one of the following procedures to recover your system. You will need your bootable media (CD or DVD media), your most recent full backup and any incremental or differential backups.

NOTE: Data that has changed since the last full backup will not be restored. You must restore the rest of your data from incremental or differential backups. Any data that has not been backed up must be recreated. Therefore, you should only use Disaster Recovery as a last resort.

Disaster recovery from CD or DVD

Do not restore incremental or differential backup media until after you complete disaster recovery.

1. If you are using a bootable CD or DVD:
    a. Insert the disaster recovery CD or DVD into your computer.
    b. Power on your computer.
    c. Perform any special steps for booting your computer from CD or DVD (refer to your system documentation).
    d. The system boots from the CD or DVD.
2. Insert the first disaster recovery media.

NOTE: For disaster recovery, use only full backup media that were created with the **Overwrite all media** option. After disaster recovery is complete and your system has restarted, use the standard Data Protector Express options to restore any incremental or differential media to your system. The standard Data Protector Express restore procedure optimizes restoration and restores incremental and differential media faster than the disaster recovery process.

3. When the **Disaster Recovery (Phase 2)** screen appears, select one of the following options:
    - **Recover Boot Disk** Select this option to only recover the boot disk. Use it if your boot disk is corrupt or if you replaced the boot disk. This option does not usually affect the data on other hard disks.
    - **Recover Entire System** Select this option to recover data to multiple hard disks, including the boot disk. Use this option if you replaced one or more hard disks.
4. Press **Enter**.
5. If a warning screen appears, read it and then press **F10**.
6. Read through each information screen. Press **F10** to advance to the next screen.
7. When the first confirmation message appears (**Are you sure?**), select the appropriate **Yes** option and press **Enter**.
8. When the second confirmation message appears, select **Yes, Perform the Recovery** and press **Enter**.

    The system does not require any input from you until it finishes restoring the first media to your system. Restoring the first media can take from 15 minutes to two or three hours, depending on the amount of data on the media, the speed and capabilities of the tape drive and whether you are recovering the entire system or just the boot disk.
9. After the system has restored the media, it asks for the next media to restore. Select **Yes** or press **F10** to restore another media.

10. After restoring the last media, remove the disaster recovery CD or DVD so that you can boot from the hard disk in subsequent steps.
11. Press **Esc**. A message screen appears.
12. Press **F10**. Data Protector Express restarts your computer.

    You can now use Data Protector Express to restore the data from your incremental and differential backup media, if needed.

Disaster recovery from bootable media

Do not restore incremental or differential backup media until after you complete disaster recovery.

1. Remove all media from all tape drives and/or library magazine slots.
2. Insert the first bootable media:
   - If you are using a single tape drive, insert the first bootable media into the drive.
   - If you are using a library, insert the first (or only) bootable media into slot 1 of the magazine. If the full backup used two or more media, insert the rest of the full backup media into the library magazine in their proper order.

   NOTE: Slot 1 must contain the first (or only) bootable media from the most recent full backup. When you use the **Overwrite all media** option, Data Protector Express makes each media bootable (see *Create the Disaster Recovery Backup* on page 250). For example, if the full backup uses three media, all three media are bootable.

3. Perform any special steps for booting your computer from the tape drive (refer to your system documentation). Most bootable drives use a combination of power cycling and pressing the **Eject** button on the front panel. Many also require that you update the computer BIOS.

   NOTE: For disaster recovery, use only full backup media that were created with the **Overwrite all media** option. After disaster recovery is complete and your system has restarted, use the standard Data Protector Express options to restore any incremental or differential media to your system. The standard Data Protector Express restore procedure optimizes restoration and restores incremental and differential media faster than the disaster recovery process.

4. When the **Disaster Recovery (Phase 2)** screen appears, select one of the following options:
   - **Recover Boot Disk:** Select this option to only recover the boot disk. Use it if your boot disk is corrupt or if you replaced the boot disk. This option does not usually affect the data on other hard disks.
   - **Recover Entire System:** Select this option to recover data to multiple hard disks, including the boot disk. Use this option if you replaced one or more hard disks.
5. Press **Enter**.
6. If a warning screen appears, read it and then press **F10**.
7. Read through each information screen. Press **F10** to advance to the next screen.
8. When the first confirmation message appears (**Are you sure?**), select the appropriate **Yes** option and press **Enter**.
9. When the second confirmation message appears, select **Yes, Perform the Recovery** and press **Enter**.

The system does not require any input from you until it finishes restoring the first tape to your system. Restoring the first tape can take from 15 minutes to two or three hours, depending on the amount of data on the tape, the speed and capabilities of the tape drive and whether you are recovering the entire system or just the boot disk.

10. After the system has restored the tape, it asks you to insert the next tape to restore. Select **Yes** or press **F10** to restore another tape.
11. After restoring the last tape, remove the tape.
12. Press **Esc**. A message screen appears. Then Data Protector Express restarts your computer.

    You can now use Data Protector Express to restore the data from your incremental and differential backup media, if needed.

Troubleshooting recovering from a disaster

When attempting to recover your system, the following are common errors that occur:

- Get or set server failure

  This message appears when Data Protector Express cannot reconfigure the disk drives and volumes on the target system. Make sure that all disks are powered on and ready and that any new disks are the same size or larger than the old disks. Make sure that the geometries of any new disks are also the same size or larger. Make sure you have enabled logical block addressing in your BIOS configuration and that any SCSI controllers are configured the same as when you created the recovery tape. If you changed SCSI adapters, Data Protector Express may not be able to access any peripherals from the new adapter unless it uses the same driver as the old adapter.

- Unable to boot from tape

  This message appears if the tape does not contain a valid disaster recovery boot track. Try another tape or tape drive, if available.

- Dynamic disk failure

  In some dynamic disk configurations under Windows 2000/XP/Server 2003, including RAIDs and mirrors, you may receive a dynamic disk failure message. The layout is usually recovered successfully. You simply have to re-activate the mirror set.

Using Disaster Recovery with Libraries

When using Disaster Recovery with a library, remember the following:

- Make sure the most recent full backup media is loaded into slot 1 of the library. Data Protector Express will only boot from the tape in slot 1. Make sure the media was created using the **Overwrite all media** option.
- Data Protector Express will restore all media that are contained in the library during the final recovery process. Therefore, make sure that you only load media in the library that you will need to restore during recovery. For example, if you are using the Simple 10-tape schedule, Data Protector Express will have four daily differential backups, two weekly full backups and two monthly full backups. You should only perform disaster recovery with the latest full backup. After your system has been recovered, use the standard Data Protector Express restore procedures to recover any other changes from the differential backups.

- Remove all media not associated with the recovery from the library. If the full backup spans more than one media, put the additional full backup media into additional slots. Data Protector Express will then restore these media along with the slot 1 media.

NOTE: Slot 1 must contain the first (or only) bootable media from the most recent full backup. When you use the **Overwrite all media** option, Data Protector Express makes each media bootable (see *Create the Disaster Recovery Backup* on page 250). For example, if the full backup uses three media, all three media are bootable.

Using Disaster Recovery with Windows Active Directory

When performing disaster recovery on a system with Windows Active Directory, use the following general steps:

1. Perform the general system-level disaster recovery to restore the basic system data.
2. When the **Starting Windows** screen appears during system startup, press **F8**.
3. Select Directory Services Restore Mode and press Enter.
4. Log in to the system.
5. Log in to Data Protector Express.
6. Create a restore job.
7. Select **Windows Active Directory** for the restore job from the **Selection page**.
8. Run the restore job.
9. Exit Data Protector Express.
10. Restart the computer, letting Windows load normally.
11. Verify that Windows active directory is running properly.

Appendix D - Troubleshooting Guide

This appendix contains useful information about commonly encountered problems and frequently asked questions when using Data Protector Express.

In this section

- Troubleshooting Backup Jobs
- Troubleshooting Restore Jobs
- Troubleshooting Verify Jobs
- Troubleshooting the Catalog
- Troubleshooting Error Messages

NOTE: Please refer to the Data Protector Express *Installation Guide* for useful information about installing Data Protector Express.

Troubleshooting Backup Jobs

When I run a backup job, it uses the backup device on my local machine instead of the one on the server.

On the **Options page** of the job, you have probably accepted the default **Network** device selection. When this is enabled, Data Protector Express will use any device on the network, in this case, your local backup device.

To send the job to a specific device:

1. Access the **Options page** for the backup job.
2. Delete the current network device:
   - Select the path to the device in the **Devices to be used** field.
   - Click **Delete**. The path disappears from the **Devices to be used** field.
3. Add the local device:
   - Click **Add**. The Browse screen appears.
   - Select the local device.

- Click OK. The path to the local device appears in the **Devices to be used** field.

My scheduled job is not running.

Verify the following to determine why your scheduled job is not running.

1. Make sure the job is scheduled. Check the **Schedule** page for the job's properties. After reviewing the schedule, close the property page or the job will not run. Then check the **Job Status** view to verify that the job is scheduled.
2. If you have not installed Data Protector Express as a service, make sure Data Protector Express is open and running. If you exit Data Protector Express, the job cannot execute. We recommend that you log out of Data Protector Express to prevent unauthorized access to Data Protector Express.
3. If you have installed Data Protector Express as a service, make sure the service has been started.

   To start the service on Windows operating systems, select **Start→ Administrative Tools → Services**.

   On Linux operating systems, open a terminal window (if necessary). Then access the directory where you installed Data Protector Express, e.g., usr/local/hp/dpx. Type ./dplinsvc.

   For additional information, see *Automatically running scheduled jobs* on page 123 and *Logging out and running scheduled jobs* on page 12.

I have two tape drives, but it is only using one to run a job.

Data Protector Express uses "data streams" to divide a job up and to assign the job to devices for backup. By default, it creates a new stream for each disk volume to be backed up, e.g., one each for **C:** and **D:** drives. If you only have a single volume, Data Protector Express only creates one stream by default.

To use multiple devices, you must first add each device to the device list. Access the **Device/Media page** for the backup job. Then click **Add** to display **Select a device or device container** window. Select the local device and click **OK**. The path to the local device appears in the **Devices to be used** field.

To create additional streams for different objects, change the **Backup stream** setting to **Create new stream** on the **Storage** page for each object. Then the streams will be distributed evenly across all available backup devices. For further information, see *Storage page* on page 241 and *Strategies for Faster Jobs* on page 156.

NOTE: Since multiple streams run concurrently, creating multiple streams on the same physical disk drive does not necessarily result in faster backup jobs. The drive tries to stream to multiple devices at once, which requires numerous seek and read commands from various sectors at the same time. The end result is a shortened lifespan for the drive.

How do I replace media in a rotation group?

Data Protector Express automatically creates a series of folders and media for use with rotation jobs. These folders control the daily, weekly, monthly and yearly media.

To remove a piece of media that is lost or damaged physically, select the media on the **Jobs and Media** view and delete it. When you use replacement media, Data Protector Express will automatically format it if necessary.

To move media to an offsite location, create a new media folder called **Offsite Media** (or similar) in your User/Group folder. Then use the **Move** command to move the media to this folder. If the media is required by Data Protector Express during the rotation schedule, it will automatically create a new media to replace the media that you moved offsite.

How can I tell when the next job will run and which media is required?

Click the Favorites view and select Instructions and Recent Logs.

You can also select the job and view the **Logs** property page to view information about a specific job.

How can I determine which files were not backed up?

Check the the job log for any failed objects. Access the **Logs** page for the backup job and select the date of the backup you want to check. Data Protector Express uses the text editor specified on the **Preferences** screen to display the job log. Then you can save the log to a file after editing. Data Protector Express can also print the log directly to the printer.

NOTE: You are only working with a copy of the log. The original log is still available.

Troubleshooting Restore Jobs

I can’t restore a backup to a different operating system.

Windows, NetWare and Linux systems store information in different formats. For example, if you backed up NetWare information in a compressed format, Windows cannot read the NetWare compressed data.

To restore to a different operating system, even to a different version of the *same* operating system, you must create the backup in a generic format.

NOTE: If you did not create your backup in a generic format, you may not be able to restore it to a different operating system. You should either restore it on a similar operating system or create a new backup.

1. Access the backup job’s **Options** page.
2. Click the **Advanced options** button. The **Advanced Options** window for the job appears.
3. Deselect the **Native data streams format** option. When you run the backup job, Data Protector Express decompresses the data and strips the information specific to the operating system before backing it up.

NOTE: You may lose security information under certain operating systems.

For additional information, see *Moving data between operating systems* on page 163.

How can I restore data to a different file name?

Select the file, directory or volume you wish to restore with a different name. Then open the properties page for that object. On the **General** page, type in the new name and press **OK**.

For additional information, see *Restoring Files with New Names and Locations* on page 78.

How can I restore data to another location?

To restore data to another location, open the **Selection page** of the restore job. Click the folder or file you want restored to a different location, then use the **Move** command to move that folder or file to the new target location. To use the keyboard, use CTRL+C to copy the object and CTRL+V to move the object to its new location.

If you have not backed up the target directory, that is, the directory to move the files to, it will not be displayed. In this case, right-click the files or directories to move, and then select **Move** from the shortcut menu. Select the target directory to complete the move command.

How can I restore all the files from a single version?

Every version of a file or directory backed up during a single job has the same version date. You can use this information to select all the files from a single backup job.

On the **Selection page** of the restore job, highlight the file, directory or volume to restore. Press the **Select Version** button on the tool bar to open the **Versions of…** window. Select the date of the version you want restored. All children (objects) having the same version will also be selected.

For additional information, see *Selecting versions from a specific job* on page 160.

How can I determine which files are on particular media?

On the **Favorites** desk bar, open the **Wizards** view. Open the **Media** wizards and select **Media Content**. Follow the instructions on the wizard to select some media and determine its contents.

When restoring, I get many alerts. What is wrong?

If you select many devices or set the **Devices to be used** field on the **Device/Media** page of the job to **Network** (the default setting), Data Protector Express will attempt to complete the restore job using *all* the devices listed or found. If a device does not contain media or the device contains the wrong media, an alert is sent. This alert informs you to put the desired media into the appropriate device.

For example, suppose you are restoring from a single media but the **Devices to be used** field on the **Device/Media** page lists four devices. If the target media is in the third device listed, Data Protector Express will issue two alerts, one for each of the first two devices. These alerts can be ignored.

Also note that you do not have to insert the *requested* media into the device. To fulfill the request, you can place any media required by the job into the device. Data Protector Express will then use the media that you actually did put into the device.

If you want the job to use a specific device, first delete the **Network** object in the **Devices to be used** field. Then click **Add** and add the specific device you want the restore job to use.

Does Data Protector Express back up files as compressed?

Data Protector Express will copy files to tape in compressed format without decompressing them first. This significantly enhances the speed of the backup.

Troubleshooting Verify Jobs

I occasionally get a 'stream sync error' when verifying media.

This is usually caused by a physical read problem from the backup device. The data Data Protector Express expected from the media was not found. This can be caused by:

- *Bad media:* Try replacing the media.
- *Read errors on the drive:* Try cleaning the drive heads.
- *SCSI errors:* Try checking the SCSI termination.

- *Driver errors:* Try checking to see that you are not using a real mode ASPI drive. Check your config.sys file for something like:

```
device=ASPI4DOS.SYS, ASPI8DOS.SYS...
```

Troubleshooting the Catalog

How do I select the location of the catalog in a network installation?

The network location of the catalog can be very important. On larger networks, to minimize the time required to perform disaster recovery, install the catalog on a dedicated backup server. This server performs no operations except the storage management processing. Then install the tape devices to the servers to be backed up. If the storage manager server fails, no data is lost and recovery of the server can proceed in a non-critical manner. If any other server fails, recovery can be quickly performed because the backup server is still operational.

On smaller networks, you can install the catalog on the same server as the tape devices. Recovery does not take as much time because the catalogs are smaller.

For additional information, see *Tips for Managing the Catalog* on page 153.

How do I create a Data Protector Express management domain?

When you install Data Protector Express, you can choose to either join an existing Data Protector Express management domain or create a new one. The Data Protector Express management domain is associated with the same computer on which its catalog is installed.

To create a new Data Protector Express management domain, run the Data Protector Express installer. When prompted, enter the name for the storage domain and the disk location for the catalog. The default location is the Data Protector Express directory on your system, e.g., c:\Program Files\HP\Data Protector Express on a Windows computer.

For additional information, see the Data Protector Express *Installation Guide*.

When recovering from a backup server failure, does Data Protector Express recover all of the catalog information?

Most of the catalog information is restored when you restore the catalog. The only thing that will not be restored is the complete log of the job that was running when the catalog was backed up. The reason for this is that the log is not written until after the job has completed. Jobs are not completed until the catalog is written to the media.

Troubleshooting Error Messages

Catalog corrupt appears during a backup or when adding a new object.

Normally, if the catalog is corrupted, Data Protector Express automatically repairs it during initialization. However, the quick check used during initialization may not detect any errors. To repair the Data Protector Express catalog manually:

1. Close Data Protector Express.

2. Stop the Data Protector Express service:
    a. Open a Command Prompt window.
    b. Change to the Data Protector Express directory:

       ```
       Program Files\HP\Data Protector Express
       ```

    c. Type the following command at the Command Prompt:

       ```
       dpwinsvc –x
       ```

       This command stops the Data Protector Express service on the local machine.

3. Edit the dpconfig.ini file in the Data Protector Express directory (`HP\Data Protector Express\config` by default) on the $Option_masterserver$.

4. In the **[configuration]** section, add the following line:

   ```
   repairDatabase=Yes
   ```

   The configuration section should now look like this:

   ```
   [configuration]
   lastUser=admin
   lastDomain=My Domain
   nodeGuid={00001001-421F132A-0003F771-FFE580D7}
   databaseServerAddress=localhost
   isDatabaseServer=Yes
   databaseServerName=My Domain
   disableNetwork=No
   remoteAdmin=No
   repairDatabase=Yes
   ```

5. Save and close this file.

6. Open Data Protector Express. **Do not restart the service.**

   The catalog repair will run automatically. After the repair have completed, the Logon screen will appear.

7. Restart the Data Protector Express service:
    a. Open a Command Prompt window.
    b. Change to the Data Protector Express directory:

       ```
       Program Files\HP\Data Protector Express
       ```

    c. Type the following command at the Command Prompt:

       ```
       dpwinsvc –s
       ```

       This command starts the Data Protector Express service on the local machine.

Unknown error appears when I restore files on Microsoft Windows.

Windows stores security information in the data stream on the backup media. This information depends on the registry from the file's original location. If you are restoring to a different system or are restoring files to the same machine with a new registry, the security information on the media is no longer valid.

To prevent this problem, open the **Advanced Options** window from the **Options page** of the restore job and clear the **Parent security** and **Child security** options. This causes Data Protector Express to restore the data in the file, but not the security information, such as the owner or access control lists for the file.

Unable to create a directory appears when I restore files on Microsoft Windows.

This message appears if you do not have the appropriate Windows rights to the hard drive during the restore. Make sure you have full control on the **CREATOR OWNER** and **SYSTEM** rights on the **Local Disk Properties** screen for the hard drive. Then try again. After you have restored the files, you can change the Windows rights to their original settings.

Appendix E - Navigation keys in the text user interface

Data Protector Express provides many navigation keys for use in the text user interface. Different keys are available on all screens. The status bar at the bottom of each screen lists the available navigation keys and a brief description of their functions. Since some telnet systems do not support function keys, alternative shortcut keys appear in parentheses.

Esc: Stop the current action. Press Escape to cancel the current command.

Enter: Select the current object or action. Press Enter to select an object on a screen or to invoke a selected command.

Space: Toggle between the current command and an alternate command. For example, if you expand a tree branch view on a menu, press the Space key to collapse the view.

Ins: Create a new object, for example, a new backup or restore job.

Del: Delete an existing object, for example, a backup or restore job.

PgUp/PgDn: View the next or previous page of a log or instruction file.

Up/Down arrows: Use the up and down arrow keys to scroll through the fields on a screen or to scroll through a text box that is longer than a single screen.

Tab/Shift-Tab: Switch to the next or previous page.

+ / -: Expand or collapse a tree branch view.

F1 (?): Display the help for this screen.

F2: Print instructions or log files.

F3: Edit properties. Press F3 to edit object information on the Properties page.

Shift-F3: Display the driver message log at any time while Data Protector Express is running.

F4: Find an object.

Shift-F4: Find an object again.

F5 ([ ): Select an object.

Shift-F5: Select all objects.

F6 ( ]): Deselect an object.

Shift-F6: Deselect all objects.

F7: Filter a list.

F8 (=): Switch between panes.

Shift-F8: Refresh a tree branch view.

F9: View more options. This command is available on menus that contain more options than fit on the screen.

Shift-F9: Refresh all tree branch views.

F10 (\ ): Press this key when you complete an action on a screen. Data Protector Express returns to the previous menu.

Appendix F - Working with Microsoft Exchange Server

This appendix contains important information pertaining to backing up and restoring Microsoft Exchange Server databases and configuration data. If you are using Data Protector Express to back up and restore Microsoft Exchange Server databases, be sure read these instructions carefully.

In this section

Supported platforms

The Data Protector Express Agent for Microsoft Exchange supports backup and restore operations for Microsoft Exchange 2000 Server and Microsoft Exchange Server 2003.

Installing the Data Protector Express Agent for Microsoft Exchange

By default, an evaluation version of the Data Protector Express agent for Microsoft Exchange is installed automatically when you install Data Protector Express on a Windows server machine that is running Microsoft Exchange. You can use this evaluation license for 60 days. To continue using the agent, contact your sales representative to purchase a license.

Activating the license

1. Select **Licenses** from the **Help** menu.
2. In the object detail area of the screen, right-click and select New from the shortcut menu.
3. Enter the license key.

4. The license will take effect immediately.

Configuring a Microsoft Exchange Server

As with any other objects that are configurable in Data Protector Express, you can configure the Microsoft Exchange Server for backups if you have the correct permissions.

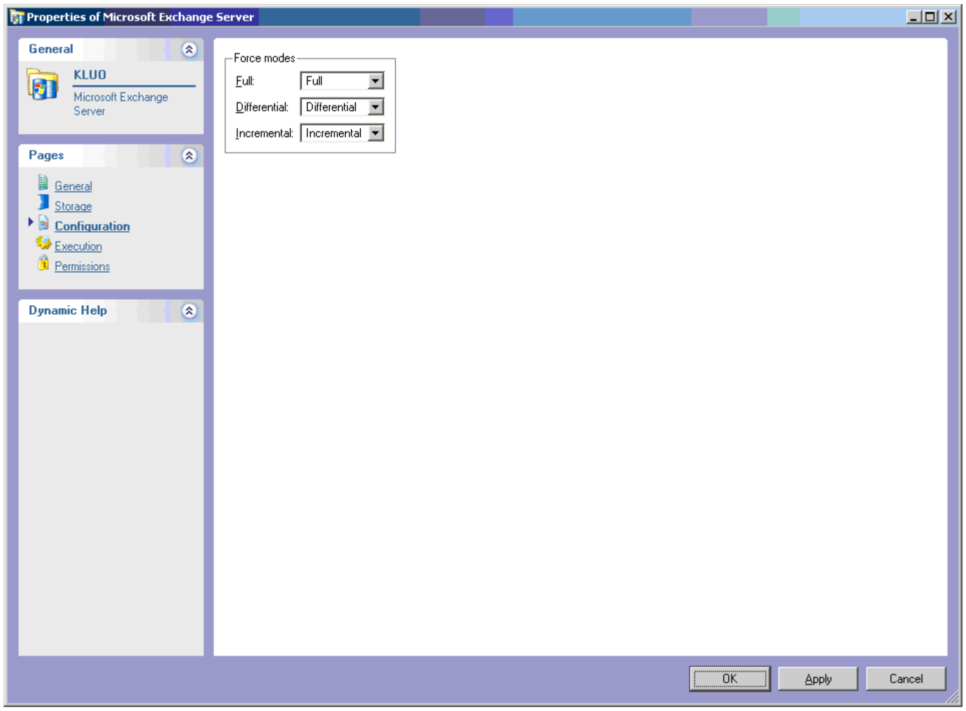
1. Open the **Administration** desk bar and select **Catalog** view.
2. Select Network, then locate and select the Microsoft Exchange Server on your system.

TIP: Switch to the **Folders** view to display a hierarchical tree of the Data Protector Express management domain.

---

3. Right-click the server and select the **Configuration** command.

   The **Configuration** property page appears.



Force modes

Full: Full

Differential: Differential

Incremental: Incremental

Update the following settings that control how Data Protector Express works with Microsoft Exchange Server.

Force Modes

As explained in the next section, the **Backup mode** setting of a backup job affects Microsoft Exchange Server databases differently than file types. The **Force modes** settings control how Data Protector Express backs up the databases.

Note that the settings here are only applicable to Microsoft Exchange Server databases; all other file types are backed up in the job’s default mode. For example, if the **Backup mode** of a job is set to **Incremental** and the **Force modes** setting for incremental jobs is set to **Full**, Data Protector Express will back up the Exchange Server databases in **Full** mode, but all other file types in **Incremental** mode.

TIP: You can use this feature to ensure that the databases are always backed up in full mode, but that other objects are only backed up when changed. This guarantees the greatest security for the most crucial files (that is, the Exchange Server databases), while not making jobs unnecessarily large by *not* backing up the entire network (that is, by backing up only the changed files).

Full: When the **Backup mode** of a job is set to **Full**, Data Protector Express checks this setting to see how the job should be run with Microsoft Exchange Server databases. **Full** is the only possible setting, so the databases will be backed up in this mode. In this case, both the database files and the transaction logs are backed up.

Differential: When the **Backup mode** of a job is set to **Differential**, Data Protector Express checks this setting to see how the job should be run with Exchange databases. By default, Data Protector Express runs the job as an incremental job and so only the transaction logs are backed up.

If you want jobs with a **Differential** backup mode to back up both the database files *and* the transaction logs, change this setting to **Full**. In this case, Data Protector Express will treat the Exchange Server databases as if it were running a job in **Full** backup mode.

Incremental: When the **Backup mode** of a job is set to **Incremental**, Data Protector Express checks this setting to see how the job should be run with Exchange databases. By default, Data Protector Express runs the job as an incremental job and so only the transaction logs are backed up.

If you want jobs with an **Incremental** backup mode to back up both the database files *and* the transaction logs, change this setting to **Full**. In this case, Data Protector Express will treat the Exchange Server databases as if it were running a job in **Full** backup mode.

About Working with Microsoft Exchange Server

When you use Data Protector Express to back up and restore Microsoft Exchange Server databases, you must pay special attention to the role Windows NT security serves in Microsoft Exchange and the backup mode of the Data Protector Express backup jobs.

Microsoft Exchange and Windows NT

Microsoft Exchange uses Windows NT security information for authentication and thus when planning a comprehensive backup program, you must consider the Windows NT operating system as well. Be certain to include backup and restoration of the Windows NT operating system as part of your Microsoft Exchange disaster recovery plan.

Backup modes

You can use the **Options** tab of a job to set the **Backup mode** for any type of backup jobs: *full*, *incremental*, *differential* or *copy*. For scheduled automatic rotation jobs, Data Protector Express automatically updates this job setting to the value indicated on the **Schedule** tab of the job. For further information, see *Backup Job Options*.

When the **Backup mode** is set to **Full**, all files selected are backed up, including the entire information store and directory databases. Transaction logs are also backed up and then purged.

When the **Backup mode** is set to **Incremental**, only changes that have occurred since the last backup job are backed up. In particular, for databases, only the .log files are included in the backup job. *These .log files are then purged.*

When the **Backup mode** is set to **Differential**, for databases, only the .log files are included in the backup job, *but these files are not purged.*

When the **Backup mode** is set to **Copy**, Data Protector Express runs the job in **Full** backup mode. Note that this will cause the transaction logs to be reset (truncated). For this reason, running a job in **Copy** mode can compromise your comprehensive backup strategy if you are not careful to archive the media created by these jobs.

Backup modes and circular logging

Microsoft Exchange Server supports database circular logging. Circular transaction logs differ from normal logs in that only a few log files are maintained. These files are purged automatically as new log files are created. When the transactions in the circular log files are recorded in the database, the log files are then deleted. New transactions are recorded in newly created log files.

If circular logging is enabled, *you cannot do incremental or differential backups.* These backup modes rely upon past transaction logs and thus are not available when circular logging in enabled. When circular logging in enabled, Data Protector Express will revert to *full* backup mode.

You can check to see if circular logging in enabled for a particular server by examining the **Advanced** tab of that server's **Properties** window. If you turn circular logging off, Microsoft Exchange Server will stop the database service and restart it after making the changes.

Restoring Microsoft Exchange Databases

NOTE: To restore a Microsoft Exchange server, see the section, *Disaster Recovery with Microsoft Exchange Server*.

To restore the Microsoft Exchange Server databases, you must restore the database files and all of the log files created since the last full backup job. To do so, you either (1) restore the databases from the last full backup *if the last backup (the previous day's) was a full backup;* (2) restore the databases from the most recent full backup and the last differential backup *if the last backup was a differential backup;* or (3) restore the databases from the last full backup and all of the *incremental* backups made between that day and the present day.

Note that when you restore the databases, you must create and run a separate job for each set of transaction logs you need to restore. You cannot skip any logs and the logs must be restored in sequential order. Thus, when recreating the databases, you must first restore the actual databases (created by a backup job running in *full* backup mode). Next, you must restore the transaction logs in the order created *and* in separate jobs. No log can be skipped when restoring.

For example, if you did a *full* backup on Monday and *incremental* backups each day Tuesday through Friday, in order to restore the databases to their state at the close of business Friday, you must run five separate jobs: one restoring the actual databases from Monday's full backup job and then four additional *separate* jobs restoring each transaction log in sequential order, beginning Tuesday and continuing with each log sequentially until Friday.

To restore the Microsoft Exchange Server Databases

1. Find the date of the last full backup of the databases.
2. Create a restore job.
3. On the **Selection** property page, locate and select the Microsoft Exchange Server storage group.
4. In the **Versions of...** window, click the **Details** button.

5. Sequentially move through the versions in the **Available versions** list by date until you find the most recent full backup of the storage group. This version will be selected for restoring when it is selected in the **Available versions** list.
6. Click **OK** to restore that version.
7. If the most recent backup was a full backup, skip the rest of these steps and restart the Microsoft Exchange Server storage group. As the service is restarted, it automatically restores all of the transactions from the transaction logs.
8. If the most recent backup job was a differential job *and you have performed no incremental jobs between the date of the last full backup and the most recent backup,* then create and run a new restore job, selecting the latest version of the storage group. Then restart the Microsoft Exchange Server storage group. As the service is restarted, it automatically restores all of the transaction from the transaction logs.

NOTE: If you have performed any incremental jobs since the date of the last full backup, continue with the next step.

9. If you have run an incremental backup job after the most recent full backup job, you must create and run a separate restore job for each backup performed after the most recent full backup. Sequentially select versions of the storage group from the **Available versions** field in the **Versions of...** window of the storage group. Run and complete each restore job before creating and running a new restore job.
10. Continue to create and run restore jobs until you have restored the latest version of the storage group. Then restart the Microsoft Exchange Server storage group. As the service is restarted, it automatically restores all of the transaction from the transaction logs.

Disaster Recovery with Microsoft Exchange Server

The Data Protector Express Agent for Microsoft Exchange lets you work with databases instead of individual information stores. Each storage group is identified as a single object, which you can back up and restore.

To recover from a disaster

When you recover from a disaster, you need to perform these tasks:

- System-level Disaster Recovery
- Preparing to Restore the Microsoft Exchange Server
- Restoring the Microsoft Exchange MTA Database
- Restoring Microsoft Exchange Databases

System-level Disaster Recovery

1. Perform a general system-level disaster recovery to restore the basic system data (see *Appendix I — Disaster Recovery*).
2. A Microsoft Exchange Server requires the Windows Active Directory to be restored. Microsoft recommends restoring the entire Windows Active Directory system state. Follow the steps below to restore the Windows Active Directory.

   a. When Windows restarts the first time after the recovery, the Starting Windows screen appears during startup. Press F8.

   b. Select Directory Services Restore Mode and press Enter.

c. Log in to the system.

d. Start Data Protector Express.

e. Create a restore job.

f. Select Active Directory Database for the restore job from the list on the Selection page.

g. Run the restore job.

h. Exit Data Protector Express.

Preparing to Restore the Microsoft Exchange Server

1. Restart the computer, letting Windows load normally.
2. Verify that the various Microsoft Exchange services are loaded and running.
3. From the Windows Start menu, select Microsoft Exchange, System Manager.
4. For each storage group to be restored, dismount and change the properties for each store with a storage group:

   a. Right-click the store within the storage group. A pop-up menu appears.

   b. Select **Properties**. The Properties screen appears.

   c. Select the **Database** tab.

   d. Select **This database can be overwritten by a restore**.

   e. Click **OK**.

   f. Right-click the store again. A pop-up menu appears.

   g. Select **Dismount Store**, if the option is available.

   h. Click **Yes** to confirm. The store is dismounted, which means it can be restored.

   i. Exit the System Manager.

5. Access the Exchange Server subdirectory on the computer, for example, `c:\Program Files\Exchsrvr\mdbdata`.
6. Delete all storage group and log files associated with each storage group to be restored.

WARNING: Do **NOT** delete the actual subdirectories.

7. If you do not have a default installation, use the Exchange system manager to locate the following files and then delete them:

   a. Log file (.LOG) for each storage group.

   b. Exchange database (.EDB) for each store in the storage group.

   c. Exchange streaming database (.STM) for each store in the storage group.

Restoring the Microsoft Exchange MTA Database

1. Restore the Microsoft Exchange MTA (Message Transfer Agent) database:

   a. Access Data Protector Express.

   b. Create a restore job.

c. Click the Microsoft Exchange Server in the **Folders** panel to display the MTA database, **Queued Messages (MTA)**, in the list in the **Name** column to the right of the Folders panel.

d. Select **Queued Messages (MTA)** from the list in the **Name** column to the right of the Folders panel.

e. Run the restore job.

f. Exit Data Protector Express.

2. Start the MTA service:

   a. Right-click **My Computer** on the desktop. A pop-up menu appears.

   b. Select **Manage**. The Computer Management screen appears.

   c. Expand the Services and Applications folder.

   d. Scroll down and right-click on **Microsoft Exchange MTA Stacks**. A pop-up menu appears.

   e. Select **Start**.

   f. Close the Computer Management screen.

Restoring Microsoft Exchange Databases

1. Restore the appropriate Exchange databases:

   a. Access Data Protector Express.

   b. Create a restore job.

   c. Click the Microsoft Exchange Server in the Folders panel to display the storage groups in the list in the Name column to the right of the Folders panel.

   d. Select the storage groups you want to include in the restore job from the list in the Name column to the right of the Folders panel.

   e. Run the restore job.

   f. Exit Data Protector Express.

2. Mount the Exchange databases for each storage group that you restored:

   a. From the Start menu, select Microsoft Exchange, System Manager.

   b. Right-click the database within the storage group. A pop-up menu appears.

   c. Select **Mount**. The system mounts the database.

   d. Click **OK**.

   e. Exit the System Manager.

Appendix G - Working with Microsoft SQL Server

This appendix contains important information pertaining to backing up and restoring Microsoft SQL Server database instances. If you are using Data Protector Express to back up and restore SQL Server database instances, be sure read these instructions carefully.

In this section

- Installing the Data Protector Express Agent for Microsoft SQL Server
- Configuring the Microsoft SQL Server
- Notes for Backup Jobs with Microsoft SQL Server
- Notes for Restore Jobs with Microsoft SQL Server

Overview

Microsoft SQL Server environments are frequently mission-critical and must be maintained 24 hours a day, seven days a week. Procedures and plans must be in place to ensure the quick recovery of data in the event of data loss.

Using the transaction logs associated with each database, you can quickly recover your databases. Transactions that were not committed can be rolled back, while transactions that were committed can be written to disk.

While transaction logs assure that only committed transactions are written and restored, in order to use them correctly, you must have a comprehensive backup plan that regularly backs up these logs. Additionally, when you reconstruct a database, you must restore the database files and logs using only the procedures set out below.

Supported platforms

The Data Protector Express Agent for Microsoft SQL Server supports Microsoft SQL Server 7 and Microsoft SQL Server 2000.

Installing the Data Protector Express Agent for Microsoft SQL Server

When you install Data Protector Express on a machine that is running Microsoft SQL Server, an evaluation version of the agent for Microsoft SQL Server is also automatically installed. You can use the optional agent for a 60-day evaluation period. To continue using the agent beyond the evaluation period, you must purchase a license and activate it from the Data Protector Express License Manager.

Activating the license

1. Select Licenses from the Help menu.
2. In the object detail area of the screen, right-click and select New from the shortcut menu.
3. Enter the license key.

The license will take effect immediately.

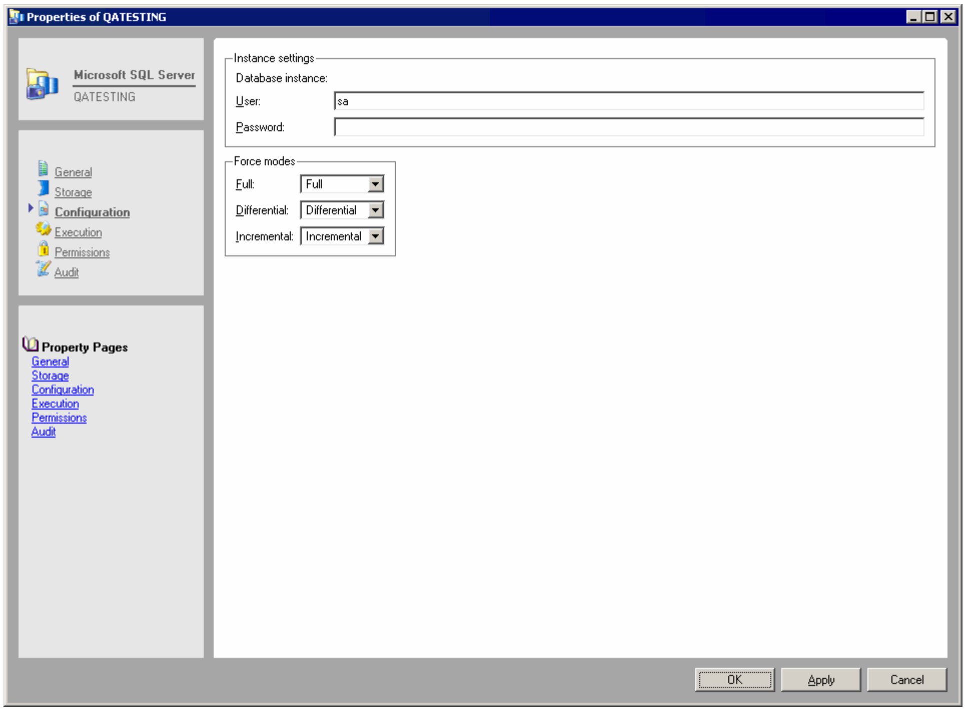
Configuring the Microsoft SQL Server

You can configure any Data Protector Express feature by selecting the object from the **Catalog** view and updating information on its property pages.

1. Select the Administration desk bar and open the Catalog view.
2. Select **Network**, then select the Microsoft SQL Server on your system.
3. Expand the object until you see a list of database instances.

TIP: Switch to the **Folders** view to display a hierarchical tree of the Data Protector Express management domain.

4. Right-click the database instance and display its property pages.
5. Select the **Configuration** command to display the **Configuration** page.



Instance settings

Database instance:

User: sa

Password:

Force modes

Full: Full

Differential: Differential

Incremental: Incremental

Use the **Microsoft SQL Configuration** property page to set certain settings that control how Data Protector Express works with SQL Server.

NOTE: We recommend that you use the default values on the **Configuration** page.

User name: Data Protector Express sends this name to Microsoft SQL Server whenever the SQL administrator user name is required. Type the Microsoft SQL administrator name in this field. The default is **sa**.

Password: Data Protector Express sends this SQL administrator password to Microsoft SQL Server with the SQL administrator's user name whenever required. There is no default value.

Force Modes: As explained in the next section, the Backup mode setting of a backup job affects Microsoft SQL Server database instances differently than file types. The Force modes settings control how Data Protector Express backs up the database instances.

Note that the settings here are only applicable to Microsoft SQL Server database instances; all other file types are backed up in the job's default mode. For example, if the **Backup mode** of a job is set to **Incremental** and the **Force modes** setting for incremental jobs is set to **Full**, Data Protector Express will back up the SQL Server database instance in **Full** mode, but all other file types in **Incremental** mode.

TIP: You can use this feature to ensure that the databases in the instance are always backed up in full mode, but that other files are only backed up when changed. This guarantees the greatest security for the most crucial files (that is, the SQL Server database instances), while not making jobs unnecessarily large by *not* backing up the entire network (that is, by backing up only the changed files).

Full: When the **Backup mode** of a job is set to **Full**, Data Protector Express checks this setting to see how the job should be run with SQL database instances. **Full** is the only possible setting, so the database instances will be backed up in this mode. In this case, both the databases and the transaction logs are backed up.

Differential: When the **Backup mode** of a job is set to **Differential**, Data Protector Express checks this setting to see how the job should be run with SQL database instances. By default, Data Protector Express runs the jobs as an incremental job and so only the transaction logs are backed up. *There is no distinct **Differential** job mode for SQL Server* database instances.

If you want jobs with a **Differential** backup mode to back up both the database and the transaction logs, change this setting to **Full**. In this case, Data Protector Express will treat the SQL Server database instances as if it were running a job in **Full** backup mode.

Incremental: When the **Backup mode** of a job is set to **Incremental**, Data Protector Express checks this setting to see how the job should be run with SQL databases. By default, Data Protector Express runs the jobs as an incremental job and so only the transaction logs are backed up.

If you want jobs with an **Incremental** backup mode to back up both the database and the transaction logs, change this setting to **Full**. In this case, Data Protector Express will treat the SQL Server database files as if it were running a job in **Full** backup mode.

Notes for Backup Jobs with Microsoft SQL Server

Two additional concerns are present when you back up SQL Server database instances: setting the **Backup mode** of a job to either **Full**, **Incremental,** or **Differential**; and configuring Data Protector Express to work with SQL Server's default backup routine.

NOTE: Anytime Data Protector Express returns an error message that is greater than 10000, a Microsoft SQL or Exchange error has occurred. Refer to your Microsoft documentation for more information as this is a Microsoft error code.

Microsoft SQL Server Databases and the backup mode

The **Backup mode** on the **Options** tab of a job that backs up SQL Server database instances is especially critical.

Backup modes

When the **Full** setting is selected, all files selected for backup are backed up, including SQL Server database instances and databases. However, when either the **Incremental** or **Differential** option is selected, Data Protector Express backs up only the transaction logs for each database. *There is no difference between* ***Incremental*** *and* ***Differential*** *jobs for SQL Server databases.*

When the **Backup mode** is set to **Copy**, Data Protector Express runs the job in **Full** backup mode. Note that this will cause the transaction logs to be reset (truncated). For this reason, running a job in **Copy** mode can compromise your comprehensive backup strategy if you are not careful to archive the media created by these jobs.

Additional Conditions

Master, Model, MSDB and Pubs databases support only full backups. The **Backup mode** option is automatically set to **Full** when backing up these databases.

If you set a job to run in either **Incremental** or **Differential** mode and the job can only run as a full backup (as a result of the provision above), the job will fail to run on each of its initial passes, but will run in **Full** backup mode on its final pass.

Using Data Protector Express with SQL Server's Backup Routine

Microsoft SQL Server has default utilities and commands for backing up data. When you use Data Protector Express to back up SQL Server databases, you can still use these default SQL Server utilities and commands.

For example, you can use the DUMP command to dump transaction logs to the dump device (preferably, a separate disk drive). You can set this up to occur at regular intervals, such as every 15 minutes or every hour. Next, you can create a backup job that backs up these transaction logs onto archival media every day.

In general, when you implement Data Protector Express to back up your SQL Server databases, continue to use SQL Server's internal commands to duplicate and back up transaction logs. Set up a separate Data Protector Express backup job to write these duplicated transaction logs to archival media.

Notes for Restore Jobs with Microsoft SQL Server

When restoring SQL Server databases, you must:

1. Restore a full backup of the SQL Server database.
2. Restore the logs in the order created.
3. Follow special procedures when renaming databases (if you rename databases).

NOTE: Any time Data Protector Express returns an error message that is greater than 10000, a Microsoft SQL or Exchange error has occurred. Refer to your Microsoft documentation for more information as this is a Microsoft error code.

Restoring Microsoft SQL Server databases and transaction logs

When recreating a database, you must first restore the whole database (created by a backup job running in *full* backup mode).

Next, you must restore the transaction logs in the order created *and* in separate jobs. No log can be skipped when restoring.

For example, if you did a *full* backup on Monday and *incremental* backups each day Tuesday through Friday, you must run five separate jobs: one restoring the database from Monday's full backup job and then four additional *separate* jobs restoring each transaction log in sequential order, beginning Tuesday and continuing with each log sequentially until Friday.

You do not have to follow these procedures when restoring databases backed up with *full* backup jobs. (**Full** backup jobs back up the entire database, while **Incremental** and **Differential** jobs only back up the database logs.)

Restoring Microsoft SQL Server databases with a new name

You can rename a database while restoring using the normal procedures for renaming files outlined in Restoring a file with a new name on page 78. This method involves changing the name on the **Selection** tab of the restore job. However, you cannot rename the master database. When you restore a master database, you must follow the procedures specified in the section below, *Restoring Microsoft SQL Server master databases*.

Restoring Microsoft SQL Server 2000 and SQL Server 7 user databases

To restore a database, begin by restoring the most recent **full** backup of the database, followed by *all* the database logs, that is, backups made with the **Backup mode** set to either **incremental** or **differential**.

When a database is restored, if the database does not yet exist, Data Protector Express will create the database where the database was originally located.

To restore a lost or damaged database

1. If the transaction log of the damaged or inaccessible user database is on an undamaged device, make a backup of the transactions before proceeding. (This lets you preserve up to the minute transactions that are not included on the backup tape.)

   You may use either a DUMP TRANSACTION statement on the SQL server or use a Data Protector Express **Incremental** backup job to back up only the transactions logs.

2. If you are restoring the database because the data in the database is no longer needed or is incorrect, skip to step 3. The following instructions are for recreating database devices and the database which had existed previously.

   During the restore processes, Data Protector Express will recreate the database and all segments exactly as they existed when the backup was performed.

   To do this, Data Protector Express first determines if the database exists. If the database does exist, Data Protector Express will use the database as is *without any further processing or changes*.

If the database does not exist, Data Protector Express next identifies the database devices on which the database was originally located. If the appropriate database *device* already exists, Data Protector Express will use that device as is without further processing.

If the database *device* does not exist, Data Protector Express *recreates* the database device at its *original* location and with its original size. After all the database devices are created, Data Protector Express then creates the database with all the original options at the original locations.

TIP: This method makes disaster recovery simple. The user simply create a restore job and allows Data Protector Express to recreate whatever is needed in order to successfully restore the database.

Note, however, if a disk drive fails and is not replaced, Data Protector Express will be unable to restore your database because it will be unable to recreate a database device. For example, if a segment of your database resides on a database named 'DATA' at D:\MSSQL\DATA\DATA.DAT, if D: is lost and not replaced, when Data Protector Express attempts to recreate the database device, it will fail, since D: no longer exists.

To avoid this problem, manually recreate the database device at some other location. It must be at least as large as the original database device since Data Protector Express will attempt to create a database segment on it the same size as the original database.

An alternative method is to manually create the entire database itself. Thus, when Data Protector Express attempts to restore the database, since the database already exists, it will use that preexisting database. This allows you to restore a database in a new location, since Data Protector Express does not check to see if it is the original device before restoring the database, because the database already exists.

NOTE: Data Protector Express tracks databases *by name*. So, if a database already exists with the same name, Data Protector Express will use that database.

3. Using Data Protector Express, create a restore job and run the job to restore the database. You must start with a full backup version of the database to restore which was created using a Full backup job.
4. Create additional restore jobs to restore each transaction log backed up after the full database you restored. You must create and run a separate restore job for each transaction log.

   For example, if you ran a full backup on Friday and incremental jobs (that is, jobs that backed up only the transaction logs) on the following Monday and Tuesday, you must first restore the database using Friday's version of the database. Next, create a run and restore job that restores Monday's version (Monday's transaction log). Finally, create and run a job that restores Tuesday's version (Tuesday's transaction log).

   In the *last* incremental restore job, click the **Advanced Options** button and select the **Recover databases** checkbox. If you do not select this checkbox, the database will be offline.

Restoring Microsoft SQL Server 2000 master databases

A damaged master database is evident by the failure of the SQL Server to start, by segmentation faults or input/output errors or by a report from DBCC. An example of an error might be damage caused by media failure in the area in which master database is stored.

The procedure used to recover a damaged master database is different from the procedure used to recover user databases. If the master database becomes unusable, it must be restored from a previous dump. All changes made to the master database after the last dump are lost when the dump is reloaded and therefore must be reapplied.

It is strongly recommended that the master database be backed up each time it is changed. This is best accomplished by prohibiting the creation of user-defined objects in the master database and by being aware of the statements and system procedures, and the equivalent actions in SQL Enterprise Manager, that modify it.

The most common statements and system procedures that modify master are:

- CREATE DATABASE
- ALTER DATABASE
- sp_dropremotelogin
- sp_addumpdevice
- sp_dropdevice
- sp_addlogin
- sp_droplogin
- sp_addserver
- sp_dropserver
- sp_addremotelogin

If a user database is created, expanded or shrunk after the most recent dump (backup) of the master database and if it becomes necessary to reload the master database, then that user database and all data in will be lost and must be restored from backup. Because of this, *always dump (back up) the master database after creating, expanding or shrinking user databases.*

To recover a damaged master database

1. Stop the Data Protector Express and SQL Server services.
2. Rebuild the master database.
3. Restart SQL Server in single-user mode.
4. Restore the master database from the most recent backup.
5. Apply to the master database any changes that were not included in the most recent backup.
6. Drop invalid databases from the newly restored master database.
7. Start the Data Protector Express and SQL Server services.
8. Restore the msdb database.

Each of these steps is described below in more detail.

Step 1: Stop the Data Protector Express and SQL Server services

1. Exit Data Protector Express.
2. Stop the HP Data Protector Express service by using one of the following methods:
   - Using the Windows Command Line
     a. Open a command prompt.
     b. Switch to the following directory:
        ```
        HP\Data Protector Express
        ```
     c. Type the following command at the command prompt:
        ```
        dpwinsvc –x
        ```

   This command stops the HP Data Protector Express service on the local machine.

- Using the Microsoft Management Console (MMC):
    a. Right-click the **My Computer** icon and select **Manage**.
    b. In the left pane of the window, select **Services and Applications → Services**.
    c. In the right pane of the window, locate the HP Data Protector Express service.
    d. Right-click the service and select **Stop**.

3. Stop the SQL Server service using the SQL Server Enterprise Manager.

Step 2: Rebuild the master database

1. Open a command prompt.
2. Switch to the Program Files\Microsoft SQL Server\80\Tools\Binn directory.
3. Run Rebuildm.exe.
4. In the **Rebuild Master** dialog box, click **Browse**.
5. In the **Browse for Folder** dialog box, select the \Data folder on the SQL Server 2000 compact disc or in the shared network directory from which SQL Server 2000 was installed, and then click **OK**.
6. Click **Settings**. In the **Collation Settings** dialog box, verify or change settings used for the **master** database and all other databases.
   Initially, the default collation settings are shown, but these may not match the collation selected during setup. You can select the same settings used during setup or select new collation settings. When done, click **OK**.
7. In the **Rebuild Master** dialog box, click **Rebuild** to start the process.
   The Rebuild Master utility reinstalls the **master** database.

N**ote** To continue, you may need to stop a server that is running.

Step 3: Restart SQL Server in single-user mode

1. Open a command prompt.
2. Switch to the Program Files\Microsoft SQL Server\mssql\binn directory.
3. Issue the following command:

```
sqlservr -c -m
```

If you are restoring the master database for a named instance, issue the following command instead:

```
sqlservr -c -m -s name
```

where `name` is the name of the named instance.

4. Leave the command prompt open.

Step 4: Restore the master database from the most recent backup

1. Open Data Protector Express (with the service stopped).
2. Create a restore job, selecting only the master database.
3. Run the restore job.

NOTE: This may take some time, typically 10 to 15 minutes, depending on the size of the master database. Restore only the master database while in single user mode. Do not restore any other databases.

If, for some reason, your restore operation doesn't work, rebuild the master database and attach all of your databases that reside in the data directory. To attach databases:

In Enterprise Manager, right-click **Databases** and select **Attach Database**.

In Query Analyzer, write and run a script that is similar to the following sample:

```
EXEC sp_attach_db @dbname = N'test_database',
    @filename1 = N'c:\Program Files\Microsoft SQL Server\MSSQL\Data\
    test_database.mdf',
    @filename2 = N'c:\Program Files\Microsoft SQL Server\MSSQL\Data\
    test_database.ldf'
```

Step 5. Apply changes to the master database

1. Go to the SQL Server Enterprise Manager and right-click the SQL server instance. Select **Properties** to open the SQL Server Properties window.
2. Under the General tab in the SQL Server Properties window, open the Startup Parameters window and remove `-m` from the list of existing parameters.
3. Restart the SQL server instance. (Right-click the SQL server instance and select **Stop**; right-click the SQL server instance and select **Start**.)

If there have been no changes to the master database since the last dump, then proceed to step 6 "Drop invalid databases and database devices."

4. If login IDs or devices have been added to or dropped from the master database since the last backup, those changes must be reapplied. Restart the server and reapply the changes manually or from saved batch files.
5. If databases have been created, expanded or shrunk since the last dump of master, those databases must be dropped and then restored.

Step 6. Drop invalid databases

1. Use the SQL Enterprise manager to drop any invalid database devices and databases from the newly restored master database.

NOTE: If you are recovering from a disaster where you have lost a database device file, the master database you have just restored still contains a reference to it. Data Protector Express will not be able to restore any databases contained on the database device until the file is restored or the database device is dropped. If the database device is dropped, Data Protector Express will automatically recreate the device when a database contained on the device is restored.

Step 7: Start the HP Data Protector Express and SQL Server services

1. Start the HP Data Protector Express service by using one of the following methods:
   - Using the Windows Command Line
     a. Open a command prompt.
     b. Switch to the following directory:

        `HP\Data Protector Express`

c. Type the following command at the command prompt:

```
dpwinsvc -s
```

This command starts the HP Data Protector Express service on the local machine.

- Using the Microsoft Management Console (MMC):
    a. Right-click the **My Computer** icon and select **Manage**.
    b. In the left pane of the window, select **Services and Applications → Services**.
    c. In the right pane of the window, locate the HP Data Protector Express service.
    d. Right-click the service and select **Start**.

3. Restart the SQL Server service using the SQL Server Enterprise Manager.

Step 8. Restore the msdb database

Refer to *Restoring SQL Server User Databases* earlier in this appendix for specific information on restoring SQL Server databases.

When restoring the msdb database, keep the following considerations in mind:

- The msdb database supports SQL Executive and provides a storage area for scheduling information. The schedules that you implement using SQL Enterprise Manager are maintained in the msdb database. This includes such things as the tasks that you schedule from the Task Scheduling window, the automatic backups you schedule from the Database Backup/Restore window and all replication tasks, which are automatically created by the system if the server is configured as a replication distributor.
- During installation of a server, the setup program automatically creates two devices (of 2MB and 1MB) on the same disk drive as the master database and then places the msdb database on the 2MB device (MSDBDATA) and its transaction log on the 1MB device (MSDBLOG). Scheduling information is then stored in this database.
- During a rebuild of the master database, the setup program drops and re-creates the msdb database, which results in a loss of all scheduling information.

Restoring Microsoft SQL Server 7 master databases

A damaged master database is evident by the failure of the SQL Server to start, by segmentation faults or input/output errors or by a report from DBCC. An example of an error might be damage caused by media failure in the area in which master database is stored.

The procedure used to recover a damaged master database is different from the procedure used to recover user databases. If the master database becomes unusable, it must be restored from a previous dump. All changes made to the master database after the last dump are lost when the dump is reloaded and therefore must be reapplied.

It is strongly recommended that the master database be backed up each time it is changed. This is best accomplished by prohibiting the creation of user-defined objects in the master database and by being aware of the statements and system procedures, and the equivalent actions in SQL Enterprise Manager, that modify it.

The most common statements and system procedures that modify master are:

- DISK INIT
- CREATE DATABASE

- ALTER DATABASE
- DISK MIRROR
- DISK UNMIRROR
- DISK REMIRROR
- sp_dropremotelogin
- sp_addumpdevice
- sp_dropdevice
- sp_addlogin
- sp_droplogin
- sp_addserver
- sp_dropserver
- sp_addremotelogin

If a user database is created, expanded or shrunk after the most recent dump (backup) of the master database and if it becomes necessary to reload the master database, then that user database and all data in will be lost and must be restored from backup. Because of this, *always dump (back up) the master database after creating, expanding or shrinking user databases.*

To recover a damaged master database

1. Use the SQL Setup program to rebuild the master database.

   You must rebuild using the same character set and sort order as the master database dump that will be reloaded.

2. Restart SQL Server in single-user mode.
3. Restore the master database from the most recent backup.
4. Apply to the master database any changes that were not included in the most recent backup.
5. Drop any databases from the newly restored master database.
6. Restore the msdb database.

Each of these six steps is described below in more detail:

Step 1. Rebuild the master database

1. From Windows Explorer select Start, Programs, Microsoft SQL Server, then select the SQL Setup icon.

   (Alternatively, from the distribution media, from the directory containing the software compatible with your hardware platform's processor architecture, run SETUP.EXE.)

2. Respond to the on-screen instructions until the Options window appears.
3. Select Rebuild Master Database and click Continue. A confirmation window appears.
4. Click Resume. The Rebuild Options window appears.
5. To specify the character set, click Sets and complete the Select Character Set window that appears. Skip this step if you are using the default character set (ISO 8859-1).

   NOTE: You must use the same character set and sort order that were previously used for this master database.

6. To specify the sort order, click Orders and complete the Select Sort Order window that appears. Skip this step if you are using the default sort order (dictionary order, case-insensitive).

7. In the Rebuild Options window, click Continue. The SQL Server Installation Path window appears.
8. If not correctly displayed in the SQL Server Installation Path window, enter the location of the existing SQL Server installation and click Continue.

   The Rebuild Master Database window appears.
9. If it is not correctly displayed in the Rebuild Master Database window, enter the location and name of the existing MASTER device. Also enter a MASTER device size and click Continue.

   The setup program will then rebuild the master database.
10. When rebuilding is complete and the completion window appears, click Exit.

NOTE: The files MASTER.DA@ and MASTER.AL@ are stored in the \MSSQL\INSTALL directory. When rebuilding the master database (or when installing SQL Server), one of these two files is used by the setup program. When the default sort order and character set are selected, MASTER.DA@ is expanded and copied onto the server, replacing MASTER.DAT. When an alternate character set and/or sort order is selected, MASTER.AL@ is expanded, copied onto the server, and several SQL scripts are run.

Step 2. Restart Microsoft SQL Server in single-user mode

Before you can restore the master database, you must start Microsoft SQL Server in single-user mode.

1. Go to the SQL Server Enterprise Manger and right-click the SQL server instance. Select Properties to open the SQL Server Properties window.
2. Under the General tab in the SQL Server Properties window, open the Startup Parameters window and type –m in the Parameter field.
3. Click the Add command, and then click OK. Close the SQL Server Properties window by clicking OK.
4. Restart the SQL server instance. (Right-click the SQL server instance and select Stop; right-click the SQL server instance and select Start.)

NOTE: You may find it convenient to start the SQL Server in single-user mode using the command line program, *SQLSERVER.EXE*, with option */m*. This procedure will only work, however, if the SQL Server is configured to start using the current interactive user's account.

Step 3. Restore the master database from the most recent backup

1. Create a restore job and select the most recent backup version of the master database.
2. Run the restore job.

NOTE: This may take some time, typically 10 to 15 minutes, depending on the size of the master database. Restore only the master database while in single user mode. Do not restore any other databases.

Step 4. Apply changes to the master database

1. Go to the SQL Server Enterprise Manger and right-click the SQL server instance. Select Properties to open the SQL Server Properties window.
2. Under the General tab in the SQL Server Properties window, open the Startup Parameters window and remove –m from the list of existing parameters.
3. Restart the SQL server instance. (Right-click the SQL server instance and select Stop; right-click the SQL server instance and select Start.)

If there have been no changes to the master database since the last dump, then proceed to step 5 "Drop invalid databases and database devices."

4. If login IDs or devices have been added to or dropped from the master database since the last backup, those changes must be reapplied. Restart the server and reapply the changes manually or from saved batch files.
5. If databases have been created, expanded or shrunk since the last dump of master, those databases must be dropped and then restored.
6. If you have made many changes and have no recent dump, it is possible that by reloading master in some cases you can regain data in user databases that has been lost. This technique requires the use of DISK REINIT and DISK REFIT and can involve manual modifications to the master database tables.
   - Use DISK REINIT to re-create rows in sysdevices for all database devices that have been added after the most recent dump. DISK REINIT updates sysdevices just as DISK INIT does, but it does not format the physical disk file, so existing data is preserved.
   - Use DISK REFIT to re-create rows in sysusages and sysdatabases for all CREATE and ALTER DATABASE statements that were performed after the most recent dump.

     DISK REFIT scans the physical file associated with each space that is allocated to databases. It also adds the corresponding sysdatabases entries. Some of the information is not reconstructed perfectly. For example, the original virtual device number is not assigned, because it is not known. Instead, virtual device numbers are assigned sequentially. The database owner is not extracted while scanning the physical files; ownership is set to the system administrator. It is also not possible to determine how many sysusages entries originally existed. DISK REFIT inserts a separate entry for each different segment type.
   - When this is done, correct the entries made by DISK REFIT to sysdatabases and sysusages (if desired) and also add to syslogins any login IDs that were not retained. Then shut down and restart SQL Server.

WARNING: Capturing the latest changes made to a database by using DISK REFIT and DISK REINIT to re-create the master database is possible, but it is preferable to keep the master database current by dumping it after creating or altering databases. Using DISK REFIT and DISK REINIT is a complicated process that can result in data loss because many of the changes made to a database often must be reconstructed manually in the master database. If you feel this technique is necessary, contact your primary support provider before beginning the recovery process.

Step 5. Drop invalid databases and database devices

1. Use the SQL Enterprise manager to drop any invalid database devices and databases from the newly restored master database.

NOTE: If you are recovering from a disaster where you have lost a database device file, the master database you have just restored still contains a reference to it. Data Protector Express will not be able to restore any databases contained on the database device until the file is restored or the database device is dropped. If the database device is dropped, Data Protector Express will automatically recreate the device when a database contained on the device is restored.

Step 6. Restore the msdb database

Refer to *Restoring SQL Server User Databases* earlier in this appendix for specific information on restoring SQL Server databases.

When restoring the msdb database, keep the following considerations in mind:

- The msdb database supports SQL Executive and provides a storage area for scheduling information. The schedules that you implement using SQL Enterprise Manager are maintained in the msdb database. This includes such things as the tasks that you schedule from the Task Scheduling window, the automatic backups you schedule from the Database Backup/Restore window and all replication tasks, which are automatically created by the system if the server is configured as a replication distributor.
- During installation of a server, the setup program automatically creates two devices (of 2MB and 1MB) on the same disk drive as the master database and then places the msdb database on the 2MB device (MSDBDATA) and its transaction log on the 1MB device (MSDBLOG). Scheduling information is then stored in this database.
- During a rebuild of the master database, the setup program drops and re-creates the msdb database, which results in a loss of all scheduling information.

Appendix H - Working with Microsoft Data Protection Manager (DPM)

This appendix contains important information pertaining to backing up and restoring Microsoft DPM Servers.

In this section

- Overview
- Installing the Data Protector Express Agent for Microsoft DPM
- Activating the license
- Backing up the DPM Application
- Protecting Production Servers
- Restoring DPM files
- Using Disaster Recovery with the DPM server

Overview

The Microsoft DPM product protects multiple computers, called **production servers**, simultaneously by replicating selected volumes and file system shares to its **replica disks**. It creates and maintains copies, called **snapshots**, of the replicas so a user can quickly restore protected files to a point in time.

Data Protector Express can back up the production servers' data captured in the DPM server's replicas. By backing up these replicas, HP extends the DPM server's data protection capabilities to a much longer data protection period.

Replica data that has been backed up with Data Protector Express can be restored either to the DPM server or directly to the original production server that it came from.

Installing the Data Protector Express Agent for Microsoft DPM

When you install Data Protector Express on a machine that is running Microsoft DPM, an evaluation version of the Data Protector Express DPM Agent is also automatically installed. You can use the optional agent for a 60-day evaluation period. To continue using the agent beyond the evaluation period, you must purchase a license and activate it from the Data Protector Express License Manager.

Activating the license

1. Select Licenses from the Help menu.
2. In the object detail area of the screen, right-click and select New from the shortcut menu.
3. Enter the license key.

The license will take effect immediately.

Backing up the DPM Application

Backing up the DPM application consists of backing up the DPM database and the replicas on the disks it is managing.

The DPM database is a Microsoft SQL database instance managed by a special Microsoft SQL Server installation. The Data Protector Express SQL agent separates the DPM database from any other database instances on the server to ensure that it is backed up only once and to indicate that it is part of the DPM application. Other instances will only exist if there is an additionl Microsoft SQL installation on the server.

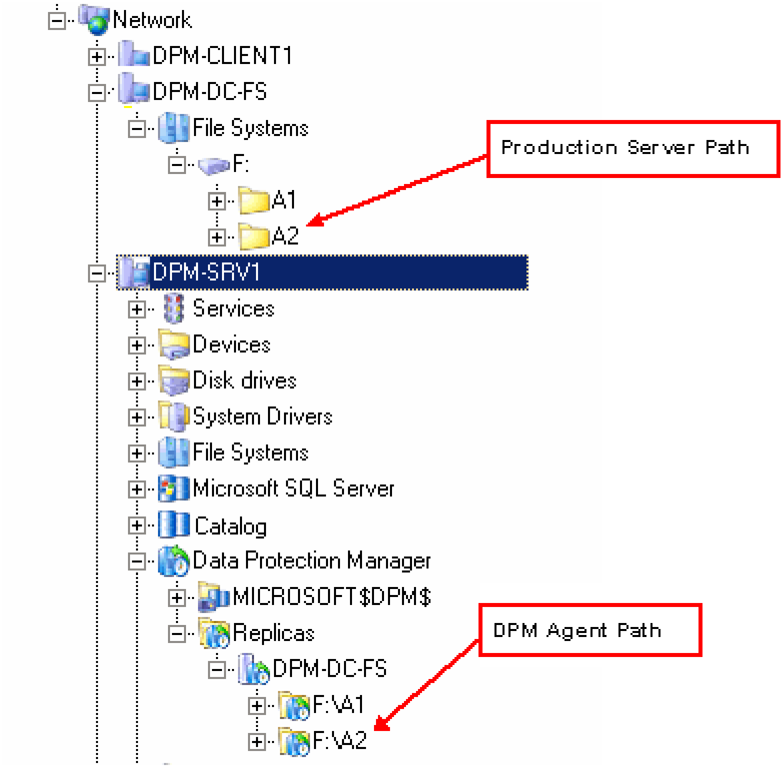
Likewise, the replica content is separated from other files protected by the Data Protector Express File System agent. Data Protector Express provides the interface the user needs to backup and restore replica data. While the replicas are stored in the file system, the File System agent will not show them. Rather, the Data Protector Express DPM agent will show these files. This ensures that the replicas don't get backed up twice.

Replica content is found under **the DPM agent path** in Data Protector Express**:**

```
\Network\<Server-Name>\Data Protection Manager\Replicas
```

When replica content files are selected for backup, the backup will also create an entry in the Data Protector Express catalog at the **production server path** that indicates where that the files originally came from so that they can be restored directly to the production server. The backup will create an instance for each path when the file is backed up even though the file is stored only once on tape.

The picture below shows both DPM agent paths and production server paths.



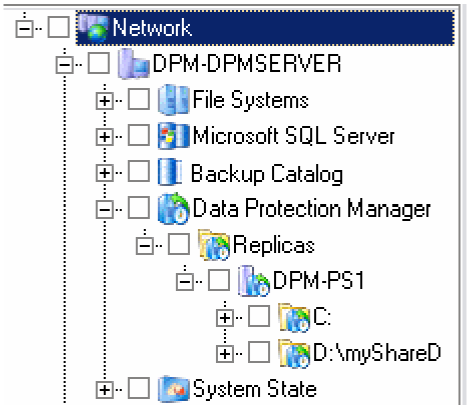
If the production server does not have a client-licensed version of Data Protector Express on it, its icon will appear in the catalog as offline. (The icon will have on it an exclamation point in a yellow circle.)

The Data Protector Express DPM agent uses VSS to ensure the integrity of the replica data at backup time. Data Protector Express logs the success or failure of the snapshots associated with DPM. If a DPM snapshot fails, then Data Protector Express skips all DPM replica data associated with that volume, and logs the failed replica with the associated snapshot error. This differs from other volumes protected by VSS which will read data directly if the snapshot fails. Microsoft requires that DPM replicas use VSS or risk damaging the replicas.

You must have the Windows backup operator privilege to execute a backup or standalone verify on DPM replica data.

To select DPM files

Select the *Data Protection Manager* icon in the selection tree and expand the tree.



Backing up the entire DPM server

If you want to back up the entire DPM server, check the icon for the server. This selection will backup all replicas and the DPM database as well as the file systems, the system state and the backup catalog, if the backup server is installed on that server.

Backing up all the replicas

If you want to back up the replicas of all the files in all the production servers that are protected by the DPM server, check the *Replicas* icon.

Backing up individual production servers

If you want to back up all the files in one or more production servers that are protected by the DPM server, check one or more of the appropriate *Protected Server* icons.

Backing up individual shares

If you want to back up all the files in one or more shares in a production server that is protected by the DPM server, check one or more of the appropriate *Share* icons.

Backing up individual files

Finally, you can back up individual files by checking one or more of the appropriate *File* icons to back up the files you select.

Protecting Production Servers

The Data Protector Express DPM agent does not provide complete data protection for production servers; it only protects data that is being protected by the DPM server. It cannot fully protect system state data on the production server.

For disaster recovery protection, you need to install a client-licensed version of Data Protector Express on the production server and prepare it for disaster recovery as described in the DR section. You can exclude from this job all data protected by the Microsoft DPM server. This job should be scheduled regularly to account for changes to the system.

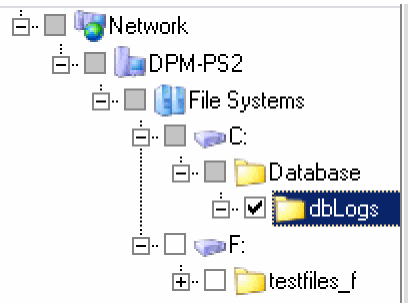
DPM-specific backup jobs read the replicated data from the DPM server. Thus after the initial production server backup, most future backups can consist of backing up the single centralized DPM server machine.

Restoring DPM files

You can restore data to the production server or the DPM server. If you lose the data on your DPM data disk, you can restore to the replica content area on the DPM server to reduce network traffic when synchronizing the DPM server or if you don't have a license for the production server. However, it is recommended that you restore data directly to the production server. Once restored, DPM will synchronize the production data with the replica on the DPM server. Please refer to Microsoft's documentation for how to synchronize data between the DPM server and the production servers.

When an object is backed up, the catalog generates two versions of it in the catalog: one on the production server and one on the DPM server. Either version can be restored.

When you open the Selection wizard page, you will see the Network icon. Double-click the Network icon to see a list of servers that have backed up files. Expand the selection tree on this wizard page to choose the servers, shares, and files you want to restore.



Restore data to the production server by selecting the instance from the production server path (as shown). Select the instance from the DPM agent path to restore the data to the DPM server replica area.

Using Disaster Recovery with the DPM server

Microsoft DPM requires a minimum of two disks for installation: one for the DPM server installation and at least one to hold replication data. When recovering a DPM server in the case of a disaster, we recommend restoring all disks on the machine.

To recover a DPM server:

1. Do a full system disaster recovery restore of all tapes. This will not restore the DPM server database or the DPM managed replicas. Additional steps need to be taken to complete the full restore.
2. Stop the MICROSOFT$DPM$ service using the service control manager.
3. Restore the DPM master database:
    a. Stop the Data Protector Express service.
    b. Open a command prompt and change the directory to `<dpm_install_dir>\Prerequisites\MSSQL$DPM$\Binn.`
    c. Start the DPM SQL server in single server mode by running the following command:

       ```
       sqlservr.exe –c –m –s MICROSOFT$DPM$.
       ```

       Leave the command prompt window open.
    d. Start the Data Protector Express user interface (not the service).
    e. Create and run a job to restore the master database found at the following path:

       ```
        \Network\<dpm_server>\Data Protection
       Manager\MICROSOFT$DPM$\master
       ```
4. Restart the MICROSOFT$DPM$ service using the service control manager.
5. Restore all other databases of the MICROSOFT$DPM$ SQL instance with the SQL agent. The DPM databases can be found under the following path when creating a restore job:

   ```
   \Network\<DPM SERVER MACHINE>\Data Protection Manager\MICROSOFT$DPM$
   ```
6. If new disks were added to the machine, the DPM configuration may need to be updated:
    a. Open the DPM console, remove any disks that no longer exist, and add any newly installed disks.
    b. Run DPMSYNC.EXE, which will re-create DPM partitions and mount points and ensure that the DPM database is consistent with a modified disk configuration,
7. [Optional] Restore DPM Replica content. If you choose not to do this step, the next step will recreate your replicas by synchronizing the data directly from the production servers.

Restoring replica content can reduce traffic on your network during the recovery process. To recover content from tape, create and run a restore job selecting the following path:

```
<dpm installation directory>\DPM\Volumes\Replica
```

8. Complete the recovery of your system by opening the DPM Admin Console, going to the **Protection** tab and selecting the **Synchronize…** menu item to do a full synchronization with a consistency check.
9. Verify that the DPM server is functioning properly.

Index

www.hp.com

invent