IBM Tivoli Continuous Data Protection for Files
Version 6.3

Installation and User's Guide

SC14-7653-00

IBM Tivoli Continuous Data Protection for Files
Version 6.3

Installation and User's Guide

SC14-7653-00

Note

Before using this information and the product it supports, read the information in "Notices" on page 121.

This edition applies to Version 6.3.0 of IBM Tivoli Continuous Data Protection for Files (product numbers 5608-APG, 5724-S64, 5641-FSE) and to all subsequent releases and modification until otherwise indicated in new editions or technical newsletters.

Contents

Preface

This publication helps you install and use Tivoli® Continuous Data Protection for Files.

Who should read this publication

This publication is intended for users of Tivoli Continuous Data Protection for Files clients.

Publications

Publications for Tivoli Continuous Data Protection for Files are available online.

Tivoli Continuous Data Protection for Files publications are available at the information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v12r1/index.jsp.

You can download PDF versions of publications from the information centers or from the IBM® Publications Center at http://www.ibm.com/shop/publications/order/.

Go to Tivoli Documentation Central to find information centers that contain official product documentation for current and previous versions of Tivoli products, including Tivoli Continuous Data Protection for Files. You can find Tivoli Documentation Central at https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home.

You can also order some related publications from the IBM Publications Center website. The website provides information about ordering publications from countries other than the United States. In the United States, you can order publications by calling 1-800-879-2755.

Tivoli Continuous Data Protection for Files publications

The following table lists the publications that make up the Tivoli Continuous Data Protection for Files library.

Table 1. Tivoli Continuous Data Protection for Files publications

Publication title	Order number
IBM Tivoli Continuous Data Protection for Files Installation and User's Guide	SC14-7653-00
IBM Tivoli Continuous Data Protection for Files Messages	SC27-4046-00

Support information

You can find support information for IBM products from various sources.

Start at the IBM Support Portal: http://www.ibm.com/support/entry/portal/. You can select the products that you are interested in and search for a wide variety of relevant information.

Getting technical training

Information about Tivoli technical training courses is available online.

Go to the following websites to sign up for training, ask questions, and to interact with others who use IBM storage products.

Tivoli software training and certification
Choose from instructor led, online classroom training, self-paced Web classes, Tivoli certification preparation, and other training options at http://www.ibm.com/software/tivoli/education/.

Tivoli Support Technical Exchange
Technical experts share their knowledge and answer your questions in webcasts at http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html.

Storage Management community
Interact with others who use IBM storage management products at http://www.ibm.com/developerworks/servicemanagement/sm/index.html.

Global Tivoli User Community
Share information and learn from other Tivoli users throughout the world at http://www.tivoli-ug.org/.

IBM Education Assistant
View short "how to" recordings designed to help you use IBM software products more effectively at http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/index.jsp.

Searching knowledge bases

If you have a problem with Tivoli Continuous Data Protection for Files, you can search for information in a knowledge base.

Search the Tivoli Continuous Data Protection for Files V6.3.0 Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v12r1/index.jsp.

Search the internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem.

To search multiple Internet resources for your product, go to the Tivoli Continuous Data Protection for Files support Web site at http://www.ibm.com/software/sysmgmt/products/support/ITCDP_Support_Options.html and search support for the product. From this section, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks®
- Forums and newsgroups

Using IBM Support Assistant

At no additional cost, you can install on any workstation the IBM Support Assistant, a stand-alone application. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use.

The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem. The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, see the IBM Support Assistant Web site at http://www.ibm.com/software/support/isa/.

You can also install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use. Find add-ons for specific products at http://www.ibm.com/support/docview.wss?uid=swg27012689.

Finding product fixes

A product fix to resolve your problem might be available from the IBM Support Assistant website.

About this task

To check what fixes are available for your product, follow these steps:

Procedure

- From the IBM Support Assistant Web site at http://www.ibm.com/support/entry/portal/, click **Downloads**.
- Click **Search for recommended fixes**.
- Choose content filters to find fixes for your product level and operating system.

Receiving notification of product fixes

You can receive notifications about fixes, flashes, upgrades, and other news about IBM products.

About this task

To sign up to receive notifications about IBM products, follow these steps:

Procedure

1. From the IBM Support Assistant Web site at http://www.ibm.com/support/entry/portal/, click **Sign in to create, manage, or view your subscriptions** in the **Notifications** pane.
2. Sign in using your IBM ID and password. If you do not have an ID and password, click **register now** and complete the registration process.
3. Click **Manage all my subscriptions** in the **Notifications** pane.
4. Click the **Subscribe** tab and then click **Tivoli**.
5. Select the products for which you want to receive notifications and click **Continue**.
6. Specify your notification preferences and click **Submit**.

Contacting IBM Software Support

You can contact IBM Software Support if you have an active IBM subscription and support contract and if you are authorized to submit problems to IBM.

About this task

To obtain help from IBM Software Support, complete the following steps:

Procedure

1. Ensure that you have completed the following prerequisites:
   a. Set up a subscription and support contract.
   b. Determine the business impact of your problem.
   c. Describe your problem and gather background information.
2. Follow the instructions in "Submitting the problem to IBM Software Support" on page ix.

Setting up a software maintenance contract

Set up a software maintenance contract. The type of contract that you need depends on the type of product you have.

Procedure

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere® products that run on Microsoft Windows or UNIX operating systems), enroll in IBM Passport Advantage® in one of the following ways:
  - **Online:** Go to the Passport Advantage Web page at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
  - **By Phone:** For the phone number to call in your country, go to the IBM Software Support Handbook Web page at http://techsupport.services.ibm.com/guides/contacts.html and click **Contacts**.
- For server software products, you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for server software products, go to the IBM Technical support advantage Web page at http://www.ibm.com/servers/eserver/techsupport.html.

What to do next

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. For a list of telephone numbers of people who provide support for your location, go to the Software Support Handbook page at http://www.ibm.com/support/customercare/sas/f/handbook/home.html.

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you must understand and assess the business impact of the problem you are reporting.

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.

Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing the problem and gathering background information

When explaining a problem to IBM, it is helpful to be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? For example, hardware, operating system, networking software, and so on.
- Are you using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submitting the problem to IBM Software Support

You can submit the problem to IBM Software Support online or by telephone.

Online

Go to the IBM Software Support website at http://www.ibm.com/support/entry/portal/Open_service_request/Software/Software_support_(general). Sign in to access IBM Service Requests and enter your information into the problem submission tool.

By telephone

For the telephone number to call in your country, go to the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html and click **Contacts**.

Chapter 1. Product Overview

This chapter provides an introduction to the Tivoli Continuous Data Protection for Files client and briefly describes enhancements for this version of the product.

New in version 6.3.0

Tivoli Continuous Data Protection for Files is updated for version 6.3.0 and includes new enhancements and features.

Configuration wizard enhancements
When the installation completes, use the configuration wizard to configure your protection settings. You can choose to configure a new computer for the first time, or recover an existing configuration. Data can be recovered from a remote server.

Increased include and exclude list size limit
The character limits on the contents of the **include**, **exclude**, and **vault lists** is increased to a maximum of 16,000 characters.

Schedule backups to expire
Use the Expiration panel of the notebook to specify when deleted files are removed from the remote backup location. This conserves storage space, and you can set backups of deleted files to expire after a certain number of days. You can configure the expiration process to run at scheduled intervals.

Support for IPv6
Support was added for IPv6. IPv6 removes the IP addressing limitation of IPv4, and provides improved quality of service and IP security.

Email backup operations are no longer reliant on subfile settings
Email backups can run without any dependency on subfile settings.

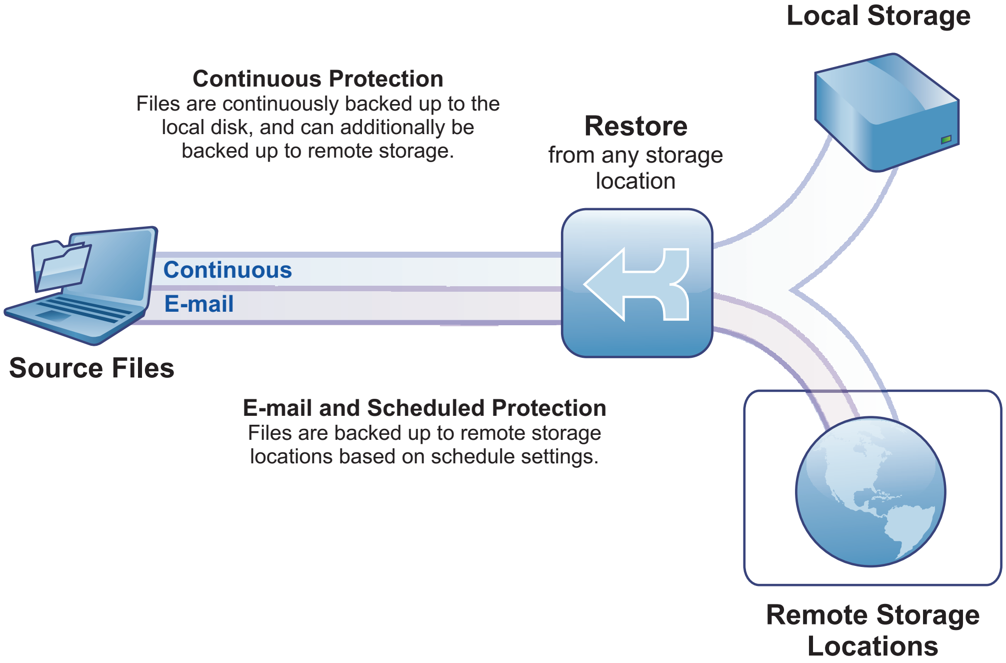
Introduction to Tivoli Continuous Data Protection for Files client

The Tivoli Continuous Data Protection for Files client provides a flexible, easy to use file protection system. Your most important files can be continuously protected. Your less important files can be protected at scheduled intervals to save time and storage space. Email files can also be protected. And you can prevent any changes (including deletions) to files in folders that you designate as vaults.

Continuously protected files are backed up to a local drive. This means that backup copies are created even when network conditions prevent storing backup copies remotely. Continuously protected files can also be stored on remote storage locations, when network connections allow. If a remote location is not available when you change a continuously protected file, the Tivoli Continuous Data Protection for Files client makes a backup copy on that device as soon as the device becomes available. Scheduled backup copies are created on the interval that you configure (hourly, weekly, daily, or monthly). If the remote device for scheduled backups is not available at the time of the backup, theTivoli Continuous Data Protection for Files client makes backup copies on the remote location as soon as that device becomes available.

Every time you change a file, a backup copy is created. You can choose which version of a protected file you want to restore, and configure how many backup copies to save.

This diagram provides an overview of how the Tivoli Continuous Data Protection for Files client protects your data.


Local Storage
Continuous Protection
Files are continuously backed up to the local disk, and can additionally be backed up to remote storage.
Restore
from any storage location
Continuous
E-mail
Source Files
E-mail and Scheduled Protection
Files are backed up to remote storage locations based on schedule settings.
Remote Storage Locations

After installation of a Tivoli Continuous Data Protection for Files client, the client immediately provides continuous protection for a pre-configured list of files. You can see the backup copies in the `\RealTimeBackup\` folder in the root of your primary drive. The backup copies can also be seen in the list of files that you can restore with the Restore Wizard of the client. The default space allocated for your backup copies is 500 MB.

Tivoli Continuous Data Protection for Files can store backup copies on a Tivoli Storage Manager server, but there is no requirement to use Tivoli Storage Manager. Tivoli Continuous Data Protection for Files is a stand-alone product and has no dependencies on Tivoli Storage Manager or Tivoli Storage Manager FastBack®.

Types of protection

The Tivoli Continuous Data Protection for Files client offers three types of protection for your files: continuous protection, scheduled protection, and vaulting.

Continuous protection means that every time a file is saved, a backup copy is created. Hence, the backup copy exactly matches the original file as you last saved it. If you choose to save more than one version of a backup copy, the previous backup copies match the previous versions of your file.

Files that are protected by schedule are copied to the remote storage area on a regular schedule. They are not backed up every time you save them, as are continuously protected files. Hence, scheduled protection yields fewer backup copies. If a file is lost between the time it is saved and the time it is backed up, you are able to restore only a previous version of the file.

Email files are protected on a schedule.

If the storage area is unavailable when a protected file is saved, the client notes that the file was changed. When the storage area becomes available, the client makes a backup copy of the most recent version of the file.

Table 2. Comparison of the three types of protection

Type of Protection	**Continuous Protection**	**Scheduled Protection (includes email)**	**Vaulting**
Advised for what files	Advised for your most important files. Not advised for large dynamic files like email files.	Advised for large, dynamic files like email.	Advised for files that you do not want to be changed nor deleted.
How protected	Backup copies are created on storage areas.	Backup copies are created on a storage area.	Vaulted files and folders cannot be modified nor deleted.
Frequency of backups	File is backed up whenever it is saved.	File is backed up only at the scheduled time, and only if it was saved since the previous schedule.	No backups
Backup copy storage area	Local or remote	Remote only	Not applicable
Files protected	Files selected in the **Folders and Files** and **Applications** boxes in the **Files to Protect** panel in the Settings Notebook of the client.	Files selected in the **E-mail Protection** panel and by the **Scheduled Backup Settings** link in the **Advanced** panel in the Settings Notebook of the client.	Files selected in the **Vault** box in the **Files to Protect** panel of the Settings Notebook of the client.

For more information about scheduled backup, see “Considerations for scheduled backups” on page 55.

Chapter 2. Installing the Tivoli Continuous Data Protection for Files client

This chapter contains information for installing and initially configuring the Tivoli Continuous Data Protection for Files client.

Basic installation of the Tivoli Continuous Data Protection for Files client

Basic installation of the client includes a wizard-guided configuration, and is suitable for installation on a single local computer. You can also upgrade and uninstall on a single computer.

For installing the client to a remote computer, installing without user interaction, or installing to many computers, see "Advanced installation of the Tivoli Continuous Data Protection for Files client" on page 21.

System requirements

Tivoli Continuous Data Protection for Files client requires a Windows server or workstation with minimum levels of hardware and software.

For current software and hardware requirements, see CDP V6.3.0 Hardware and Software Requirements, available at http://www.ibm.com/support/docview.wss?uid=swg21569819.

Installing the Tivoli Continuous Data Protection for Files client

You can install the Tivoli Continuous Data Protection for Files client on a single computer and follow a wizard to configure your protection settings.

Before you begin

This section describes interactive client installation on a single computer and configuration using a wizard. To do a silent client installation (without user interaction) and to push Tivoli Continuous Data Protection for Files clients to other computers, see "Advanced installation of the Tivoli Continuous Data Protection for Files client" on page 21.

If you are upgrading from a previous version of the client, see "Considerations for upgrading a client" on page 25.

- You must have administrator authority to install the client.
- Your computer must have the necessary hardware and software. See "System requirements."
- If you are reinstalling or upgrading from a previous version of the client, close all other applications (especially email programs) before you install. You must reboot immediately after the installation is complete.

About this task

Follow these steps to interactively install the client on a single computer.

Procedure

1. Double-click the Tivoli Continuous Data Protection for Files client installer icon. The installer shows the language selection dialog. The default is English.
2. Choose your preferred language and click **OK**. The Tivoli Continuous Data Protection for Files information window shows the build number.
3. Choose whether to install the Tivoli Storage Manager API. This is necessary for backups to a Tivoli Storage Manager server.
4. Click **Next**. The **License Agreement** window displays.
5. Read the License Agreement, and indicate if you accept the terms of the agreement. Click **Next**. The **Destination Folder** window displays.
6. Accept the default installation location, or click **Change** to specify another location. Click **Next**. The **Ready to Install the Program** window displays.
7. Confirm that the information is correct and click **Next**.

   The installation window shows a progress bar indicating that the necessary files are being installed on your computer. It also shows a command prompt window as the installer runs several scripts.

   The Installation Complete window displays.
8. If you are installing on Windows Vista, and there is an existing Tivoli Continuous Data Protection for Files client, you see the Files in Use window. Click **OK**. You also see a warning that the setup was unable to automatically close all requested applications. Click **OK**.
9. If it is your first installation of the Tivoli Continuous Data Protection for Files client on this computer, a configuration wizard helps you choose your protection settings. See "Navigating the configuration wizard" on page 7.
10. Click **Finish**. The installer indicates that you must reboot in the following situations:
    - You are reinstalling or upgrading Tivoli Continuous Data Protection for Files.
    - A product that uses the Tivoli Storage Manager API is installed and running. Tivoli Storage Manager Backup-Archive client is such a product.

What to do next

Note: If you are upgrading from version 2.1.x on a non-English operating system, you do not see all national language text until you restart the computer.

If you upgrade over a previous version of Tivoli Continuous Data Protection for Files, you must restart the computer for the new settings to become active and for your protection to continue.

After installation (and restart, if required), the client immediately starts protecting your files.

If you want to change your protection settings, see "Settings Notebook" on page 31.

Attention: Before having multiple clients back up files to the same remote file server, the server Access Control List (ACL) settings must be configured. Complete the configuration tasks described in "Limit user access to files on a target file server" on page 114.

Configuring clients by using the configuration wizard

After you install Tivoli Continuous Data Protection for Files, you must configure the client. Use the Configuration wizard to step you through the configuration process.

After the installation completes successfully, the configuration wizard starts automatically. The wizard steps you through a new configuration or the recovery of an existing configuration. You can modify the configuration using the notebook settings after you complete the initial configuration. The Configuration wizard does not startup after an upgrade.

Navigating the configuration wizard

After you installed Tivoli Continuous Data Protection for Files, the configuration wizard helps you configure your protection settings.

If you close the wizard before you finish configuring the client, the changes that you made are canceled. Tivoli Continuous Data Protection for Files protects your files according to the configuration settings that were defined for installation. You can view and change your settings at a later time with the Settings Notebook.

To configure a new computer, the wizard guides you through the following tasks:

- “**What is Critical** page” on page 8.
- “**Email Protection** page” on page 13.
- “**Remote Storage** page” on page 14.
- “**Initial Backup** page” on page 17.
- “**Summary** page” on page 20.

To recover an existing configuration, the wizard guides you through the following tasks:

- “**Specify Backup Server** page” on page 18.
- “**Identify the Backup** page” on page 19.
- “**Start Restore Wizard** page” on page 19.
- “**Summary** page” on page 20.

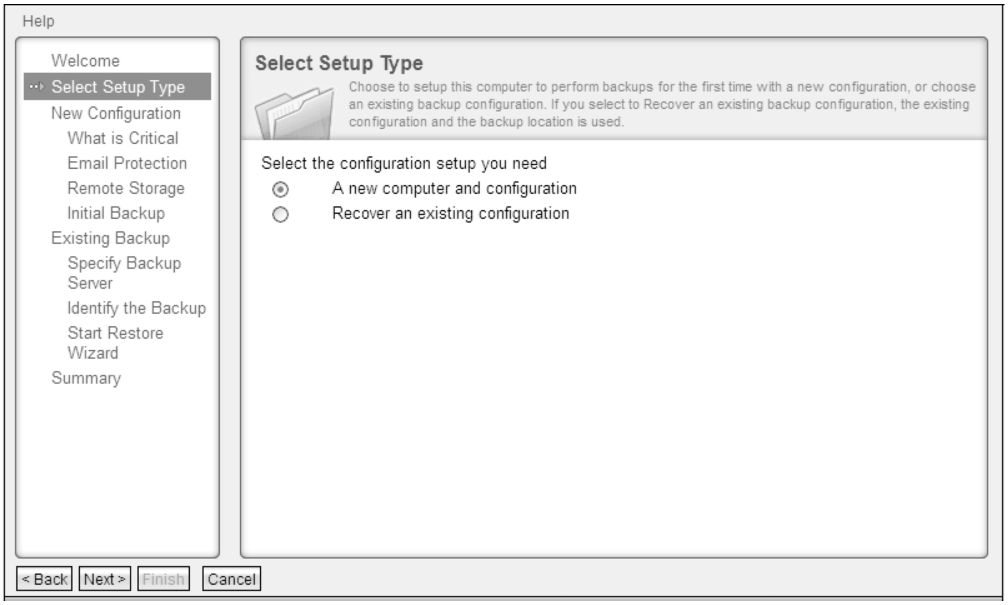
Configuration wizard Welcome page:

The **Welcome** page lists the steps that you must complete to configure your computer for the first time, or to configure your computer from an existing backup on a remote server.

Click the **Next** button to open the **Select Setup Type** page of the wizard. Alternatively, click back to change the configuration type. Only click **Cancel** if you want to exit the wizard without changing the configuration settings.

Select Setup Type page:

The **Select Setup Type** page gives you a choice between configuring your computer for the first time, or for configuring your computer from an existing backup on a remote server.



Select Setup Type

Choose to setup this computer to perform backups for the first time with a new configuration, or choose an existing backup configuration. If you select to Recover an existing backup configuration, the existing configuration and the backup location is used.

Select the configuration setup you need

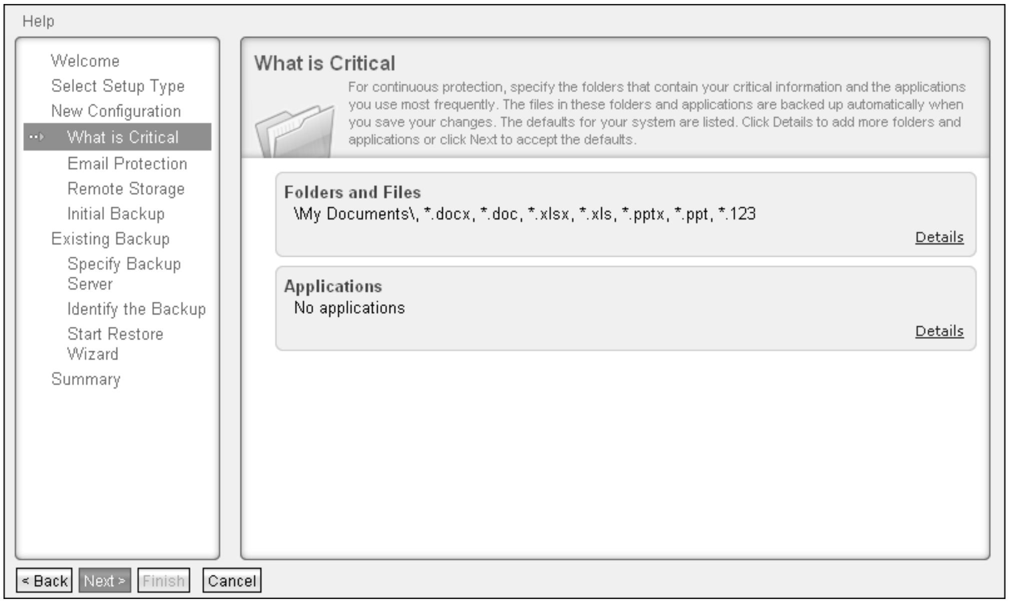
● A new computer and configuration

○ Recover an existing configuration

Select **Next** to open the **Specify Backup Server** page of the wizard. Alternatively, click **Cancel** to exit the wizard without changing the initial protection settings.

What is Critical page:

Specify the files and folders that you want to protect. The specified files and folders and applications will be continuously protected. Tivoli Continuous Data Protection for Files creates backup copies on a storage area as soon as the files are changed.



What is Critical

For continuous protection, specify the folders that contain your critical information and the applications you use most frequently. The files in these folders and applications are backed up automatically when you save your changes. The defaults for your system are listed. Click Details to add more folders and applications or click Next to accept the defaults.

Folders and Files
\My Documents\, *.docx, *.doc, *.xlsx, *.xls, *.pptx, *.ppt, *.123

Applications
No applications

When Tivoli Continuous Data Protection for Files is installed, it is preconfigured with a list of files and folders to continuously protect. Use this page to confirm that the initial protection settings are correct for your system, or change the settings as appropriate.

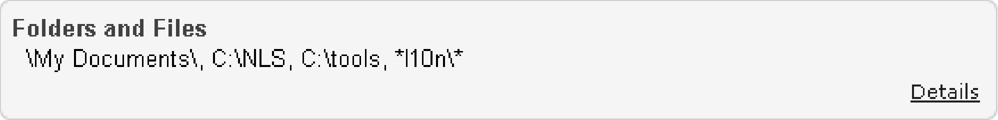
The protected files are listed by **Folders and Files** and by **Applications**. These lists are not exclusive of one another, but offer two views of what is protected.

If you want to view the file paths, names, and extensions that are protected, use the **Folders and Files** summary pane. You can use a file tree to specify what to protect.

If you want to view the applications that are protected, use the **Applications** box. You can specify the applications from a list. Files that are created by the listed applications are protected. The file extensions associated with the application are added to the **Folders and Files** list.

Note: Email applications are specified in the **Email Protection** page. Because these files are often very large, their protection settings are configured separately.

Folders and Files *summary pane of Tivoli Continuous Data Protection for Files:*



Folders and Files

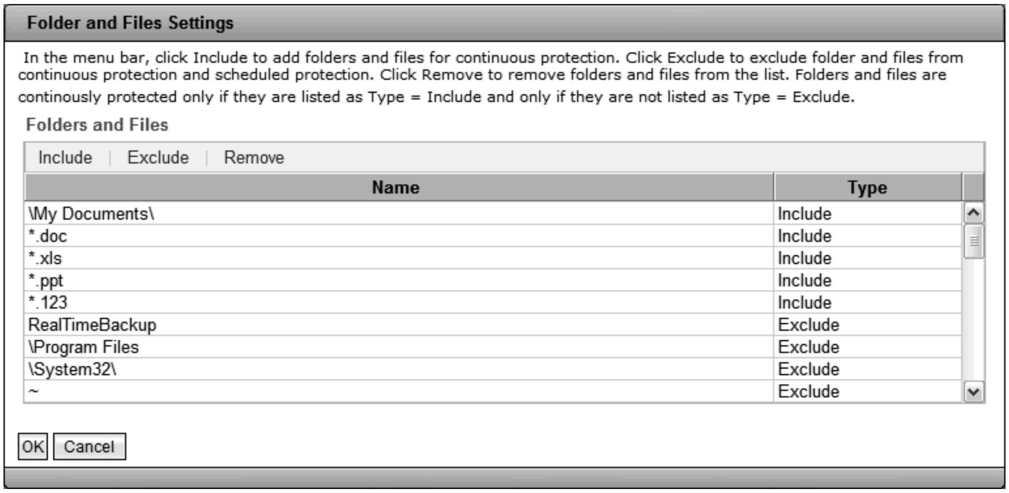
\My Documents\, C:\NLS, C:\tools, *l10n*

This pane gives a summary of the folders and files that are continuously protected. The number of items protected refers to the items in the list of folders and files. A single list item can specify more than one file. Click the **Details** link to view all items in the list and modify the list.

Folders and Files Settings *page for continuous protection by Tivoli Continuous Data Protection for Files:*

Specify which folders and files to continuously protect by selecting the files to include and exclude.

List of Folders and Files to Include and Exclude



Folder and Files Settings

In the menu bar, click Include to add folders and files for continuous protection. Click Exclude to exclude folder and files from continuous protection and scheduled protection. Click Remove to remove folders and files from the list. Folders and files are continously protected only if they are listed as Type = Include and only if they are not listed as Type = Exclude.

Folders and Files

Name	Type
\My Documents\	Include
*.doc	Include
*.xls	Include
*.ppt	Include
*.123	Include
RealTimeBackup	Exclude
\Program Files	Exclude
\System32\	Exclude
~	Exclude

You can include and exclude or remove an item from the list:

Include
: Click **Include** to add files and folders that you want to continuously protect.

Exclude
Click **Exclude** to add files and folders that you want to exclude from continuous and scheduled protection.

Remove
Select a list item, and then click **Remove** to remove that list item.

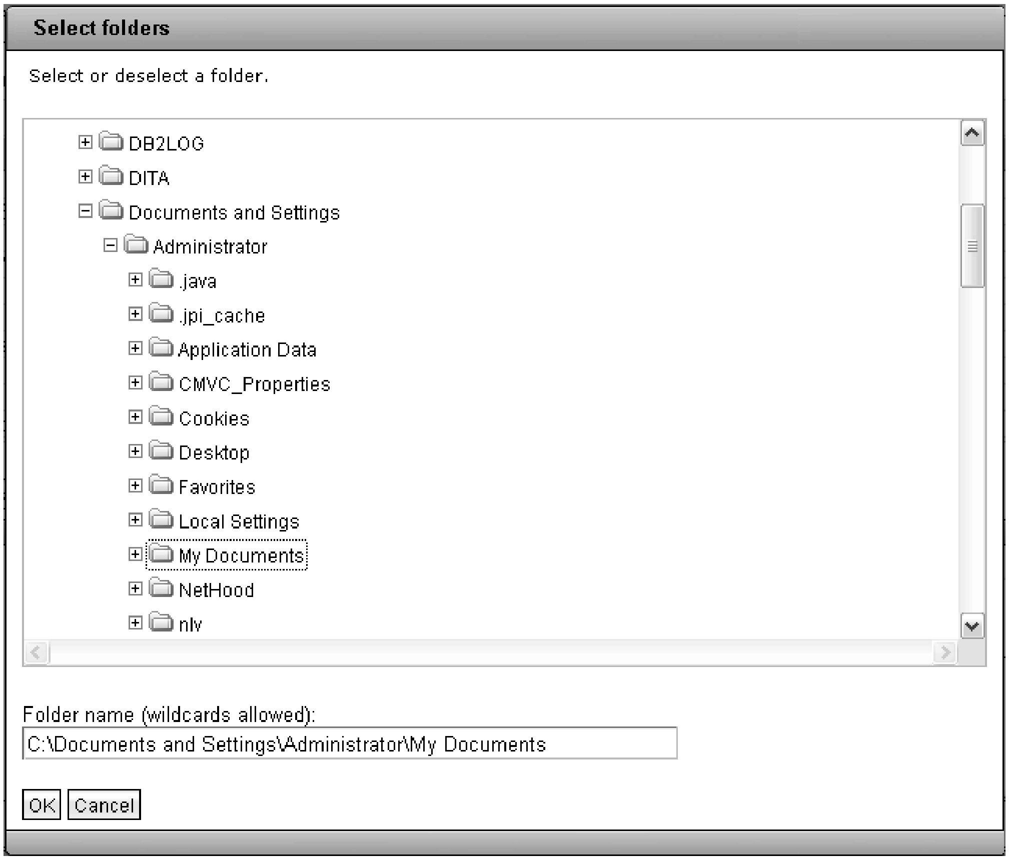
The list contains these columns:

Name Patterns in the **Name** column specify one or more files or folders. See “Wildcards in file specifications” on page 11 to determine what files and folders match a **Name** pattern with blanks or asterisks. When a folder is protected, all of its files and subfolders are protected.

Type Values in the **Type** column indicate whether the files and folders should be included or excluded from protection. Files and folders that are excluded from continuous and scheduled protection. Files that are included are protected. Files that are excluded have precedence over files that are included. As a result, any file or folder that matches an exclude pattern are not protected, even if the same file or folder matches an include pattern. (See “Including and excluding files from protection” on page 37).

Note: The Initial Configuration Wizard. However, the Initial Configuration Wizard only allows file additions (of type Include). Any exclude patterns exclude files from protection as soon as Tivoli Continuous Data Protection for Files is installed, but they are hidden from view during installation. Although exclude patterns are exposed in the Settings Notebook, you can specify advanced configuration options.

Select folders *page of Tivoli Continuous Data Protection for Files:*



Select or deselect a folder.

Folder name (wildcards allowed): C:\Documents and Settings\Administrator\My Documents

Specify files and folders in the **Select folders** page. You can browse to select a folder, or type the name of a file or folder in the **Folder name**.

Important: Only your internal drives can be protected. Any external storage devices are considered remote storage devices.

Wildcards in file specifications:

You can use wildcards to specify the files that you want to protect.

You can enter the complete path of a file that you want to protect. For example, `C:\Documents and Settings\Administrator\My Documents\Soccer\2005AYSO\Parent Info U8B.doc`. The complete path must match a single file. You can use asterisks and blanks as wildcards to specify several files.

An asterisk matches any number of characters in a file path. If there are no asterisks, Tivoli Continuous Data Protection for Files matches any file whose fully expanded path name has that exact pattern anywhere in the path or filename. The pattern is not case-sensitive.

If there are no asterisks, blank spaces before and after the pattern are interpreted as asterisks. For example, `\myDocs\` and `*\myDocs\*` yield the same matches. If there are asterisks in the pattern, blank spaces before or after the pattern match no characters. For example, `\myDir\`, `*\myDir\`, and `\myDir\*` can yield three different matches.

For example, assume a pattern `fish`. This pattern matches: `C:\dir\fish.doc` and `C:\fish\anyfile.doc` and `c:\Dirfishfood\something`.

If the pattern has slashes around it (`\fish\`), it matches any object with `\fish\` somewhere in the path. This pattern matches `C:\fish\anyfile.doc` but not `C:\dir\fish.doc` and not `c:\Dirfishfood\something`.

This table provides examples of how patterns match files and folders.

Table 3. File and folder pattern matches

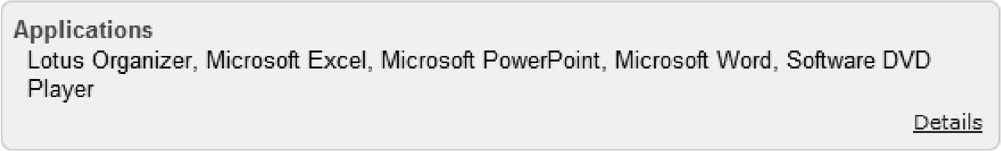
This pattern ...	**... matches these folders and files on your computer:**
\myDir\ or \mYdiR\ or *\myDir* or *\mydir*	c:\myDir\ c:\myDir\Contacts\ c:\myDir\Contacts\contacts.txt c:\Projects\myDir\ c:\Projects\myDir\myThings\ c:\Projects\myDir\myThings\things.doc c:\Projects\myDir\myThings\myPhoto.jpg d:\Notes\myDir\
*\myDir\	c:\myDir\ c:\Projects\myDir\ d:\Notes\myDir\
d:*\mydir*	d:\Notes\myDir\
\my best	c:\Books\My Best.doc c:\Photos.jpg\My Best Photo\ c:\Photos.jpg\My Best Photo\Best.jpg f:\Projects\My Best Project\ f:\Projects\My Best Project\Dream.xls

Table 3. File and folder pattern matches (continued)

This pattern ...	**... matches these folders and files on your computer:**
.jpg	c:\Photos.jpg\ c:\Photos.jpg\myHouse.bmp c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
*.jpg	c:\Photos.jpg\ c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
E:\ E:\*	All files and folders on the E: drive.

Applications *pane of Tivoli Continuous Data Protection for Files:*

This pane lists the applications that are protected.



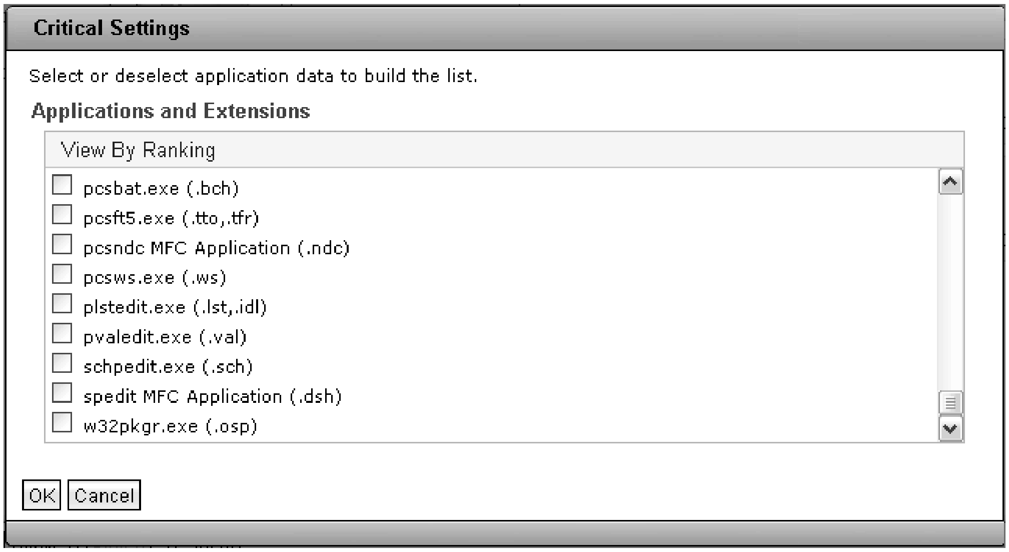
Applications

Lotus Organizer, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Software DVD Player

To see the complete list of the applications that are protected, click **Details**.

Critical Settings *page:*

Use the Critical Settings page to specify a list of applications to protect.



Critical Settings

Select or deselect application data to build the list.

Applications and Extensions

View By Ranking

- ☐ pcsbat.exe (.bch)
- ☐ pcsft5.exe (.tto,.tfr)
- ☐ pcsndc MFC Application (.ndc)
- ☐ pcsws.exe (.ws)
- ☐ plstedit.exe (.lst,.idl)
- ☐ pvaledit.exe (.val)
- ☐ schpedit.exe (.sch)
- ☐ spedit MFC Application (.dsh)
- ☐ w32pkgr.exe (.osp)

The **Applications and Extensions** pane presents a list of applications and file extensions. Select the applications that you want to continuously protect.

The list of applications has two views. Click on View By Ranking to change the list to be ordered alphabetically.

View by Ranking
The applications that have the greatest quantity of files on your computer

are presented at the start of the list. The applications that have the least quantity of files on your computer are presented at the end of the list.

View Alphabetically
The applications are presented in alphabetical order.

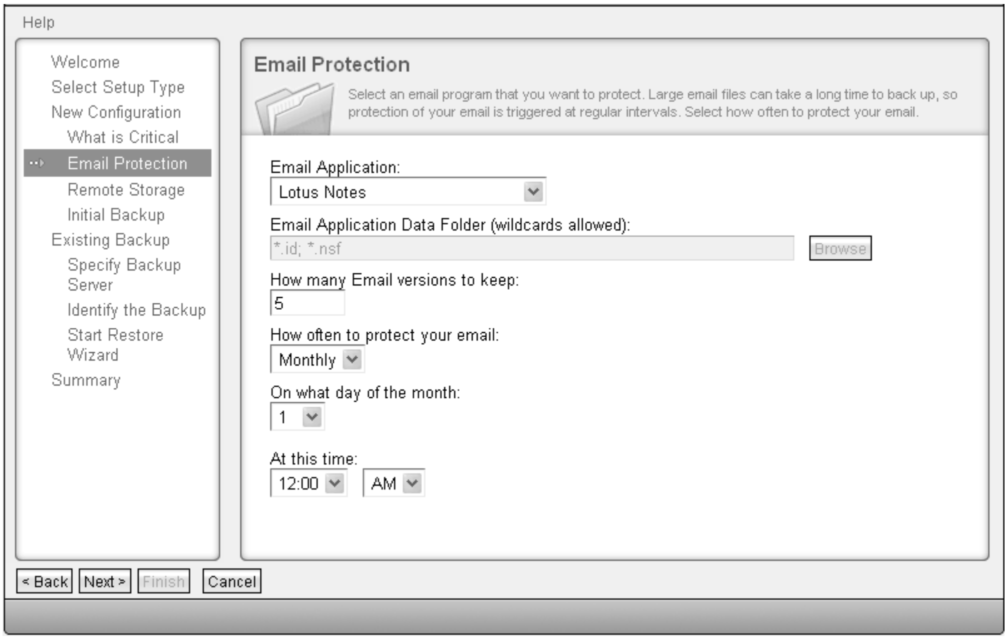
If you select a checkbox, all file extensions associated with that application are added to the list of protected files.

If you clear a checkbox, all files with that extension are removed from the list of protected files. Removing file extensions from the list of protected files does not add those files to the list of files that are explicitly excluded from protection.

You can add files to be protected in the **Critical Settings** page, but these applications are protected only if the files are not explicitly excluded. For more information, see "Including and excluding files from protection" on page 37.

Email Protection page:

Use this page to select the email applications that you want to protect. Specify the schedule for protecting the email applications.



Email Protection

Select an email program that you want to protect. Large email files can take a long time to back up, so protection of your email is triggered at regular intervals. Select how often to protect your email.

Email Application: Lotus Notes
Email Application Data Folder (wildcards allowed): *.id; *.nsf
How many Email versions to keep: 5
How often to protect your email: Monthly
On what day of the month: 1
At this time: 12:00 AM

Because email files typically are large, they are not backed up continuously, but only on the schedule that you select.

Email files are backed up only to remote storage. If the remote storage is not available at the scheduled backup time, Tivoli Continuous Data Protection for Files backs up the email files when the remote storage area becomes available.

Email Application list

Select one of the email applications in the list.

If your application is not listed, select **Other**.

Email Application Data Folder field

If you choose your email application from the **Email Application** list, the default file type for that application is shown in this box, and you are not able to update the file specification. You can update this field only if you select **Other** in the **Email Application** list.

How Many Email Versions to Keep field

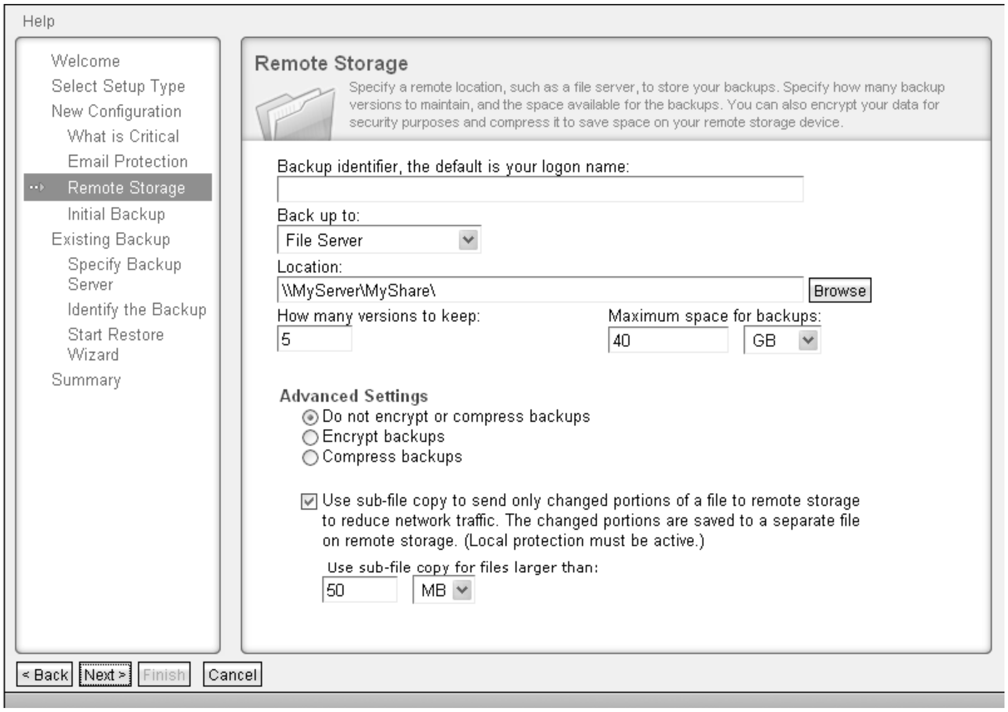
You can specify how many versions of the email file to keep on remote storage in this field.

How often to protect your email list

You can schedule email protection at one of several intervals:
- **Never**: Email is not protected.
- **Hourly**: Email files will be backed up every hour, just after the hour.
- **Daily**: If you choose this interval, also select the time for the backup.
- **Weekly**: If you choose this interval, also select the day and time for the backup.
- **Monthly**: If you choose this interval, also select the day of the month and time for the backup.

Remote Storage page:

Use this page to specify the remote storage for backups of your protected files.



Remote Storage

Specify a remote location, such as a file server, to store your backups. Specify how many backup versions to maintain, and the space available for the backups. You can also encrypt your data for security purposes and compress it to save space on your remote storage device.

Backup identifier, the default is your logon name:

Back up to: File Server

Location: \\MyServer\MyShare\

How many versions to keep: 5

Maximum space for backups: 40 GB

Advanced Settings

● Do not encrypt or compress backups

○ Encrypt backups

○ Compress backups

☑ Use sub-file copy to send only changed portions of a file to remote storage to reduce network traffic. The changed portions are saved to a separate file on remote storage. (Local protection must be active.)

Use sub-file copy for files larger than: 50 MB

Storing files in a remote storage area protects the files in case local copies are lost. Backups of continuously protected files, and files protected on a schedule, are stored in the same remote area. Tivoli Continuous Data Protection for Files is tolerant of intermittently available networks. If the remote storage area is temporarily unavailable, Tivoli Continuous Data Protection for Files queues backup copies until the remote storage becomes available.

Remote Storage server or device name and location:

Use the Remote Storage page to specify the remote storage server or device and its location for your backup copies. You can also specify how many versions to keep.

Select the type of storage device or server for the backup files to be stored to.

Backup Identifier

In this field, type the name that helps you to identify your backup files on the remote server. The default is your logon name. The backup identifier is only used for recovery purposes, and not for typical file restore. The backup identifier is used to locate the remote server location for a computer when restoring the configuration with the configuration wizard.

Location for the External Device or File Server

Select a file server or removable disk to store the backup copies. The remote device can be another computer (such as network-attached storage or a file server), a remote disk, or a removable disk.

If you choose a remote server in the **Location** field, you can use Universal Naming Convention (UNC) specifications for the file server instead of drive letters. Drive letters can change after you restart the system and often do not reconnect automatically.

If you choose a USB external device, you can select the drive letter. However, removable external device drive letters can change. To configure USB drives for remote storage, see Instructions on how to setup a USB device as the remote backup location., available at https://www.ibm.com/support/docview.wss?uid=swg21245761.

Click **Browse** to view a **Browse for folder** dialog box. Use this dialog box to go to the location for your remote storage area. If this dialog becomes hidden behind other windows, click the task bar to bring it to the front.

Tivoli Continuous Data Protection for Files creates backup copies in a subfolder called `\RealTimeBackup\`*`computer name`*. For example, if a computer name is Computer1, and the remote storage location is configured with the value `\\remote\share`, backup copies are stored in `\\remote\share\RealTimeBackup\Computer1\`.

If you log on to your computer with a user name and password that is also valid on your remote storage location, Tivoli Continuous Data Protection for Files authenticates your credential at that location. If the user name and password is not valid on your remote storage location, you must log on to the network using another account with regular privileges. You can log in interactively by using the **`Net Use`** command.

Some versions of Microsoft Windows use simplified file sharing, which allows one computer to connect to another computer over the network. The resulting connection allows only limited file system capabilities, and inhibits the creation of backup copies. Some information such as access control lists or file streams might be lost. You can disable simplified file sharing on the remote storage area.

WebDAV Server storage location

Some Internet Service Providers (ISPs) provide Web-based Distributed Authoring and Versioning, or WebDAV. With the WebDAV protocol, you can create, change, and move documents on a remote server. The WebDAV protocol is useful for authoring the documents that a web server serves, but can also be used for general web file storage. If your ISP provides WebDAV functions, Tivoli Continuous Data Protection for Files can store backups on a web-based server.

In the **Location** field, enter your WebDAV server location using the following format: `https://MyISP.com/MyAcct`.

When using WebDAV, Tivoli Continuous Data Protection for Files can use the basic authentication method. Because this authentication method sends the password as clear text over the network, the web server is configured to use secure sockets.

Tivoli Storage Manager storage location

Tivoli Continuous Data Protection for Files can store backup copies on a Tivoli Storage Manager server.

In the **Location** field, specify the Tivoli Storage Manager server location, using the following format: *tsm://Host.com*. You can also use an IP address for the server address.

You can use Tivoli Storage Manager server version 6.1 or later with Tivoli Continuous Data Protection for Files.

Configure the Tivoli Storage Manager server before you connect from Tivoli Continuous Data Protection for Files. Register the computer as a Tivoli Storage Manager node. Tivoli Continuous Data Protection for Files prompts you for the password for this node in order to connect to the Tivoli Storage Manager server. For more information about registering a Tivoli Storage Manager node for your computer, see *IBM Tivoli Storage Manager for Windows Administrator's Guide*.

If you specify a Tivoli Storage Manager server as the backup target and you want encryption or compression features applied to the backup, you must specify these options in the `dsm.opt` file in the Tivoli Continuous Data Protection for Files subfolder of the "Program data folder" on page 50.

Restriction: You cannot use a subfile backup feature when the Tivoli Storage Manager server is the backup target.

In addition to backing up data directly to a Tivoli Storage Manager server, you can back up data using a two-stage method. First, use Tivoli Continuous Data Protection for Files to create remote backups on a file server. Then, schedule a Tivoli Storage Manager backup-archive client on that file server to back up the files to a Tivoli Storage Manager server.

Restriction: If you use Tivoli Continuous Data Protection for Files encryption, you cannot use Tivoli Storage Manager compression.

To manage storage space, the Tivoli Storage Manager administrator must grant authority to the Tivoli Storage Manager client node to delete backup copies. For steps to assign authority to delete backup copies, see the topic in the problem determination section: " Tivoli Storage Manager client node lacks authority to delete backup copies" on page 110.

To avoid problems when using the Tivoli Storage Manager server, see "Files are not backed up to Tivoli Storage Manager server" on page 110.

Remote Storage advanced settings:

Depending on the remote storage location that you specified, use the advanced settings in the Remote Storage page to select to encrypt or compress files. You can specify whether to use subfile copies when backing up larger files.

Tip: The default size for the remote storage area is 40 GB. If you increase the number of backup versions to keep, consider increasing your storage area size. If you are unsure of how much space to allocate, you can monitor the space usage on the Status panel and adjust the version and space settings accordingly.

When the storage space becomes full, Tivoli Continuous Data Protection for Files deletes older backup copy versions of files that have several backup copy versions. If more space is needed for new backup copies, Tivoli Continuous Data Protection for Files deletes backup copies of files to make room for the newest backup copy.

If you try to remotely back up a file that is larger than the space you have allocated, Tivoli Continuous Data Protection for Files purges all older file versions, and the backup might fail. Ensure that the maximum space for your remote storage areas is greater than the maximum file size for remote backup in the **Advanced** page of the Settings Notebook. For example, if you decrease the maximum space for backups to 1 GB, you must decrease the maximum file size for remote backup from the default of 1 GB.

Advanced settings

When storing data onto an external device or file server, you can specify the following advanced settings. Select one option:

- Do not encrypt or compress backups
- Encrypt backups
- Compress backups

When storing data onto an external device or a file server you can choose to use sub-file copy function. Select this option to send only changed portions of a file to remote storage and to reduce network traffic. The changed portions are saved to a separate file on the remote storage.

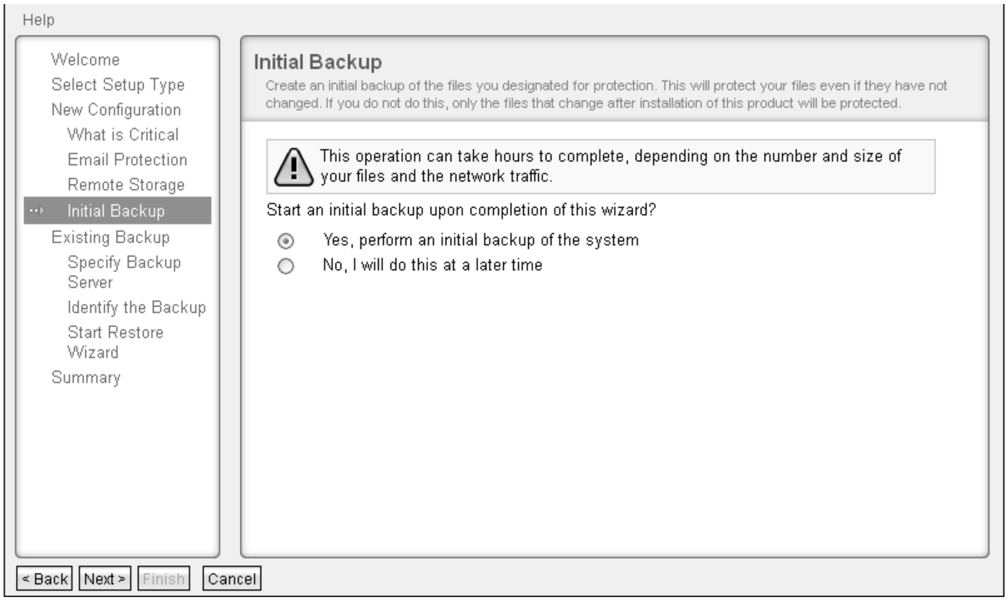
The preceding options are not available when you use the Tivoli Storage Manager as the remote storage server. If you must encrypt or compress your data, then use the Tivoli Storage Manager server compression or encryption features.

Related information:

Chapter 3, "Changing Protection Settings," on page 31

Initial Backup page:

Use the **Initial Backup** page to select whether you want to back up all your files when you finish the configuration wizard.



Initial Backup

Create an initial backup of the files you designated for protection. This will protect your files even if they have not changed. If you do not do this, only the files that change after installation of this product will be protected.

This operation can take hours to complete, depending on the number and size of your files and the network traffic.

Start an initial backup upon completion of this wizard?

● Yes, perform an initial backup of the system

○ No, I will do this at a later time

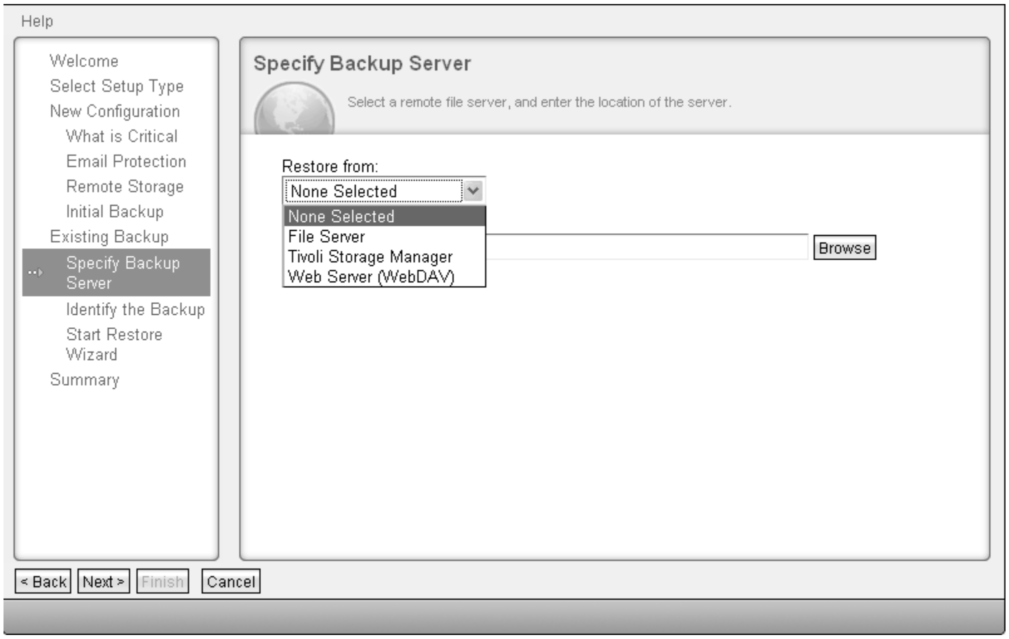
After the first installation of the Tivoli Continuous Data Protection for Files client, you can immediately back up all files that you configured for protection. In the initial backup, newly created files and existing files that are changed are protected. Existing files that are not changed are backed up after the initial scan is done.

The initial backup scans all of your local drives, looking for files that you selected for protection. All files that meet the specifications are backed up to local or remote storage areas. This process can take a long time and affect the performance of your computer. Start this initial backup when you will not be using your computer for other applications.

If you do not back up data using the installation wizard, you can force a complete backup at a later time. When you run a complete backup, use the **Files to Protect** page of the Settings Notebook.

Specify Backup Server page:

On the **Specify Backup Server** page in the configuration wizard, you can choose to restore data from a Tivoli Storage Manager server, the web, a file server or an external device.



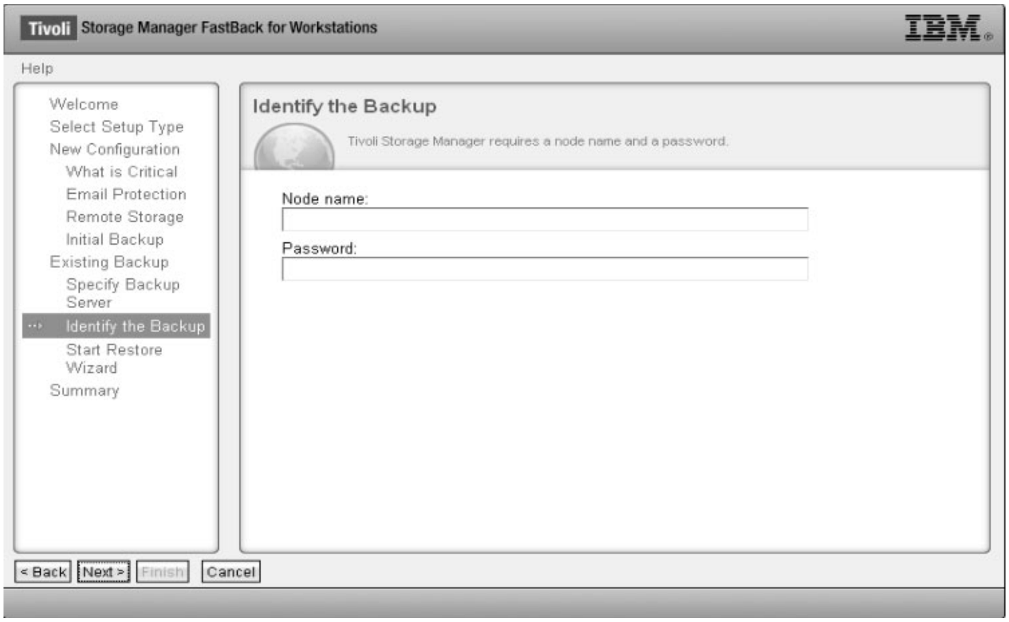
Specify Backup Server

Select a remote file server, and enter the location of the server.

After you select one of the backup server options from the menu, you must specify the target location of the server that you selected. When you are restoring from the file server, you can either input the server location or click **Browse** to locate the server.

Identify the Backup page:

You must enter a Tivoli Storage Manager node name and password, or select a backup location from a list of backup identifiers.



Identify the Backup

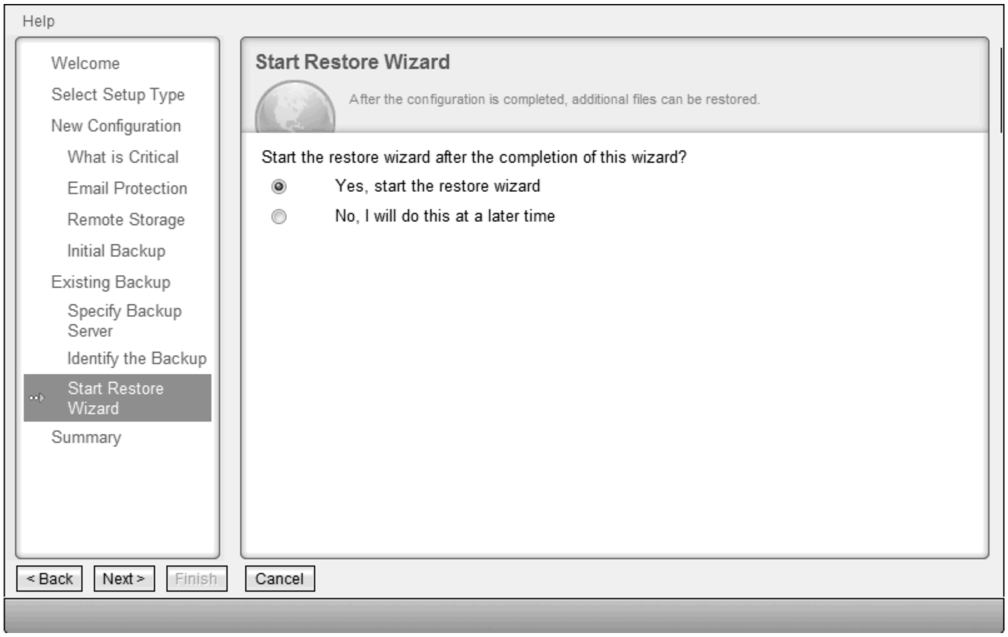
Tivoli Storage Manager requires a node name and a password.

Enter the node name and password if you are restoring data from a Tivoli Storage Manager server. If you are restoring data from a file server or a web server, select the backup identifier to verify the remote location.

Start Restore Wizard page:

Use the Start Restore Wizard page to start the restore wizard or to delay this action until a later time.

Use the **Start Restore Wizard** page to choose whether to start the restore wizard when the configuration completes.



Start Restore Wizard

After the configuration is completed, additional files can be restored.

Start the restore wizard after the completion of this wizard?

● Yes, start the restore wizard

○ No, I will do this at a later time

Select the **Yes** option to start the Restore wizard when you click **Finish** on the Summary page. The Restore wizard steps you through the process of selecting the files you want to restore, and choosing the location to store the restored files, see “Restore Wizard of Tivoli Continuous Data Protection for Files” on page 90. If you decide not to start the restore wizard, you can access it by selecting the Restore icon on the Tivoli Continuous Data Protection for Files Status page.

Summary page:

Use the **Summary** page to view the summary information for your configuration of Tivoli Continuous Data Protection for Files. When you click **Finish** the configuration is complete.

The **Summary** page lists the configuration details you specified in the previous pages of the wizard.

Choose **Back** to return to a previous page to modify your configuration choices.

Choose **Finish** to apply your configuration choices. Tivoli Continuous Data Protection for Files continues to run in the background and to protect your data by using your configuration settings. When you recover an existing configuration, if you selected to start the restore wizard on completing the configuration the restore wizard opens when you click finish. Otherwise the status page is opened.

Choose **Cancel** to exit the wizard without applying your configuration choices.

Depending on the configuration chosen, the summary lists:
- The remote storage location,
- The backup location or the node name of the remote server,

- The files for restoring,
- A warning that the backups will continue to run. You should also ensure that no other computer is backing up to the same node or to the same location.

If you cancel the configuration wizard, Tivoli Continuous Data Protection for Files continues to run in the background and protect your files using the pre-configured settings.

Uninstalling the Tivoli Continuous Data Protection for Files client

Uninstall the Tivoli Continuous Data Protection for Files client with the following steps.

Before you begin

Close the Tivoli Continuous Data Protection for Files client GUI (graphical user interface) before running the uninstallation.

Procedure

1. From the Windows **Start** menu, choose **Control Panel**.
2. Choose **Add or Remove Programs**. A list of installed programs is displayed.
3. Scroll down and choose the product.
4. Click **Remove**. A dialog opens asking for confirmation that you want to remove the product.
5. Click **Yes**. Several windows display, indicating the activities to uninstall the product.
6. If you are uninstalling on Windows Vista, the Files in Use window opens. Click **OK**. A warning that the setup was unable to automatically close all requested applications also opens. Click **OK**.
7. A window confirming successful removal displays, and asks if you want to reboot now. Click **Yes** to reboot your system to remove file system filters.
8. Click **Finish** to exit the uninstall wizard.

   Note: This procedure applies to computers running Windows XP Professional. For computers running other Windows operating systems open the Control Panel, select Programs, and select Program and Features. Select the product to uninstall and click uninstall.

Advanced installation of the Tivoli Continuous Data Protection for Files client

The "Basic installation of the Tivoli Continuous Data Protection for Files client" on page 5 describes an installation that requires user interaction, and installs the Tivoli Continuous Data Protection for Files client on a single machine. There are more options for installing, upgrading, and reconfiguring the client.

There are several ways to install or upgrade the client without user interaction.

Silent installation on a local computer
You can install the client on your local computer in silent mode. The installer wizard is not displayed if you supply the `fpa.txt` configuration file. Use Notebook settings to configure Tivoli Continuous Data Protection for Files when the installation completes. Depending on the options that

you specified for the silent installation, you can either use the configuration wizard or the notebook to configure Tivoli Continuous Data Protection for Files.

Silent product upgrades and configuration updates on a local or remote computer

You can upgrade the product level and change protection settings on a local or remote computer silently. When you put a new client installer file or a new configuration file in the administration folder, the client pulls the information. The client adopts the new product level from the installer file or the new protection settings from the configuration file.

Silent installation pushed to a remote computer

Using the silent installation method, you can push the client to remote computers. If you are using a Windows 7 and Windows Vista operating system, you cannot push installations using `fpPushInst.exe`.

When the client is installed, it pulls product upgrades and configuration information from the administration folder.

Silent local upgrade

You can upgrade the product level on your local computer by putting the upgraded installer in the administration folder. The client pulls the new code. After a reboot, the product protects your files at the new level.

Silent installation pushed to another computer

An administrator can push the client to other computers.

Install the Tivoli Continuous Data Protection for Files client silently on a single local computer

You can install the Tivoli Continuous Data Protection for Files client on your local computer silently. In a silent installation, you do not interact with the installation wizard. If you provide a configuration file, you do not interact with the client initial configuration wizard.

Silent installation on a computer requires you to do the following:

- Invoke the installer with appropriate parameters.
- Optionally, you can provide a configuration file for the client. See "Use Tivoli Continuous Data Protection for Files to create a configuration file" on page 28. If you do not provide a configuration file, the initial configuration wizard will start after installation.

Silent installation command for the Tivoli Continuous Data Protection for Files client

Use this command to silently install the Tivoli Continuous Data Protection for Files client.

The client installer is an executable file with a name like `6.3.X.X-TIV-CDP-x86_windows.exe` for 32 bit, or `6.3.X.X-TIV-CDP-x64_windows.exe` for 64 bit. The installer name must include CDP and must be file type `.exe`. The version number in the executable file name changes from one version to the next.

Start the operation using the installer file name followed by parameters.

Parameters

All parameters are optional. You must specify a blank space before each parameter.

/S This parameter specifies a silent installation. If you do not specify this parameter, you install the product interactively through the installation wizard and the initial configuration wizard.

/v This parameter specifies whether to pass options that can be used by the Windows Installer to the MSI package. No space is allowed between the parameter /v and the options list. You must enclose the options list in quotation marks if there are blank spaces in the options list. The following options are allowed:

- **/qn** Everything except setup.exe is silent.
- **/l*v log file path**
  Specify a file to log the installation activities.
- **CUSTOM_CONFIG_FILES_PATH=configuration file path**
  This parameter specifies the path to the directory where the configuration files are stored. The configuration files include `fpa.txt`, `dsm.opt`, and `networks.xml`.
- **DONT_LAUNCH_FILEPATHSRV=1**
  This option is required when the installation is pushed down to the computer or the installation is being performed by a user other then user that the application is intended for. Example: Use the option if an Administrator is installing the software for another user.
- **INSTALLDIR=folder**

  The default new installation folder is `C:\Program Files\Tivoli\CDP_for_Files`.If you want to install to another folder, use this option and specify the folder. For example, you can specify `C:\applications\cdp`.

  Restriction: You cannot specify the root folder of a drive. For example, you cannot specify `C:\`.
- **REBOOT=ReallySuppress**
  Suppress system reboot after installation. This option is useful when you are pushing installation to a remote computer, because rebooting after installation can be disruptive to users on the remote system. This option should not be used for a local installation when a previous version of the client exists.

Example of a silent installation with default options

To issue a silent installation with default settings, and include a system restart after installation if the client was not previously installed, use this syntax:

```
TivoliCDP_CDPForFiles_6.3.X.X_windows.exe /S /v"/qn "
```

Restriction: Do not include a blank space between the **/v** parameter and the double quotation mark delimiter of the options list.

Example of a silent installation with options

To install silently to a folder other than the default, `c:\newdir`, and to log the installation activities to `c:\temp\msi.log`, ensure that the system is not restarted after installation, use this syntax:

```
TivoliCDP_CDPForFiles_6.3.X.X_windows.exe
/S /v" /qn INSTALLDIR=c:\newdir /l*v c:\temp\msi.log REBOOT=ReallySuppress "
```

Upgrade the Tivoli Continuous Data Protection for Files client silently

Once you install the Tivoli Continuous Data Protection for Files client, you can upgrade to a new product version by putting an installer executable file or a configuration file in the administration folder. The client pulls the software update or new configuration.

Upgrade the product level

To upgrade the product, put a new client installer in the downloads folder. (For information about the downloads folder, see “Administration folders” on page 101). The client pulls the new product code and notify you to reboot the computer.

The client checks for new installer and configuration files every 10 – 20 minutes. If the date of an installer file is more recent than the file used for the current product level, the client adopts the new product level. When the client detects a new installer file, a message opens from the system tray indicating that a new version of the software is being installed. When the installation is complete, a message opens from the system tray indicating that the new software was loaded. You must reboot to resume data protection. Between the time that the client pulls the upgrade and until the computer is rebooted, the client stops protecting your files. After the reboot, the client continues protecting your files. Your protection settings are the same as in the previous version of the product.

Restriction: Until you restart the system, the client does not back up any files. You do not lose any existing backup copies, but any changes you make are not protected. If there is a long delay between the time you install the product and the time that you restart the system, consider forcing a backup of all protected files to protect any files that were changed during that time. To force a backup, open the settings notebook and click **Files to Protect**. Select the **Start an initial backup with the new settings** check box and click OK.

Change protection settings

To change the protection settings, put a new configuration file in the downloads folder. To create a configuration file with Continuous Data Protection for Files, see “Use Tivoli Continuous Data Protection for Files to create a configuration file” on page 28. If the modification date of a configuration file is more recent than the file used for the current configuration, Tivoli Continuous Data Protection for Files adopts the new configuration.

You can use central administration features to manage the configuration of several Tivoli Continuous Data Protection for Files clients. See Chapter 8, “Tivoli Continuous Data Protection for Files central management considerations,” on page 97 for instructions to set up and manage your clients.

The central administration feature allows you to manage existing client configurations, but does not support management of product upgrades.

Considerations for upgrading a client

You can upgrade the client from previous releases as well as from a previous build of the current release.

The new client installer file name must contain the string CDP and be of file type .exe. For example, a typical name is `6.3.0-TIV-CDP-x86_windows.exe`.

The date of the new installer file must be more recent than the date of the installer file that was used for the current product level.

After upgrading to a new product version, you must restart your computer.

Files stored on Tivoli Storage Manager

Tivoli Continuous Data Protection for Files version 2.1 uses the Tivoli Storage Manager Backup-Archive client to store files on Tivoli Storage Manager server. These files must be restored by invoking the Tivoli Storage Manager Backup-Archive client. These files cannot be restored by the Tivoli Continuous Data Protection for Files version 2.2 and higher user interface.

Tivoli Continuous Data Protection for Files version 2.2 and higher uses the Tivoli Storage Manager API to store files on the Tivoli Storage Manager server. These files can be restored directly by the Tivoli Continuous Data Protection for Files client or Tivoli Storage Manager FastBack for Workstations user interface. These files cannot be restored by the Tivoli Storage Manager Backup-Archive client.

Cleaning up after uninstallation

If you uninstall the client, you must clean your data files before installing the client again. When the client is uninstalled, some files are not removed by the installer. The old files can cause problems for a new installation of the client.

After uninstalling the client, and before installing it again, remove files in the following areas:

local storage area
The local storage area is the `RealTimeBackup` folder on a local drive. Rename this folder if you want to save the backup copies.

remote storage area for the computer
The remote storage area is in the `RealTimeBackup\`*`computer_name`* folder of the remote device that you configured for the previous installation. Rename this folder if you want to save the backup copies.

installation folder
The default installation folder is `C:\Program Files\Tivoli\CDP_for_Files`.

The program data folder
The program data folder varies according to operating system and previously installed versions.

Pull upgrade from version 2 to version 3

If your version 2 Tivoli Continuous Data Protection for Files client pulls the installation of version 3.1, your version 2 client must be at level 2.2.1.20 or later. If you install by invoking the installer, the previous client level is not an issue.

Deploying the client to other computers

There are several ways to deploy the initial installation of the Tivoli Continuous Data Protection for Files client to other computers.

- Use Microsoft Systems Management Server to install the Tivoli Continuous Data Protection for Files.msi package. See Microsoft Systems Management Server documentation.
- Use IBM Tivoli Provisioning Manager Express®. For more information, see the product website at IBM Tivoli Provisioning Manager Express.
- Place the installer on a file server and ask users to start the installer.

When the Tivoli Continuous Data Protection for Files client is initially installed, the installer retrieves configuration data from the files `\System32\fpa.txt`, `\System32\dsm.opt`, or `\System32\networks.xml` in the Windows installation folder. You can also specify another directory to store the configuration files by using the **`CUSTOM_CONFIG_FILES_PATH`** command-line parameter. If these files do not exist, Tivoli Continuous Data Protection for Files is installed with the default configuration settings.

Restriction: If more than one client is backing up files to the same remote file server, you must configure the server Access Control List (ACL) settings. For more information about the configuration tasks, see "Limit user access to files on a target file server" on page 114.

FpPushInst.exe (push installation command)

The `FpPushInst.exe` executable file pushes a client installer to another computer.

The `FpPushInst.exe` executable file can be found at the root of the installation folder.

The default installation folder is `C:\Program Files\Tivoli\CDP_for_Files`.

The `FpPushInst.exe` executable file pushes the Tivoli Continuous Data Protection for Files client installer executable to the \System32\ subfolder of the `ADMIN$` share on the target computer. (See "Windows installation folder" on page 29). The `FpPushInst.exe` executable file can also copy a local configuration file `fpa.txt`, to `\System32\` in the Windows installation folder. `FpPushInst.exe` executable file then starts a service on the remote computer to start a silent installation. Due to firewall and other system settings, the `FpPushInst.exe` executable file does not work in some environments.

Note: `FpPushInst.exe` is not supported on systems running Microsoft Vista, Microsoft Windows 7, or Microsoft Windows Server 2008.

Syntax

FpPushInst.exe remote computer name **/user:**user name **/pwd:**password **/c:**local path of configuration file **/r** local path of installer "**/S /v**\" **/qn** options \""

Parameters

There must be a blank space before each parameter. Blank space is optional between parameters and their values.

remote computer name
The host name of the computer where you want to install Tivoli Continuous Data Protection for Files.

/user:user name /pwd:password
An administrative user account and password on the remote computer.

/c:local path and file name of configuration file
The path and file name of a Tivoli Continuous Data Protection for Files configuration file on the local computer. To create a configuration file with Continuous Data Protection for Files, see “Use Tivoli Continuous Data Protection for Files to create a configuration file” on page 28 The `FpPushInst.exe` executable copies the local configuration file to the `\System32\` folder in the Windows installation folder of the remote computer. This parameter is optional. If not specified, the configuration of the remote Tivoli Continuous Data Protection for Files client is the default configuration.

Note: The Tivoli Continuous Data Protection for Files installer looks for a configuration file named `fpa.txt` in the `\System32\` folder in the Windows installation folder of the remote computer. Tivoli Continuous Data Protection for Files installer does not use a configuration file in that folder with any name other than `fpa.txt`. Hence, in most circumstances, the file you specify with this parameter should be named `fpa.txt`.

/r local path and file name of installer file
The path and file name of Tivoli Continuous Data Protection for Files installer file on local computer. Separate the parameter and the value with a blank space.

The installer file name must contain the string CDP and end with .exe. For example, a valid path and name is `6.3.0-TIV-CDP-x86_windows.exe`.

/S The /S parameter is passed to the installer executable file and indicates silent installation. This parameter is required in a push installation. No space is allowed between the setup.exe initial parameter list delimiter ("" and the initial parameter (/S).

/v This parameter allows you to pass options supported by the Windows Installer to the MSI package. No space is allowed between /v and the options list. The options list must be enclosed in quotation marks if there are blank spaces in the options list. The following options are allowed:

/qn Everything except setup.exe is silent. This option is required in a push installation.

/l*v log file path
Specify a file to log the installation activities. The path corresponds to the remote computer.

DONT_LAUNCH_FILEPATHSRV=1
This option is required for push installation. A pushed installation runs in the system context. You should not start Tivoli Continuous Data Protection for Files in the system context after installation. Running Tivoli Continuous Data Protection for Files in the system context can lead to failures when backing up files, or failures later when a user tries to restore files. Use this option to suppress starting Tivoli Continuous Data Protection for Files in the system context immediately after installation.

INSTALLDIR=folder
The default installation folder is `C:\Program Files\Tivoli\`

`CDP_for_Files`. If you want to install to another folder, use this option and specify the folder. The path corresponds to the remote computer.

REBOOT=ReallySuppress

Suppress system reboot after installation. You can use this option when you are pushing installation to a remote computer as rebooting after installation can be disruptive to users on the remote computer. Do not use this option for a local installation when a previous version of Tivoli Continuous Data Protection for Files exists.

Example

This example pushes the installer file (`6.3.0-TIV-CDP-x86_windows.exe`) to the remote computer (Computer1). It also pushes a local configuration file `c:\fpa.txt` to the remote computer Windows installation folder as `\System32\fpa.txt`. The **`/user`** and **`/pwd`** values are used to log in to the remote computer for this operation. `FpPushInst.exe` then starts a service on the remote computer to start the installer, passing to it the parameters: **`/S`**, REBOOT=ReallySuppress, DONT_LAUNCH_FILEPATHSRV=1. This command tells the installer to install silently; do not reboot after installation, and do not start Tivoli Continuous Data Protection for Files in the system context immediately after installation. The installer adopts the protection settings in the configuration file in the Windows installation folder `\System32\fpa.txt`.

```
FpPushInst.exe \\Computer1 /user:Administrator /pwd:secret /c:c:\fpa.txt
/r  C:\TivoliSoftware\TivoliCDP_CDPForFiles_6.3.X.X_windows.exe
"/S /v\" /qn REBOOT=ReallySuppress  DONT_LAUNCH_FILEPATHSRV=1 \""
```

Use Tivoli Continuous Data Protection for Files to create a configuration file

Creating a configuration file to use when installing Tivoli Continuous Data Protection for Files.

About this task

When Tivoli Continuous Data Protection for Files is initially installed, the installer can get configuration data from a file `\System32\fpa.txt` in the Windows installation folder. For more information, see “Windows installation folder” on page 29. If this file does not exist, the installer installs Tivoli Continuous Data Protection for Files with default configuration.

When the Tivoli Continuous Data Protection for Files is initially installed, the installer retrieves configuration data from the files `\System32\fpa.txt, \System32\dsm.opt, or \System32\networks.xml` in the Windows installation folder. You can also specify another directory to store the configuration files by using the CUSTOM_CONFIG_FILES_PATH command-line parameter. If these files do not exist, Tivoli Continuous Data Protection for Files is installed with the default configuration settings

After the initial installation, Tivoli Continuous Data Protection for Files will pull future configuration settings from configuration files placed in a downloads folder in the central administration area. New configurations will be adopted within 10 to 20 minutes after being placed in the downloads folder. For more information about the downloads folder, see “Administration folders” on page 101. For more information about the central administration area, see Chapter 8, “Tivoli Continuous Data Protection for Files central management considerations,” on page 97.

Create a configuration file from an existing client:

Procedure

1. Use the Settings Notebook to configure the client as you want the configuration for other Tivoli Continuous Data Protection for Files clients.
2. Publish the configuration. Use the **Publish** check box in the **Central Administration** page of the user interface. A configuration file called `fpcommands.xml` is created in the global downloads folder in the central administration area.

What to do next

If you will use the file to change configuration after an initial installation, do not rename the file. Tivoli Continuous Data Protection for Files pulls configuration data only from a file named `fpcommands.xml`.

To use the published configuration settings when starting the installer, rename the file to `fpa.txt` and place it in the `\System32\` folder in the Windows installation folder.

To use the published configuration settings after an initial installation, place the `fpcommands.xml` file in the downloads folder of the Tivoli Continuous Data Protection for Files client that will use these settings.

If you use the configuration file for a push installation, do not configure a forced backup. If you force a backup on a pushed installation, Tivoli Continuous Data Protection for Files attempts to back up files in the system context. These backups can fail, and when a logged on user later attempts to restore these files the restore can fail. To avoid a forced backup, do not check the **Run Scan Now on other computers** check box in the **Central Administration Settings** window.

Windows installation folder

The Tivoli Continuous Data Protection for Files client references the Windows installation folder during installation. During the installation, the client can get configuration information from the file named `fpa.txt`, `dsm.opt` or `networks.xml` files in the `\System32\` subfolder in the Windows installation folder.

The Windows installation directory is also known by the environment variable %WINDIR%, and as shared drive ADMIN$. Typically, the Windows installation directory is `C:\Windows`.

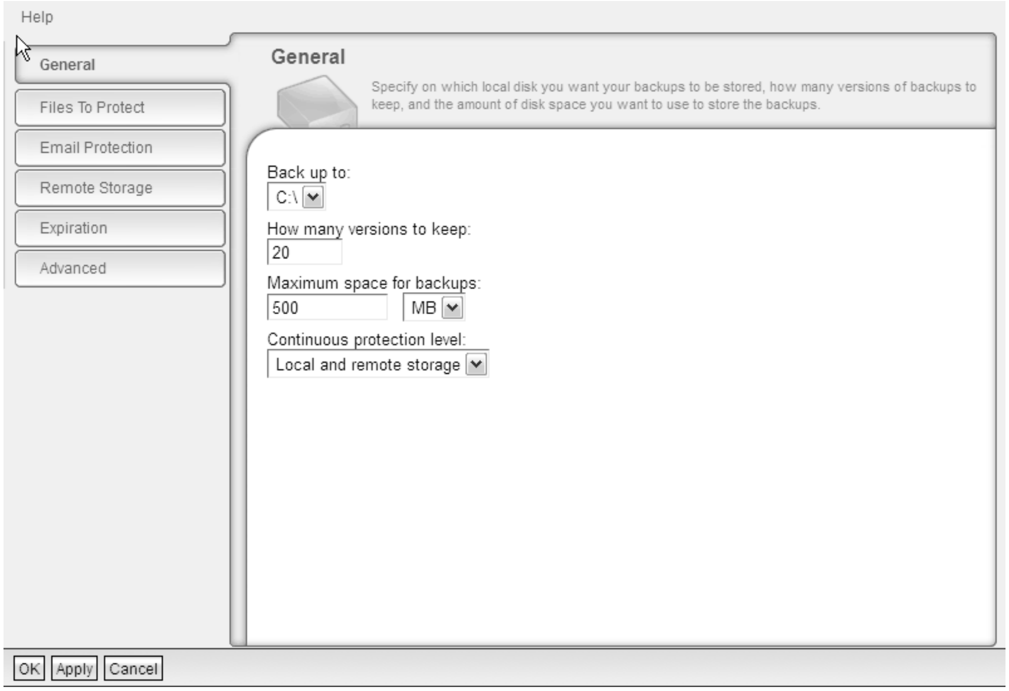
You can also use the **`CUSTOM_CONFIG_FILES_PATH`** install parameter to specify another directory path for the configuration files.

Chapter 3. Changing Protection Settings

When you initially install the Tivoli Continuous Data Protection for Files client, the Initial Configuration Wizard guides you to set your protection settings. After installation, you can change your protection settings with the Settings Notebook. If you are managing other Tivoli Continuous Data Protection for Files clients, see alsoChapter 8, "Tivoli Continuous Data Protection for Files central management considerations," on page 97. If you are managing a server, see also Chapter 9, "Protecting a server with Tivoli Continuous Data Protection for Files," on page 107.

Settings Notebook

After the initial installation and configuration, you can change your protection settings with the Settings Notebook.



General

Specify on which local disk you want your backups to be stored, how many versions of backups to keep, and the amount of disk space you want to use to store the backups.

Back up to: C:\

How many versions to keep: 20

Maximum space for backups: 500 MB

Continuous protection level: Local and remote storage

Open the Settings Notebook by clicking **Settings** from the menu of the Tivoli Continuous Data Protection for Files Status panel.

Use the tabs to navigate to any panel whose settings you want to change. Click the **OK** button to apply your new settings and return to the Tivoli Continuous Data Protection for Files Status panel. Click the **Apply** button to apply your new settings and stay in the Settings Notebook. Click the **Cancel** button to exit the Settings Notebook without applying your changes.

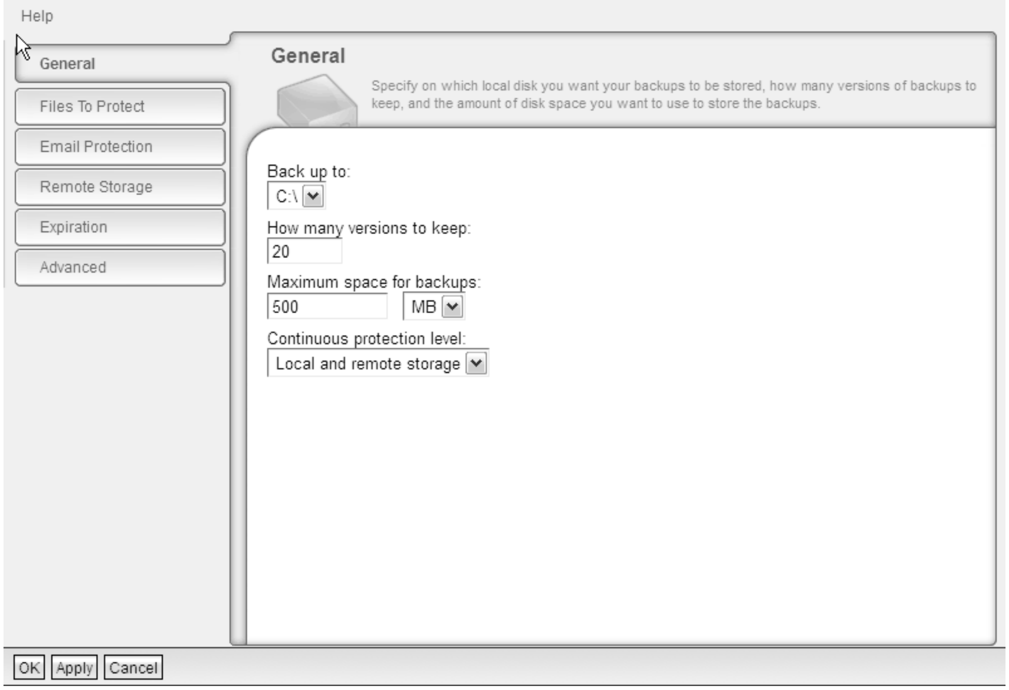
The Settings Notebook has six panels:

- Use the "**General** panel of client Settings Notebook" on page 33 for these settings:
  - Which drive to use for your local storage area.

  - How many versions of protected files to keep on local storage area.
  - The maximum size of your local storage area.
  - Whether you want to store backup copies on local storage area, remote storage area, neither, or both.
- Use the “**Files to Protect** panel of client Settings Notebook” on page 34 to specify:
  - Which folders and files to continuously protect.
  - Which folders to vault.
  - A forced backup of all protected files when you change which files are continuously protected.
- Use the “**E-mail Protection** panel of client Settings Notebook” on page 45 for your email protection settings, including the schedule to protect your email and all files that are backed up on a schedule. You can also specify how many versions of the email files to keep.
- Use the “**Remote Storage** panel of client Settings Notebook” on page 46 to specify:
  - A backup identifier name to help you find the backup on the remote server during the recovery process of an existing machine.
  - A remote storage area.
  - How many versions of protected files to keep on the remote storage area.
  - The maximum size of your remote storage area.
  - Whether to encrypt, compress, or use sub-file copy for backup copies stored on a remote storage area, depending on what type of remote storage is used.
- Use the “**Expiration** panel of client Settings Notebook” on page 52 to specify:
  - Whether to remove backups of files that were deleted from the backed up computer.
  - How long to keep copies of deleted files before they are removed from the remote storage.
  - How often to check for deleted files to be removed from the remote storage.
- Use the “**Advanced** panel of client Settings Notebook” on page 52 to specify:
  - Whether to allow program messages to display.
  - Performance settings include:
    - Maximum size of file to protect on local storage area.
    - Maximum size of file to protect on remote storage area.
  - The Advanced panel contains a link to set your scheduled backups. Follow the link to:
    - Choose which files to back up on a schedule.
    - Start a backup of your scheduled files immediately.
    - View reports of your scheduled backups.
  - The Advanced panel also contains a link to manage the throttle settings. Follow the link to:
    - Manage the network rules settings.
    - Manage bandwidth usage.
    - Define throttle speed.

General panel of client Settings Notebook

Use the **General** panel to choose the local storage area for the backup copies of your continuously protected files. Choose the storage location and space, and how many versions of protected files you want to keep.



General

Specify on which local disk you want your backups to be stored, how many versions of backups to keep, and the amount of disk space you want to use to store the backups.

Back up to: C:\

How many versions to keep: 20

Maximum space for backups: 500 MB

Continuous protection level: Local and remote storage

Back up to: drop-down list

Choose the location to store your local backup copies. Local backup copies are stored in a folder on one of your local drives. The default configuration is the non-removable local drive which has the most free space.

Note: Select a non-removable drive. Only non-removable drives can be used as the storage location for local backup copies.

Tivoli Continuous Data Protection for Files creates backup copies in a subfolder named `\RealTimeBackup\`. For example, if the local storage area is configured as the `C:\` drive, backup copies are stored in `C:\RealTimeBackup\`.

Note: The drive selected in the **Back up to:** area specifies the location where the backup copies are stored. The **Back up to:** location does not specify the files and folders to protect.

How many versions to keep: field

Tivoli Continuous Data Protection for Files can save more than one backup version of each file. When you restore a file, you can choose which version of the file you want to restore. When the configured number of versions is reached, older versions of a file are deleted. Keeping more versions requires more storage space, but allows you more choices when restoring a file.

Maximum space for backups: field

Specify how much space to use for all backup copies on local storage. When the storage area becomes full, older versions of files are deleted until the storage area is at about 80 percent of the configured maximum. If, after deleting all versioned backup copies, local storage space is still insufficient, Tivoli Continuous Data Protection for Files will delete the oldest non-versioned files.

Note: No warning message is shown when the maximum space is reached.

The default space for local backups is 500 MB.

During a forced backup of all protected files, Tivoli Continuous Data Protection for Files can use more space than you configured for local storage. (A forced backup of all files occurs during the initial backup when you install Tivoli Continuous Data Protection for Files, and when you check the **Back up with new settings** box in the Settings Notebook). The excessive space condition is only temporary. After the forced backup of all files is complete, the first time you change a protected file, Tivoli Continuous Data Protection for Files purges files from the local storage area, if necessary, to meet the space you configured.

Note: If you try to back up a file which is larger than the allocated space for your storage area, Tivoli Continuous Data Protection for Files purges all older versions of your files, and then fails to back up the file. Make sure that the maximum space for your storage areas is greater than the file size limit in the **Advanced** panel of the Settings Notebook.

Continuous protection level: drop-down list

Tivoli Continuous Data Protection for Files offers two levels of protection for your files: continuous protection and scheduled protection. See “Types of protection” on page 2 for a discussion of these two types of protection.

Use this box to select which storage areas to use for continuously protected files.

None Files are not protected.

Local storage only
Tivoli Continuous Data Protection for Files creates backup copies only on the local storage area.

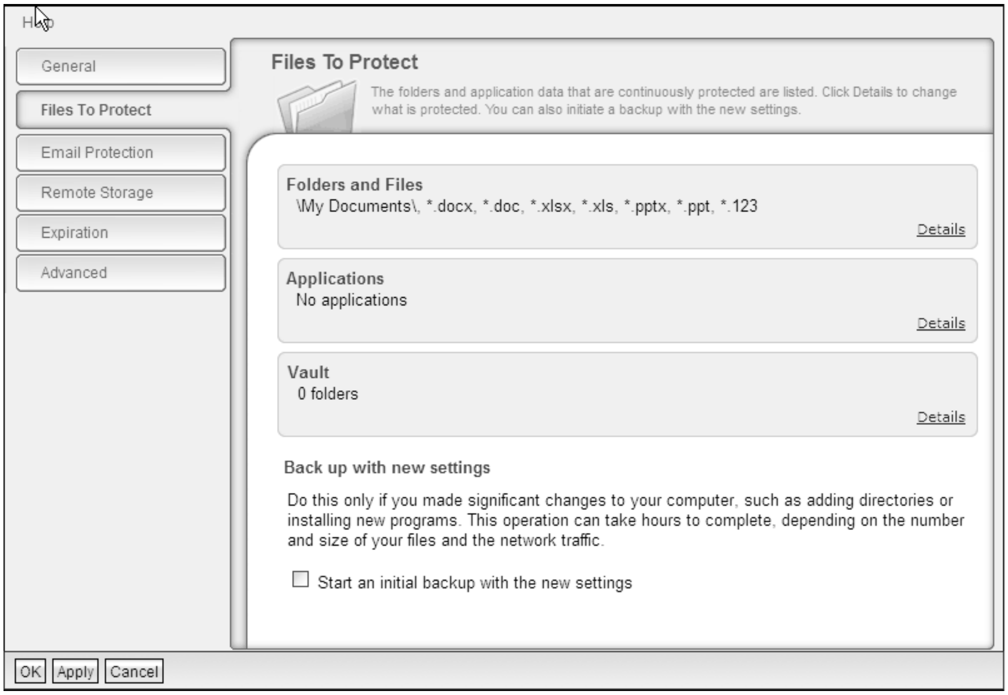
Remote storage only
Tivoli Continuous Data Protection for Files creates backup copies only on the remote storage area.

Local and remote storage
Tivoli Continuous Data Protection for Files creates backup copies on both the local and remote storage areas. This provides the most protection for your files, and is the default choice.

Files to Protect panel of client Settings Notebook

Select the files and folders that you want to continuously protect, and the files and folders you want to vault.

You can specify the files to protect by using **Folders and Files** and **Applications**. You can also specify those folders that you want to vault. Vaulted folders cannot be modified nor deleted.



Files To Protect

The folders and application data that are continuously protected are listed. Click Details to change what is protected. You can also initiate a backup with the new settings.

Folders and Files
\My Documents\, *.docx, *.doc, *.xlsx, *.xls, *.pptx, *.ppt, *.123
Details

Applications
No applications
Details

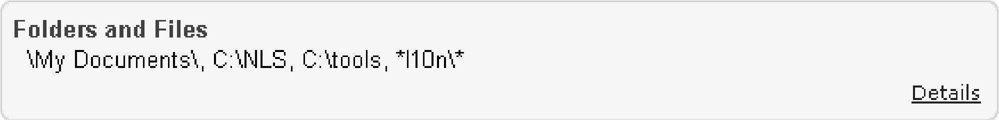
Vault
0 folders
Details

Back up with new settings

Do this only if you made significant changes to your computer, such as adding directories or installing new programs. This operation can take hours to complete, depending on the number and size of your files and the network traffic.

☐ Start an initial backup with the new settings

Folders and Files box (Settings Notebook) of Tivoli Continuous Data Protection for Files



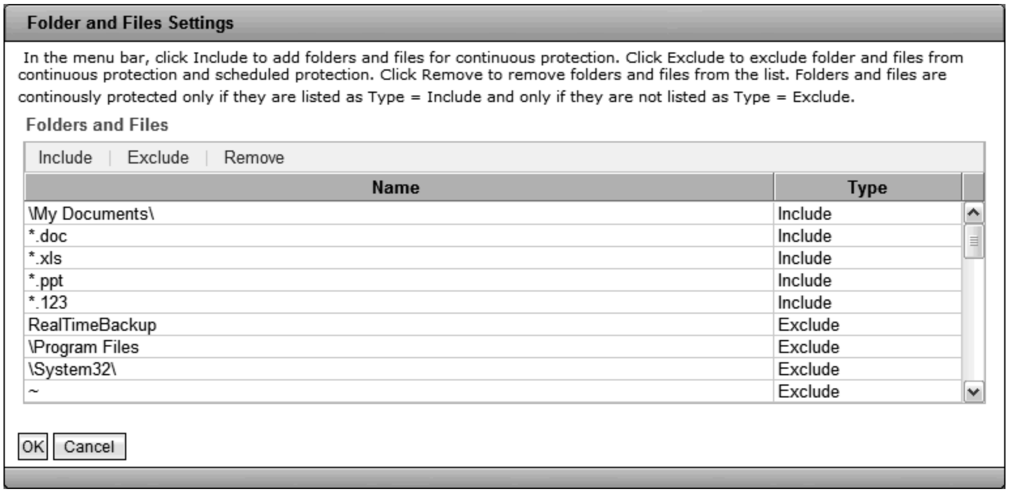
Folders and Files
\My Documents\, C:\NLS, C:\tools, *l10n*
Details

This box gives a summary of the folders and files that are continuously protected. The number of items protected refers to the items in the list of folders and files. A single list item can specify more than one file. Click the **Details** link to view all items in the list and modify the list. The **Folders and Files Settings** dialog will display.

Folders and Files Settings page for continuous protection by Tivoli Continuous Data Protection for Files:

Specify which folders and files to continuously protect by selecting the files to include and exclude.

List of Folders and Files to Include and Exclude



Folder and Files Settings

In the menu bar, click Include to add folders and files for continuous protection. Click Exclude to exclude folder and files from continuous protection and scheduled protection. Click Remove to remove folders and files from the list. Folders and files are continously protected only if they are listed as Type = Include and only if they are not listed as Type = Exclude.

Folders and Files

Name	Type
\My Documents\	Include
*.doc	Include
*.xls	Include
*.ppt	Include
*.123	Include
RealTimeBackup	Exclude
\Program Files	Exclude
\System32\	Exclude
~	Exclude

You can include and exclude or remove an item from the list:

Include
Click **Include** to add files and folders that you want to continuously protect.

Exclude
Click **Exclude** to add files and folders that you want to exclude from continuous and scheduled protection.

Remove
Select a list item, and then click **Remove** to remove that list item.

The list contains these columns:

Name Patterns in the **Name** column specify one or more files or folders. See “Wildcards in file specifications” on page 11 to determine what files and folders match a **Name** pattern with blanks or asterisks. When a folder is protected, all of its files and subfolders are protected.

Type Values in the **Type** column indicate whether the files and folders should be included or excluded from protection. Files and folders that are excluded from continuous and scheduled protection. Files that are included are protected. Files that are excluded have precedence over files that are included. As a result, any file or folder that matches an exclude pattern are not protected, even if the same file or folder matches an include pattern. (See “Including and excluding files from protection” on page 37).

Note: The Initial Configuration Wizard. However, the Initial Configuration Wizard only allows file additions (of type Include). Any exclude patterns exclude files from protection as soon as Tivoli Continuous Data Protection for Files is installed, but they are hidden from view during installation. Although exclude patterns are exposed in the Settings Notebook, you can specify advanced configuration options.

Protected drives:

All files that meet the include and exclude specifications, and that appear to Tivoli Continuous Data Protection for Files as internal drives, are protected.

In some cases, an external USB drive looks like an internal drive, and Tivoli Continuous Data Protection for Files tries to protect the files on that drive. If you do not want to protect that drive, add the drive letter to the exclusion list so that all files on the USB drive are excluded from protection. For example, if your `E:` drive is a USB drive, add `E:\` to the list of excluded items.

Including and excluding files from protection:

Protected files are specified by including files and by explicitly excluding files.

Continuous and scheduled protection (not vaulted)

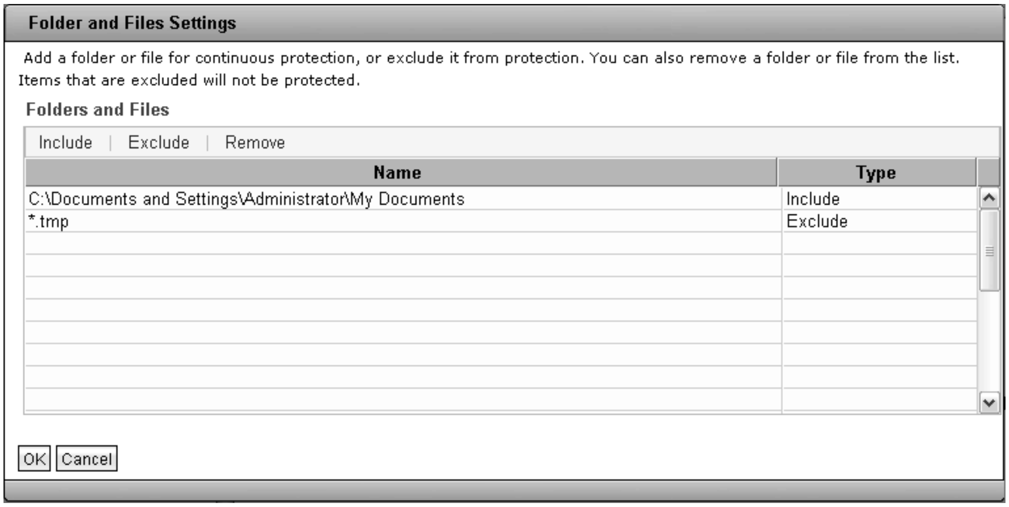
Tivoli Continuous Data Protection for Files keeps a list of files that are included for protection, and a list of files that are explicitly excluded from protection. The list of included files is separated into those files that are included for continuous protection, and those files that are included for scheduled protection. If a file is excluded, it is excluded from both continuous and scheduled protection.

- A file is on the include list for continuous protection if it is defined as type **Include** in the **Folders and Files** box, or if it is defined in the **Applications** box. Both of these boxes are in the **Files to Protect** panel in the Settings Notebook of the client.
- A file is on the include list for scheduled protection if it is defined in the **Email Protection** panel or the **Scheduled Backup Settings** link in the **Advanced** panel in the Settings Notebook of the client.
-
- A file is on the exclude list if it is defined as type **Exclude** in the **Folders and Files** box in the **Files to Protect** panel in the Settings Notebook of the client.
-
- If a file (or folder) is on the exclude list, it is not protected by continuous protection or by scheduled protection. Even if the file or folder is also on an include list, it is not protected.
- If a file is on an include list and not on the exclude list, it is protected.
- If a file is not on an include list, it is not protected.
- It is possible that a file can be on both the include list and the exclude list.

Table 1 summarizes the interaction of inclusion and exclusion.

Table 4. Inclusion and exclusion. File protection by Include list and Exclude list.

	File is not specified in Include list.	**File is specified in Include list.**
File is specified in Exclude list.	File is not protected.	File is not protected.
File is not specified in Exclude list.	File is not protected.	File is protected.



Add a folder or file for continuous protection, or exclude it from protection. You can also remove a folder or file from the list. Items that are excluded will not be protected.

Name	Type
C:\Documents and Settings\Administrator\My Documents	Include
*.tmp	Exclude

Assume that the **Folders and Files** box includes only `\My Documents\`, and explicitly excludes only `*.tmp`. The result is that any files with `.tmp` file extension in `\My Documents\` folder is not protected. All other files in `\My Documents\` folder and its subfolders are protected.

As another example, assume the pictured list. If you choose an application in the "Application settings for Tivoli Continuous Data Protection for Files" on page 40 that typically creates files with extension `.tmp`, those `.tmp` files are not protected.

Tivoli Continuous Data Protection for Files provides a default list of files and folders to be included and excluded. This list excludes from protection various Windows operating system files, the **Program Files** folder, and temporary files.

If you have leading or trailing blank spaces in your file specifications, or if you use wildcards in your file specifications, the specifications in your files list can match more than one folder or file. See "Wildcards in file specifications" on page 11 for an explanation of how specifications match file and folder names.

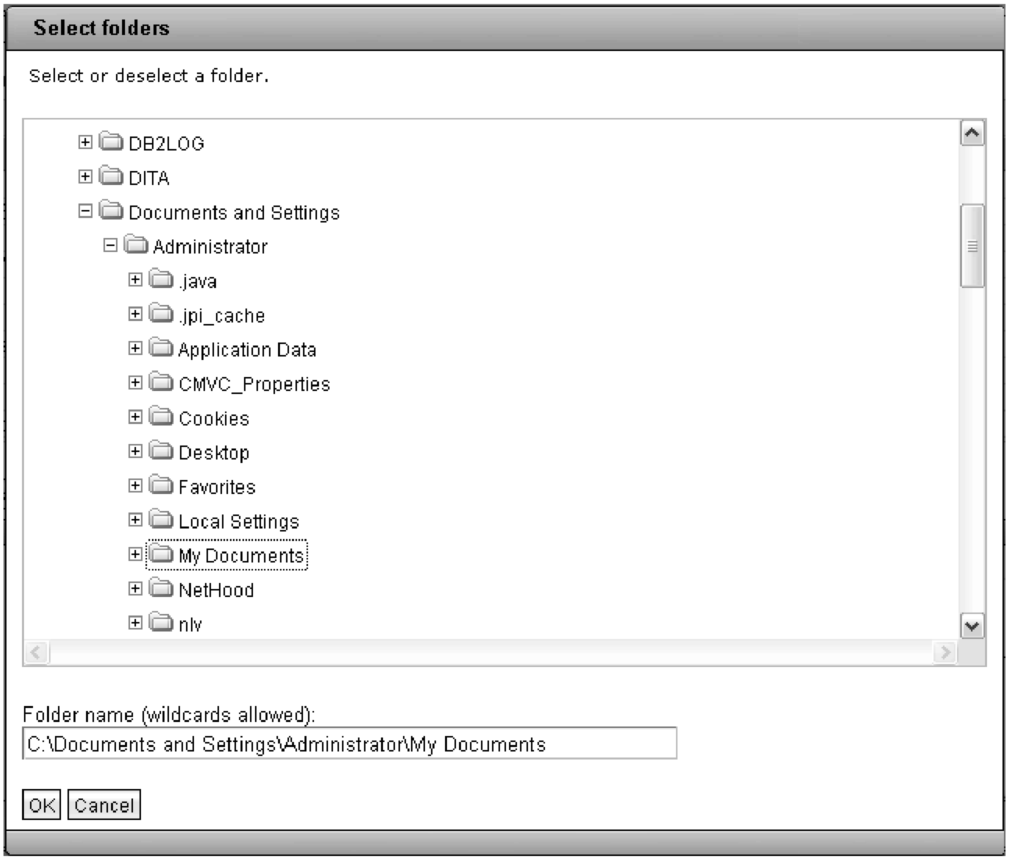
For example, consider a small variation to an excluded specification: `\temp\`. If you use instead `\temp` (without the closing folder delimiter), there is a different effect. This small change has a potentially large impact. All files which have `\temple`, `\temptation\`, `\temperature\`, `\template\`, and other variations of `\temp*`, would be excluded from protection.

Consider another example. You choose to exclude `*.gif` so you can avoid backing up files saved by your browser when you open different websites. This specification also excludes all `.gif` files in `\My Pictures\` folder.

Vaulted folders

Vaulted folders, and the files in them, are not affected by the lists of files that are included for continuous or scheduled protection. However, excluded files and folders are not vaulted. All files that you define in the **Vault settings** dialog in the **Files to protect** panel of the Settings Notebook of the client are vaulted, unless they are excluded items.

Select folders page of Tivoli Continuous Data Protection for Files:



Folder name (wildcards allowed): C:\Documents and Settings\Administrator\My Documents

Specify files and folders in the **Select folders** page. You can browse to select a folder, or type the name of a file or folder in the **Folder name**.

Important: Only your internal drives can be protected. Any external storage devices are considered remote storage devices.

Wildcards in file specifications:

You can use wildcards to specify the files that you want to protect.

You can enter the complete path of a file that you want to protect. For example, `C:\Documents and Settings\Administrator\My Documents\Soccer\2005AYSO\Parent Info U8B.doc`. The complete path must match a single file. You can use asterisks and blanks as wildcards to specify several files.

An asterisk matches any number of characters in a file path. If there are no asterisks, Tivoli Continuous Data Protection for Files matches any file whose fully expanded path name has that exact pattern anywhere in the path or filename. The pattern is not case-sensitive.

If there are no asterisks, blank spaces before and after the pattern are interpreted as asterisks. For example, `\myDocs\` and `*\myDocs\*` yield the same matches. If there are asterisks in the pattern, blank spaces before or after the pattern match no characters. For example, `\myDir\`, `*\myDir\`, and `\myDir\*` can yield three different matches.

For example, assume a pattern `fish`. This pattern matches: `C:\dir\fish.doc` and `C:\fish\anyfile.doc` and `c:\Dirfishfood\something`.

If the pattern has slashes around it (`\fish\`), it matches any object with `\fish\` somewhere in the path. This pattern matches `C:\fish\anyfile.doc` but not `C:\dir\fish.doc` and not `c:\Dirfishfood\something`.

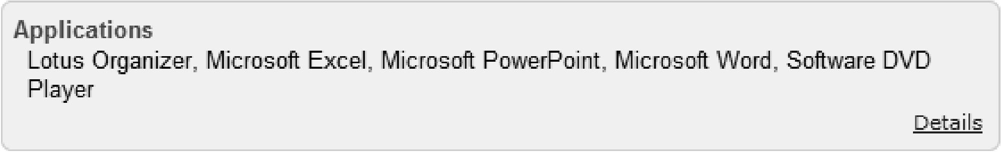
This table provides examples of how patterns match files and folders.

Table 5. File and folder pattern matches

This pattern ...	**... matches these folders and files on your computer:**
\myDir\ or \mYdiR\ or *\myDir* or *\mydir*	c:\myDir\ c:\myDir\Contacts\ c:\myDir\Contacts\contacts.txt c:\Projects\myDir\ c:\Projects\myDir\myThings\ c:\Projects\myDir\myThings\things.doc c:\Projects\myDir\myThings\myPhoto.jpg d:\Notes\myDir\
*\myDir\	c:\myDir\ c:\Projects\myDir\ d:\Notes\myDir\
d:*\mydir*	d:\Notes\myDir\
\my best	c:\Books\My Best.doc c:\Photos.jpg\My Best Photo\ c:\Photos.jpg\My Best Photo\Best.jpg f:\Projects\My Best Project\ f:\Projects\My Best Project\Dream.xls
.jpg	c:\Photos.jpg\ c:\Photos.jpg\myHouse.bmp c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
*.jpg	c:\Photos.jpg\ c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
E:\ E:\*	All files and folders on the E: drive.

Applications box (Settings Notebook) of Tivoli Continuous Data Protection for Files

This box gives a short list of the applications that are protected.



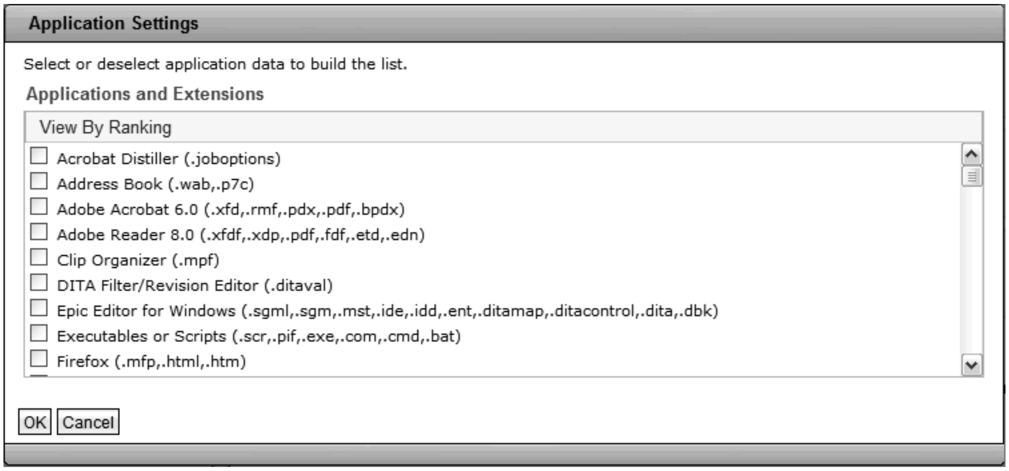
Applications

Lotus Organizer, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Software DVD Player

To see the complete list of the applications that are protected, click **Details**. The **Application Settings** dialog will display.

Application settings for Tivoli Continuous Data Protection for Files:

Specify a list of applications to protect.


Application Settings

Select or deselect application data to build the list.

Applications and Extensions

View By Ranking

☐ Acrobat Distiller (.joboptions)
☐ Address Book (.wab,.p7c)
☐ Adobe Acrobat 6.0 (.xfd,.rmf,.pdx,.pdf,.bpdx)
☐ Adobe Reader 8.0 (.xfdf,.xdp,.pdf,.fdf,.etd,.edn)
☐ Clip Organizer (.mpf)
☐ DITA Filter/Revision Editor (.ditaval)
☐ Epic Editor for Windows (.sgml,.sgm,.mst,.ide,.idd,.ent,.ditamap,.ditacontrol,.dita,.dbk)
☐ Executables or Scripts (.scr,.pif,.exe,.com,.cmd,.bat)
☐ Firefox (.mfp,.html,.htm)

The **Applications and Extensions** lists applications and their associated file extensions. When an application is checked, all files with the associated extensions are protected. For example, when Adobe Acrobat is checked, all files with extension `.xfd`, `.rmf`, `.pdx`, `.pdf`, and `.bpdx` are protected. You can check and clear applications to suit your protection needs.

The list of applications has two views. Each view orders the applications in a different way.

View by Ranking
The applications that have the greatest quantity of files on your computer are presented at the start of the list. The applications that have the least quantity of files on your computer are presented at the end of the list.

View Alphabetically
The applications are presented in alphabetical order.

If you check a box, all file extensions associated with that application are added to the list of protected files.

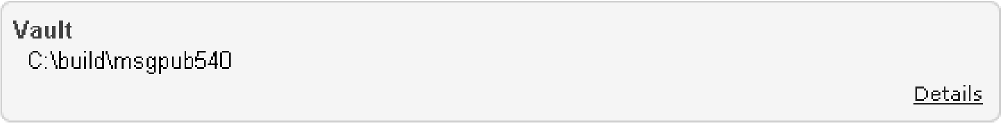
If you clear a box, all files with that extension are removed from the list of protected files. Removing file extensions from the list of protected files does not mean adding those files to the list of files that are explicitly excluded from protection.

Click **OK** in any of the views to update the list of protected files. Click **Cancel** to leave the dialog without changing the list of protected files.

You can add files to be protected in the **Application Settings** dialog, but these applications are protected only if the files are not explicitly excluded. For more information, see "Including and excluding files from protection" on page 37.

Vault box of Tivoli Continuous Data Protection for Files

Displays a summary of vaulted folders.

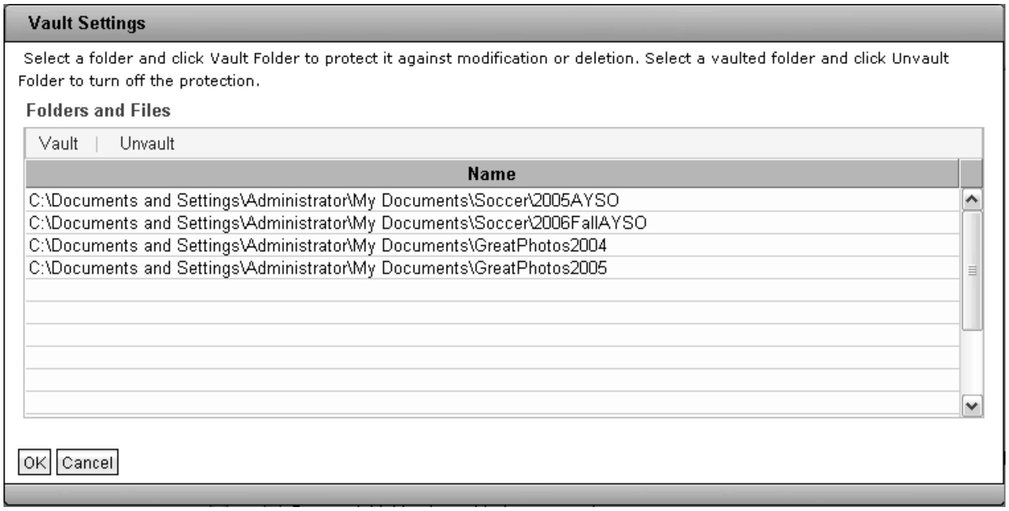

Vault

C:\build\msgpub540

To change the folders that are protected, click **Details**.

Vault Settings dialog of Tivoli Continuous Data Protection for Files:

Specify a list of folders. All files in that folder and all subfolders will be protected from being changed or deleted.



Select a folder and click Vault Folder to protect it against modification or deletion. Select a vaulted folder and click Unvault Folder to turn off the protection.

C:\Documents and Settings\Administrator\My Documents\Soccer\2005AYSO
C:\Documents and Settings\Administrator\My Documents\Soccer\2006FallAYSO
C:\Documents and Settings\Administrator\My Documents\GreatPhotos2004
C:\Documents and Settings\Administrator\My Documents\GreatPhotos2005

Vaulted folders cannot be modified nor deleted. Files can be added to the folder, but the files in the folder cannot be changed nor deleted.

The **Folders and Files** box lists the files that are protected by vault.

Click **Vault** to open a browser to choose files to protect.

Click **Unvault** to remove vault protection from the selected folder, and all its files and sub-folders.

The **Include** items from other dialogs does not affect the list of vaulted folders. However, items in the **Exclude** list will not be vaulted. All folders in the **Vault settings** dialog will be vaulted, unless they are excluded.

Click the **OK** button to add your changes to the pending settings updates.

Note: The configured settings are not applied until you click the Settings Notebook **OK** or **Apply** button

Click the **Cancel** button to exit the dialog without applying changes.

Vault duration:

You can specify the duration of vaulting by using special folder names. Files in these folders are vaulted for a specific period of time and after that time the files are not vaulted.

To specify duration of vaulting, create a folder named `\KeepSafe\` in any vaulted area. In the `\KeepSafe\` folder, create folders that indicate the vaulting period. For example, `C:\MyImportantDir\KeepSafe\Retain 3 years\`. Any file created in that folder are prevented from alteration or deletion for three years. After the expiration time, the file is no longer vaulted. There are three ways to indicate the vaulting period. Each way requires that you use a keyword in the folder name.

1. **`\KeepSafe\RetainForever\`**

   Files in this folder are vaulted forever. Such material can never be moved to another folder with shorter vaulting duration. Material can be moved within the folder tree and to other folders of the same duration.

2. **`\KeepSafe\Retain Duration\`**

   Specify exact vaulting periods using English terminology. Duration is specified by a combination of the following time units:

   Years
   Days
   Hours
   Minutes
   Seconds

   Use 1 or more time units. Each time unit you use must be preceded by a number up to five digits long. You can include spaces or underlines or dashes and mix case in the folder name. The following are valid examples:

   \Retain23days4hours\
   \Retain 3years\
   \Retain_3years\
   \Retain-23DAYS_4minutes\
   \Retain 1000 days\

3. **`\KeepSafe\RetainUntil Date\`**

   Specify a date after which the vaulting expires. The date must include year, month, and day in the following format: yyyymmddhhmmss. The hours, minutes, and seconds are optional. The default time is 00:00:00. The following are valid examples:

   \RetainUntil20191231235959\
   \RetainUntil 20200101\
   \RetainUntil20200101\
   \RetainUntil_20200101\

Note:

You cannot create a `\Retain...` folder within a vaulted `\Retain...` folder.

You cannot move material that is in one vaulted `\Retain...` folder to a `vaulted \Retain...` folder that has an earlier expiration date.

Back up with new settings check box of Tivoli Continuous Data Protection for Files

Scan all drives and back up all files that are configured for protection.

If you changed the specifications for **Folders and Files** or **Applications** to include files that were not previously protected, it is highly recommended that you back up those files now. Check the box to scan and protect all files when you click the Settings Notebook **OK** or **Apply** button.

During a forced backup of all protected files, Tivoli Continuous Data Protection for Files can use more space than you configured for local storage. (A forced backup of all files occurs during the initial backup when you install Tivoli Continuous Data Protection for Files, and when you check the **Back up with new settings** box in the Settings Notebook). The excessive space condition is only temporary. After the forced backup of all files is complete, the first time you change a protected file, Tivoli Continuous Data Protection for Files purges files from the local storage area, if necessary, to meet the space you configured.

A backup is not necessary to activate vault protection. If you changed **Vault** settings, the folders become vaulted when you click the Settings Notebook **OK** or **Apply** button.

Do not check this box if you are creating a configuration file for a push installation. If you use this configuration setting in a push install, the backup copies will be created in the system context. When you later run Tivoli Continuous Data Protection for Files in the user context, you can have problems restoring these files.

When to back up all files:

At certain times, you need to back up all files. Without this backup, some files are not protected.

After the first installation of the Tivoli Continuous Data Protection for Files client, you can immediately back up all files that you configured for protection. In the initial backup, newly created files and existing files that are changed are protected. Existing files that are not changed are backed up after the initial scan is done.

One exception is when you push an installation of Tivoli Continuous Data Protection for Files to a remote computer and do not reboot. If you force a backup on a pushed installation without rebooting, Tivoli Continuous Data Protection for Files attempts to back up files in the system context. These backups can fail, and when a logged-on user later attempts to restore these files the restore can fail.

After the initial backup, the typical rate of file changes does not require that you again back up all files immediately. If you change the protection settings to include files that were not previously protected, the files need to be backed up. Until you change these files, and without a forced backup, Tivoli Continuous Data Protection for Files does not back up these files. To protect these files, you must force a backup of all files.

If you do not change the configuration but make large changes to the files that are configured for protection, you must force a backup of all files. You need to force a backup when you add a new drive that contains files configured for protection.

A forced backup causes Tivoli Continuous Data Protection for Files to scan all local drives looking for files that you designated for protection. Every file in every directory will be investigated, and all files that meet the include, exclude, and size criteria are copied to the local, remote or both storage areas. The creation of backup copies may take several hours. It also takes significant processing resources. Plan the backup at a time when you do not need computing resources for other activities.

When the scan and backup complete, Tivoli Continuous Data Protection for Files continues to operate in the background without any significant impact on your regular computing activities.

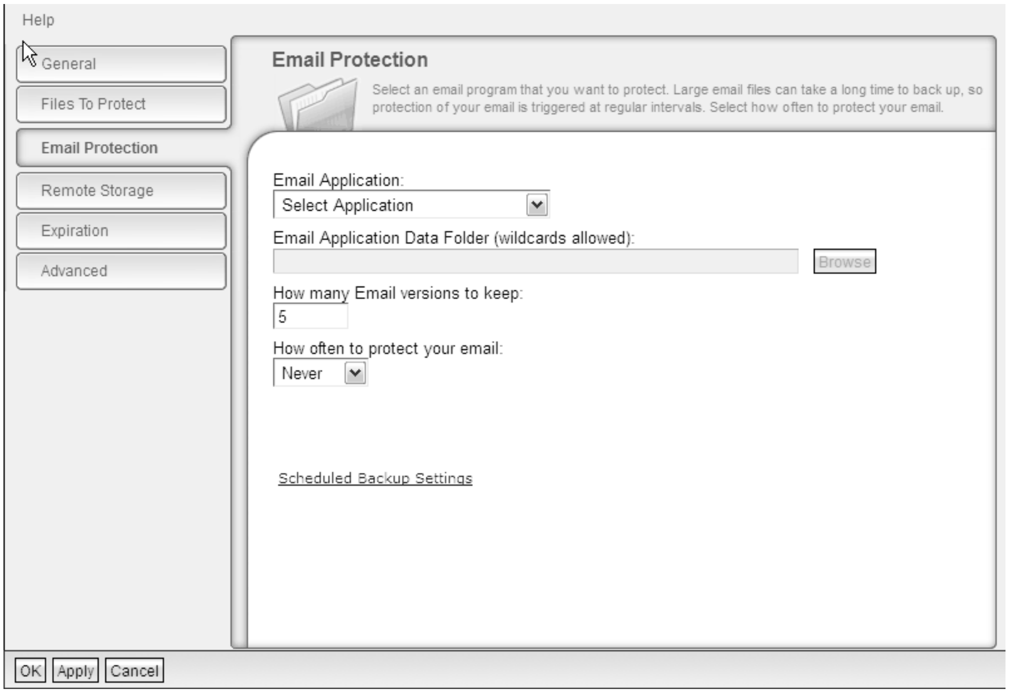
Changing the **Vault** settings does not require a forced backup.

With a client, you can force a backup of your continuously protected files in two places:

- The Initial Configuration Wizard, when you initially configure the Tivoli Continuous Data Protection for Files client
- The **Files to Protect** panel in the Settings Notebook of the client, any time after initial configuration.

E-mail Protection panel of client Settings Notebook

Select the email applications that you want to protect. Select a schedule for protecting the email applications.



Select an email program that you want to protect. Large email files can take a long time to back up, so protection of your email is triggered at regular intervals. Select how often to protect your email.

Email Application: Select Application

How many Email versions to keep: 5

How often to protect your email: Never

Because email files typically are large, they are not backed up continuously, but only on the schedule that you select.

Email files are backed up only to remote storage. If the remote storage is not available at the scheduled backup time, Tivoli Continuous Data Protection for Files backs up the email files when the remote storage area becomes available.

Email Application list

Select one of the email applications in the list.

If your application is not listed, select **Other**.

Email Application Data Folder field

If you choose your email application from the **Email Application** list, the default file type for that application is shown in this box, and you are not able to update the file specification. You can update this field only if you select **Other** in the **Email Application** list.

How Many Email Versions to keep field

This field allows you to specify how many versions of the Email file you want to keep on the remote storage.

How often to protect your email list

You can schedule email protection at one of several intervals:

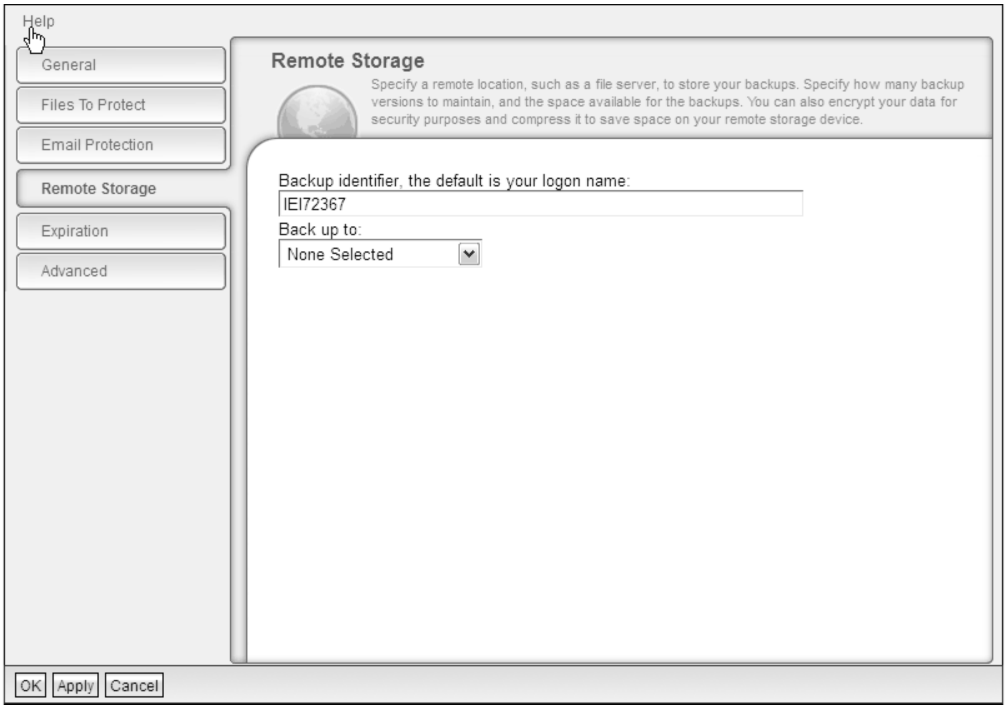
- **Never**: Email is not protected.
- **Hourly**: Email files will be backed up every hour, just after the hour.
- **Daily**: If you choose this interval, also select the time for the backup.
- **Weekly**: If you choose this interval, also select the day and time for the backup.
- **Monthly**: If you choose this interval, also select the day of the month and time for the backup.

Scheduled Backup Settings link

Click the **Scheduled Backup Settings** link to open the **Folders and Files Settings** dialog for scheduled backup.

Remote Storage panel of client Settings Notebook

Use the Remote Storage panel to specify the location of the remote storage for backup files. Ensure to type in a backup identifier to help you to find your backups on the remote server.



Specify a remote location, such as a file server, to store your backups. Specify how many backup versions to maintain, and the space available for the backups. You can also encrypt your data for security purposes and compress it to save space on your remote storage device.

Backup identifier, the default is your logon name: IEI72367

Back up to: None Selected

Storing files in a remote storage area protects the files in case local copies are lost. Backups of continuously protected files, and files protected on a schedule, are stored in the same remote area. Tivoli Continuous Data Protection for Files is tolerant of intermittently available networks. If the remote storage area is temporarily unavailable, Tivoli Continuous Data Protection for Files queues backup copies until the remote storage becomes available.

Remote Storage server or device name and location

Use the Remote Storage page to specify the remote storage server or device and its location for your backup copies. You can also specify how many versions to keep.

Select the type of storage device or server for the backup files to be stored to.

Backup Identifier

In this field, type the name that helps you to identify your backup files on the remote server. The default is your logon name. The backup identifier is only used for recovery purposes, and not for typical file restore. The backup identifier is used to locate the remote server location for a computer when restoring the configuration with the configuration wizard.

Location for the External Device or File Server

Select a file server or removable disk to store the backup copies. The remote device can be another computer (such as network-attached storage or a file server), a remote disk, or a removable disk.

If you choose a remote server in the **Location** field, you can use Universal Naming Convention (UNC) specifications for the file server instead of drive letters. Drive letters can change after you restart the system and often do not reconnect automatically.

If you choose a USB external device, you can select the drive letter. However, removable external device drive letters can change. To configure USB drives for remote storage, see Instructions on how to setup a USB device as the remote backup location., available at https://www.ibm.com/support/docview.wss?uid=swg21245761.

Click **Browse** to view a **Browse for folder** dialog box. Use this dialog box to go to the location for your remote storage area. If this dialog becomes hidden behind other windows, click the task bar to bring it to the front.

Tivoli Continuous Data Protection for Files creates backup copies in a subfolder called `\RealTimeBackup\`*`computer name`*. For example, if a computer name is Computer1, and the remote storage location is configured with the value `\\remote\share`, backup copies are stored in `\\remote\share\RealTimeBackup\Computer1\`.

If you log on to your computer with a user name and password that is also valid on your remote storage location, Tivoli Continuous Data Protection for Files authenticates your credential at that location. If the user name and password is not valid on your remote storage location, you must log on to the network using another account with regular privileges. You can log in interactively by using the **`Net Use`** command.

Some versions of Microsoft Windows use simplified file sharing, which allows one computer to connect to another computer over the network. The resulting connection allows only limited file system capabilities, and inhibits the creation of backup copies. Some information such as access control lists or file streams might be lost. You can disable simplified file sharing on the remote storage area.

WebDAV Server storage location

Some Internet Service Providers (ISPs) provide Web-based Distributed Authoring and Versioning, or WebDAV. With the WebDAV protocol, you can create, change, and move documents on a remote server. The WebDAV protocol is useful for authoring the documents that a web server serves, but can also be used for general web file storage. If your ISP provides WebDAV functions, Tivoli Continuous Data Protection for Files can store backups on a web-based server.

In the **Location** field, enter your WebDAV server location using the following format: `https://MyISP.com/MyAcct`.

When using WebDAV, Tivoli Continuous Data Protection for Files can use the basic authentication method. Because this authentication method sends the password as clear text over the network, the web server is configured to use secure sockets.

Tivoli Storage Manager storage location

Tivoli Continuous Data Protection for Files can store backup copies on a Tivoli Storage Manager server.

In the **Location** field, specify the Tivoli Storage Manager server location, using the following format: *tsm://Host.com*. You can also use an IP address for the server address.

You can use Tivoli Storage Manager server version 6.1 or later with Tivoli Continuous Data Protection for Files.

Configure the Tivoli Storage Manager server before you connect from Tivoli Continuous Data Protection for Files. Register the computer as a Tivoli Storage Manager node. Tivoli Continuous Data Protection for Files prompts you for the password for this node in order to connect to the Tivoli Storage Manager server. For more information about registering a Tivoli Storage Manager node for your computer, see *IBM Tivoli Storage Manager for Windows Administrator's Guide*.

If you specify a Tivoli Storage Manager server as the backup target and you want encryption or compression features applied to the backup, you must specify these options in the `dsm.opt` file in the Tivoli Continuous Data Protection for Files subfolder of the “Program data folder” on page 50.

Restriction: You cannot use a subfile backup feature when the Tivoli Storage Manager server is the backup target.

In addition to backing up data directly to a Tivoli Storage Manager server, you can back up data using a two-stage method. First, use Tivoli Continuous Data Protection for Files to create remote backups on a file server. Then, schedule a Tivoli Storage Manager backup-archive client on that file server to back up the files to a Tivoli Storage Manager server.

Restriction: If you use Tivoli Continuous Data Protection for Files encryption, you cannot use Tivoli Storage Manager compression.

To manage storage space, the Tivoli Storage Manager administrator must grant authority to the Tivoli Storage Manager client node to delete backup copies. For steps to assign authority to delete backup copies, see the topic in the problem determination section: “ Tivoli Storage Manager client node lacks authority to delete backup copies” on page 110.

To avoid problems when using the Tivoli Storage Manager server, see “Files are not backed up to Tivoli Storage Manager server” on page 110.

How many versions to keep

Specify how many backup versions of a file to keep on remote storage.

Tivoli Continuous Data Protection for Files can store more than one backup version of each file. When you restore a file, you can choose which version of the file you want to restore. When the configured number of versions is reached, older versions of a file are deleted. Keeping more versions requires more storage space, but allows you more choices when restoring a file.

Remote Storage advanced settings

Depending on the remote storage location that you specified, use the advanced settings in the Remote Storage page to select to encrypt or compress files. You can specify whether to use subfile copies when backing up larger files.

Tip: The default size for the remote storage area is 40 GB. If you increase the number of backup versions to keep, consider increasing your storage area size. If you are unsure of how much space to allocate, you can monitor the space usage on the Status panel and adjust the version and space settings accordingly.

When the storage space becomes full, Tivoli Continuous Data Protection for Files deletes older backup copy versions of files that have several backup copy versions. If more space is needed for new backup copies, Tivoli Continuous Data Protection for Files deletes backup copies of files to make room for the newest backup copy.

If you try to remotely back up a file that is larger than the space you have allocated, Tivoli Continuous Data Protection for Files purges all older file versions, and the backup might fail. Ensure that the maximum space for your remote storage areas is greater than the maximum file size for remote backup in the **Advanced** page of the Settings Notebook. For example, if you decrease the maximum space for backups to 1 GB, you must decrease the maximum file size for remote backup from the default of 1 GB.

Advanced settings

When storing data onto an external device or file server, you can specify the following advanced settings. Select one option:

- Do not encrypt or compress backups
- Encrypt backups
- Compress backups

When storing data onto an external device or a file server you can choose to use sub-file copy function. Select this option to send only changed portions of a file to remote storage and to reduce network traffic. The changed portions are saved to a separate file on the remote storage.

The preceding options are not available when you use the Tivoli Storage Manager as the remote storage server. If you must encrypt or compress your data, then use the Tivoli Storage Manager server compression or encryption features.

Related information:

Chapter 3, “Changing Protection Settings,” on page 31

Encrypt backups

Set encryption for remote backup copies.

The encryption feature provides extra security on your remote location. The encryptions feature can be useful if multiple people have access to the remote server location, and you need to ensure that data is protected from other users who have access to the remote server.

When you click the button labeled **Encrypt backups**, Tivoli Continuous Data Protection for Files will present a dialog so you can create a password for the encrypted files. This password is required to view or access any files which are backed up by Tivoli Continuous Data Protection for Files. The encrypted password is kept in the “Program data folder.” If the files in the program data folder are lost, you will be prompted to enter a new password.

Once encryption has been enabled, the password is stored. If you disable encryption, then enable again, you are not prompted for a new password.

Tivoli Continuous Data Protection for Files does not support prompted encryption. Hence, if you specify Tivoli Storage Manager server as your remote storage area, you must configure non-prompted encryption in the Tivoli Storage Manager `dsm.opt` options file. In the `dsm.opt` file, use the statement: `encryptkey generate`. See *Tivoli Storage Manager for Windows Backup-Archive Client Installation and User's Guide* for information about setting encryption options in Tivoli Storage Manager `dsm.opt` file. Tivoli Continuous Data Protection for Files supports AES128 encryption but does not support AES56 encryption.

The dsm.opt file is in the “Program data folder.”

Files stored on the local storage area are not encrypted. Files that are compressed can not be encrypted, and the user interface does not allow you to configure both encryption and compression. Files that use sub-file copy can be encrypted.

Tivoli Continuous Data Protection for Files cannot protect backup copies that it has encrypted. This means that Tivoli Continuous Data Protection for Files cannot create encrypted backup copies, and then make backup copies (encrypted or not) of those backup copies.

This is an issue only if you store backup copies on a file server, and then use Tivoli Continuous Data Protection for Files to protect the files on the file server. If you configure Tivoli Continuous Data Protection for Files to encrypt the backup copies to a file server, you must not use Tivoli Continuous Data Protection for Files to protect the encrypted backup copies on that file server. You can use Tivoli Storage Manager or another backup solution to protect the encrypted backup copies on that file server.

You do not have to choose either encryption or compression. By clicking the buttons, you can clear both buttons, and select neither encryption or compression.

Program data folder: The program data folder varies according to the operating system and installation of the Tivoli Continuous Data Protection for Files client. This list indicates the program data folder for each operating system and product version:

Microsoft Windows XP, upgrade from version 2.2
`C:\Program Files\Tivoli\CDP_for_Files\`

Microsoft Windows XP, new installation of version 6.3.0
`C:\Documents and Settings\All Users\Application Data\Tivoli\CDP_for_Files\`.

Note: `\Application Data\` is a hidden folder, and to see it you must modify your view preferences in **Explorer** to show hidden files and folders.

Microsoft Windows Vista, new installation of version 6.3.0
`C:\ProgramData\Tivoli\CDP_for_Files\`.

Note: `\ProgramData\` is a hidden folder, and to see it you must modify your view preferences in **Explorer** to show hidden files and folders.

Microsoft Windows 7, new installation of version 6.3.0
`C:\ProgramData\Tivoli\CDP_for_Files\`.

Note: `\ProgramData\` is a hidden folder, and to see it you must modify your view preferences in **Explorer** to show hidden files and folders.

Compress backups option

Set compression for remote backup copies.

Use compression to save space on your remote storage location. The compression feature is not compatible with the encryption feature. You can use compression or encryption, but not both simultaneously. Files backed up using the compression function must be restored using Tivoli Continuous Data Protection for Files.

If you select both options, subfile copy has precedence. The file that is larger than the minimum for subfile copy is not compressed. Only files smaller than the minimum size for subfile copy are compressed.

You can choose to select neither encryption or compression.

Use sub-file copy option

Set the sub-file copy option for remote storage backup copies.

Initially, an entire file is copied to the storage areas. When sub-file copy is turned on and the file size exceeds the sub-file limit, if the file changes only the changed information is copied to the storage area. The sub-file copies are saved as separate files on the remote storage areas.

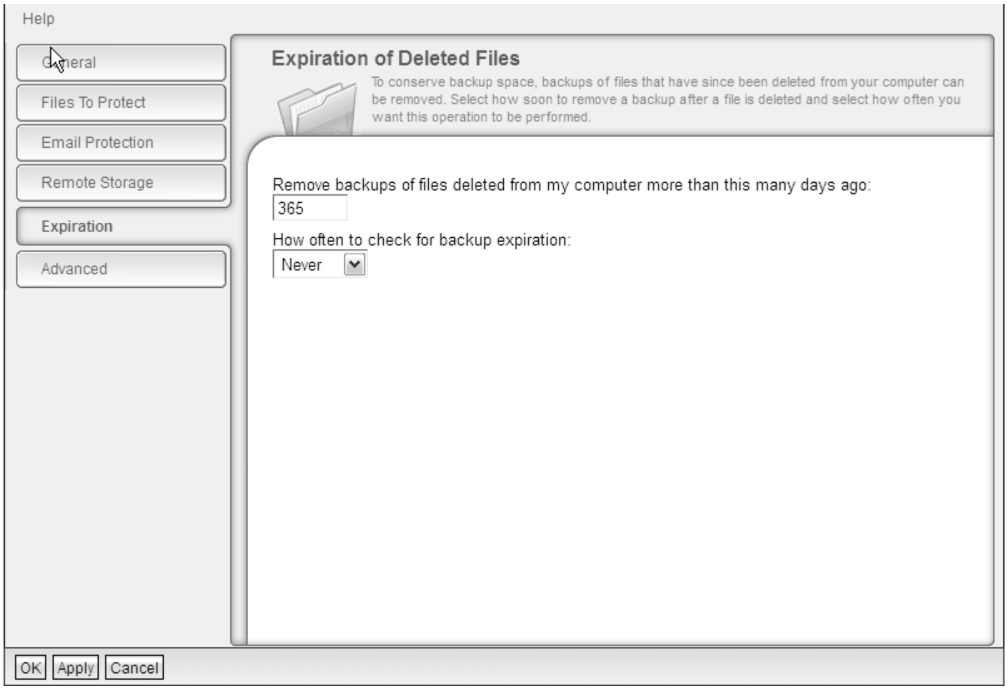
Sub-file copy can significantly reduce the amount of network traffic. However, sub-file copy uses more processing resources on your computer. The default setting is to use sub-file copy for files larger than 50 MB. If you need to conserve more network resources, you can reduce the size setting so sub-file copy is not used on even smaller files.

To use sub-file copy to remote storage, you must have a backup copy of your files on local storage. In the **General** panel of the Settings Notebook, set the **Continuous protection level** field to Local and remote storage. Then you can set the sub-file backup option.

Check the check box to turn on sub-file copy. In the **Use sub-file copy for files larger than** field, specify the file size threshold for using sub-file copy. For files larger than this size, only the changed information is copied to the storage area.

Expiration panel of client Settings Notebook

Specify whether deleted files are removed from the remote backup location.



Expiration of Deleted Files

To conserve backup space, backups of files that have since been deleted from your computer can be removed. Select how soon to remove a backup after a file is deleted and select how often you want this operation to be performed.

Remove backups of files deleted from my computer more than this many days ago: 365

How often to check for backup expiration: Never

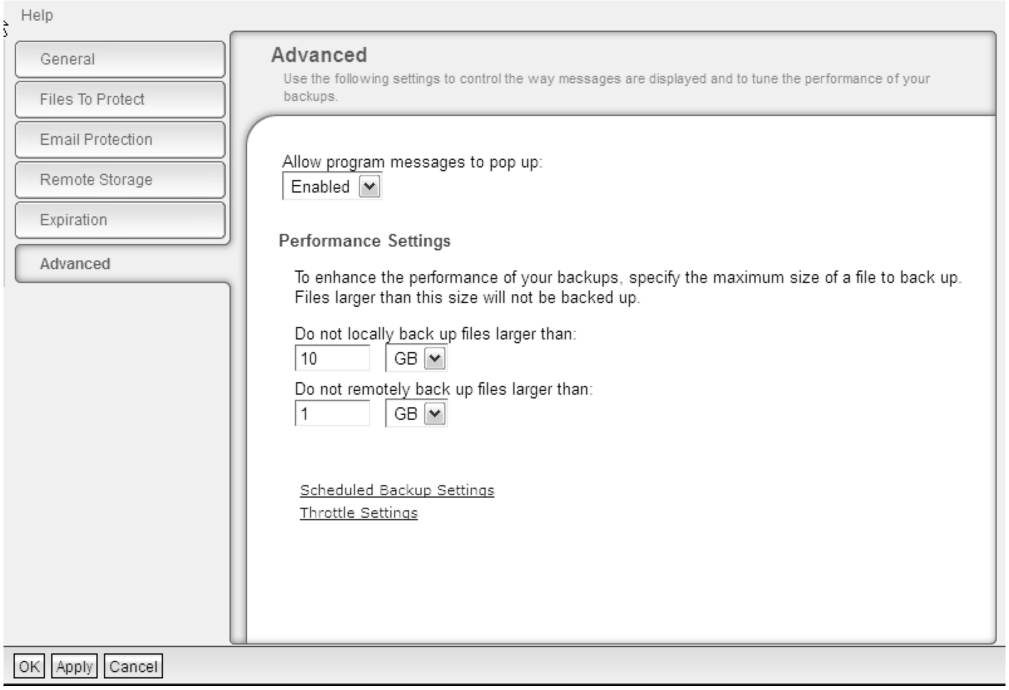
When files are deleted from a computer they are still stored in the backup location on the remote storage. You can use the **Expiration** panel to remove backups of files that were already deleted from the backed up computer. You can specify how long to keep copies of deleted files before they are removed from the remote storage location. It also allows you to set how often to check for files to be removed from the remote storage location.

Enter the number of days to keep backups of deleted files in the `Remove backups of files deleted from my computer more than this many days ago` field.

Specify how often files will be removed from the remote backup location in the `How often to check for backup expiration` field. You can select **Never**, **Daily**, **Weekly**, or **Monthly**. Select **Never** if you do not want deleted files to be removed from the remote backup location.

Advanced panel of client Settings Notebook

The **Advanced** panel allows you to control displaying messages, and to tune performance.



Advanced

Use the following settings to control the way messages are displayed and to tune the performance of your backups.

Allow program messages to pop up: Enabled

Performance Settings

To enhance the performance of your backups, specify the maximum size of a file to back up. Files larger than this size will not be backed up.

Do not locally back up files larger than: 10 GB

Do not remotely back up files larger than: 1 GB

Scheduled Backup Settings

Throttle Settings

Allow program messages to display

For certain types of activities or notifications, Tivoli Continuous Data Protection for Files opens messages from the icon in the system tray. To prevent the messages from opening, select **disabled**.

Note: If messaging is disabled, important program messages regarding the failure of Tivoli Continuous Data Protection for Files operations is suppressed, which may lead to potential loss of data.

Performance Settings

Do not locally back up files larger than
Use this field to specify the size of files that are backed up to your local storage area. If you try to back up a file that is larger than the space allocated, Tivoli Continuous Data Protection for Files purges all older versions of your files, and fails to back up the file. Ensure that the file size limit, and the size limit for files backed up to remote storage, is less than the maximum space for your storage areas.

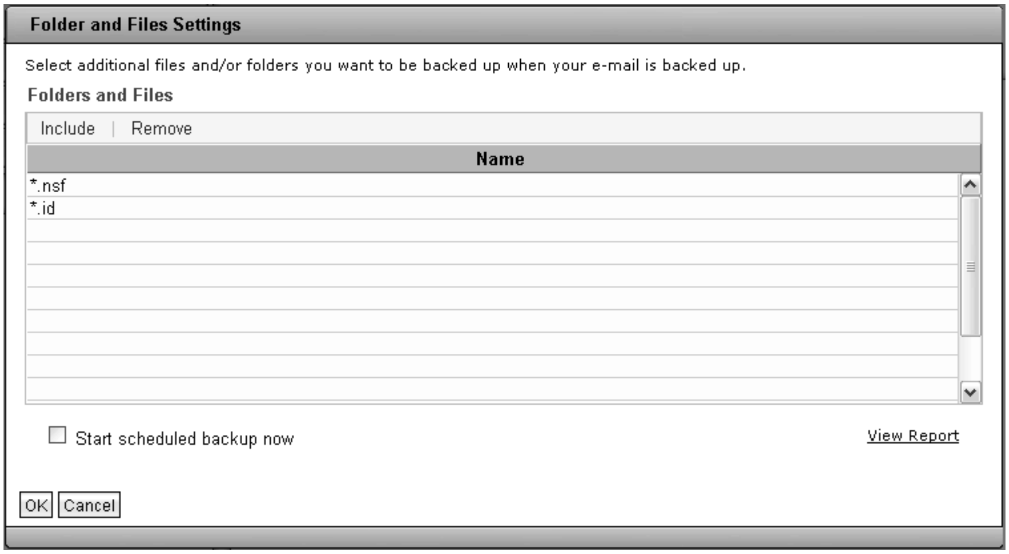
Do not remotely back up files larger than
Use this field to specify the maximum size of files that are backed up to your remote storage area.

Scheduled Backup Settings
Open the Folder and Files Settings by clicking the Scheduled Backup Settings link. You can use this window to create, modify, and remove scheduled backups.

Throttle Settings
Open the Network Rules Settings by clicking the Throttle Settings link. You can use this window to create, modify, and remove network rules.

Folders and Files Settings dialog for scheduled backups by Tivoli Continuous Data Protection for Files

Specify folders and files to back up on the same schedule as email files are backed up.



Folder and Files Settings

Select additional files and/or folders you want to be backed up when your e-mail is backed up.

Folders and Files

Name
*.nsf
*.id

☐ Start scheduled backup now

When considering what files to protect on a schedule, see "Types of protection" on page 2 and "Considerations for scheduled backups" on page 55.

List of folders and files to include

Use Include and Remove to add and remove items from the list.

Include
Click **Include** to open the **Select folders** window and add files to protect.

Remove
Select a list item, then click **Remove** to remove that list item.

Each row in the list has one column.

Name Patterns in the **Name** column specify one or more files or folders. See "Wildcards in file specifications" on page 11 to determine what files and folders match a **Name** pattern with blanks or asterisks. When a folder is protected, all of its files and subfolders are protected.

Starting a scheduled backup

The folders and files that you specify will be backed up on the same schedule as your email backups. If you want to force a backup, check the **Start scheduled backup now** box and click **OK**.

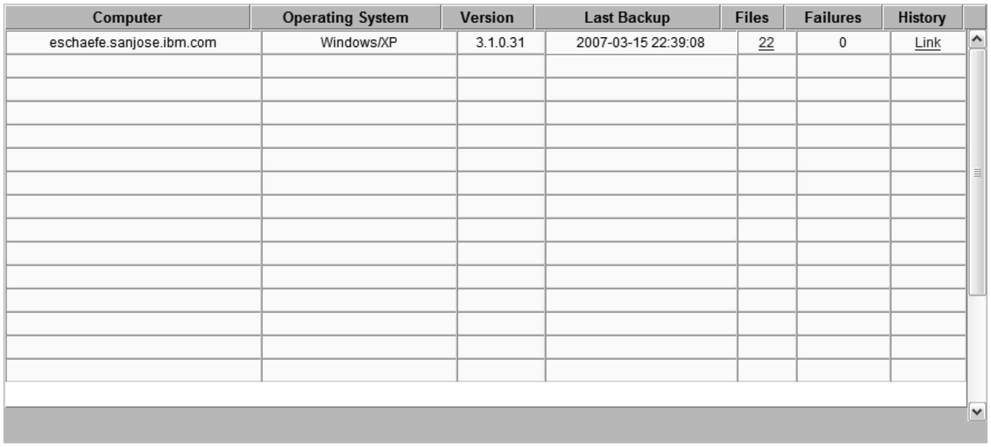
View Report link

Click the **View Report** link to open a table of scheduled backup reports for all computers that share a common central administration folder.

Scheduled backup reports table of Tivoli Continuous Data Protection for Files:

Use the reports table to monitor scheduled backups to remote storage areas.

The reports table shows summary information of all users who back up files to the same remote storage location. Click the links in the table to show more detailed information.



Computer	Operating System	Version	Last Backup	Files	Failures	History
eschaefe.sanjose.ibm.com	Windows/XP	3.1.0.31	2007-03-15 22:39:08	22	0	Link

The scheduled backup reports table gives a summary of scheduled backups to remote storage areas for all computers who share a common central administration folder. For more information about central administration folders, see "Administration folders" on page 101.

To see the reports table, you must be connected to your remote storage area.

Each row identifies the reports associated with one Tivoli Continuous Data Protection for Files client, and contains the following cells:

Version
The version of Tivoli Continuous Data Protection for Files.

Last Backup
The last completed scheduled backup.

Files A number indicating approximately how many files were successfully backed up at the last schedule. Due to the nature of the program and how the logging is done, this number is only an approximation.

Click the number to open a complete report of the scheduled backup. In addition to files backed up, the report shows administrative activities and failed backup attempts.

Failures
This column indicates how many errors there were during the backup.

Click on the number to open a report of the errors during scheduled backup.

History
Click the link to open a list of the historical backup and failure logs. Select the logs to view more information. Only reports that had files backed up are listed as active links.

Considerations for scheduled backups:

Protect appropriate files on a schedule, and prepare the files for backup.

Files that are appropriate to protect on a schedule

Large or frequently saved files can consume considerable computing or network resources when they are backed up. You can schedule periodic backups of these files when the burden on computing or network resources are least inconvenient.

Some files are not often closed and saved, but must be backed up periodically. Files protected by schedule are backed up even if they are open, but you can try to schedule the backup for a time when the files are closed.

Scheduled backup can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but offer fewer opportunities when you want to restore a file.

When does a scheduled backup occur

The files that you select for scheduled protection are backed up at the scheduled time, if they change during the scheduled interval. If a file changed several times during the schedule, only the last version of the file is backed up at the scheduled time.

If the remote storage area is not available at the scheduled backup time, the files that have changed at that time are noted and are backed up when the remote storage becomes available. If a noted file changes after the scheduled backup time, and before the remote storage becomes available, only the last version of the file is backed up.

If the computer is powered off or Tivoli Continuous Data Protection for Files is not running at the schedule time, the scheduled backup runs when the computer is powered on and Tivoli Continuous Data Protection for Files is running.

If you shut down a computer or stop the Tivoli Continuous Data Protection for Files client when a scheduled backup is running, the backup resumes when the client is running again and the remote storage is available.

If you forced a backup of scheduled files during the 30 minutes prior to the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

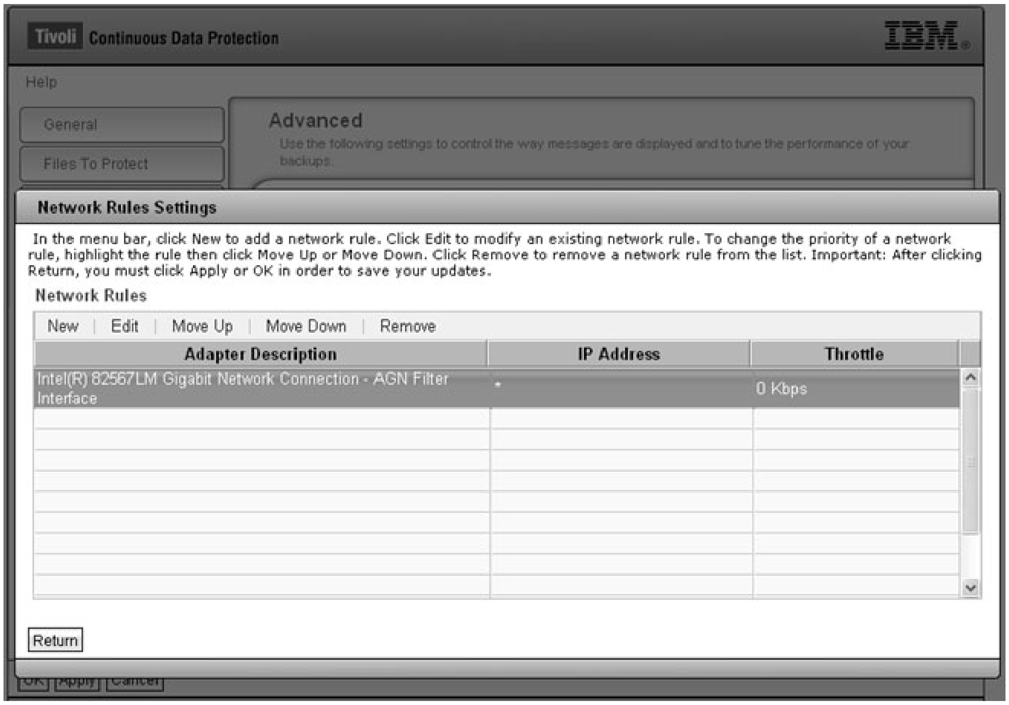
Tivoli Continuous Data Protection for Files backs up all files that have changed during the schedule interval, including files that are still open at the time of backup. The backup copies of files that are backed up while open can be corrupted. So it is suggested that you close applications before a scheduled backup. Tivoli Continuous Data Protection for Files offers an opportunity to close applications before a scheduled backup.

At the beginning of a scheduled backup, Tivoli Continuous Data Protection for Files attempts to close all files that are listed in a text file called `closeapps.txt` in the installation directory. Each line in the file must be a program name, with name and extension, but no folder path. Tivoli Continuous Data Protection for Files sends a close command to each instance of every program named in the `closeapps.txt` file. Note that Tivoli Continuous Data Protection for Files does not send a start command to any of those programs when the scheduled backup is finished.

Specifying throttle settings and network rules for Tivoli Continuous Data Protection for Files

You can modify or create policy rules that manage bandwidth usage in the networks that you have specified.

Use the **Network Rules** settings to manage bandwidth usage for each network. When a network is accessed, Tivoli Continuous Data Protection for Files uses the first rule in the list that matches the network. As a result, the throttle setting does not require a manual update every time Tivoli Continuous Data Protection for Files accesses a different network. When a new network is detected, a default network rule is created. This default rule is added to the end of the network rule list.


Tivoli Continuous Data Protection
IBM
Help
General
Files To Protect
Advanced
Use the following settings to control the way messages are displayed and to tune the performance of your backups.
Network Rules Settings
Network Rules
New | Edit | Move Up | Move Down | Remove
Return
OK Apply Cancel

In the menu bar, click New to add a network rule. Click Edit to modify an existing network rule. To change the priority of a network rule, highlight the rule then click Move Up or Move Down. Click Remove to remove a network rule from the list. Important: After clicking Return, you must click Apply or OK in order to save your updates.

Adapter Description	IP Address	Throttle
Intel(R) 82567LM Gigabit Network Connection - AGN Filter Interface	*	0 Kbps

Using Network Rules

Use the Network Rules window to add new network rules, edit existing network rules, and change the order of network rules listed in the window.

New Click **New** to create a network rule using the **New Network Rules** dialog.

Edit Select a list item, then click **Edit** to modify the value for an adapter, IP address, or throttle setting.

Move Up
Select a list item and click **Move Up** to increase the priority of this rule. When searching for rules to apply to a network, Tivoli Continuous Data Protection for Files searches the list in order from highest to lowest.

Move Down
Select a list item and click **Move Down** to decrease the priority of this rule. When searching for rules to apply to a network, Tivoli Continuous Data Protection for Files searches the list in order from highest to lowest.

Remove
Select a list item, then click **Remove** to remove that network rule from the list.

Create a Network Rule

Use the New Network window to create new network rules and specify the settings of the new rules.

Adapter
Select an adapter from the list. Once selected, the fields in the dialog are auto-filled.

Description
A description of the selected adapter displays. This field cannot be updated.

DNS Suffix
The Domain Name System information is displayed.

IP Address
The IP address associated with the selected adapter displays. To change this value, enter another IP address. You can use an asterisk (*). For example:

```
192.168.*
```

IPv6 Address
If your system supports IPv6, an IPv6 field is displayed with an IP address.

Throttle
Type in the throttle level you want to set, in the Throttle field and select the size (Kbps, Mbps or Gbps) from the dropdown menu.

Click OK to create the network rule, or click Cancel to cancel the operation.

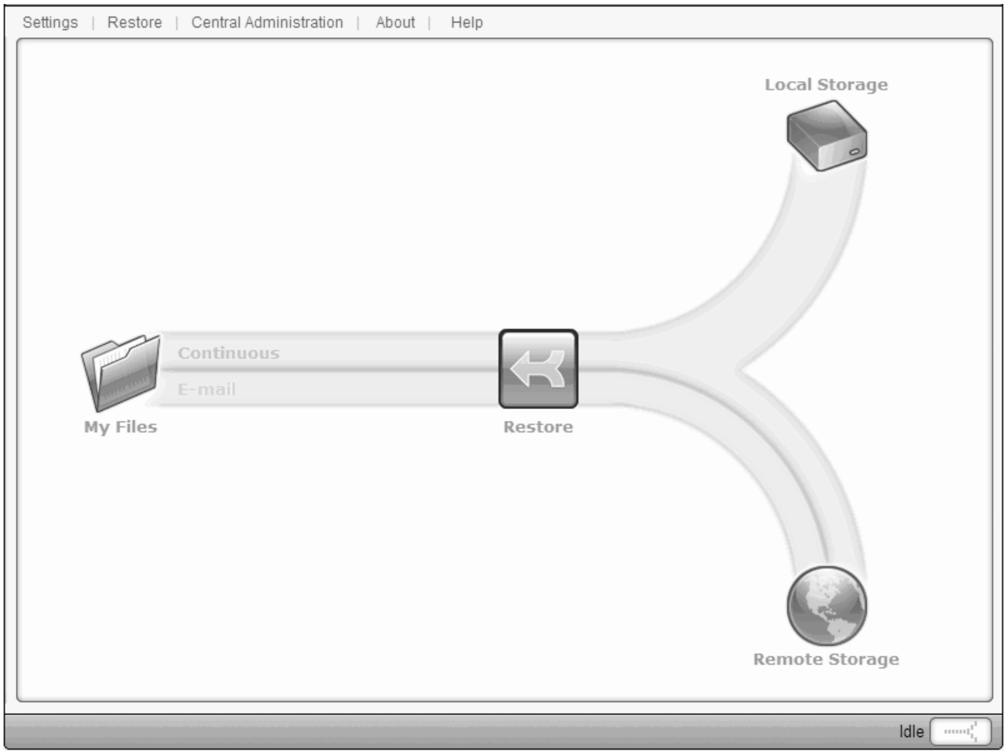
When you successfully create a network rule, it is added to the network rule list.

Changing protection settings for the Tivoli Continuous Data Protection for Files client

You can change which files and applications are protected, and how they are protected.

These tasks assume that you have installed the Tivoli Continuous Data Protection for Files client. If you are configuring the client during product installation, see "Navigating the configuration wizard" on page 7.

These tasks also assume that you start from the Tivoli Continuous Data Protection for Files Status panel.



The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

Specifying which files and applications are protected by Tivoli Continuous Data Protection for Files

You can specify which files are continuously protected, which files are protected on a schedule, and which files are vaulted. For an explanation of the different kinds of protection, see "Types of protection" on page 2.

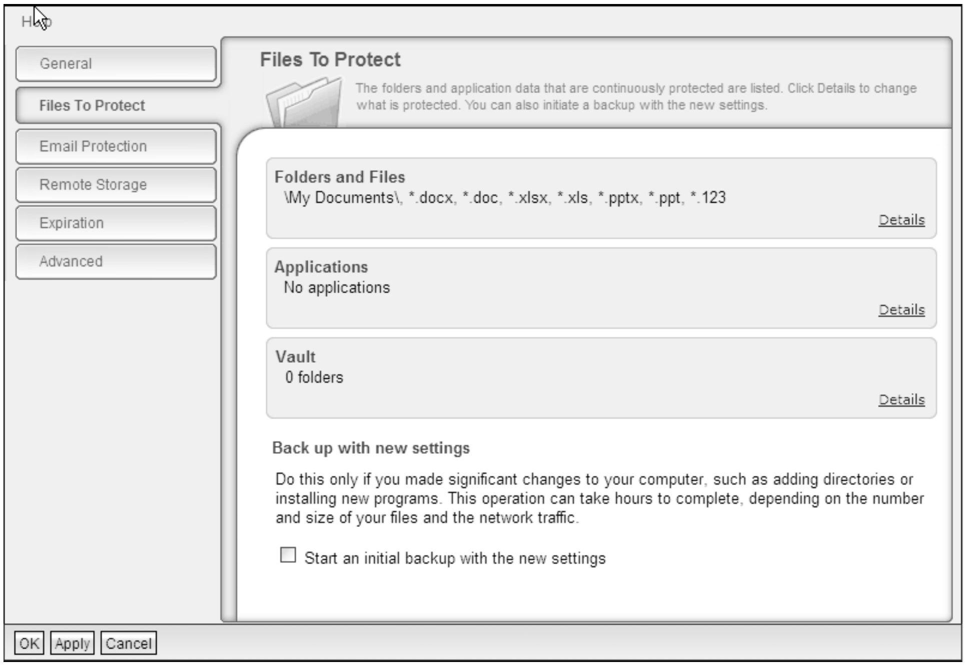
Specifying which files and applications are continuously protected by Tivoli Continuous Data Protection for Files

You can specify which files are protected continuously. You can restore the latest version of these files. You can restore different versions of these files.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Click on **Settings**. The Settings Notebook displays.
3. In the Settings Notebook, click the **Files to Protect** tab of the notebook. The **Files to Protect** page displays. The page has three summary boxes: **Folders and**

Files, **Applications**, and **Vault**.



Files To Protect

The folders and application data that are continuously protected are listed. Click Details to change what is protected. You can also initiate a backup with the new settings.

Folders and Files
\My Documents\, *.docx, *.doc, *.xlsx, *.xls, *.pptx, *.ppt, *.123
Details

Applications
No applications
Details

Vault
0 folders
Details

Back up with new settings

Do this only if you made significant changes to your computer, such as adding directories or installing new programs. This operation can take hours to complete, depending on the number and size of your files and the network traffic.

☐ Start an initial backup with the new settings

4. In the **Applications** box, click the **details** link. The **Applications Settings** dialog displays, and the **Files to Protect** page becomes inactive.
5. Check the applications whose files you want to protect. Clear those applications whose files you do not want to protect.
6. Click **OK**. The **Applications Settings** dialog exits, and the **Files to Protect** page again becomes active.
7. Optional: If you want to add or exclude files and folders by specifying file paths, in the **Folders and Files** box, click the **details** link. The **Folder and Files Settings** dialog displays, and the **Files to Protect** page becomes inactive. For an explanation of how to include and exclude files in this dialog, see “**Folders and Files Settings** page for continuous protection by Tivoli Continuous Data Protection for Files” on page 9
8. If you added applications or file specifications, you must force a backup to ensure that all the new files are immediately protected. See “When to back up all files” on page 44 for an explanation. Check the **Start and initial backup with the new settings** check box.
9. Click **OK**. The Settings Notebook exits and your new settings are applied.

Results

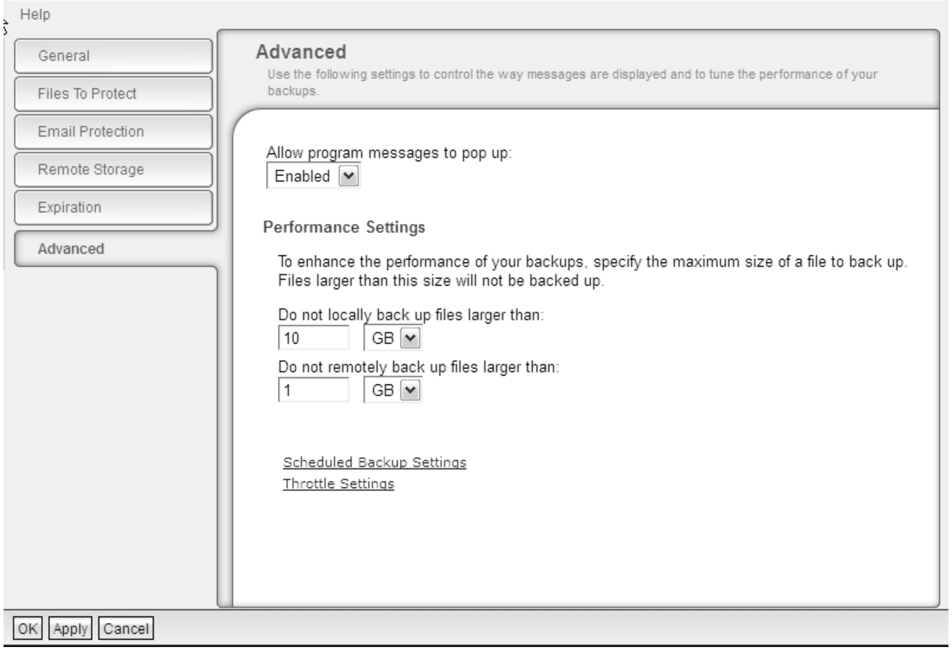
If you forced a backup, your system performance becomes slower during the extensive scan of your protected drives.

Specifying which files and applications are protected on a schedule by Tivoli Continuous Data Protection for Files

You can Specify which files are protected on a schedule. You will be able to restore the last version of the file that you saved before the scheduled backup. You will not be able to restore versions of the file that were saved between scheduled backups.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Click the **Settings** menu item. The Settings Notebook displays.
3. In the Settings Notebook, click the **Advanced** tab. The **Advanced** page displays.



Advanced

Use the following settings to control the way messages are displayed and to tune the performance of your backups.

Allow program messages to pop up: Enabled

Performance Settings

To enhance the performance of your backups, specify the maximum size of a file to back up. Files larger than this size will not be backed up.

Do not locally back up files larger than: 10 GB

Do not remotely back up files larger than: 1 GB

4. Click the **Scheduled Backup Settings** link. The **Folders and Files Settings** dialog for scheduled backups displays, and the **Advanced** page becomes inactive.
5. Click the **Include** menu item. The **Select Folders** dialog displays, and the **Folders and Files Settings** dialog becomes inactive.
6. Choose a folder in the folders tree, or specify a folder in the **Folder name (wildcards allowed)** field. You can specify individual files or folders. With wildcards, you can specify all files and folders that match your pattern. See "Wildcards in file specifications" on page 11 for details.
7. Click the **OK** button. The **Select Folders** dialog exits, and the **Folders and Files Settings** dialog for scheduled backups again becomes active. The file or folder that you specified is added to the list.
8. Repeat the previous 3 steps to specify more folders to protect.
9. In the **Folders and Files Settings** dialog, select the files and folders that you no longer want protected on a schedule, and click the **Remove** menu item. The files and folders are removed from the list.
10. Click the **OK** button. The **Folders and Files Settings** dialog exits, and the **Advanced** page in the Settings Notebook again becomes active.
11. Click the **OK** button. The Settings Notebook exits and your new settings are applied.

Considerations for scheduled backups:

Protect appropriate files on a schedule, and prepare the files for backup.

Files that are appropriate to protect on a schedule

Large or frequently saved files can consume considerable computing or network resources when they are backed up. You can schedule periodic backups of these files when the burden on computing or network resources are least inconvenient.

Some files are not often closed and saved, but must be backed up periodically. Files protected by schedule are backed up even if they are open, but you can try to schedule the backup for a time when the files are closed.

Scheduled backup can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but offer fewer opportunities when you want to restore a file.

When does a scheduled backup occur

The files that you select for scheduled protection are backed up at the scheduled time, if they change during the scheduled interval. If a file changed several times during the schedule, only the last version of the file is backed up at the scheduled time.

If the remote storage area is not available at the scheduled backup time, the files that have changed at that time are noted and are backed up when the remote storage becomes available. If a noted file changes after the scheduled backup time, and before the remote storage becomes available, only the last version of the file is backed up.

If the computer is powered off or Tivoli Continuous Data Protection for Files is not running at the schedule time, the scheduled backup runs when the computer is powered on and Tivoli Continuous Data Protection for Files is running.

If you shut down a computer or stop the Tivoli Continuous Data Protection for Files client when a scheduled backup is running, the backup resumes when the client is running again and the remote storage is available.

If you forced a backup of scheduled files during the 30 minutes prior to the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

Tivoli Continuous Data Protection for Files backs up all files that have changed during the schedule interval, including files that are still open at the time of backup. The backup copies of files that are backed up while open can be corrupted. So it is suggested that you close applications before a scheduled backup. Tivoli Continuous Data Protection for Files offers an opportunity to close applications before a scheduled backup.

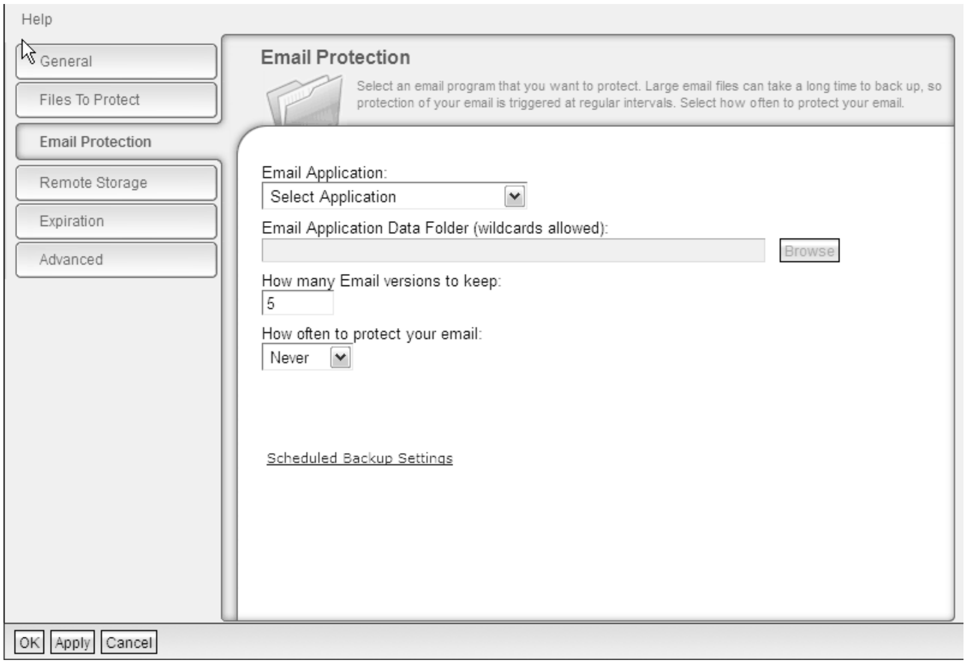
At the beginning of a scheduled backup, Tivoli Continuous Data Protection for Files attempts to close all files that are listed in a text file called `closeapps.txt` in the installation directory. Each line in the file must be a program name, with name and extension, but no folder path. Tivoli Continuous Data Protection for Files sends a close command to each instance of every program named in the `closeapps.txt` file. Note that Tivoli Continuous Data Protection for Files does not send a start command to any of those programs when the scheduled backup is finished.

Specifying which email applications are protected by Tivoli Continuous Data Protection for Files

Use the Email Protection panel to specify an email application to protect.

Procedure

1. Start Tivoli Continuous Data Protection for Files Status panel.
2. Click on **Settings**. The Settings Notebook displays.
3. In the Settings Notebook, click the **Email Protection** tab. The **Email Protection** page displays.



Select an email program that you want to protect. Large email files can take a long time to back up, so protection of your email is triggered at regular intervals. Select how often to protect your email.

Email Application: Select Application

Email Application Data Folder (wildcards allowed):

How many Email versions to keep: 5

How often to protect your email: Never

4. Choose your email application from the **Email Application** list. If your application is not listed in the list, choose **Other**. If you chose **Other**, the **Email Application Data Folder (wildcards allowed)** field becomes active.
5. If you chose **Other**, enter a file specification in the **Email Application Data Folder (wildcards allowed)** field. You can type the specification or browse for the folder.
6. Specify **How many Email versions keep** on the remote storage.
7. Click **OK**. The Settings Notebook exits and your new settings are applied.

Related tasks:

"Specifying the period for scheduled protection by Tivoli Continuous Data Protection for Files" on page 65
All files that are protected on a schedule are protected on the schedule that is configured in the **E-mail Protection** page in the Settings Notebook. When you change the schedule for e-mail files, you change the schedule for all files that are protected on a schedule.

Specifying which files and applications are vaulted by Tivoli Continuous Data Protection for Files

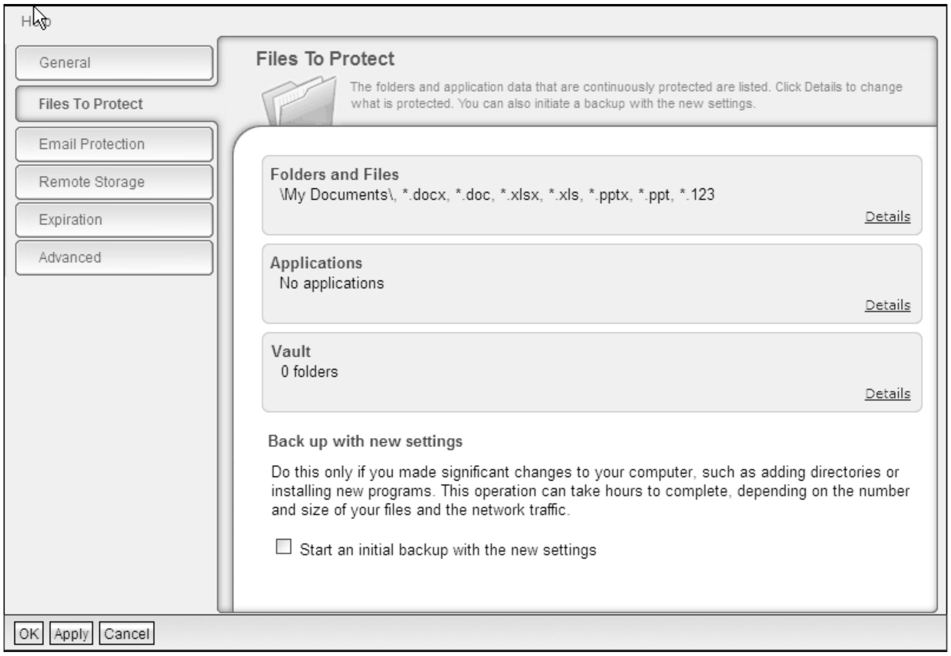
Use vaulting for files that you do not want to modify or delete. Vaulted files and folders cannot be modified or deleted.

About this task

Information on vaulting can be found in the “Types of protection” on page 2 section.

Procedure

1. Click the **Settings** menu item. The Settings Notebook displays.
2. In the Settings Notebook, click the **Files to Protect** tab. The **Files to Protect** page displays. The page has three summary boxes: **Folders and Files**, **Applications**, and **Vault**.



Files To Protect

The folders and application data that are continuously protected are listed. Click Details to change what is protected. You can also initiate a backup with the new settings.

Folders and Files
\My Documents\, *.docx, *.doc, *.xlsx, *.xls, *.pptx, *.ppt, *.123

Applications
No applications

Vault
0 folders

Back up with new settings

Do this only if you made significant changes to your computer, such as adding directories or installing new programs. This operation can take hours to complete, depending on the number and size of your files and the network traffic.

☐ Start an initial backup with the new settings

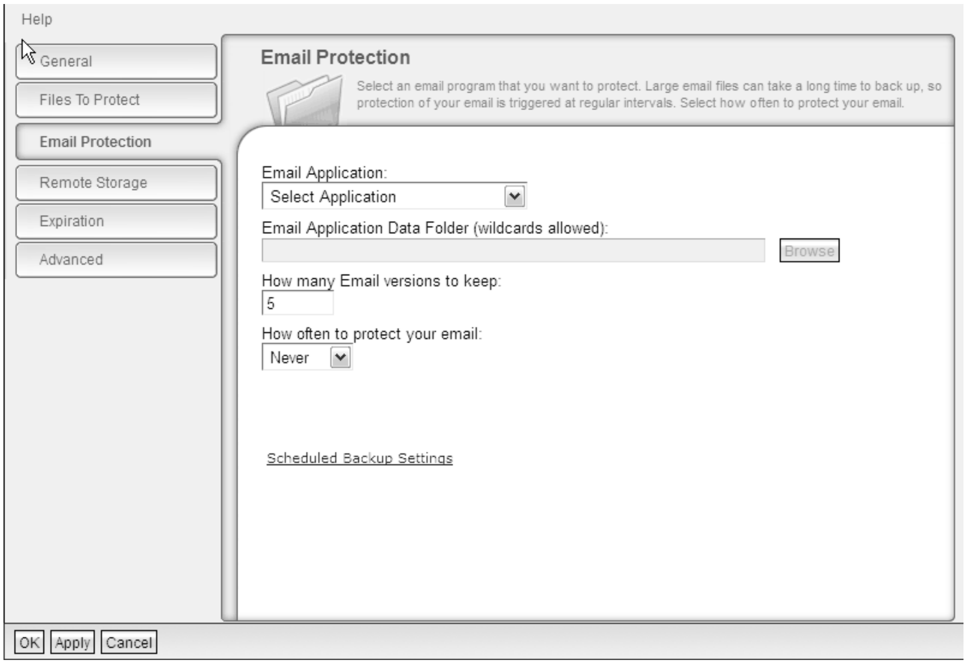
3. In the **Vault** box, click the **details** link. The **Vault Settings** dialog displays, and the **Files to Protect** page becomes inactive.
4. Click the **Vault** menu item. The **Select Folders** dialog displays, and the **Vault Settings** dialog becomes inactive.
5. Choose a folder in the folders tree, or specify a folder in the **Folder name (wildcards allowed)** field. You cannot specify individual files. With wildcards, you can specify all folders that match your pattern. See “Wildcards in file specifications” on page 11 for details.
6. Click the **OK** button. The **Select Folders** dialog exits, and the **Vault Settings** dialog again becomes active. The folder that you specified is added to the list.
7. Repeat the previous three steps to specify more folders to vault.
8. In the **Vault Settings** dialog, select the folders that you no longer want vaulted, and click the **Unvault** menu item. The folders that you specified are removed from the list.
9. Click **OK**. The **Vault Settings** dialog exits, and the **Files to Protect** page in the Settings Notebook again becomes active.
10. Click **OK**. The Settings Notebook exits, and your folders become vaulted.

Specifying the period for scheduled protection by Tivoli Continuous Data Protection for Files

All files that are protected on a schedule are protected on the schedule that is configured in the **E-mail Protection** page in the Settings Notebook. When you change the schedule for e-mail files, you change the schedule for all files that are protected on a schedule.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Click the **Settings** menu item. The Settings Notebook displays.
3. In the Settings Notebook, click the **E-mail Protection** tab. The **E-mail Protection** page displays.



Email Protection

Select an email program that you want to protect. Large email files can take a long time to back up, so protection of your email is triggered at regular intervals. Select how often to protect your email.

Email Application: Select Application

Email Application Data Folder (wildcards allowed):

How many Email versions to keep: 5

How often to protect your email: Never

4. Choose the schedule period in the **How often to protect your e-mail:** drop down list. Depending on the schedule period that you chose, day or time fields will display
5. If applicable for the scheduled period, choose the day and time to perform the backup.
6. Click the **OK** button. The Settings Notebook exits and your new settings are applied.

Specifying storage for backup copies by Tivoli Continuous Data Protection for Files

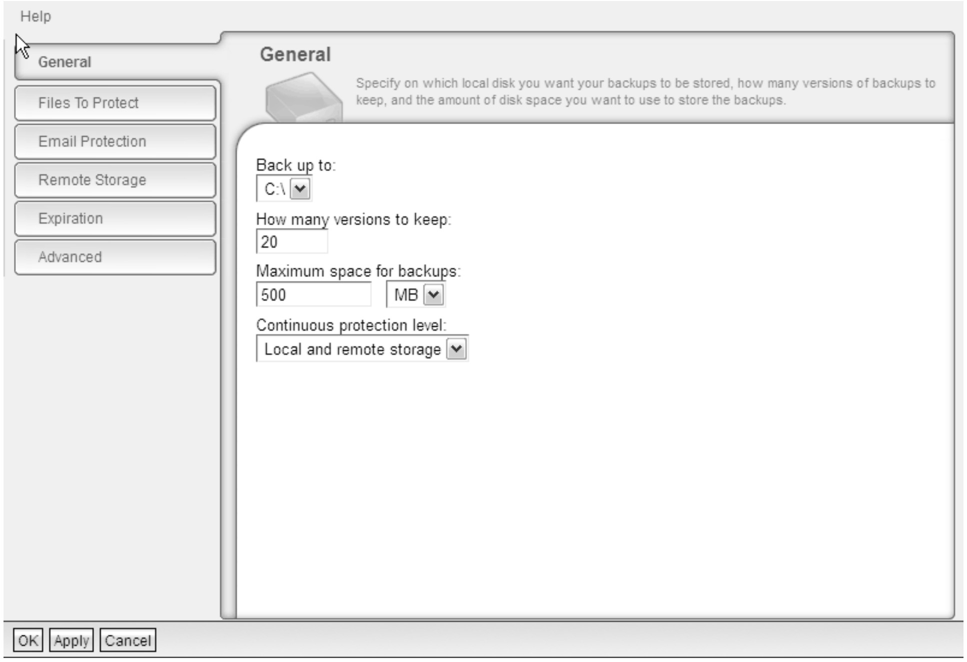
You can specify local storage areas, remote storage, and on which storage areas to store backup copies.

Specifying the local storage area for backup copies by Tivoli Continuous Data Protection for Files

You can specify on which local drive to store backup copies. You can specify how many versions to keep, and the maximum space for backup copies. Specify also whether to use local storage, remote storage, both, or neither.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Click the **Settings** menu item. The **General** page the Settings Notebook displays.



General

Specify on which local disk you want your backups to be stored, how many versions of backups to keep, and the amount of disk space you want to use to store the backups.

Back up to: C:\

How many versions to keep: 20

Maximum space for backups: 500 MB

Continuous protection level: Local and remote storage

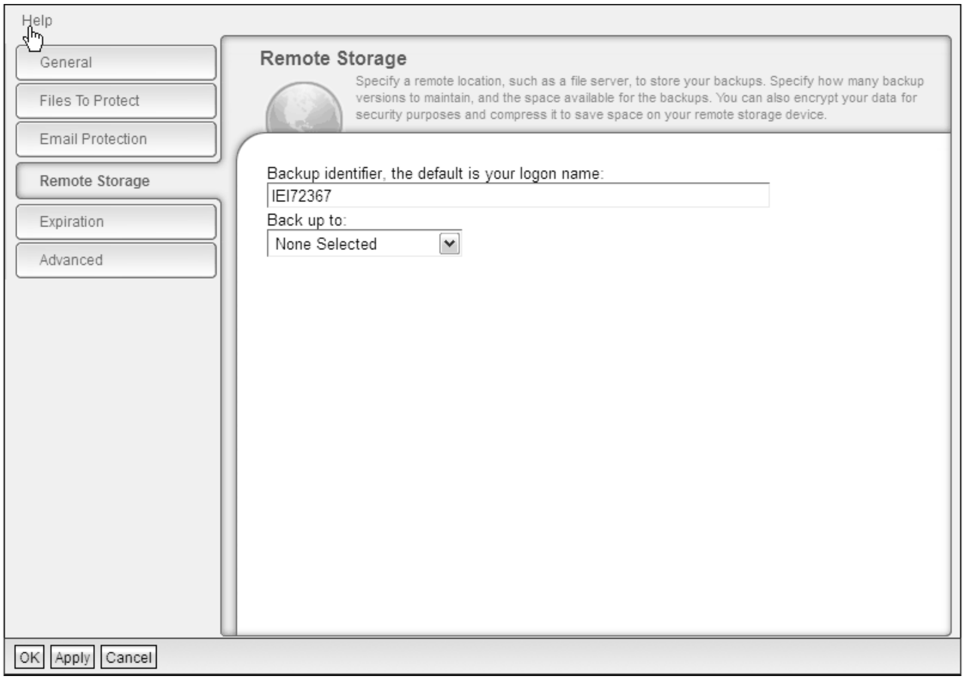
3. Choose the location, number of versions, space for local backup copies, and level of continuous protection. For explanations of the fields on this page, see "**General** panel of client Settings Notebook" on page 33.
4. Click the **OK** button. The Settings Notebook exits and your new settings are applied.

Specifying the remote storage area for backup copies by Tivoli Continuous Data Protection for Files

You can specify where backup copies are stored on your remote and external devices. You can specify how many versions to keep, the backup identifier, and the maximum space for backup copies.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Click the **Settings** menu item. The Settings Notebook displays.
3. In the Settings Notebook, click the **Remote Storage** tab. The **Remote Storage** page displays.



Remote Storage

Specify a remote location, such as a file server, to store your backups. Specify how many backup versions to maintain, and the space available for the backups. You can also encrypt your data for security purposes and compress it to save space on your remote storage device.

Backup identifier, the default is your logon name: IEI72367

Back up to: None Selected

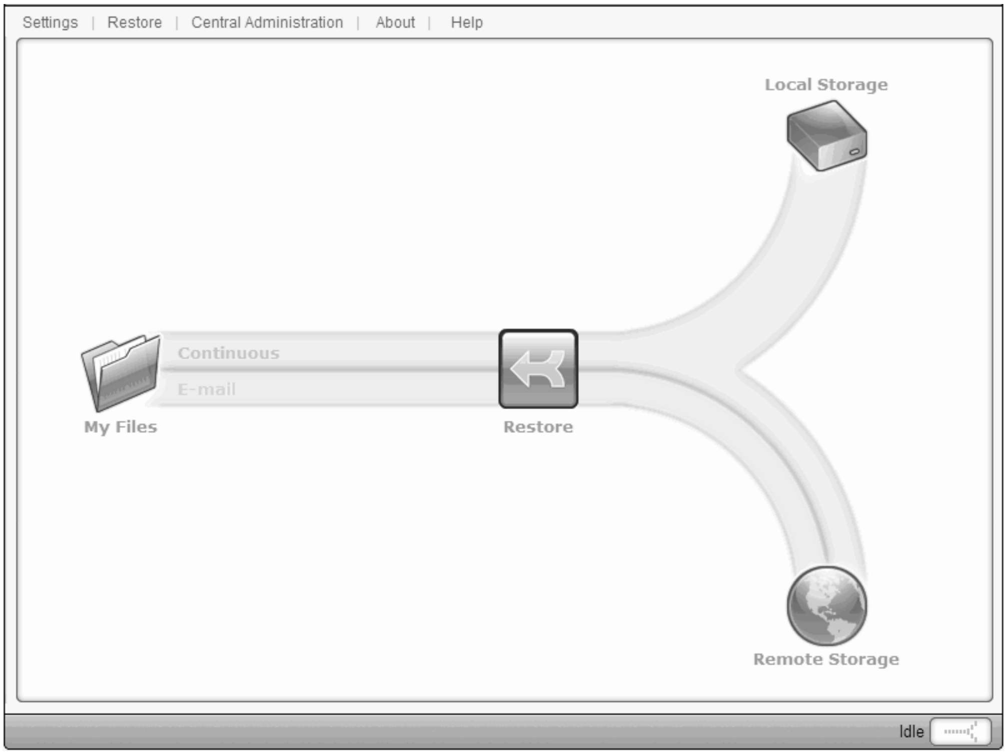
4. Choose appropriate values for the remote storage area fields. For explanations of the fields on this page, see "**Remote Storage** panel of client Settings Notebook" on page 46.
5. Click the **OK** button. The Settings Notebook exits and your new settings are applied.

Forcing a backup by Tivoli Continuous Data Protection for Files

When you change your configuration so that a new set of files is protected, either by continuous protection or scheduled protection, it is recommended that you back up all protected files. Failing to back up all protected files will yield protection only for those files that you change.

You can force a backup of all protected files; force a scheduled backup before the scheduled period elapses; and stop a forced backup.

These tasks assume that you start from the Tivoli Continuous Data Protection for Files Status panel.



The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

Backing up all files that are protected by Tivoli Continuous Data Protection for Files

When you change your configuration to extend continuous or scheduled protection to more files, it is recommended that you back up all protected files. Failing to back up all protected files will yield protection only for those files that you change.

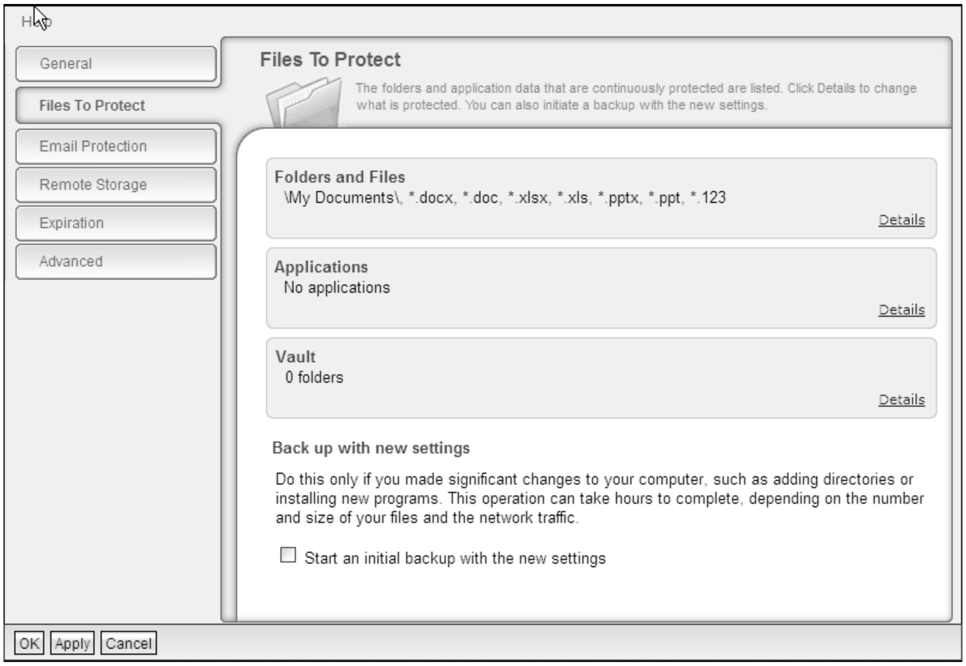
About this task

For an explanation of when to back up all files, see “When to back up all files” on page 44.

Follow these instructions to force a backup of all files that are continuously protected and all files that are protected on a schedule.

Procedure

1. Start the Tivoli Continuous Data Protection for Files Status panel.
2. Click on**Settings** to open the Settings Notebook.
3. In the Settings Notebook, click the **Files to Protect** tab. The **Files to Protect** page displays.



Files To Protect

The folders and application data that are continuously protected are listed. Click Details to change what is protected. You can also initiate a backup with the new settings.

Folders and Files
\My Documents\, *.docx, *.doc, *.xlsx, *.xls, *.pptx, *.ppt, *.123

Applications
No applications

Vault
0 folders

Back up with new settings

Do this only if you made significant changes to your computer, such as adding directories or installing new programs. This operation can take hours to complete, depending on the number and size of your files and the network traffic.

☐ Start an initial backup with the new settings

4. Click on **Start an initial backup with the new settings**.
5. Click **OK**. The Settings Notebook exits and Tivoli Continuous Data Protection for Files begins to scan your protected drives and back up all files that you designated for continuous or scheduled protection. Your system performance will become slower during the extensive scan of your protected drives.

Forcing a scheduled backup by Tivoli Continuous Data Protection for Files

You can force a scheduled backup before the schedule period expires. As a result, you do not need to wait for the schedule period to expire. All files with changes since the last scheduled backup can be backed up.

About this task

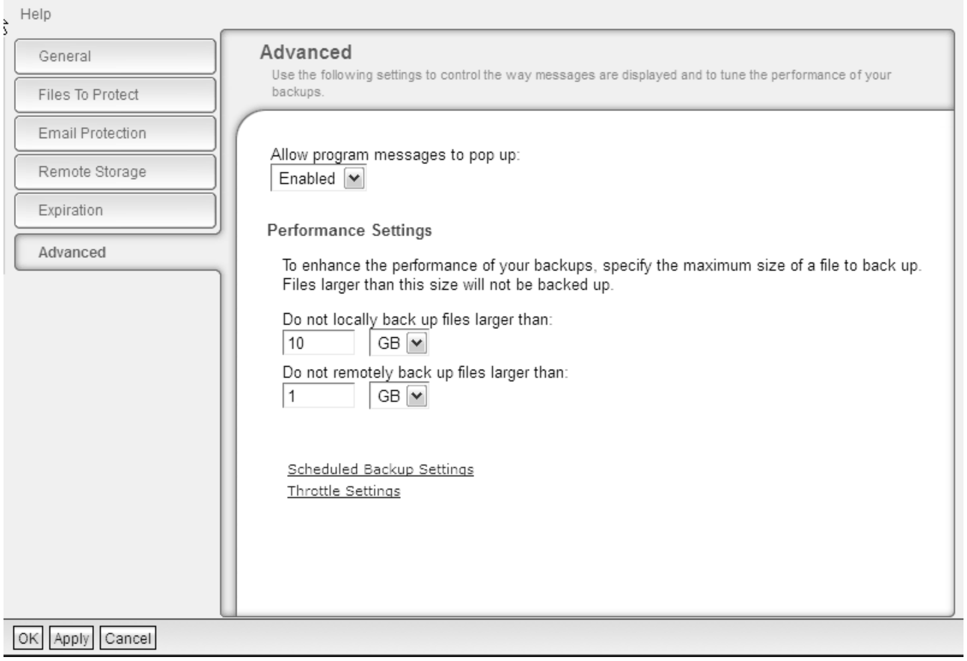
Before a scheduled backup, you might want to back up files that are part of a schedule. In this case, you can force a backup of all files that have changes. If you force a backup of scheduled files during the 30 minutes before the scheduled time, the scheduled backup does not occur. If the remote storage area is not available, changed files are noted and the most recent versions are backed up when the remote storage becomes available.

Note: Only the files with changes, since the last scheduled backup are, backed up.

To force a scheduled backup, start at the Status panel.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Click on **Settings**. The Settings Notebook displays.
3. In the Settings Notebook, click the **Advanced** tab. The **Advanced** page displays.



Advanced

Use the following settings to control the way messages are displayed and to tune the performance of your backups.

Allow program messages to pop up: Enabled

Performance Settings

To enhance the performance of your backups, specify the maximum size of a file to back up. Files larger than this size will not be backed up.

Do not locally back up files larger than: 10 GB

Do not remotely back up files larger than: 1 GB

Scheduled Backup Settings

Throttle Settings

4. Click the **Scheduled Backup Settings** link. The **Folders and Files Settings** dialog for scheduled backups displays, and the **Advanced** page becomes inactive.
5. Check on **Start scheduled backup now**.
6. Click **OK**. The **Folders and Files Settings** dialog exits, and the **Advanced** page in the Settings Notebook becomes active.
7. Click **OK**. The Settings Notebook exits and Tivoli Continuous Data Protection for Files backs up the files that changed since the last scheduled backup.

Stopping backup activity by Tivoli Continuous Data Protection for Files

How to stop Tivoli Continuous Data Protection for Files backing up files.

About this task

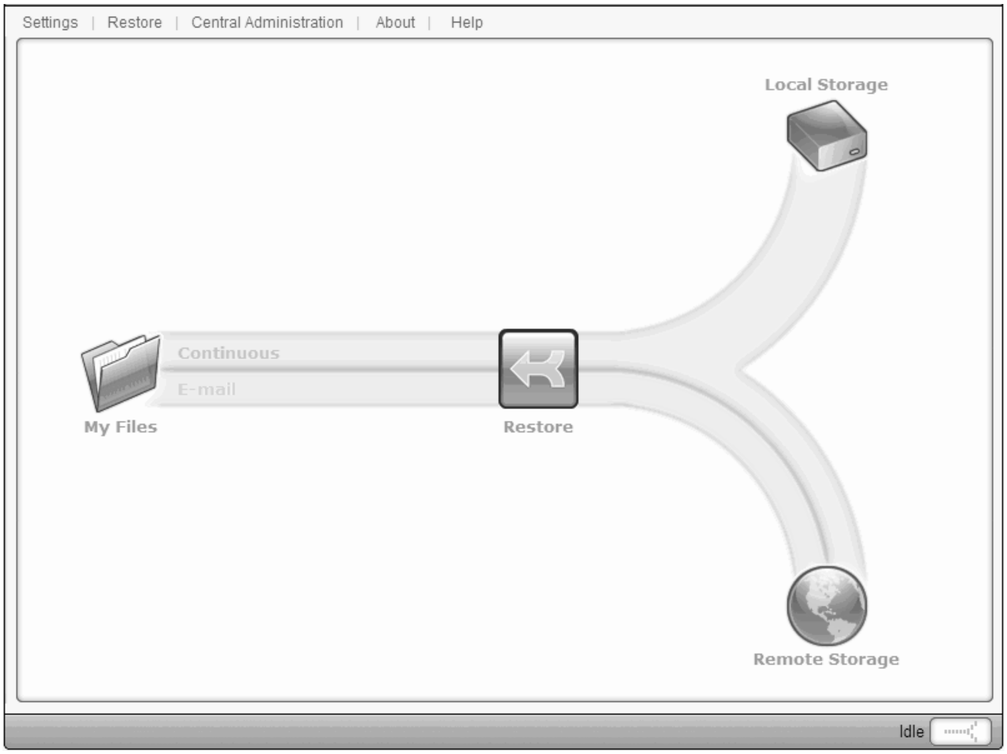
The steps for stopping any kind of backup activity or restore activity are very similar to each other. See “Stopping backup or restore activity by Tivoli Continuous Data Protection for Files” on page 75.

Chapter 4. Starting and stopping protection activity of the Tivoli Continuous Data Protection for Files client

How to administer the Tivoli Continuous Data Protection for Files client. You can find out how to start, stop, and restart the client, how to force a backup, and how to run the client as a service.

Starting the client GUI

Start the client GUI to work with the Tivoli Continuous Data Protection for Files client. From the Status panel of the GUI, you can modify data protection settings, restore files, and monitor protection activity.



The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

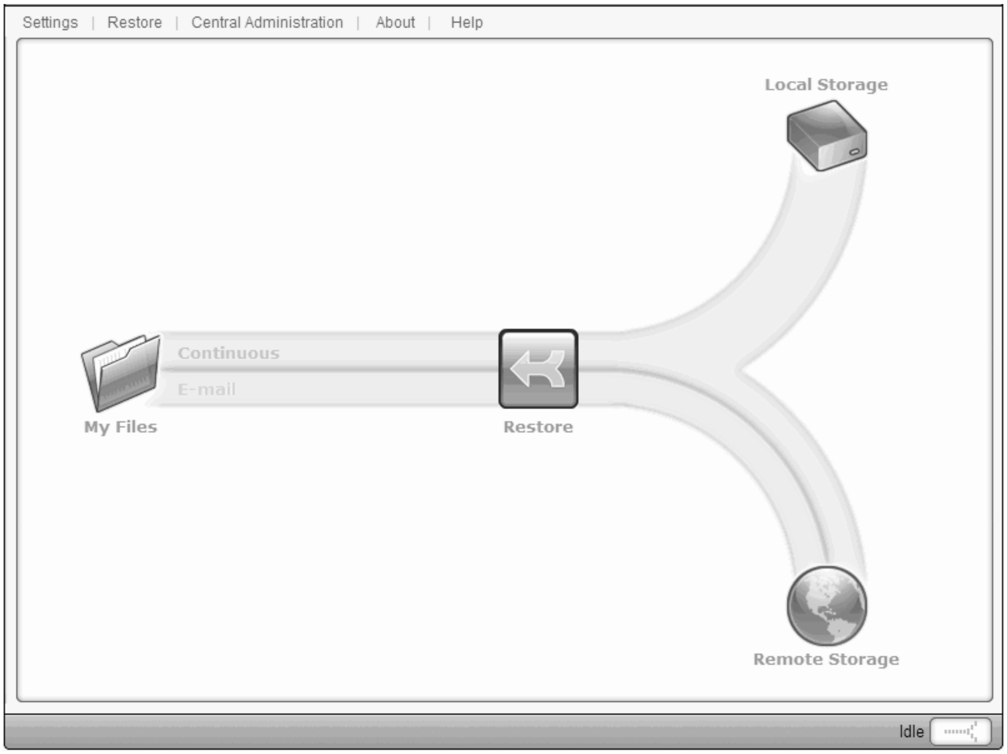
You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

Forcing a backup by Tivoli Continuous Data Protection for Files

When you change your configuration so that a new set of files is protected, either by continuous protection or scheduled protection, it is recommended that you back up all protected files. Failing to back up all protected files will yield protection only for those files that you change.

You can force a backup of all protected files; force a scheduled backup before the scheduled period elapses; and stop a forced backup.

These tasks assume that you start from the Tivoli Continuous Data Protection for Files Status panel.



The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

When to back up all files

At certain times, you need to back up all files. Without this backup, some files are not protected.

After the first installation of the Tivoli Continuous Data Protection for Files client, you can immediately back up all files that you configured for protection. In the initial backup, newly created files and existing files that are changed are protected. Existing files that are not changed are backed up after the initial scan is done.

One exception is when you push an installation of Tivoli Continuous Data Protection for Files to a remote computer and do not reboot. If you force a backup on a pushed installation without rebooting, Tivoli Continuous Data Protection for Files attempts to back up files in the system context. These backups can fail, and when a logged-on user later attempts to restore these files the restore can fail.

After the initial backup, the typical rate of file changes does not require that you again back up all files immediately. If you change the protection settings to include files that were not previously protected, the files need to be backed up. Until you change these files, and without a forced backup, Tivoli Continuous Data Protection for Files does not back up these files. To protect these files, you must force a backup of all files.

If you do not change the configuration but make large changes to the files that are configured for protection, you must force a backup of all files. You need to force a backup when you add a new drive that contains files configured for protection.

A forced backup causes Tivoli Continuous Data Protection for Files to scan all local drives looking for files that you designated for protection. Every file in every directory will be investigated, and all files that meet the include, exclude, and size criteria are copied to the local, remote or both storage areas. The creation of backup copies may take several hours. It also takes significant processing resources. Plan the backup at a time when you do not need computing resources for other activities.

When the scan and backup complete, Tivoli Continuous Data Protection for Files continues to operate in the background without any significant impact on your regular computing activities.

Changing the **Vault** settings does not require a forced backup.

With a client, you can force a backup of your continuously protected files in two places:
- The Initial Configuration Wizard, when you initially configure the Tivoli Continuous Data Protection for Files client
- The **Files to Protect** panel in the Settings Notebook of the client, any time after initial configuration.

Backing up all files that are protected by Tivoli Continuous Data Protection for Files

When you change your configuration to extend continuous or scheduled protection to more files, it is recommended that you back up all protected files. Failing to back up all protected files will yield protection only for those files that you change.

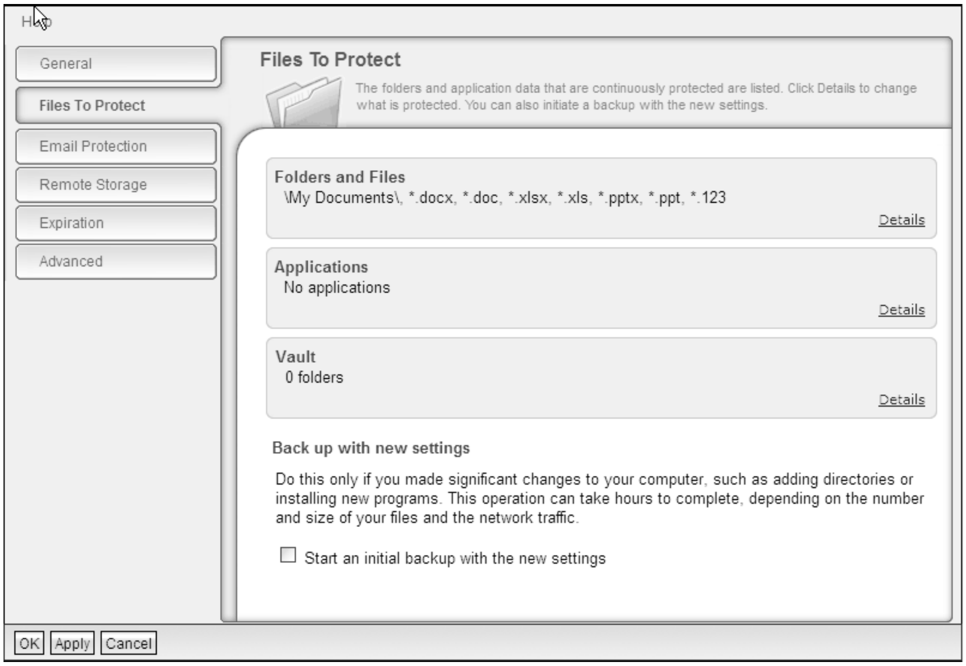
About this task

For an explanation of when to back up all files, see “When to back up all files” on page 44.

Follow these instructions to force a backup of all files that are continuously protected and all files that are protected on a schedule.

Procedure

1. Start the Tivoli Continuous Data Protection for Files Status panel.
2. Click on**Settings** to open the Settings Notebook.
3. In the Settings Notebook, click the **Files to Protect** tab. The **Files to Protect** page displays.



Files To Protect

The folders and application data that are continuously protected are listed. Click Details to change what is protected. You can also initiate a backup with the new settings.

Folders and Files
\My Documents\, *.docx, *.doc, *.xlsx, *.xls, *.pptx, *.ppt, *.123

Applications
No applications

Vault
0 folders

Back up with new settings

Do this only if you made significant changes to your computer, such as adding directories or installing new programs. This operation can take hours to complete, depending on the number and size of your files and the network traffic.

☐ Start an initial backup with the new settings

4. Click on **Start an initial backup with the new settings**.
5. Click **OK**. The Settings Notebook exits and Tivoli Continuous Data Protection for Files begins to scan your protected drives and back up all files that you designated for continuous or scheduled protection. Your system performance will become slower during the extensive scan of your protected drives.

Forcing a scheduled backup by Tivoli Continuous Data Protection for Files

You can force a scheduled backup before the schedule period expires. As a result, you do not need to wait for the schedule period to expire. All files with changes since the last scheduled backup can be backed up.

About this task

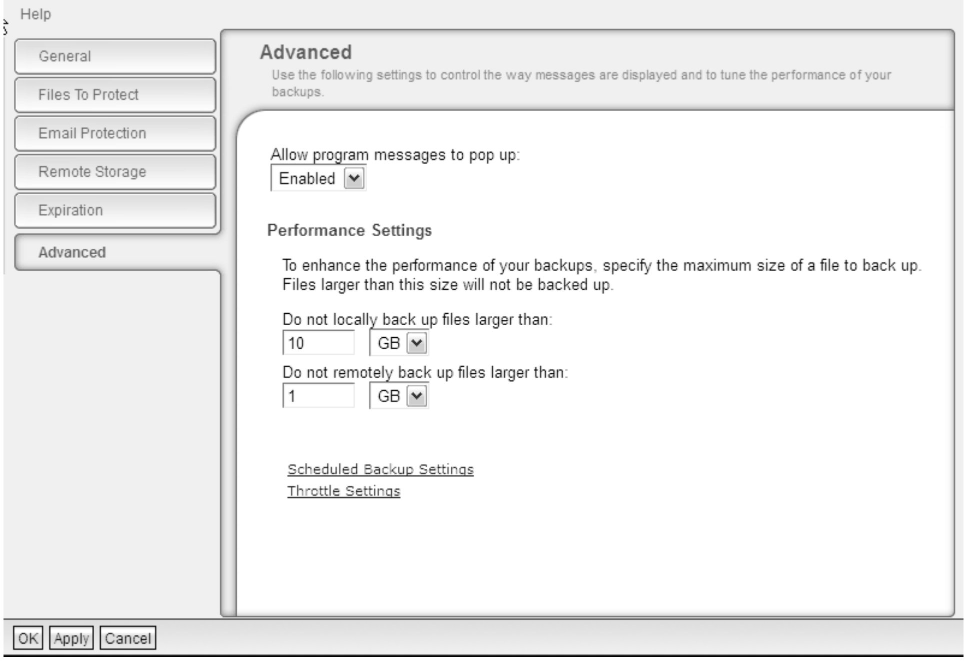
Before a scheduled backup, you might want to back up files that are part of a schedule. In this case, you can force a backup of all files that have changes. If you force a backup of scheduled files during the 30 minutes before the scheduled time, the scheduled backup does not occur. If the remote storage area is not available, changed files are noted and the most recent versions are backed up when the remote storage becomes available.

Note: Only the files with changes, since the last scheduled backup are, backed up.

To force a scheduled backup, start at the Status panel.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Click on **Settings**. The Settings Notebook displays.
3. In the Settings Notebook, click the **Advanced** tab. The **Advanced** page displays.



Advanced

Use the following settings to control the way messages are displayed and to tune the performance of your backups.

Allow program messages to pop up: Enabled

Performance Settings

To enhance the performance of your backups, specify the maximum size of a file to back up. Files larger than this size will not be backed up.

Do not locally back up files larger than: 10 GB

Do not remotely back up files larger than: 1 GB

4. Click the **Scheduled Backup Settings** link. The **Folders and Files Settings** dialog for scheduled backups displays, and the **Advanced** page becomes inactive.
5. Check on **Start scheduled backup now**.
6. Click **OK**. The **Folders and Files Settings** dialog exits, and the **Advanced** page in the Settings Notebook becomes active.
7. Click **OK**. The Settings Notebook exits and Tivoli Continuous Data Protection for Files backs up the files that changed since the last scheduled backup.

Stopping backup activity by Tivoli Continuous Data Protection for Files

How to stop Tivoli Continuous Data Protection for Files backing up files.

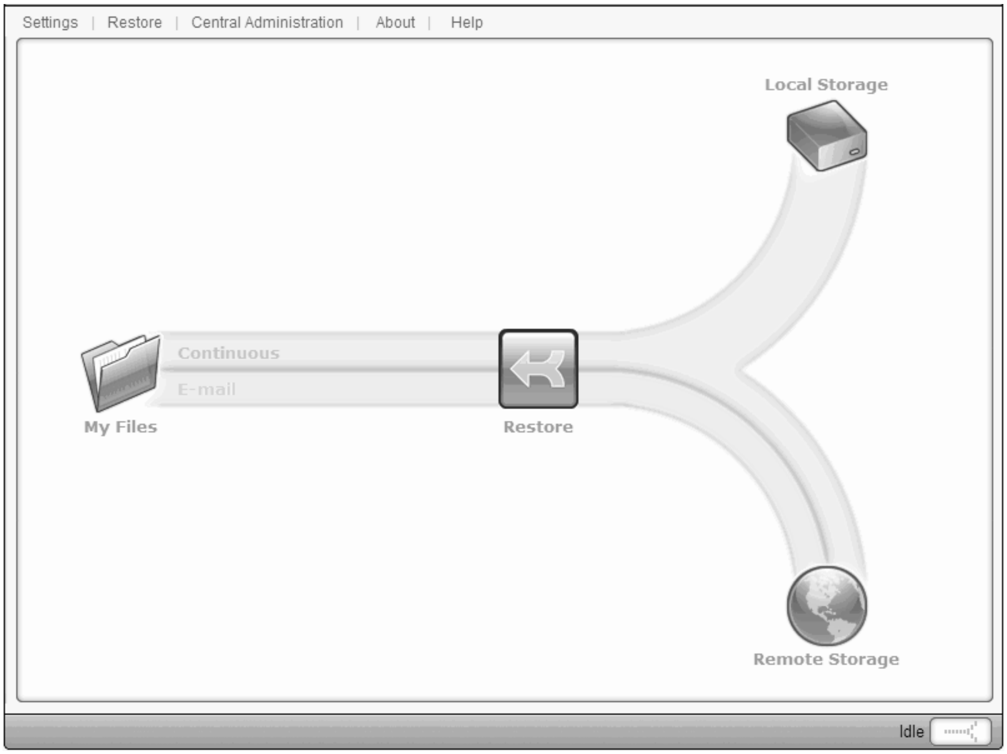
About this task

The steps for stopping any kind of backup activity or restore activity are very similar to each other. See “Stopping backup or restore activity by Tivoli Continuous Data Protection for Files.”

Stopping backup or restore activity by Tivoli Continuous Data Protection for Files

You can stop any backup or restore activity.

This task assumes that you start from the Tivoli Continuous Data Protection for Files Status panel.

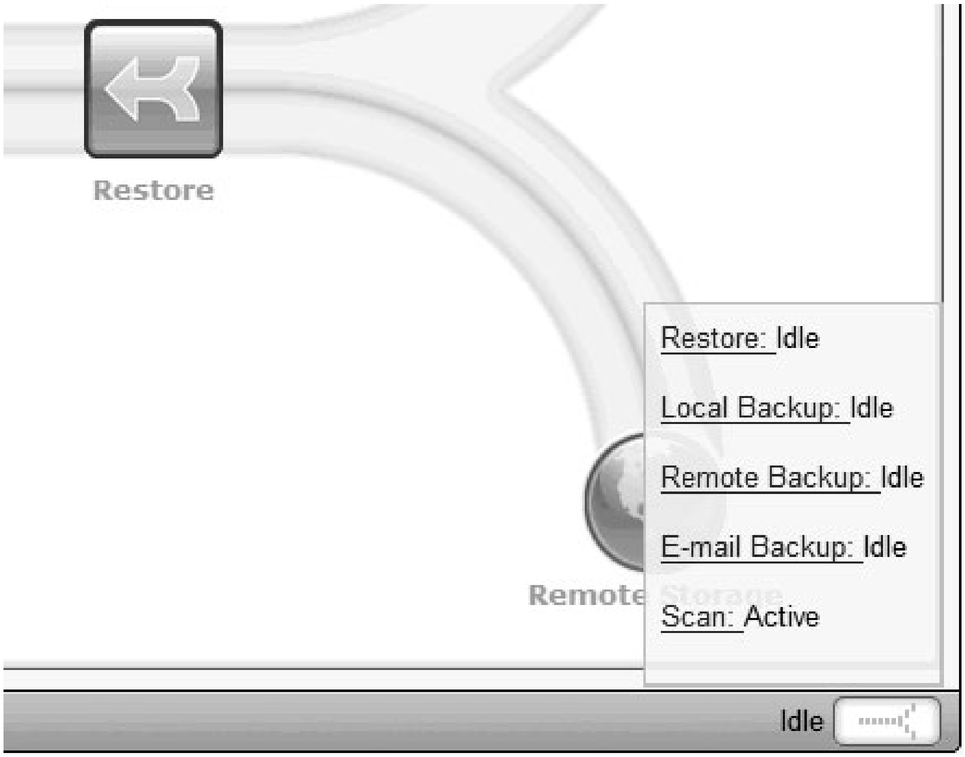


The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

1. The bar at the end of the Status panel displays a brief text message of the status of backup and restore activities. Hover your cursor over the icon next to the text. A summary of activities opens from the bar. The summary lists five activities. For each activity, there is a link to a detailed status dialog, and a brief text that indicates the status of the activity.



Restore: Idle

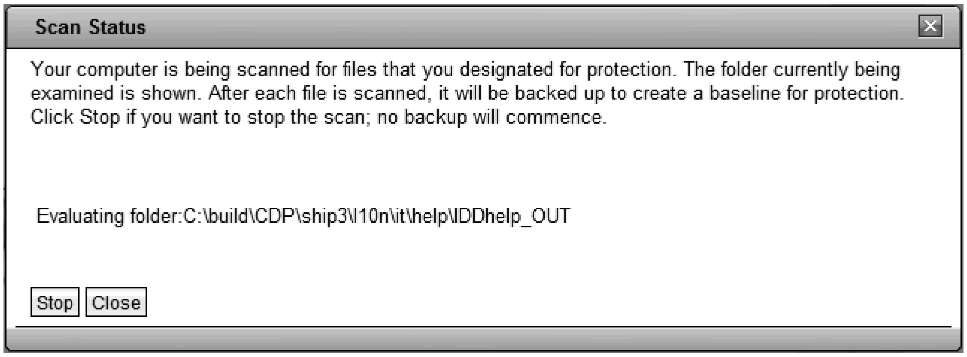
Local Backup: Idle

Remote Backup: Idle

E-mail Backup: Idle

Scan: Active

2. Click the link for the activity you want to skip or stop or close. The detailed status dialog for that activity displays, and the Status panel becomes inactive.



Your computer is being scanned for files that you designated for protection. The folder currently being examined is shown. After each file is scanned, it will be backed up to create a baseline for protection. Click Stop if you want to stop the scan; no backup will commence.

Evaluating folder:C:\build\CDP\ship3\l10n\it\help\IDDhelp_OUT

3. In the Status dialog that you selected, you can click **Skip** to skip a restore or backup operation, or the **Stop** to stop a restore or backup operation. Click **Close** to exit, and the Status panel becomes active again. Within a short time, the activity completes.

Managing Tivoli Continuous Data Protection for Files Clients

To use central administration features, you must configure the managing client (administrator) and managed clients. For configuration information, and instructions for centrally administering properly configured clients, see Chapter 8, “Tivoli Continuous Data Protection for Files central management considerations,” on page 97.

Restarting the Tivoli Continuous Data Protection for Files client process

The `FilePathSrv.exe` client process is started automatically every time the computer starts. If the `FilePathSrv.exe` client process does not start automatically or stops running, your files are not protected.

To determine if the `FilePathSrv.exe` process is running, look for the FilePathSrv.exe process in Task Manager. If you cannot see this process, the process is not running.

To restart the process on a Command Prompt window, do the following:
1. Open a Command Prompt window.
2. Navigate to the Tivoli Continuous Data Protection for Files installation folder. The default installation folder is `C:\Program Files\Tivoli\CDP_for_Files`.
3. Type the following: `filepathsrv -d`.

Confirm that the process is running by checking the System Event log or Task Manager. In the System Event log, there should be an entry which states: `HTML listener started successfully and listening on port 9003`. This is event # 6049. In Task Manager, you should see FilePathSrv.exe process.

You can also restart the process from the **Start** menu. Choose **Start > All Programs > Startup >CDPforFilesSrv**.

Run the Tivoli Continuous Data Protection for Files client as a service

You can run the client as a service instead of a logged-in application.

If the client runs on a server, it needs to run as a service instead of as a logged-in application. The product provides this capability.

In the client installation directory, there is a program called `FpForFileServers.js`. If you start this executable file, the client runs as a service instead of as a logged-in application.

Note: When using Microsoft Vista or Microsoft Windows 7, the file needs to be run from an elevated command window.

The default account for services on Microsoft Windows has no privilege for accessing folders shared on a network. The `FpForFileServers.js` executable file launches the Microsoft Windows services configuration panel so that you can update the FilePathSrv service. Specify a valid account name and password that can access your remote backup locations. On Windows Vista and Windows 7, run the command in a command prompt with elevated privileges.

When you uninstall the Tivoli Continuous Data Protection for Files client, the Tivoli Continuous Data Protection for Files service is also uninstalled.

Note: The Tivoli Continuous Data Protection for Files client installation directory and tree allow full access by all users on the system during installation. This is done so that non-privileged users without administration rights can be protected by the software, and use the GUI. Consider setting more restrictive ACLs on the installation directory and tree for multiuser workstations.

Chapter 5. Monitoring the protection of Tivoli Continuous Data Protection for Files

When Tivoli Continuous Data Protection for Files is installed and configured, you can monitor the state of your protection. You can receive messages, check that the Tivoli Continuous Data Protection for Files daemon is running, and use the Tivoli Continuous Data Protection for Files user interface to check detailed status of your protection.

If you determine that Tivoli Continuous Data Protection for Files is not protecting your files as you intended, often the solution is suggested by the data available from Tivoli Continuous Data Protection for Files reports or configuration settings. If the solution is not clear, consider the information in Chapter 10, "Troubleshooting the Tivoli Continuous Data Protection for Files client," on page 109. The following monitoring opportunities are available.

Messages

When you install and configure Tivoli Continuous Data Protection for Files, it works unobtrusively in the background. As a result, you might not need to access Tivoli Continuous Data Protection for Files until you want to restore a file. Unless you want to do some active monitoring of Tivoli Continuous Data Protection for Files, it is advised that you allow Tivoli Continuous Data Protection for Files to notify you when your attention is needed for your system. For example, if you are running out of space in your storage area, Tivoli Continuous Data Protection for Files warns you with a message.

To receive messages from Tivoli Continuous Data Protection for Files, you must configure Tivoli Continuous Data Protection for Files to send you messages. By default, Tivoli Continuous Data Protection for Files sends you messages. You configure this setting in the **Allow program messages to pop up** list in the **Advanced** page of the Settings Notebook.

Tivoli Continuous Data Protection for Files Icon in the System Tray

When the Tivoli Continuous Data Protection for Files daemon is protecting your files as a logged in application, the Tivoli Continuous Data Protection for Files icon is shown in the desktop system tray. (If Tivoli Continuous Data Protection for Files is running as a service, the icon is not shown in the system tray). If you do not see the icon in your system tray, and Tivoli Continuous Data Protection for Files is not running as a service, you must restart the process. See "Restarting the Tivoli Continuous Data Protection for Files client process" on page 78.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website: http://windows.microsoft.com/en-US/windows7/Change-how-icons-appear-in-the-notification-area.

Monitoring protection with the Tivoli Continuous Data Protection for Files client

If you want to actively check the status of your protection, there are several checks you can do in the Tivoli Continuous Data Protection for Files client user interface.

Tivoli Continuous Data Protection for Files client Status page

The Status page provides status information at a glance. For an explanation of all fields on the page, see "Status panel of Tivoli Continuous Data Protection for Files" on page 83

Icon color

The icons on the Status panel reflect the status of those areas. In normal conditions, the icons are blue. The icon changes to yellow as a warning.

The **Remote storage** icon becomes yellow when you are disconnected from your remote storage area. This is not necessarily cause for alarm. For example, if you know that you will connect to your remote storage location before long, you do not need to worry. Tivoli Continuous Data Protection for Files queues changed files while the storage area is unavailable, and transfers the files when the storage becomes available. However, if you are not aware that your remote storage is unavailable, and do not know that you will soon recover your connection, you should investigate your remote storage.

The **Local Storage** icon becomes yellow if Tivoli Continuous Data Protection for Files cannot access the local storage area.

If the color of any icon is not blue and you are not aware of a transient threat to your protection system, you must investigate further.

The **Restore** icon and the **My Files** icon never change color.

Icon Displays Data and Links

Hover over an icon to show summary information and links to detailed information.

The summary information for each icon gives clues about your protection status, and the links provide details.

My Files icon

Files under protection

If the number of files under protection is not reasonable given the changes you made and list of files that you configured, you must investigate further. Verify that you accurately configured the list of files to protect.

Click the **Settings** link under **Files under protection** to configure the files to protect.

View Report

The **View Report** link opens a detailed list of recent protection activity. Failed activities are listed with messages describing the failures.

Email protection

If the **Last successful backup on** field does not indicate a recent successful backup, verify the configuration of your email application and the schedule for your email backups.

Click the **Settings** link under **Email protection** to configure your email protection.

Local Storage icon

If the **Usage** bar indicates that your local storage is full, you must investigate further. You can reconfigure your local storage area.

Click the **Settings** link to configure your local storage area.

Remote Storage

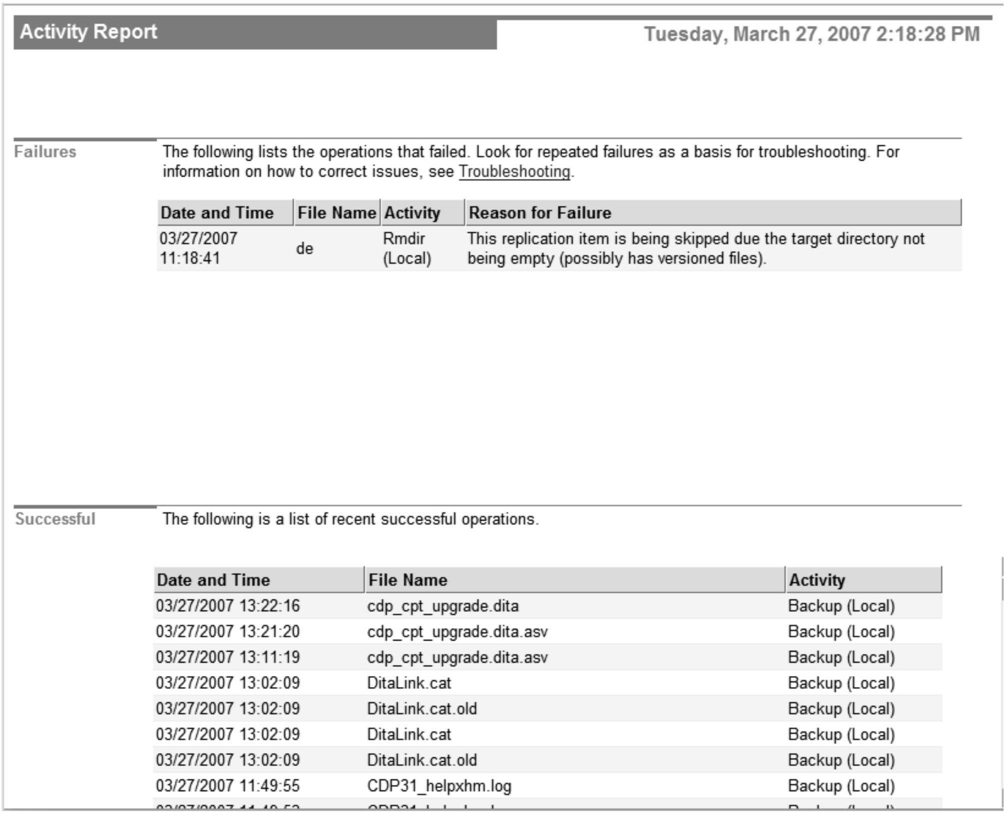
Usage bar

If the usage bar indicates that your remote storage is full, you must investigate further. You can reconfigure your remote storage area.

Click the **Settings** link to configure your remote storage area.

Continuous Protection Activity Report

A report of continuous protection activity is available from a link in the Status panel. The report is called **Activity Report**. To go to the **Activity Report**, see "Viewing the continuous protection activity report of a Tivoli Continuous Data Protection for Files client" on page 88



Activity Report

Tuesday, March 27, 2007 2:18:28 PM

Failures

The following lists the operations that failed. Look for repeated failures as a basis for troubleshooting. For information on how to correct issues, see Troubleshooting.

Date and Time	File Name	Activity	Reason for Failure
03/27/2007 11:18:41	de	Rmdir (Local)	This replication item is being skipped due the target directory not being empty (possibly has versioned files).

Successful

The following is a list of recent successful operations.

Date and Time	File Name	Activity
03/27/2007 13:22:16	cdp_cpt_upgrade.dita	Backup (Local)
03/27/2007 13:21:20	cdp_cpt_upgrade.dita.asv	Backup (Local)
03/27/2007 13:11:19	cdp_cpt_upgrade.dita.asv	Backup (Local)
03/27/2007 13:02:09	DitaLink.cat	Backup (Local)
03/27/2007 13:02:09	DitaLink.cat.old	Backup (Local)
03/27/2007 13:02:09	DitaLink.cat	Backup (Local)
03/27/2007 13:02:09	DitaLink.cat.old	Backup (Local)
03/27/2007 11:49:55	CDP31_helpxhm.log	Backup (Local)

The **Activity Report** lists failed activities at the start of the report. The failed activity is accompanied by a reason for the failure. Successful activities are listed in the next section.

The list is not a complete list of all activities, only the most recent activities are listed:

Backup
Tivoli Continuous Data Protection for Files creates a backup copy on the storage area.

Delete Tivoli Continuous Data Protection for Files deletes the most recent backup copy from the storage area.

Purge Tivoli Continuous Data Protection for Files deletes a versioned backup copy because the storage area is full.

Report
Tivoli Continuous Data Protection for Files sends a report of scheduled backup activity to the central management area.

Version
Tivoli Continuous Data Protection for Files adds a version suffix to a backup copy. A backup copy becomes versioned when Tivoli Continuous Data Protection for Files creates a newer backup copy of the same file.

Scheduled Backup Report

Reports of scheduled backup activity are available from links in the scheduled backup reports table. Because email is protected on a schedule, this report also corresponds to email protection. Reports are available for your local Tivoli Continuous Data Protection for Files client and for clients that you manage.

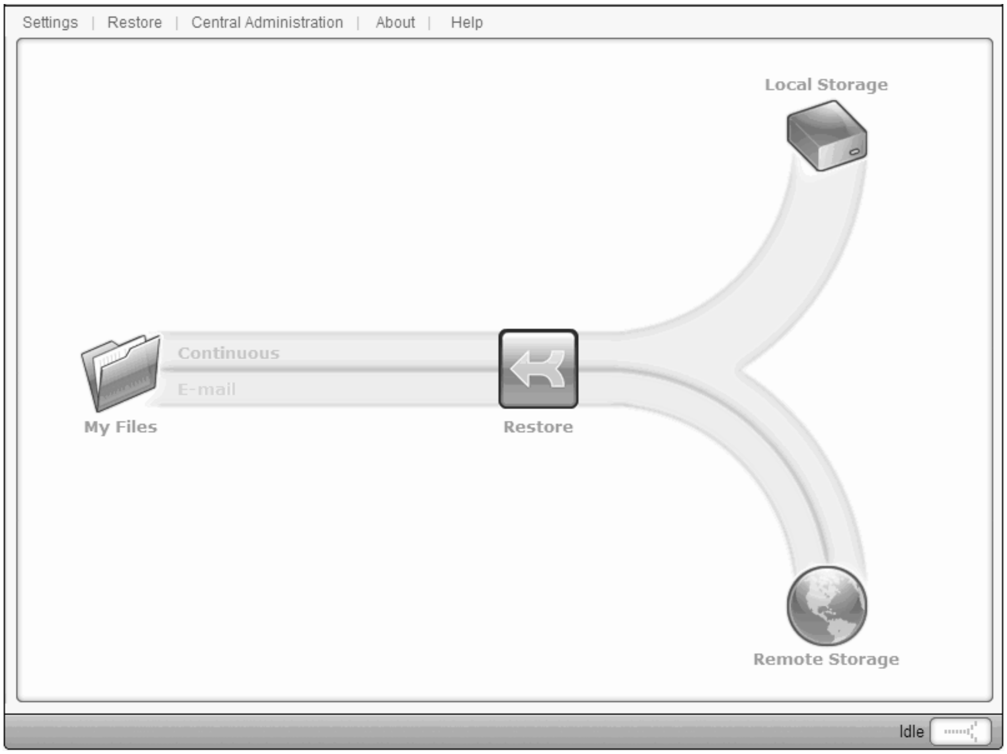
When managing Tivoli Continuous Data Protection for Files clients, you can view the reports to see when the last successful scheduled backups took place. If it was an extended time, it may indicate a problem with the Tivoli Continuous Data Protection for Files client.

For an explanation of the scheduled backup reports table, see “Scheduled backup reports table of Tivoli Continuous Data Protection for Files” on page 54

To go to the scheduled backup reports table, see “Viewing the report of scheduled backups by a Tivoli Continuous Data Protection for Files client” on page 88

Status panel of Tivoli Continuous Data Protection for Files

The Status panel is the entry to the Tivoli Continuous Data Protection for Files user interface. You can view a summary of how your files are being protected, and link to other panels to view details and change protection settings.



The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

Menu Links

This panel has either four or five links depending on if it is the standard or starter version:

Settings
Links to the “Settings Notebook” on page 31. Use the Settings Notebook to change your protection settings.

Restore
Links to the “Restore Wizard of Tivoli Continuous Data Protection for Files” on page 90. Use the Restore wizard to restore a file from a backup copy.

Central Administration
Links to the “**Central Administration Settings** window of Tivoli Continuous Data Protection for Files” on page 103. Use the Central Administration panel to manage Tivoli Continuous Data Protection for Files on other computers.

Note: The Central Administration feature is available in the OEM and in the Tivoli Continuous Data Protection for Files full versions of the product.

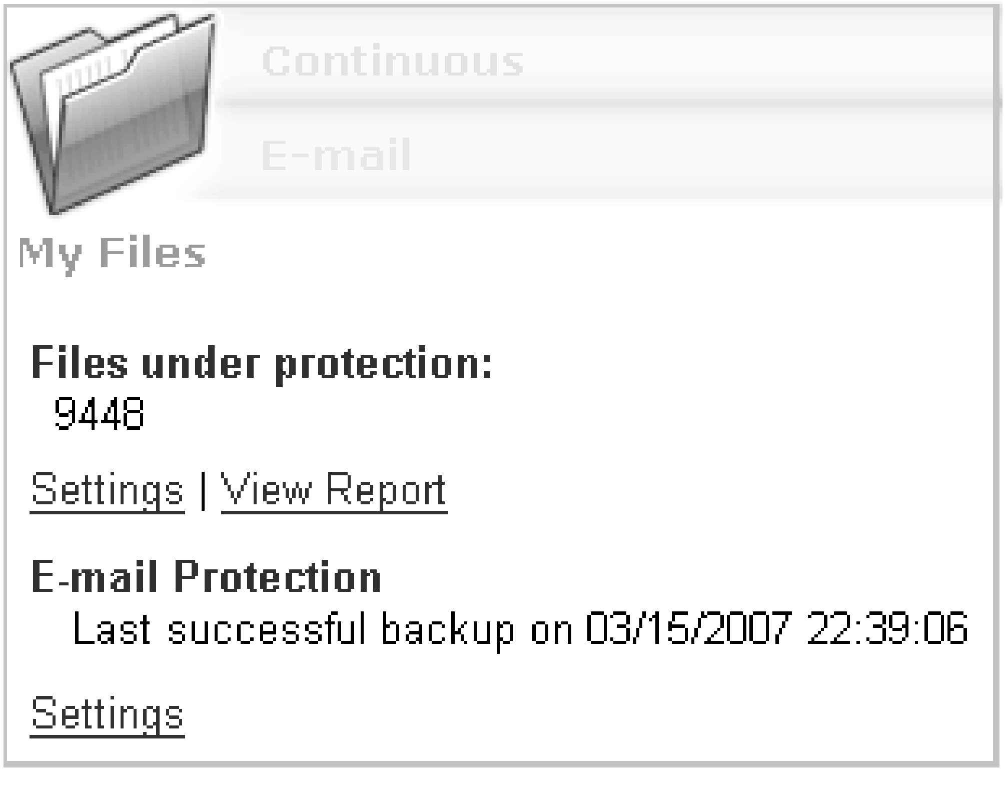
About Provides information about the product, including version level.

Help Links to the online help documentation.

Graphic Icons

The screen contains a graphic representation of Tivoli Continuous Data Protection for Files protection. Hover over an icon to show summary information and links to detailed information.

My Files



Files under protection:
9448

E-mail Protection
Last successful backup on 03/15/2007 22:39:06

Files under protection:

Number
An approximation of the total number of files that are protected. Due to the nature of the program and how the logging is done, this number is only an approximation.

Settings

Links to the **Files to Protect** panel of the Settings Notebook. Use this link to change the files that are continuously protected.

View Report

Links to the **Activity Report**. The **Activity Report** shows details of recent backup and restore activity.

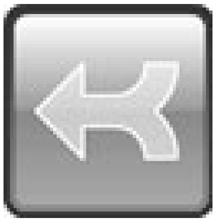
For an explanation of the **Activity Report**, see “Continuous Protection Activity Report” on page 81.

Email Protection

Settings

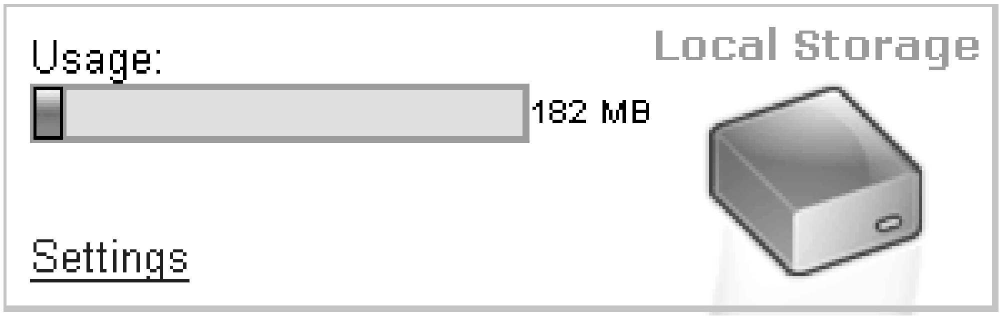
Links to the **Email** panel of the Settings Notebook. Use this link to change the email application that is protected.

Restore



Links to the restore wizard, which helps you restore files from backup copies.

Local Storage

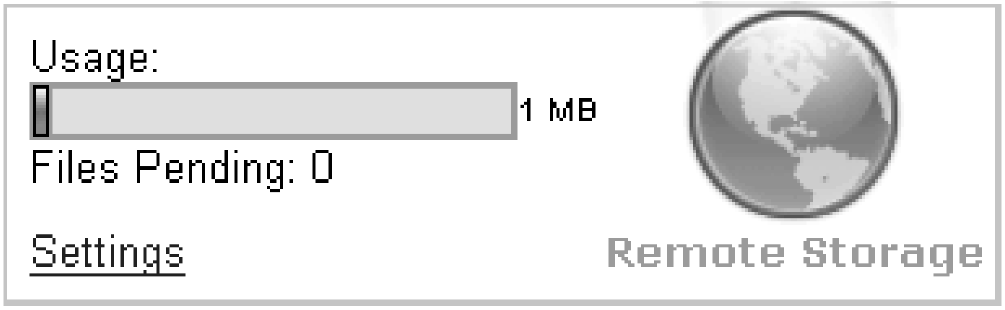


Usage Shows approximately how much space is being used by backup copies on local storage. The bar graph indicates what portion of the storage is being used. The text indicates the usage in bytes.

Settings

Links to the **General** panel of the Settings Notebook. Use this link to change the size or location of your local storage; how many versions to keep of each protected file; and whether to use local storage, remote storage, or both.

Remote Storage


Usage:

1 MB

Files Pending: 0

Usage Shows approximately how much space is being used by backup copies on remote storage. The bar graph indicates what portion of the storage is being used. The text indicates the usage in bytes.

Files Pending
When remote storage is not available, Tivoli Continuous Data Protection for Files queues backup copies that are destined for remote storage. When the remote storage becomes available, Tivoli Continuous Data Protection for Files transmits the queued backup copies. This field indicates the number of files that are destined for remote storage but were not transmitted yet.

Settings
Links to the **Remote Storage** panel of the Settings Notebook.

Status Panel

The status bar shows a brief text message of the status of backup and restore activities. Hover over the icon to view the open status of five activities, and links to detailed status reports.

The status of the activities can be:

Idle The activity is idle. An activity can become idle before finishing if it is stopped by the user.

Preempted
The activity is idle, pending a higher-priority activity.

Active The activity is active.

Paused
The activity was paused by the user.

Disconnected
The storage area is unavailable.

Disabled
The storage area is not configured.

System Tray

The System Tray shows the Tivoli Continuous Data Protection for Files icon. When you hover the cursor over this icon, the loaded version is shown. In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

If the status is disconnected or paused, the icon changes to .

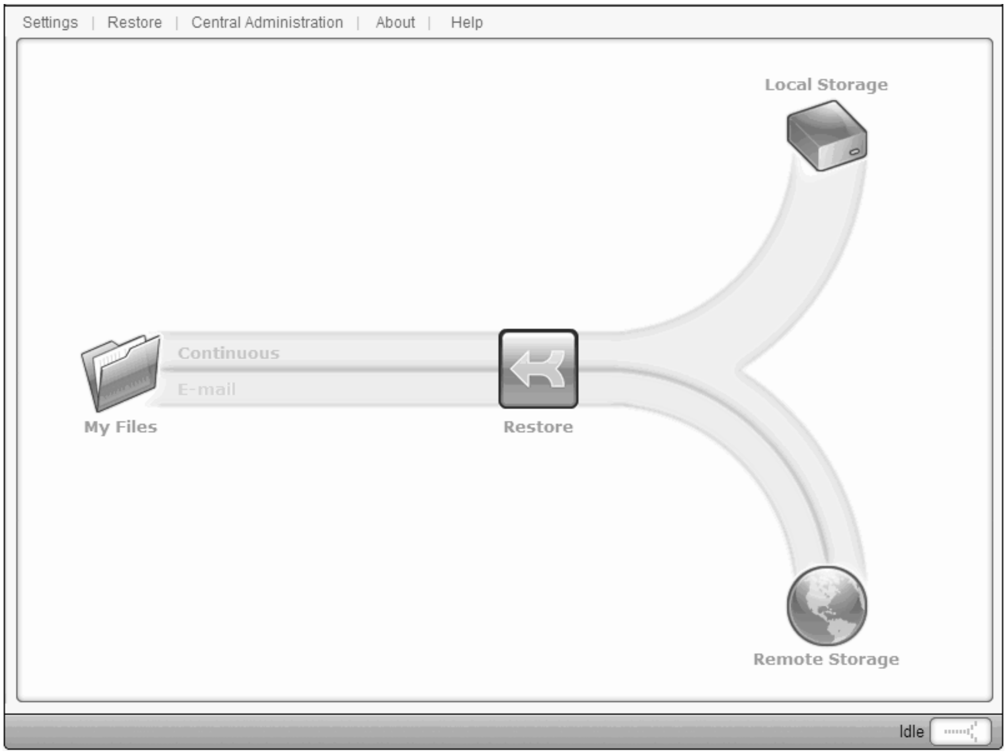
If errors occurred, the icon changes to .

Note:
- The error icon disappears when the user views the activity report. The error icon reappears when the error occurs again.
- Only the error icon is shown if errors occurred and the status is disconnected.

Viewing reports by Tivoli Continuous Data Protection for Files

You can view reports of continuous and scheduled protection activities.

Assume that you start from the Tivoli Continuous Data Protection for Files Status panel.



The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

Viewing the continuous protection activity report of a Tivoli Continuous Data Protection for Files client

You can see a detailed report of recent backup activities.

About this task

The report shows successful activities, and failed activities with messages.

Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Let your pointer hover over the **My Files** icon. Summary information and links fly down from the icon.
3. Click the link **View Report**. The **Activity Report** displays.

Viewing the report of scheduled backups by a Tivoli Continuous Data Protection for Files client

Use this report to see a detailed report of scheduled backup activities.

About this task

When viewing the report, choose from a list of backup details. The report shows successful activities, and failed activities with messages.

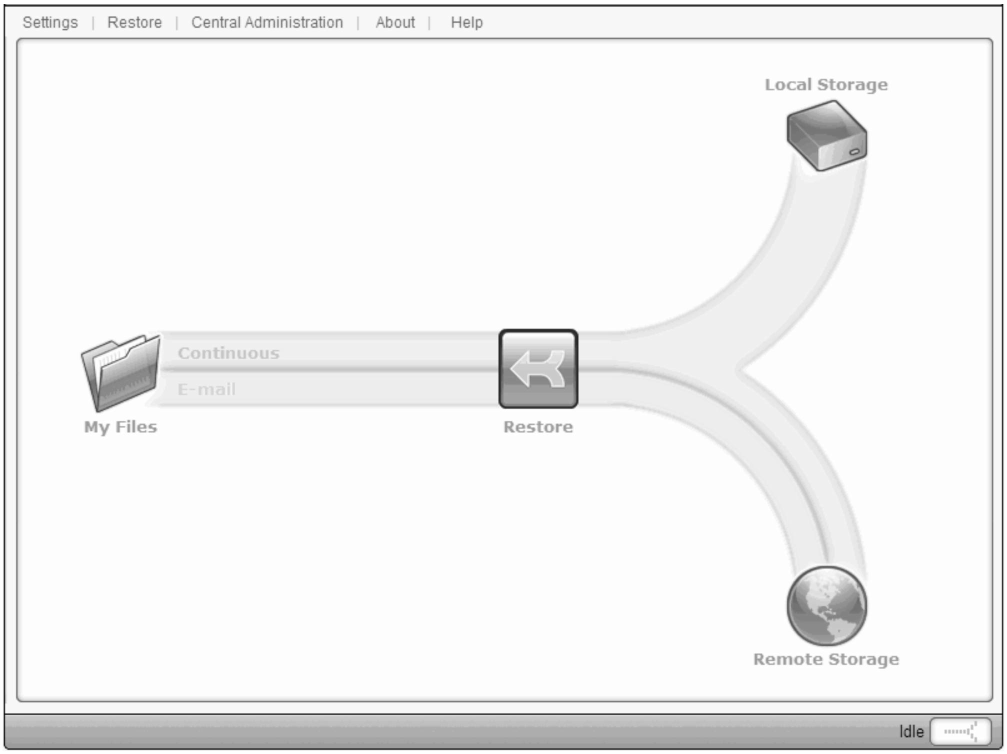
Procedure

1. Open the Tivoli Continuous Data Protection for Files Status panel.
2. Let your pointer hover over the **Remote Storage** icon. The summary information and links fly out.
3. Click the link **Settings**. The Settings Notebook displays; the **Remote Storage** page is selected.
4. Select the **Advanced** page.
5. Click the link **Scheduled Backup Settings**. The **Folders and Files Settings** dialog for scheduled backup displays.
6. Click the link **View Report**.

Chapter 6. Restoring files with the Tivoli Continuous Data Protection for Files client

The Tivoli Continuous Data Protection for Files client makes backup copies of your files so that when the time comes, you can restore your files. You can restore a file that you deleted, and you can restore an earlier version of a file that does not have your recent changes. A wizard guides you to find the file; choose the correct version, and choose the location to restore your file.

Start from the Tivoli Continuous Data Protection for Files client Status panel.



The Status panel is displayed when you click twice the Tivoli Continuous Data Protection for Files client icon ▨ in the system tray, or start the client from the **Start** menu.

Note: In Microsoft Windows 7, there are changes to the notification area where the icons are shown. All icons are hidden by default and users can control what icons are shown. For more information, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Tivoli > CDP for Files > IBM Tivoli Continuous Data Protection for Files**.

Click the large arrow in the middle of the Status panel. The Restore Wizard guides you to restore your file.

For explanations of the Restore Wizard fields, see “Restore Wizard of Tivoli Continuous Data Protection for Files.”

Restore Wizard of Tivoli Continuous Data Protection for Files

Restore a protected file with this Restore Wizard.

Use the control buttons in each wizard page to navigate to all pages. When you reach the final page, click the **Finish** button to restore your files.

The wizard has 4 pages:
- “**Welcome** panel (Restore Wizard) of Tivoli Continuous Data Protection for Files”
- “**Files to Restore** panel of Tivoli Continuous Data Protection for Files”
- “**Restore Location** panel of Tivoli Continuous Data Protection for Files” on page 93
- “Restore wizard **Summary** panel” on page 94

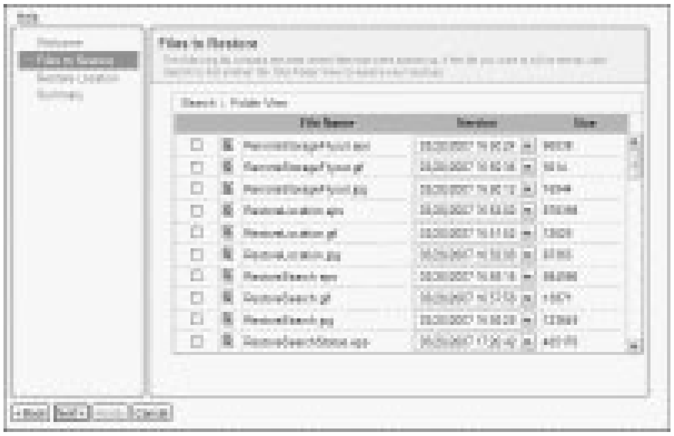
Welcome panel (Restore Wizard) of Tivoli Continuous Data Protection for Files

The **Welcome** panel lists the steps to restore your files. Click the **Next** button to advance to the next panel of the wizard. Click the **Cancel** button to exit the wizard without restoring any files.

Files to Restore panel of Tivoli Continuous Data Protection for Files

Use this panel to select the files that you want to restore.

Files to Restore list



The box contains a list of files that you can choose to restore. Each row contains the following fields:

Select Check the box if you want to restore the file.

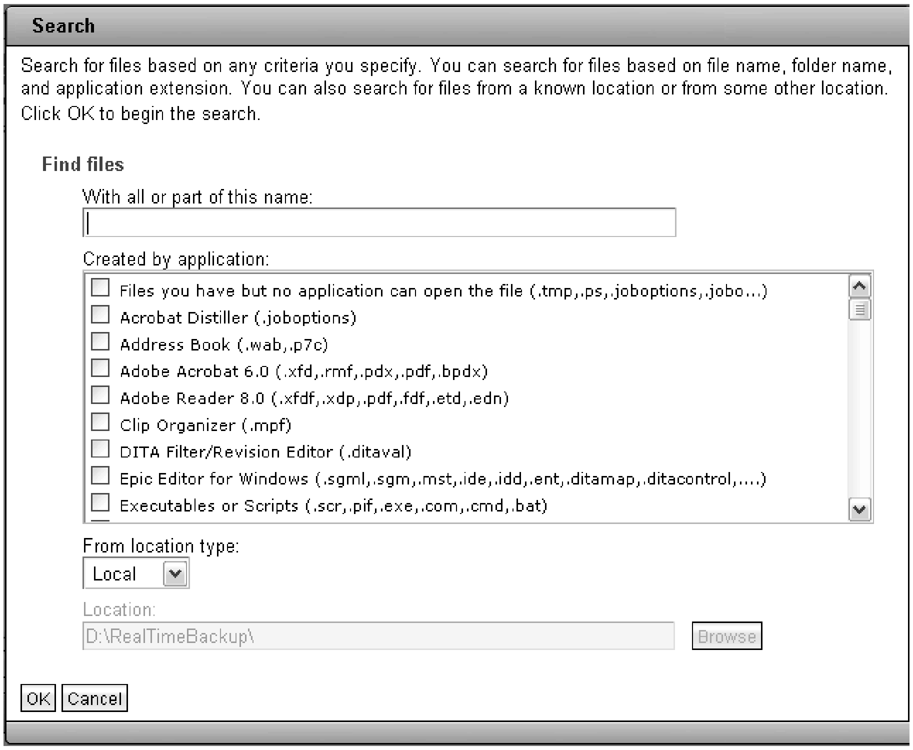
File Name
The name of the file that you can restore. Let your pointer hover over the file name to show the path of the file.

Version
The drop-down box lists the dates and times that this file was modified. Choose the version that you want to restore.

Size The size of the file.

The list initially contains approximately 20 of the files that were most recently backed up. Change the list of files by clicking the **Search** or **Folder View** menu items at the start of the box:

Search
Presents a dialog that allows you to search for backup copies to add to the list.



Search

Search for files based on any criteria you specify. You can search for files based on file name, folder name, and application extension. You can also search for files from a known location or from some other location. Click OK to begin the search.

Find files

With all or part of this name:

Created by application:

☐ Files you have but no application can open the file (.tmp,.ps,.joboptions,.jobo...)
☐ Acrobat Distiller (.joboptions)
☐ Address Book (.wab,.p7c)
☐ Adobe Acrobat 6.0 (.xfd,.rmf,.pdx,.pdf,.bpdx)
☐ Adobe Reader 8.0 (.xfdf,.xdp,.pdf,.fdf,.etd,.edn)
☐ Clip Organizer (.mpf)
☐ DITA Filter/Revision Editor (.ditaval)
☐ Epic Editor for Windows (.sgml,.sgm,.mst,.ide,.idd,.ent,.ditamap,.ditacontrol,....)
☐ Executables or Scripts (.scr,.pif,.exe,.com,.cmd,.bat)

From location type: Local

Location: D:\RealTimeBackup\

The **Search** dialog has several fields. The fields are combined to narrow the search criteria. Leaving any field blank increases the chances of finding more files.

Find files With all or part of this name
Use this field if you know the name or part of the name of the file you want to restore. You can enter a partial file name or folder and use an asterisk as wildcard. If you enter nothing, the search can yield files from any folder with any name.

Find files Created by application
Use this list if you know the application that created the file you want to restore. Check as many applications as you want. If you enter nothing, the search can yield files from any application.

Find files From location type
Choose the location of the backup copy.

You can choose from three locations:

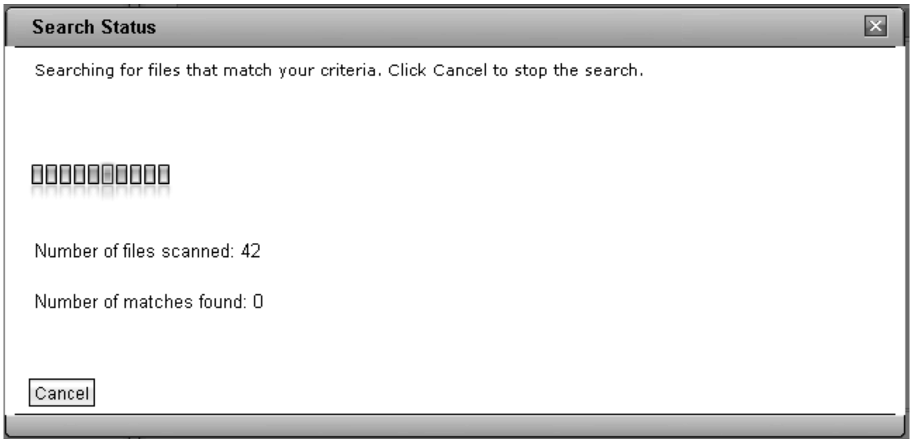
Local The local storage area that is currently configured.

Remote
The remote storage area that is currently configured.

Other Any folder of your choosing. If you previously configured your local or remote storage areas differently than your current configurations, you can search in those previously configured areas. When you choose this option, the **Location** text entry field becomes active. Type the location to search or click the **Browse** button to browse for the folder.

Click the **Search** dialog **OK** to begin searching.

Click the **Search** dialog **Cancel** button to exit the **Search** dialog without searching.



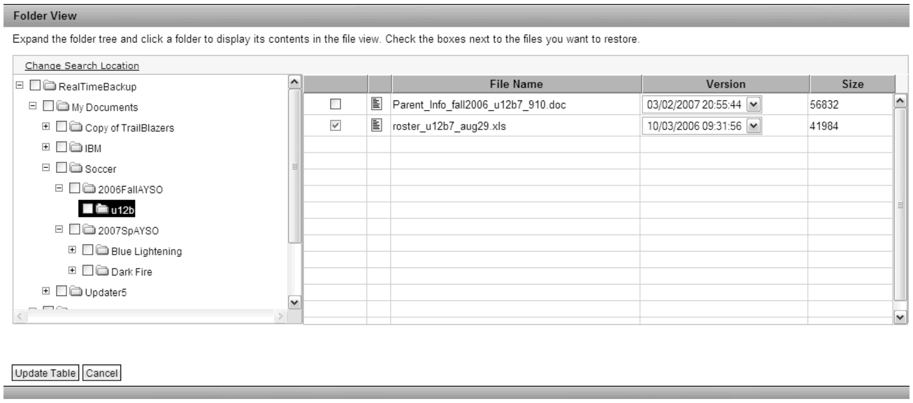
Searching for files that match your criteria. Click Cancel to stop the search.

Number of files scanned: 42

Number of matches found: 0

The **Search Status** window will show the progress of your search. The **Search Status Cancel** button will stop the search and return to the list of files without adding the files in your search criteria. If the search completes without being cancelled, the **Files to Restore** list will contain the results of your search.

Folder View



Expand the folder tree and click a folder to display its contents in the file view. Check the boxes next to the files you want to restore.

		File Name	Version	Size
☐		Parent_Info_fall2006_u12b7_910.doc	03/02/2007 20:55:44	56832
☑		roster_u12b7_aug29.xls	10/03/2006 09:31:56	41984

Presents a dialog that allows you to browse folders to find your files. **Folder View** dialog has the following fields:

Folder tree
Browse the tree to find a folder. Click a folder and the files in that folder will display in the file view the folder tree.

File view
Displays the files in a folder that you chose. Check the box in the **Select** column to select a file. The **Version** list shows the dates that the file was backed up. Choose the version that you want to restore.

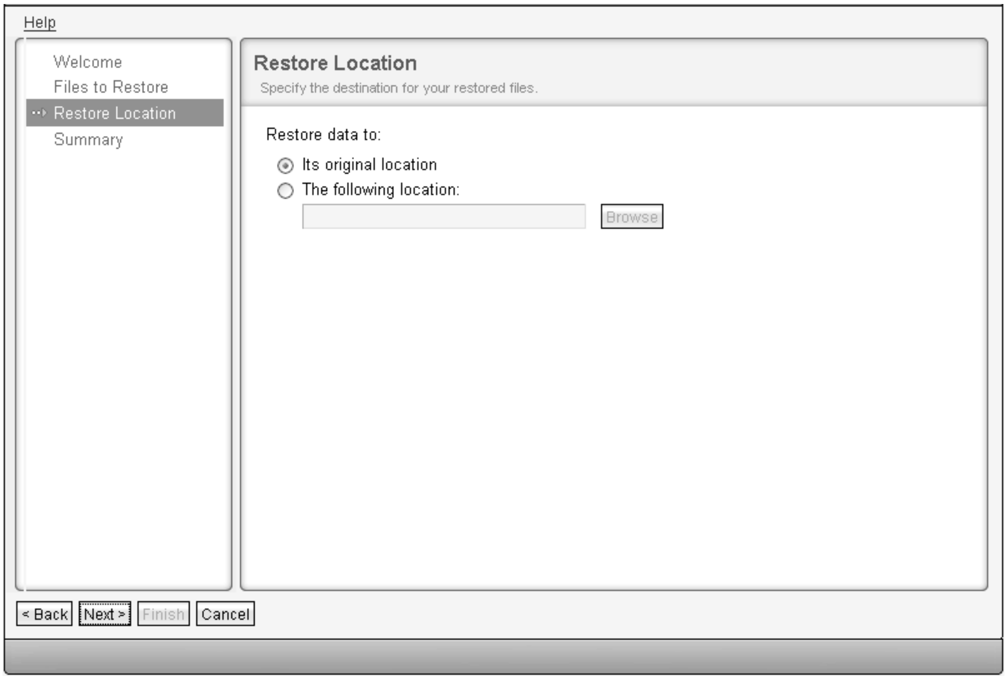
Click **Change search location** to specify the backup location to search for files to restore. The options are **Local**, **Remote**, or **Other**. The user can use the browse to a specific folder if they select **Other**.

Click **Update Table** to add the selected files to the list of files.

Click **Cancel** to exit the dialog without adding any files to the list of files.

Restore Location panel of Tivoli Continuous Data Protection for Files

Use the Restore Location panel to specify a location to restore your files.



Specify the destination for your restored files.

Restore data to:

◉ Its original location

○ The following location:

You can restore your files to their original location, or to a different location.

Restore data to its original location
Check this option if you want to restore the files you chose to their original locations. The original location is the full path that pops up when you hover over the file name in the **Files to Restore** panel.

Restore data to a new location
If you want to restore the files to a different location, check this option and enter the new location in the field. Use **Browse** to find and select the location. All files chosen are restored to the path that you specify. No part of the original path will be appended to the path that you specify.

For example, assume the original file path is `C:\Documents and Settings\Administrator\My Documents\My Pictures\Vacation2006\Family.jpg`. Assume also that you want to restore the file to a folder called `D:\BestPhotos\`. In the **Restore data to** field, you must provide the folder name and a file name. Assume that you specify `D:\BestPhotos\Family2006.jpg`. Tivoli Continuous Data Protection for Files restores the file to this path: `D:\BestPhotos\Family2006.jpg`.

If you are restoring data from the `My Documents` folder to another machine with a different user name, you cannot select to restore to the original location. Instead specify a location such as `\\users\joanne\my documents\`.

Note: When performing a restore to a new folder you must have a trailing \ after the folder name. Otherwise the file being restored is renamed to the folder that is specified. For example, if the user put `D:\BestPhotos` that would now be the name of the restored file.

Restore wizard Summary panel

Use the **Summary** panel to view a summary of your choices, and to start the restore process.

The **Summary** panel displays the locations, and the number of files that you specified in the wizard.

Choose **Back** to return to a previous panel to modify your choices.

Choose **Finish** to restore your files. The **Directory Restore** dialog opens. Use this dialog to specify whether to:

- Restore the latest version of the files in that directory, or to
- Automatically select the latest versions of the files in the folders from a specified date.

If messages are enabled, a message indicates when your restore operation is complete.

Choose **Cancel** to close the wizard without restoring your files.

Chapter 7. Storage areas of Tivoli Continuous Data Protection for Files

Tivoli Continuous Data Protection for Files stores many backup copies in the native file format. You can restore the backup copies by using native file system commands. Some backup copies are created using sub-file copy, compression, or encryption. These must be restored with the Tivoli Continuous Data Protection for Files client.

Format of backup copies created by Tivoli Continuous Data Protection for Files

Tivoli Continuous Data Protection for Files keeps most backup copies in the same format as the original file.

Tivoli Continuous Data Protection for Files provides tools and views to see the backup copies and to restore them. However, in many cases it is not necessary to use Tivoli Continuous Data Protection for Files to restore those backup copies. These files have contents exactly like the originals, in a directory tree structure that simulates the original tree.

Some backup copies are not in the same format as the original files, and must be restored using Tivoli Continuous Data Protection for Files:
- Backup copies stored on Tivoli Storage Manager server
- Backup copies that were encrypted
- Backup copies that were compressed
- Large files that were backed up with subfile copy. In the storage area, the subfile copies have -FPdelta file name suffix.
- Versions of bitmap backups. In the storage area, these backup copies have -TPdelta file name suffix.

Versioning of backup copies created by Tivoli Continuous Data Protection for Files

As you change a file, Tivoli Continuous Data Protection for Files keeps backup copies of each version of the original file.

To track versions of a file, Tivoli Continuous Data Protection for Files adds a version suffix to the file name of the backup copy. On the local storage area, all backup copies contain a version suffix. On the remote storage area, all backup copies (except the most recent backup copy) contain a version suffix. When a file is deleted on your computer, Tivoli Continuous Data Protection for Files adds a version identifier to the file name of the most recent backup copy on the remote storage area.

The version suffix is “-FP” followed by a number. For example, a file named `data.xls` could be stored as versioned backup copy `data.xls-FP1168376676.xls`.

The most recent backup copy of a file is the “active” backup copy. Older backup copies of that file are “inactive” backup copies. If storage space is approaching the limit, Tivoli Continuous Data Protection for Files will delete inactive backup copies of a file before deleting active backup copies.

A file that is protected by schedule could change several times during the schedule interval. Only the last version of the file prior to the end of the schedule will be backed up. A continuously protected file is backed up after every saved change.

Tivoli Continuous Data Protection for Files keeps as many versions of a file on local storage as you configure in the **Versions to keep** field of the **General** page of the Settings Notebook, and as space allows.

Tivoli Continuous Data Protection for Files keeps as many versions of a file on remote storage as you configure in the **Versions to keep** field of the **Remote Storage** page of the Settings Notebook, and as space allows.

Tivoli Continuous Data Protection for Files keeps as many versions of an email file as you configure in the **Versions to keep** field of the **Email Protection** page of the Settings Notebook, and as space allows.

Modifying backup copies

If you move or modify backup copies with native file system tools, the client ceases to function correctly and is not supported.

You can use native file system tools to copy backup copies to restore your original files. Do not use native file system tools to modify backup copies. Use native file system tools to remove backup copies only if you uninstall the client.

Chapter 8. Tivoli Continuous Data Protection for Files central management considerations

Use the concepts, examples, and steps for centrally managing Tivoli Continuous Data Protection for Files clients.

Note: The Central Administration Console feature is available in the OEM and in the Tivoli Continuous Data Protection for Files Standard edition versions of the product.

Configuring Manageable Clients

Tivoli Continuous Data Protection for Files has features that allow an administrator to manage the configuration of other Tivoli Continuous Data Protection for Files clients. You can manage the installed product level and configuration of other Tivoli Continuous Data Protection for Files clients. The administrator can also monitor the activity reports of the other clients. To use the Central Administration Management features, you must configure your Tivoli Continuous Data Protection for Files clients to work together.

These features allow central management:

Tivoli Continuous Data Protection for Files clients pull upgrade and configuration information

Once Tivoli Continuous Data Protection for Files is installed, you can update the product level and configuration. This is done by putting the installer and configuration file in the appropriate downloads folder for the clients. See “Advanced installation of the Tivoli Continuous Data Protection for Files client” on page 21 for details on silent installation.

You can configure the folders that Tivoli Continuous Data Protection for Files clients use to share configuration data

You can configure the downloads and reports folders of the managed clients, and the central administration folder of the managing client. You must configure each so that the managed client use the configuration and information exported by the managing client. The same configuration allows the managing client to view the activity reports of the managed clients. You can change the administration folder of the managing client to communicate with different groups of managed clients. See “Administration folders” on page 101 for details about the central administration folder, and the downloads and reports subfolders.

An Example Configuration

The key to configuring your clients to be managed is in defining the central administration folders. Assume that there is one managing (administrator) client; and two groups of clients to be managed.

In this example, the managed clients in group A do not explicitly configure the **Central administration folder:** field in the **Central Administration Settings** window, so their central administration folder defaults to the `\RealTimeBackup\` folder on the remote storage location. Both computers have the same central administration folder.

Further, this example assumes that the managed clients in group B have different remote storage locations and in one case, no remote storage. Two clients with different remote storage locations have different default central administration folders, and one client without remote storage would have no central administration folder. These three could not be managed as group unless they have a common central administration folder. You want to manage them as a group, so you must specify a common central administration folder. Configure a common central administration folder in the **Central administration folder:** field in the **Central Administration Settings** window.

The configurations of the clients may look like this:

Table 6. Central Administration folder configurations for managing clients.

Computer Name	Group	Remote storage location (configured in Settings Notebook, Remote Storage page)	Central Administration Settings window, Central administration folder field value	The settings in the 2 columns yield the central administration folder
BrightStar	Administrator	not applicable for managing other clients		
Mercury	Managed group A	`\\MyServer\MyShare\`	not configured	`\\MyServer\MyShare\RealTimeBackup`
Venus	Managed group A	`\\MyServer\MyShare\`	not configured	`\\MyServer\MyShare\RealTimeBackup`
Neptune	Managed group B	`\\SpaceMan\CDPstorage\`	`\\SpaceMan\CDPadmin\`	`\\SpaceMan\CDPadmin\`
Uranus	Managed group B	`https://MyISP.com/MyAcct`	`\\SpaceMan\CDPadmin\`	`\\SpaceMan\CDPadmin\`
Pluto	Managed group B	not configured	`\\SpaceMan\CDPadmin\`	`\\SpaceMan\CDPadmin\`

Using the Example Configuration to Manage a Group

When you want to manage group A, configure the central administration folder of BrightStar to be the same as the central administration folder for group A.

Table 7. BrightStar Central Administration folder for managing group A.

Computer Name	Group	Remote storage location (configured in Settings Notebook, Remote Storage page)	Central Administration Settings window, Central administration folder: field value	The settings in the 2 columns yield the central administration folder
BrightStar	Administrator	not applicable for managing other clients	`\\MyServer\MyShare\RealTimeBackup`	`\\MyServer\MyShare\RealTimeBackup`

For example, to manage the configuration of the clients in group A, do this:

1. Use the Settings Notebook to update the configuration of BrightStar. Configure the values that you want to export to group A.
2. Click the **Apply** button on any page of the Settings Notebook.
3. Open the **Central Administration Settings** window.
4. In the **Central administration folder** field type (or browse to)`\\MyServer\MyShare\RealTimeBackup`.
5. Click the **OK** button. The window closes.
6. Open the **Central Administration Settings** window again.
7. Check the **Publish this computer's settings as the configuration template for other computers to use** check box.

Now consider whether you want BrighStar to operate with this configuration, or if you want to return to the Settings Notebook and restore the previous configuration.

When you want to manage group B, configure the BrightStar central administration folder to be the same as the central administration folder for group B.

Table 8. BrightStar Central Administration folder for managing group B.

Computer Name	Group	Remote storage location (configured in Settings Notebook, Remote Storage page)	Central Administration Settings window, Central administration folder field value	The settings in the 2 columns yield the central administration folder
BrightStar	Administrator	not applicable for managing other clients	`\\SpaceMan\CDPadmin\`	`\\SpaceMan\CDPadmin\`

For example, follow these steps to view the backup reports of the clients in group B:

1. Open the **Central Administration Settings** window.
2. In the **Central administration folder** field type (or browse to)`\\SpaceMan\CDPadmin\`.
3. Click the **OK** button. The window closes.
4. Open the **Central Administration Settings** window again.
5. Click the **View Report** link. The remote storage reports table opens. The remote storage reports table gives a summary of scheduled backup activity for the group B computers.

Now consider whether you want BrightStar to operate with this central administration folder, or if you want to restore the previous central administration folder.

Use the Example Configuration to Manage a Single Client in a Group

When you want to manage Mercury, configure the central administration folder of BrightStar to be the same as the central administration subfolder that is unique for Mercury.

Table 9. BrightStar Central Administration folder for managing Mercury.

Computer Name	**Group**	**Remote storage location (configured in Settings Notebook, Remote Storage page)**	**Central Administration Settings window, Central administration folder field value**	**The settings in the 2 columns yield the central administration folder**
BrightStar	Administrator	not applicable for managing other clients	`\\MyServer\MyShare\RealTimeBackup\Mercury\`	`\\MyServer\MyShare\RealTimeBackup\Mercury\`

For example, follow these steps to manage the configuration of the client on Mercury:

1. Use the Settings Notebook to update the configuration of BrightStar. Configure the values that you want to export to Mercury.
2. Click the **Apply** button on any page of the Settings Notebook.
3. Open the **Central Administration Settings** window.
4. In the **Central administration folder** field type (or browse to) `\\MyServer\MyShare\RealTimeBackup\Mercury\`.
5. Click the **OK** button. The window closes.
6. Open the **Central Administration Settings** window again.
7. Check the **Publish this computer's settings as the configuration template for other computers to use** check box.

Now consider whether you want BrightStar to operate with this configuration, or if you want to return to the Settings Notebook and restore the previous configuration.

Manage clients with file system tools

The previous examples assume that you use the Tivoli Continuous Data Protection for Files feature (**Publish this computer's settings as the configuration template for other computers to use**) to distribute configurations to the managed clients. You can also use file system tools to distribute configuration files to the managed clients. You can use file system tools to copy a configuration file to the downloads folder for a single client or for a group of clients. Assume that the managed clients are configured as outlined in the previous steps, so that they can be managed individually or managed as a group. The following table indicates the appropriate downloads folder for configuring the group or the individual computer.

Table 10. Downloads folders for managing groups and clients

Computer Name	Group	Copy a configuration file to this folder to manage the group.	Copy a configuration file to this folder to manage the individual computer.
BrightStar	Administrator	Not applicable for the administrator computer	Not applicable for the administrator computer
Mercury	Managed group A	`\\MyServer\MyShare\RealTimeBackup\BackupAdmin\Downloads`	`\\MyServer\MyShare\RealTimeBackup\Mercury\BackupAdmin\Downloads`
Venus	Managed group A	`\\MyServer\MyShare\RealTimeBackup\BackupAdmin\Downloads`	`\\MyServer\MyShare\RealTimeBackup\Venus\BackupAdmin\Downloads`
Neptune	Managed group B	`\\SpaceMan\CDPadmin\BackupAdmin\Downloads`	`\\SpaceMan\CDPadmin\Neptune\BackupAdmin\Downloads`
Uranus	Managed group B	`\\SpaceMan\CDPadmin\BackupAdmin\Downloads`	`\\SpaceMan\CDPadmin\Uranus\BackupAdmin\Downloads`
Pluto	Managed group B	`\\SpaceMan\CDPadmin\BackupAdmin\Downloads`	`\\SpaceMan\CDPadmin\Pluto\BackupAdmin\Downloads`

Administration folders

Tivoli Continuous Data Protection for Files uses particular folders to manage reports, configuration settings, and product level. Clients pull configuration information and new product code from these folders. Clients store their status reports in these folders. Clients can push their configuration information to these folders for other clients to use.

The central administration folder for a group of computers can be specified in the **Central Administration Folder** field in the **Central Administration Settings** window. If the **Central Administration Folder** field is not configured, then the central administration folder defaults to the `\RealTimeBackup\` folder in the remote storage area. If neither the **Central Administration Folder** field nor a remote storage area is configured, then there is no central administration folder.

Note: There is no administration folder when you specify Tivoli Storage Manager server remote storage. If you use Tivoli Storage Manager server remote storage and you want to use administration folders, you must configure the **Central Administration Folder** field in the **Central Administration Settings** window.

The administration folder contains two levels of administrative subfolders.

Computer-specific subfolders

These folders apply to only one computer. In each computer-specific subfolder, there are two subfolders:

The Reports folder

The client stores status reports in the Reports folder. You can view the reports in the graphical user interface of the client. The full path of the reports folder is `administration folder location\computer name\BackupAdmin\Reports\`.

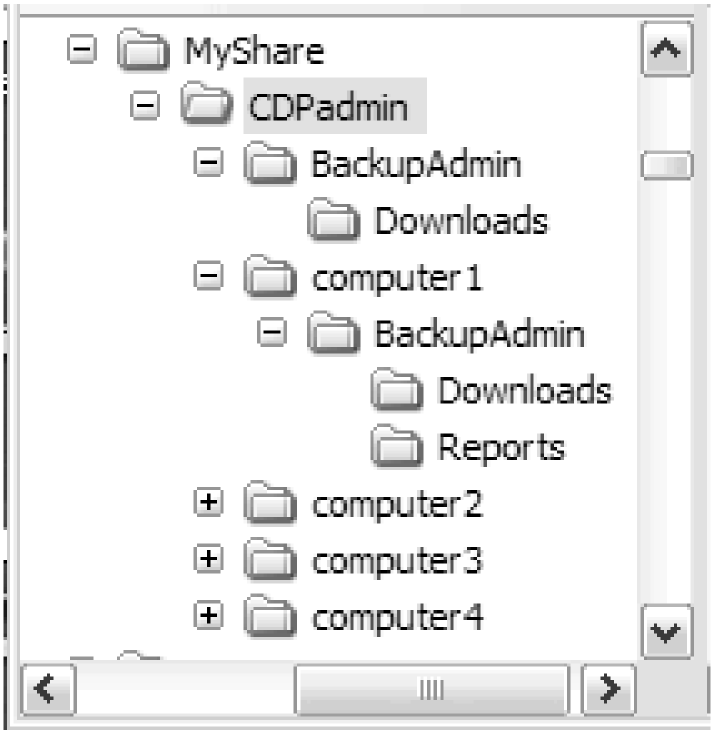
The Downloads folder

When you put product upgrades or configuration files in this folder, the client automatically adopts the product upgrades or configuration. The full path is `administration folder location\computer name\BackupAdmin\Downloads\`.

Note: The computers that use this information must have read access to the administration folders.

Group administrative subfolders

These folders apply to all computers that share this administration folder. In each group administrative subfolder, there is a Downloads subfolder. When you put product upgrades or configuration files in the group administrative Downloads subfolder, all clients that share this group administrative folder automatically adopt the product upgrades or configuration.



Example of administration subfolder names

There are examples of administration subfolder names in the table `Central Administration Folder Names`, given two specifications of the central administration folder. In one column, assume that the central administration folder is configured in the **Central Administration Folder:** field in the **Central Administration Settings** window as `\\MyServer\MyShare\CDPadmin\`. In another column, assume that the central administration folder is not configured in the **Central Administration Folder:** field in the **Central Administration Settings** window, but defaults to the remote storage location. Assume that the remote storage location is configured as `\\MyServer\MyShare\`. For both specifications, assume that your computer name is Computer1.

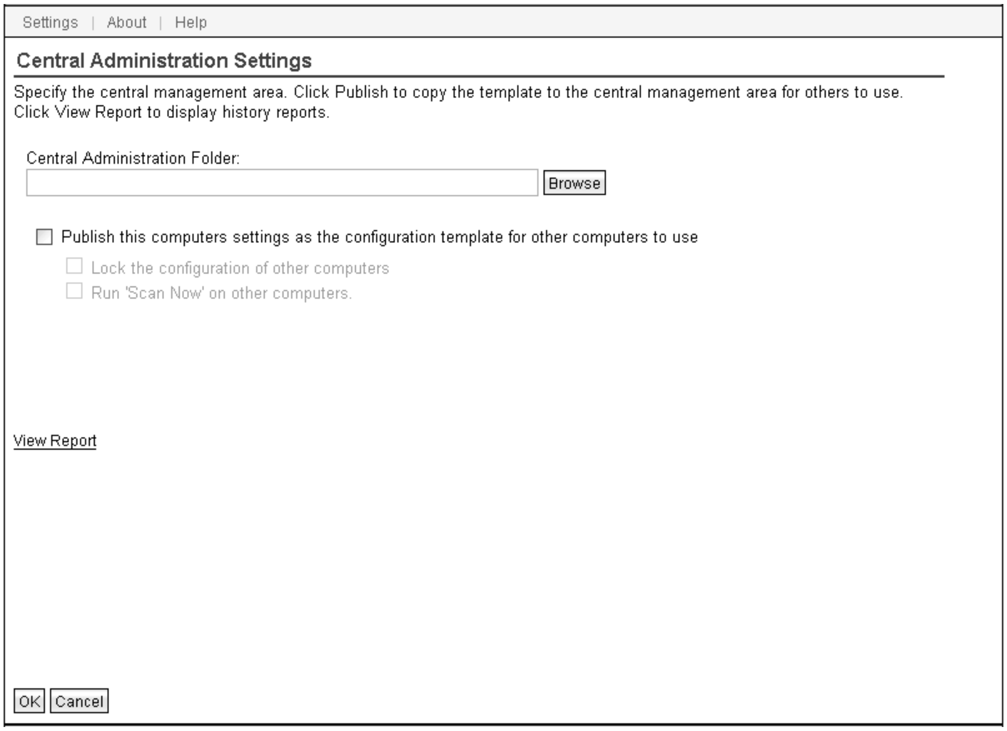
Table 11. Central Administration Folder Names

	Central Administration area is configured in the Central administration folder: field in the Central Administration Settings window as `\\MyServer\MyShare\CDPadmin\`	**Central Administration area is not configured in the Central administration folder: field in the Central Administration Settings window, but defaults to a subfolder of the remote storage location: `\\MyServer\MyShare\`**
Central administration folder:	`\\MyServer\MyShare\CDPadmin\`	`\\MyServer\MyShare\RealTimeBackup\`
Reports folder name for single computer:	`\\MyServer\MyShare\CDPadmin\Computer1\BackupAdmin\Reports\`	`\\MyServer\MyShare\RealTimeBackup\Computer1\BackupAdmin\Reports\`
Downloads folder name for single computer:	`\\MyServer\MyShare\CDPadmin\Computer1\BackupAdmin\Downloads\`	`\\MyServer\MyShare\RealTimeBackup\Computer1\BackupAdmin\Downloads\`
Downloads folder name for all computers that share the central administration folder:	`\\MyServer\MyShare\CDPadmin\BackupAdmin\Downloads\`	`\\MyServer\MyShare\RealTimeBackup\BackupAdmin\Downloads\`

Central Administration Settings window of Tivoli Continuous Data Protection for Files

Use the **Central Administration Settings** window to identify administration folders for this computer, and to manage the configuration settings on other computers.

Note: The Central Administration feature is available in the OEM and in the Tivoli Continuous Data Protection for Files Standard edition versions of the product.



Central Administration Settings

Specify the central management area. Click Publish to copy the template to the central management area for others to use. Click View Report to display history reports.

Central Administration Folder:

☐ Publish this computers settings as the configuration template for other computers to use

☐ Lock the configuration of other computers

☐ Run 'Scan Now' on other computers.

Central Administration Folder field

Type or browse for a folder that you want as the central administration folder for this computer. The administrative tasks on the **Central Administration Settings** window are limited to only those computers that are centrally managed from this folder. If you type the name of a folder that does not exist, Tivoli Continuous Data Protection for Files creates the folder.

The central administration folder is used for several purposes. You can change the folder depending on your purpose. See a discussion of central administration folder uses in "Administration folders" on page 101.

Publish settings for configurating other computers check box

When managing Tivoli Continuous Data Protection for Files on a group of computers, it is customary to configure one computer as the template for all computers in the group. If you configured other computers to share the central administration folder of this computer, they can be centrally managed by this computer. Check this box to use the settings on this computer to configure the other computers. When you click **OK**, the configuration settings file on this computer is copied to the downloads subfolder of the central administration folder that is shared by the group of computers. All computers that share the central administration folder adopt the Tivoli Continuous Data Protection for Files settings that you publish.

If you publish the settings of this computer, your management of the group can be further extended:

Lock the configuration of other computers
Check this box to prevent any of the centrally managed computers from changing their settings.

Note: If you use the published configuration file to push installation to another computer, all Tivoli Continuous Data Protection for Files clients that share the central administration folder with the new client are prevented from updating their configurations.

Run "Scan Now" on other computers

When you change a configuration to protect files and folders that were not previously protected, you should back up all files. See “When to back up all files” on page 44. Check this box to force the centrally managed computers to back up all protected files.

Note: Publishing to managed computers a configuration file with this setting can put a large burden on the network and the computing resources of the managed computers.

Note: If you use the published configuration file to push installation to another computer, do not check this box. If you use this configuration setting in a push installation, the push-installed Tivoli Continuous Data Protection for Files client creates backup copies in the system context. When you later run Tivoli Continuous Data Protection for Files in the user context, you can have problems restoring these files.

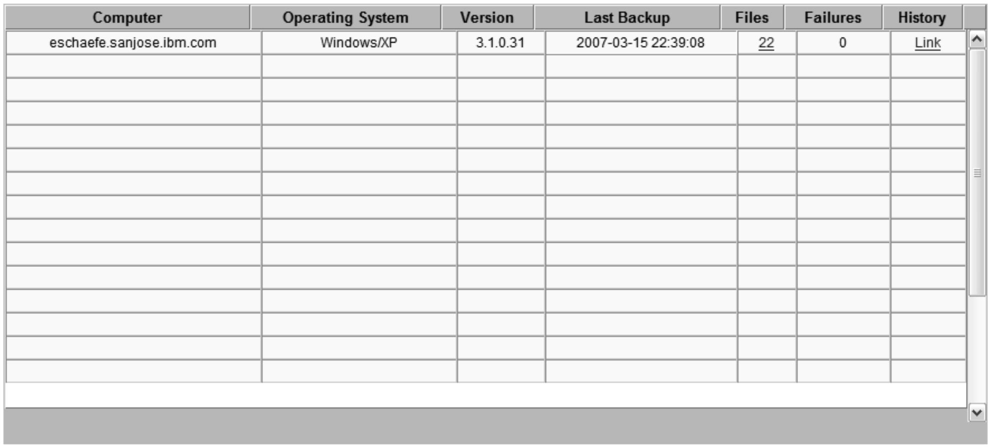
View Report link

Click the **View Report** link to show a table of scheduled backup reports for the computers that are centrally managed.

Scheduled backup reports table of Tivoli Continuous Data Protection for Files

Use the reports table to monitor scheduled backups to remote storage areas.

The reports table shows summary information of all users who back up files to the same remote storage location. Click the links in the table to show more detailed information.



Computer	Operating System	Version	Last Backup	Files	Failures	History
eschaefe.sanjose.ibm.com	Windows/XP	3.1.0.31	2007-03-15 22:39:08	22	0	Link

The scheduled backup reports table gives a summary of scheduled backups to remote storage areas for all computers who share a common central administration folder. For more information about central administration folders, see “Administration folders” on page 101.

To see the reports table, you must be connected to your remote storage area.

Each row identifies the reports associated with one Tivoli Continuous Data Protection for Files client, and contains the following cells:

Version
The version of Tivoli Continuous Data Protection for Files.

Last Backup
The last completed scheduled backup.

Files
A number indicating approximately how many files were successfully backed up at the last schedule. Due to the nature of the program and how the logging is done, this number is only an approximation.

Click the number to open a complete report of the scheduled backup. In addition to files backed up, the report shows administrative activities and failed backup attempts.

Failures
This column indicates how many errors there were during the backup.

Click on the number to open a report of the errors during scheduled backup.

History
Click the link to open a list of the historical backup and failure logs. Select the logs to view more information. Only reports that had files backed up are listed as active links.

Chapter 9. Protecting a server with Tivoli Continuous Data Protection for Files

Consider the following issues when you protect a server.

Managing a server that stores backup files

If you are protecting a server that contains remote storage areas for several Tivoli Continuous Data Protection for Files clients, you can avoid protecting all versioned backup copies. Because all versioned backup copies on a remote storage area contain an -FP suffix, you can exclude versioned backup copies from protection by excluding -FP. This way you will protect only the most recent backup copies.

Tivoli Continuous Data Protection for Files cannot protect backup copies that it has encrypted. This means that Tivoli Continuous Data Protection for Files cannot create encrypted backup copies, and then make backup copies (encrypted or not) of those backup copies.

Chapter 10. Troubleshooting the Tivoli Continuous Data Protection for Files client

Information is available for some common problems and suggested solutions are provided.

Files are not backed up by Tivoli Continuous Data Protection for Files

Files can fail backup for several reasons. Some common reasons are provided in this section.

Storage for backup copies is not correctly configured in Tivoli Continuous Data Protection for Files

If the area to store backup copies of your protected files is not properly specified, Tivoli Continuous Data Protection for Files can not back up files.

Verify that you have correctly specified local or remote storage areas in the Settings Notebook. Local storage and which location (local or remote) is specified in the "**General** panel of client Settings Notebook" on page 33 of the Settings Notebook. Remote storage is specified in the "**Remote Storage** panel of client Settings Notebook" on page 46.

Files to protect are incorrectly configured in Tivoli Continuous Data Protection for Files

The files that Tivoli Continuous Data Protection for Files protects are configurable. If you have configured your list of protected files incorrectly, Tivoli Continuous Data Protection for Files does not back up the files.

Tivoli Continuous Data Protection for Files backs up only those files that are configured for protection. The list of continuously protected files is configured in the "**Files to Protect** panel of client Settings Notebook" on page 34 of the Settings Notebook. Note that exclusions from protection have priority over inclusions. If an application or file path is explicitly included for protection, verify that no list items exclude the file from protection. See "Including and excluding files from protection" on page 37.

Files in use are not backed up by Tivoli Continuous Data Protection for Files

Attempts to perform a local or remote backup of a file that is saved but not closed can fail. This can occur with Quicken Quick Books objects (files with an extension ending in .QBW).

The failure is indicated by the message in the Windows System Tray: `The software has experienced a problem. Check for details in the View Report link from the Status page. Also check the Windows System Event log and Application log.`

Details of the failure in the linked report and in `replication.log` can look like this:

```
<replication-status when="date/time" lastStatus="FAIL"
explanation="WinErr:32(creln)"
errValue="5081" errMnemonic="SRCFILE" action="COPY"
src="X:\path\to\filename.QBW"
dst="C:\RealTimeBackup\x\path\to\filename.QBW"
```

To protect such files, add the application type to the include list for scheduled backup, and select a time for scheduled backup when the application is not in use.

Files are not backed up to Tivoli Storage Manager server

These topics discuss problems encountered when backing up files to Tivoli Storage Manager server.

Tivoli Storage Manager node name does not match the host name

If the node name assigned by the Tivoli Storage Manager administrator is different from the Tivoli Continuous Data Protection for Files client host name, back up to the Tivoli Storage Manager server fails. The reason is that the Tivoli Continuous Data Protection for Files cannot identify itself properly to the Tivoli Storage Manager server.

The following error message displays:

```
FilePath ERROR ANS1353E (RC53)
Session rejected: Unknown or incorrect ID entered
node:<node name> rc=53 reason=65535 tsm_init_api_session tsmInitEx failed
```

Tivoli Continuous Data Protection for Files uses Tivoli Storage Manager API. By default, the Tivoli Storage Manager API uses the client host name as the Tivoli Storage Manager node name when identifying itself to the Tivoli Storage Manager server. A Tivoli Storage Manager server administrator typically registers a node using the host name. In some cases, the Tivoli Storage Manager server administrator uses a name that is different from the client host name and causes the problem.

If it happens, you must configure the Tivoli Storage Manager API to use the appropriate node name when logging on to the Tivoli Storage Manager server. You can correct this problem by completing these steps:

1. Edit the `dsm.opt` file. This file is in the Tivoli Continuous Data Protection for Files subfolder of the “Program data folder” on page 50.
2. Add the node name to the `dsm.opt` file. Go to the end of the file, and on a new line add the NODENAME parameter followed by the node name. For example: `NODENAME TSMclientnode1`.
3. Save the `dsm.opt` file.

The next time Tivoli Continuous Data Protection for Files connects to the Tivoli Storage Manager server, it uses the node name you specified. Tivoli Continuous Data Protection for Files prompts you for the password, if necessary.

Tivoli Storage Manager client node lacks authority to delete backup copies

If Tivoli Continuous Data Protection for Files does not have delete backup permission on the Tivoli Storage Manager server, it cannot successfully purge older files when the designated storage space is getting full.

The following error is displayed in the `replication.log` file:

```
FilePath ERROR ANS1126E (RC27)
The file space cannot be deleted because
this node does not have permission to delete archived or backed up data.
```

The following error is displayed in a pop-up window:

```
Target file system can only handle sequential I/Os.
```

Remote backup can be suspended because the backup storage space cannot be purged to make room for new files.

Tivoli Continuous Data Protection for Files requires permission to manage space on the Tivoli Storage Manager server and to create file versions. The registered node which is used by the Tivoli Continuous Data Protection for Files client to access the Tivoli Storage Manager server must have the permission to delete the backups it creates. This function is required when Tivoli Continuous Data Protection for Files needs to purge files when the backup storage space is full.

Enable permission to delete backup copies for Tivoli Storage Manager Enterprise server as follows. This sample assumes node name of TSMclientnode1; replace the node name appropriately when you enter the command:

1. Log into the Tivoli Storage Manager server and bring up the Tivoli Storage Manager administrative command line.
2. Enter this command to the Tivoli Storage Manager server: **`update node`** TSMclientnode1 **`backdel=y`**.

Enable permission to delete backup copies for Tivoli Storage Manager Express server as follows:

1. Open an administrative command prompt.
2. Enter this command: `query session`. Note the session numbers for your client node.
3. Enter this command, where session_number is the session number you identified in the previous step: `cancel session session_number`. Repeat if there is more than one session for your client node.
4. Enter this command, where TSMclientnode1 is the name of your client node: `update node TSMnode backdel=y`

Non-system accounts do not have appropriate user security rights to use Tivoli Storage Manager

If a non-system account does not have appropriate user security rights, and Tivoli Continuous Data Protection for Files is configured to back up files to Tivoli Storage Manager server, files modified by the non-system account are not backed up.

In order to back up files to a Tivoli Storage Manager server, the proper user security rights must be given to the non-system user account to use the Tivoli Storage Manager client. Any non-system account (local or domain) must have the following rights:

- Back up files and directories
- Restore files and directories
- Manage auditing and security logs.

Tivoli Continuous Data Protection for Files user interface replaces existing browser session

When the user interface is started, it replaces an existing browser session. You can change this behavior by changing the settings in more recent versions of Mozilla Firefox and Internet Explorer. In Internet Explorer version 7, you can prevent this behavior.

In Internet Explorer version 7 and later versions, change the tabbed browsing settings as follows:

1. In **Tools** menu, choose **Internet Options**. The **Internet Options** notebook displays.
2. Select the **General** tab. The **General** page displays
3. In the **Tabs** section, click on **Settings**. The **Tabbed Browsing Settings** dialog displays.
4. In the **Open links from other programs in:** section, click the **A new window** option.
5. Click **OK**, the **Tabbed Browsing Settings** dialog exits.
6. In the **Internet Options** notebook, click **OK**.
7. The **Internet Options** notebook exits and your new settings are applied.

In Mozilla Firefox version 1.5.0.10 and later versions, change the browsing settings as follows:

1. In **Tools** menu, choose **Options**. The **Options** notebook displays.
2. Select the **Tabs** tab. The **Tabs** page displays
3. In the **Open links from other applications in:** section, click the **A new window** option.
4. Click on **OK**, the **Options** notebook exits and your new settings are applied.

Tivoli Continuous Data Protection for Files user interface contains no file data

If the Tivoli Continuous Data Protection for Files daemon is not running, or if your browser is in offline mode, the Tivoli Continuous Data Protection for Files user interface contains no file data. This condition is accompanied by an error message which begins like this: FPA_getNamedObject: **Could not find:**. There are two possible causes for this problem.

Your browser is offline.

Your browser must be in online mode to see file data. Internet Explorer and Firefox browsers are turned on- or off- line by checking or unchecking **File** > **Work Offline** from the browser menu. Confirm that this menu item is not checked.

The Tivoli Continuous Data Protection for Files daemon is not running.

To determine if the Tivoli Continuous Data Protection for Files daemon is running, and restart if necessary, see “Restarting the Tivoli Continuous Data Protection for Files client process” on page 78.

Restarting the Tivoli Continuous Data Protection for Files client process

The `FilePathSrv.exe` client process is started automatically every time the computer starts. If the `FilePathSrv.exe` client process does not start automatically or stops running, your files are not protected.

To determine if the `FilePathSrv.exe` process is running, look for the FilePathSrv.exe process in Task Manager. If you cannot see this process, the process is not running.

To restart the process on a Command Prompt window, do the following:

1. Open a Command Prompt window.
2. Navigate to the Tivoli Continuous Data Protection for Files installation folder. The default installation folder is `C:\Program Files\Tivoli\CDP_for_Files`.
3. Type the following: `filepathsrv -d`.

Confirm that the process is running by checking the System Event log or Task Manager. In the System Event log, there should be an entry which states: `HTML listener started successfully and listening on port 9003`. This is event # 6049. In Task Manager, you should see FilePathSrv.exe process.

You can also restart the process from the **Start** menu. Choose **Start > All Programs > Startup >CDPforFilesSrv**.

The number of backup copy versions is greater than configured in Tivoli Continuous Data Protection for Files

The number of backup copy versions exceeds **How many versions to keep** configuration setting.

The problem occurs when file versions are not tracked properly.

The problem can occur because data folders were not removed between an uninstall and a new installation. The new installation does not have a record of the backup copies created from the previous install and use of the product. This can occur on local storage, remote storage, or both. For a list of folders to remove after uninstall, and before installing again, see “Cleaning up after uninstallation” on page 25.

The problem can also be caused, on remote storage only, because of changes to the encryption or compression settings.

When encryption or compression settings are turned on or off, the versions counter is reset to 0, even if some backup copies exist. This behavior results because Tivoli Continuous Data Protection for Files tracks file versions without encryption/compression differently than file versions with encryption/compression.

As an example, assume that a file `file.txt` is continuously protected, and reached its five version limit (5 is the default version limit). The backup copies were not encrypted or compressed. The user then enables compression. Tivoli Continuous Data Protection for Files then creates up to five new backup copy versions of the file. The restore view shows five versions of the file having name `file.txt` (corresponding to the original five versions backed up without compression), and five versions of the file named `file.txt.cdp` (corresponding to the new five versions backed up with compression enabled).

Limit user access to files on a target file server

Set up the security permissions on a target file server to make sure that users only have access to the files that they back up.

By default, the first client that connects to a given server share creates the `RealTimeBackup` directory. Permissions assigned to the `RealTimeBackup` directory do not prevent users from reading files they do not own.

The settings used in this example assume one primary user of Tivoli Continuous Data Protection for Files on the client. This primary user is the first user from a client that connects to the server and creates the subdirectory for files backed up from that client. If Tivoli Continuous Data Protection for Files operates from other accounts on that client, failures might occur when copying files to the remote server. Error messages such as `Failed to open the destination file` are logged to the activity report.

Windows file server

This example assumes that the following conditions exist:
- The Windows XP server shares a directory named `c:\fileservertest`.
- The accounts used to access the server are members of the `Users` group.

Access Control List (ACL) settings for the `RealTimeBackup` directory

ACL settings enable client accounts to create directories that are only accessible by the account that created them. As a result, the directory that contains data for a node is not created until that node connects to the server.

Using Windows Explorer, set the ACL for the `c:\fileservertest\RealTimeBackup` directory according to these settings:

Table 12. ACL settings for the `RealTimeBackup` directory

Type	Name	Permission	Applies to
Allow	Administrators	Full Control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	This folder, subfolders, and files
Allow	Users	Special	This folder only
Allow	OWNER RIGHTS*	Full Control	This folder, subfolders, and files

* Note: The OWNER RIGHTS object must be added for Windows 2008 Servers.

The ability for objects to inherit permissions from the parent is not set. As a result, set the `Special` access for the `Users` group to only permit these settings:

```
Traverse Folder / Execute Allow
List Folder / Read Data Allow
Read Attributes Allow
Read Extended Attributes Allow
```

```
Create Files / Write Data Allow
Create Folders / Append Data Allow
Delete subfolders and files Allow
Read Permission's Allow
```

ACL settings for the `RealTimeBackup\BackupAdmin` directory

The `RealTimeBackup\BackupAdmin` directory is used by the Tivoli Continuous Data Protection for Files client to download revisions and configurations. Nodes require read-only access to these directories:

```
c:\fileservertest\RealTimeBackup\BackupAdmin
```

Table 13. ACL settings for the `RealTimeBackup\BackupAdmin` directory

Type	Name	Permission	Applies to
Allow	Users	Read, Execute	This folder, subfolders, and files
Allow	Administrators	Full Control	This folder, subfolders, and files

The ability for objects to inherit permissions from the parent is not set. As a result, set the `Special` access for the `Users` group to only permit these settings:

```
Traverse Folder / Execute Allow
List Folder / Read Data Allow
Read Attributes Allow
Read Extended Attributes Allow
Delete subfolders and files Allow
Delete Allow
Read Permission's Allow
```

UNIX file server running Samba

This example, assumes that the Samba server is set up to share a directory named `/fileservertest`.

These settings enable users to create directories under the `RealTimeBackup` directory:

```
chmod o+wrxt /fileservertest/RealTimeBackup
chmod o+rx /fileservertest/RealTimeBackup/BackupAdmin
chown root /fileservertest/RealTimeBackup/BackupAdmin
```

In the Samba configuration file (smb.conf), set the `create mask` and `directory mask` parameters to each specify *0700*. For example:

```
[fileservertest]
path = /fileservertest
writable = yes
create mask = 0700
directory mask = 0700
```

Restoring many files from a single directory Tivoli Continuous Data Protection for Files

When restoring many files from a single directory using the restore wizard, a message saying that the script is taking too long displays.

When using the restore wizard to list the contents of a directory containing over 3000 files, the browser issues a message saying that the script is taking too long. If you see this message, you can choose to allow the script to continue. Otherwise, you can also choose to customize the behavior of this dialog to avoid the message.

See the following links for details:

Firefox: http://support.mozilla.org/en-US/kb/Warning%20Unresponsive%20script?s=A+script+on+this+page&r=0&e=sph&as=s .

Microsoft Internet Explorer: http://support.microsoft.com/kb/175500.

Backup fails after configuration because of insufficient IPV6 permissions

If Tivoli Continuous Data Protection for Files does not have IPv6 or the appropriate permissions to the IPv6 path, then reports cannot be sent to the Central Administration Console.

If you do not have IPv6, Tivoli Continuous Data Protection for Files is not able to report to the Central Administration Console (CAC). After configuration, Tivoli Continuous Data Protection for Files uses the IPv6 path to reach the administration folder. If the client was using an IPv4 path prior to this release, it switches to IPv6.

Configuration scripts created using the CAC use the IPv6 path in the configuration script field to denote the location of the administration folder. If the user does not have IPv6 or does not have the appropriate permissions to the IPv6 path, then Tivoli Continuous Data Protection for Files will not be able to send reports to the CAC. To resolve the issue, set up IPv6 and ensure that the account running the client has the correct permissions to the IPv6 path.

Frequently Asked Questions

Here are some of the common questions that users have about how to use the product.

How to make sure changes to the include/exclude list are pushed to all clients on a group?

Sometimes changes made to the include / exclude list in the central administration console may not get sent to all clients in a particular group. This might be because the client cannot read the configuration file sent by the central administration console.

To ensure the client can read the configuration file:

1. Open a Windows Explorer window and navigate to the administration folder.
2. Navigate to the `RealTimeBackup\COMPUTERNAME\BackupAdmin\Downloads` directory.
3. Try to open the files in this directory using Notepad. If any of the files fail to open in Notepad then there might be a problem with the permission levels on the administration folder.

What variables are supported for the include/exclude lists?

The following variables are supported through the central administration console.

- $(USERNAME). For example: Administrator (getenv("USERNAME"))
- $(MYDESKTOP). For example: C:\Documents and Settings\Administrator\Desktop (CSIDL_DESKTOPDIRECTORY)
- $(MYFAVORITES). For example: C:\Documents and Settings\Administrator\Favorites (CSIDL_FAVORITES)
- $(MYPROFILE). For example: C:\Documents and Settings\Administrator (CSIDL_PROFILE)
- $(MYDOCUMENTS-SHORT). For example: My Documents (CSIDL_PERSONAL)
- $(MACHINE). For example: AdminLaptop (gethostname())

How to find out more information about error messages?

Detailed information on error messages can be found in the Tivoli Continuous Data Protection for Files message guides. The message guides are available in pdf format and on the product information centers.

How to get more information on how to troubleshoot problems with Tivoli Continuous Data Protection for Files?

More information on how to troubleshoot problems with Tivoli Continuous Data Protection for Files is available in Chapter 5 of the IBM Redbook "Deployment Guide Series: Tivoli Continuous Data Protection for Files V3.1". This guide is available here: http://www.redbooks.ibm.com/redbooks/SG247423/wwhelp/wwhimpl/js/html/wwhelp.htm.

A frequently asked questions tech note is available on the support site. For more information, see CDP for Files / FastBack for Workstations FAQ Document

Are there any issues when using Tivoli Continuous Data Protection for Files and other applications using GSKit8 on Windows 7 and Windows Vista?

There is a known issue when uninstalling Tivoli Continuous Data Protection for Files version 6.3.0 when other applications using GSKit8 are also installed on the system (such as the Tivoli Storage Manager Backup Archive Client).

After uninstalling Tivoli Continuous Data Protection for Files, you might see the following error message when using the Tivoli Storage Manager Backup Archive Client:

- `ANS1463E Unexpected error in cryptography library`

More information is available in the Uninstall issues with FastBack for Workstations and other applications using GSKit8 on Windows 7 and Windows Vista technote, available at http://www.ibm.com/support/docview.wss?rs=4199&tc=SS6PEB&uid=swg21584788.

Appendix. Accessibility features for Tivoli Continuous Data Protection for Files

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features of Tivoli Continuous Data Protection for Files are described in this topic.

Accessibility features

The following list includes the major accessibility features in Tivoli Continuous Data Protection for Files:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices
- User documentation provided in HTML and PDF format. Descriptive text is provided for all documentation images.

The Tivoli Continuous Data Protection for Files Information Center, and its related publications, are accessibility-enabled.

Keyboard navigation

Tivoli Continuous Data Protection for Files follows Microsoft conventions for most keyboard navigation and access. Drag and Drop support is managed using the Microsoft Windows Accessibility option known as MouseKeys. For more information about MouseKeys and other Windows accessibility options, please refer to the Windows Online Help (keyword: MouseKeys).

The following access methods differ from Microsoft conventions.

In the Tivoli Continuous Data Protection for Files client, there are several tasks in which you select files:

- Select files to include for continuous protection and to exclude from any protection.
- Select files to include for scheduled protection.
- Select files to vault

Each of these tasks presents a list of file specifications labeled **Folders and Files**. You can add file specifications to the list and remove file specifications. When you add a file specification, you can browse for files in a file tree. The file tree opens when you click **Include**, **Exclude**, or **Vault**. Navigate the file tree with the following method:

1. Press Tab and Shift+Tab to navigate to + (expand folder). Press Enter to expand the folder.
2. Press Down Arrow and Up Arrow to navigate among the objects in the folder.
3. On an expanded folder, press Enter to collapse the folder.

4. As you navigate the file tree, the object that has focus is displayed in the **Folder name (wildcards allowed)** field at the end of the panel.
5. Press Tab to navigate to the text field. Optionally, edit the text field.
6. Press Tab to navigate to **OK**. Click **OK** to add the file specification to the **Folders and Files** list.

To remove file specifications from the list, select a file specification and click **Remove**. Navigate the list of file specifications with this method:

1. Press Tab to move down to the next file specification and Shift+Tab to move up to the previous file specification.
2. Press Spacebar to select a file specification or to clear a selection.
3. Press Shift+Tab to navigate to **Remove**. Click **Remove** to remove the file specification from the **Folders and Files** list.

The **Folders and Files** list is displayed when you navigate the following paths:

- **Settings** > **Files to Protect** > **Folders and Files** box > **Details**
- **Settings** > **Files to Protect** > **Vault** box > **Details**
- **Settings** > **E-mail Protection** > **Scheduled Backup Settings**
- **Settings** > **Advanced** > **Scheduled Backup Settings**

The **Files to Restore** panel in the restore wizard also allows you to select files from a file tree, and add and remove files from a list. When you select **Folder View**, a panel with a file tree and a list of files is displayed. The restore file tree and files list is similar to other file trees and files lists. The restore controls are different in the following ways:

- The file tree folder items each have a check box.
- The items in the folders and files list each have a check box. If there are more than one versions of a file, the row contains a list of versions in the **Version** column.

Press Spacebar to select or clear a check box. If more than one version of a file is available, select the version this way:

- Press Tab to navigate to the **Version** column.
- Use Up Arrow and Down Arrow to select a version.

Related accessibility information

You can view the publications for Tivoli Continuous Data Protection for Files in Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader. You can access these or any of the other documentation PDFs at IBM Publications Center at http://www.ibm.com/shop/publications/order/.

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center at http://www.ibm.com/able.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of IBM or other companies.

Index

Glossary

This glossary includes terms and definitions.

To view glossaries for other IBM products, go to http://www.ibm.com/software/globalization/terminology.

The following cross-references are used in this glossary:

- *See* refers the reader from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- *See also* refers the reader to a related or contrasting term.

A

absolute mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also *modified mode*.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights. For example, an access control list is associated with a file that identifies the users who can access that file and their access rights.

access mode
An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume. The access mode can be read/write, read-only, or unavailable. Volumes in primary storage pools can also have an access mode of destroyed. Volumes in copy storage pools can also have an access mode of offsite.

acknowledgment
The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See *access control list*.

activate
To validate the contents of a policy set and then make it the active policy set.

active-data pool
A named set of storage pool volumes that contain only active versions of client backup data.

active file system
A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. Contrast with *inactive file system*.

active policy set
The activated policy set that contains the policy rules in use by all client nodes that are assigned to the policy domain. See also *policy domain* and *policy set*.

active version
The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. Contrast with *inactive version*.

activity log
A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup
A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client
A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the Tivoli Storage Manager server. Contrast with *backup-archive client*.

administrative command schedule
A database record that describes the planned processing of an administrative command during a specific time period. See also *client schedule*.

administrative privilege class
See *privilege class*.

administrative session
A period of time during which an administrator user ID communicates with a server to perform administrative tasks. Contrast with *client node session*.

administrator
A user who is registered to the server as an administrator, and who is authorized to perform tasks and issue commands through the assignment of an administrative privilege class.

Advanced Program-to-Program Communication (APPC)
An implementation of the SNA LU 6.2 protocol that allows interconnected systems to communicate and share the processing of programs.

agent node
A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate
An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also *logical file* and *physical file*.

aggregate data transfer rate
A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

APPC See *Advanced Program-to-Program Communication*.

application client
A program that is installed on a system to protect an application. The Tivoli Storage Manager server provides backup services to an application client.

archive
To copy programs, data, or files to other storage media, usually for long-term storage or security. Contrast with *retrieve*.

archive copy
A file or group of files that was archived to server storage.

archive copy group
A policy object containing attributes that control the generation, destination, and expiration of archived files.

archive-retention grace period
The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also *bind*.

association
(1) The defined relationship between a client node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

(2) On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

audit
To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication
The process of checking a user's password before permitting user access to the Tivoli Storage Manager server. Authentication can be turned on or off by an administrator with system privilege.

authentication rule
A specification that another user can use to either restore or retrieve files from storage.

authority
The right to access objects, resources, or functions. See also *privilege class*.

authorization rule
A specification that permits another user to either restore or retrieve a user's files from storage.

authorized user
A user who has administrative authority for the Tivoli Storage Manager client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS
See *automounted file system*.

automatic detection
A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration
The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also *threshold migration* and *demand migration*.

automatic reconciliation
The process that is used to reconcile file systems at regular intervals. The intervals are set by a user with root user authority. See also *reconciliation*.

automounted file system (AutoFS)
A file system that is managed by an automounter daemon. The automounter daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client
A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. Contrast with *administrative client*.

backup copy group
A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class.

backup-retention grace period
The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set
A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection
A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version
A file or directory that a client node backed up to server storage. More than one backup version can exist in server storage, but only one backup version is the active version. See also *active version* and *inactive version*.

bind To associate all versions of a file with a management class name. See *rebind*.

bindery
A database that consists of three system files for a NetWare server. The files contain user IDs and user restrictions.

C

cache To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file
A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD See *client acceptor*.

central scheduler
A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See *client schedule* and *administrative command schedule*.

client A software program or computer that requests services from a server.

client acceptor
An HTTP service that serves the applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX®, UNIX, and Linux systems, the client acceptor is run as a daemon, and is also called the *client acceptor daemon* (CAD).

client acceptor daemon (CAD)
See *client acceptor*.

client domain
The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node
A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session
A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. Contrast with *administrative session*.

client options file
An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client option set
A group of options that are defined on the server and used on client nodes in conjunction with client options files.

client-polling scheduling mode
A method of operation in which the client queries the server for work. Contrast with *server-prompted scheduling mode*.

client schedule
A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also *administrative command schedule*.

client/server
Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file
A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. This file is also called the dsm.sys file. See also *client user-options file*.

client user-options file
A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also *client system-options file*.

closed registration
A registration process in which only an administrator can register workstations as client nodes with the server. Contrast with *open registration*.

collocation
The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool. Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group
A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point
A point in time when data is considered consistent.

Common Programming Interface for Communications (CPI-C)
A call-level interface that provides a consistent application programming interface (API) for applications that use program-to-program communications. CPI-C uses LU 6.2 architecture to create a set of interprogram services that can establish and end a conversation, send and receive data, exchange control information, and notify a partner program of errors.

communication method
The method by which a client and server exchange information. See also *Transmission Control Protocol/Internet Protocol*.

communication protocol
A set of defined interfaces that permit computers to communicate with each other.

compression
A function that removes repetitive characters, spaces, or strings of characters from the data being processed and replaces the repetitive characters with control characters. Compression reduces the amount of storage space that is required for the data.

configuration manager
A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also *managed server* and *profile*.

conversation
A connection between two programs over a session that allows them to communicate with each other while processing a transaction.

copy backup
A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted

copy group
A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also *archive copy group*, *backup copy group*, *backup version*, and *management class*.

copy storage pool
A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also *primary storage pool* and *destination*.

CPI-C See *Common Programming Interface for Communications*.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file
A physical file in which Tivoli Storage Manager has detected read errors.

data access control mode
A mode that controls whether a command can access a migrated file, see a migrated file as zero-length, or receive an input/output error if it attempts to access a migrated file. See also *execution mode*.

database backup series
One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series.

database snapshot
A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also *database backup series*. Contrast with *full backup*.

data deduplication
A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server
A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover
A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)
A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

default management class
A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

deduplication
See *data deduplication.*

demand migration
The process that is used to respond to an out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated.

desktop client
The group of backup-archive clients that includes clients on Microsoft Windows, Apple, and Novell NetWare operating systems.

destination
A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated.

device class
A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file
(1) For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

(2) For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.

device driver
A program that provides an interface between a specific device and the application program that uses the device.

disaster recovery manager (DRM)
A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan
A file that is created by the disaster recovery manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and hardware that is used by the server, and the location of recovery media.

domain
A grouping of client nodes with one or more policy sets, which manage data or storage resources for the client nodes. See *policy domain* or *client domain*.

DRM See *disaster recovery manager*.

DSMAPI
See *data storage-management application-programming interface*.

dynamic serialization
A type of copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive.

E

EA See *extended attribute*.

EB See *exabyte*.

EFS See *Encrypted File System*.

Encrypted File System (EFS)
A file system that uses file system-level encryption.

enterprise configuration
A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also *configuration manager*, *managed server*, *profile*, and *subscription*.

enterprise logging
The process of sending events from a Tivoli Storage Manager server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also *event*.

error log
A data set or file that is used to record error information about a product or system.

estimated capacity
The available space, in megabytes, of a storage pool.

event (1) An administrative command or a client operation that is scheduled to be run using Tivoli Storage Manager scheduling.

(2) A message that an Tivoli Storage Manager server or client issues. Messages can be logged using Tivoli Storage Manager event logging.

event record
A database record that describes actual status and results for events.

event server
A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)
For processor storage, real and virtual storage, and channel volume, 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude
The process of identifying files in an include-exclude list. This process

prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup and space management, backup only, or space management only.

exclude-include list
See *include-exclude list*.

execution mode
A mode that controls the space-management related behavior of commands that run under the **`dsmmode`** command.

expiration
The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file
A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend
To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)
Names or value pairs that are associated with files or directories. There are three classes of extended attributes: user attributes, system attributes, and trusted attributes.

extent The part of a file that is created during the data-deduplication process. Extents are compared with other file extents to identify duplicates.

external library
A type of library that is provided by Tivoli Storage Manager that permits LAN-free data movement for StorageTek libraries that are managed by Automated Cartridge System Library Software (ACSLS). To activate this function, the Tivoli Storage Manager library type must be EXTERNAL.

F

file access time
On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age
For migration prioritization purposes, the number of days since a file was last accessed.

file device type
A device type that specifies the use of sequential access files on disk storage as volumes.

file server
A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space
A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore,

retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)
A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state
The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also *resident file*, *premigrated file*, and *migrated file*.

file system migrator (FSM)
A kernel extension that intercepts all file system operations and provides any space management support that is required. If no space management support is required, the operation is passed to the operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state
The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency
A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See *file space ID*.

FSM See *file system migrator*.

full backup
The process of backing up the entire server database. A full backup begins a new database backup series. See also *database backup series* and *incremental backup*. Contrast with *database snapshot*.

fuzzy backup
A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy
A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified. See also *backup version* and *archive copy*.

G

General Parallel File System
A high-performance shared-disk file system that can provide data access from nodes in a cluster environment.

gigabyte (GB)
In decimal notation, 1 073 741 824 when referring to memory capacity; in all other cases, it is defined as 1 000 000 000.

global inactive state
The state of all file systems to which space management has been added when space management is globally deactivated for a client node. When

space management is globally deactivated, hierarchical storage management (HSM) cannot perform migration, recall, or reconciliation. However, a root user can update space management settings and add space management to additional file systems. Users can access resident and premigrated files.

Globally Unique Identifier (GUID)
An algorithmically determined number that uniquely identifies an entity within a system.

GPFS™
See *General Parallel File System*.

GPFS node set
A mounted, defined group of GPFS file systems.

group backup
The backup of a group containing a list of files from one or more file space origins.

GUID See *Globally Unique Identifier*.

H

hierarchical storage management (HSM)
A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity.

hierarchical storage management (HSM) client
A client program that works with the Tivoli Storage Manager server to provide hierarchical storage management (HSM) for a system. See also *hierarchical storage management* and *space manager client*.

HSM See *hierarchical storage management*.

HSM client
See *hierarchical storage management client*.

I

ILM See *information lifecycle management*.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. Contrast with *active file system*.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. Contrast with *active version*.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also *include-exclude list*.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services.

incremental backup
(1) A copy of all database data that has changed since the most recent successful full backup operation. An incremental backup is also known as a *cumulative backup image* because each incremental backup includes the contents of the previous incremental backup.

(2) The process of backing up information in the database that is new or changed since the last full backup. Contrast with *full backup*. See also *database backup series*.

(3) For Data Protection for Microsoft Exchange Server, a backup in which the transaction logs are backed up and then cleared.

individual mailbox restore
See *mailbox restore*.

information lifecycle management (ILM)
GPFS policy-based file management for storage pools and file sets.

inode
The internal structure that describes the individual files on AIX, UNIX, or Linux systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the IP standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 210 or 1 024 bytes. For disk storage capacity and communications volume, 1 000 bytes.

L

LAN See *local area network.*

LAN-free data movement
The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network. This process is also referred to as *LAN-free data transfer*.

LAN-free data transfer
See *LAN-free data movement*.

leader data
Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library
(1) A repository for demountable recorded media, such as magnetic disks and magnetic tapes.

(2) A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client
A server that uses server-to-server communication to access a library that is managed by another storage management server. See also *library manager*.

library manager
A server that controls device operations when multiple storage management servers share a storage device. See also *library client*.

local (1) Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line.

(2) For HSM products, pertaining to the destination of migrated files that are being moved.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volumes
Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See *loopback virtual file system.*

logical file
A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also *aggregate* and *physical file*.

logical occupancy
The space that is used by logical files in a storage pool. This space does

not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy.

logical unit (LU)
An access point through which a user or application program accesses the Systems Network Architecture (SNA) network to communicate with another user or application program.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier that is used to differentiate devices, each of which is a logical unit (LU).

logical volume
A portion of a physical volume that contains a file system.

logical volume backup
A backup of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)
Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)
A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LU See *logical unit*.

LUN See *logical unit number*.

LVSA See *Logical Volume Snapshot Agent*.

M

macro file
A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. Contrast with *Tivoli Storage Manager command script*.

mailbox restore
A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object
In Tivoli Storage Manager, a definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server. In general, a managed object cannot be modified locally on the managed server. Objects can include policy, schedules, client option sets, server scripts, administrator registrations, server definitions, and server group definitions.

managed server
A Tivoli Storage Manager server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also *configuration manager*, *subscription*, and *profile*.

management class
A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also *copy group*, *space manager client*, *bind*, and *rebind*.

maximum transmission unit
The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See *megabyte*.

media server
In a z/OS® environment, a program that provides access to z/OS disk and tape storage for Tivoli Storage Manager servers that run on operating systems other than z/OS.

megabyte (MB)
(1) 1 048 576 bytes (2 to the 20th power) when used in this publication.

(2) For processor storage, real and virtual storage, and channel volume, 2 to the power of 20 or 1 048 576 bits. For disk storage capacity and communications volume, 1 000 000 bits.

metadata
Data that describes the characteristics of data; descriptive data.

migrate
To move data from one storage location to another. In Tivoli Storage Manager products, migrating can mean moving data from a client node to server storage, or moving data from one storage pool to the next storage pool defined in the server storage hierarchy. In both cases the movement is controlled by policy, such as thresholds that are set. See also *migration threshold*.

migrated file
A file that has been copied from a local file system to Tivoli Storage Manager storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also *stub file* and *resident file*. For HSM clients on UNIX or Linux systems, contrast with *premigrated file*.

migrate-on-close recall mode
A mode that causes a migrated file to be recalled back to its originating file system temporarily. Contrast with *normal recall mode* and *read-without-recall recall mode*.

migration job
A specification of files to migrate, and actions to perform on the original files after migration. See also *job file*.

migration threshold
High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

mirroring
The process of writing the same data to multiple locations at the same time. Mirroring data protects against data loss within the recovery log.

mode A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See *modified mode* and *absolute mode*.

modified mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also *absolute mode*.

mount limit
The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also *mount point*.

mount point
On the Tivoli Storage Manager server, a logical drive through which volumes in a sequential access device class are accessed. For removable-media device types, such as tape, a mount point is a logical drive that is associated with a physical drive. For the file device type, a mount point is a logical drive that is associated with an I/O stream. The number of mount points for a device class is defined by the value of the mount limit attribute for that device class. See also *mount limit*.

mount retention period
The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period
The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See *maximum transmission unit*.

N

Nagle algorithm
An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe
A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS See *network-attached storage*.

NAS node
A client node that is a network-attached storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system
A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format
A format of data that is written to a storage pool directly by the Tivoli Storage Manager server. Contrast with *non-native data format*.

NDMP
See *Network Data Management Protocol*.

NetBIOS
See *Network Basic Input/Output System*.

network-attached storage (NAS) file server
A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System (NetBIOS)
A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

Network Data Management Protocol (NDMP)
A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate
A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

node name
A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class
A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also *privilege class*.

non-native data format
A format of data that is written to a storage pool that differs from the format that the server uses for operations.

normal recall mode
A mode that causes a migrated file to be copied back to its originating file system when it is accessed.

O

offline volume backup
A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup
A backup in which the volume is available to other system applications during the backup operation.

open registration
A registration process in which users can register their workstations as client nodes with the server. Contrast with *closed registration*.

operator privilege class
A privilege class that gives an administrator the authority to disable or halt

the server, enable the server, cancel server processes, and manage removable media. See also *privilege class*.

options file
A file that contains processing options. On Windows and NetWare systems, the file is called dsm.opt. On AIX, UNIX, Linux, and Mac OS X systems, the file is called dsm.sys.

originating file system
The file system from which a file was migrated. When a file is recalled using normal or migrate-on-close recall mode, it is always returned to its originating file system.

orphaned stub file
A file for which no migrated file can be found on the Tivoli Storage Manager server that the client node is contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

out-of-space protection mode
A mode that controls whether the program intercepts out-of-space conditions. See also *execution mode*.

P

pacing
In SNA, a technique by which the receiving system controls the rate of transmission of the sending system to prevent overrun.

packet In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode
A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation
A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting. Password generation can be set in the options file (`passwordaccess` option). See also *options file*.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character
See *wildcard character*.

physical file
A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also *aggregate* and *logical file*.

physical occupancy
The amount of space that is used by physical files in a storage pool. This

space includes the unused space that is created when logical files are deleted from aggregates. See also *physical file*, *logical file*, and *logical occupancy*.

plug-in
A self-contained software component that modifies (adds, or changes) the function in a particular system. When a plug-in is added to a system, the foundation of the original system remains intact.

policy domain
A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain.

policy privilege class
A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also *privilege class*.

policy set
A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also *active policy set* and *management class*.

premigrated file
A file that has been copied to Tivoli Storage Manager storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in Tivoli Storage Manager storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. Contrast with *migrated file* and *resident file*.

premigrated files database
A database that contains information about each file that has been premigrated to Tivoli Storage Manager storage. The database is stored in a hidden directory named `.SpaceMan` in each file system to which space management has been added.

premigration
The process of copying files that are eligible for migration to Tivoli Storage Manager storage, but leaving the original file intact on the local file system.

premigration percentage
A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary storage pool
A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also *destination* and *copy storage pool*.

privilege class
A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also *node privilege class*, *operator privilege class*, *policy privilege class*, *storage privilege class*, and *system privilege class*.

profile
A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also *configuration manager* and *managed server*.

Q

quota
(1) For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.

(2) For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization
The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume
A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

read-without-recall recall mode
A mode that causes hierarchical storage management (HSM) to read a migrated file from storage without storing it back on the local file system. The last piece of information read from the file is stored in a buffer in memory on the local file system. Contrast with *normal recall mode* and *migrate-on-close recall mode*.

rebind
To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also *bind*.

recall
In Tivoli Storage Manager, to copy a migrated file from server storage back to its originating file system using the space management client. See also *transparent recall*, *selective recall*, and *recall mode*.

recall mode
A mode that is assigned to a migrated file with the **`dsmattr`** command that determines how the file is processed when it is recalled. It determines whether the file is stored on the local file system, is migrated back to Tivoli Storage Manager storage when it is closed, or is read from Tivoli Storage Manager storage without storing it on the local file system.

receiver
A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the Tivoli Storage Manager server console and activity log. See also *event*.

reclamation
The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold

The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation

The process of synchronizing a file system with the Tivoli Storage Manager server, and then removing old and obsolete objects from the Tivoli Storage Manager server.

recovery log

A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register

To define a client node or administrator ID that can access the server.

registry

A repository that contains access and configuration information for users, systems, and software.

remote

(1) Pertaining to a system, program, or device that is accessed through a communication line.

(2) For HSM products, pertaining to the origin of migrated files that are being moved.

resident file

On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in Tivoli Storage Manager storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from Tivoli Storage Manager storage and modified. Contrast with *stub file* and *premigrated file*. See *migrated file*.

restore

To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention

The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve

To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool.

roll back

To remove changes that were made to database files since the last commit point.

root user

A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See *storage area network*.

schedule
A database record that describes client operations or administrative commands to be processed. See *administrative command schedule* and *client schedule*.

scheduling mode
The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume
A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use.

script
A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. Contrast with *Tivoli Storage Manager command script*.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup
The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. Contrast with *incremental backup*.

selective migration
The process of copying user-selected files from a local file system to Tivoli Storage Manager storage and replacing the files with stub files on the local file system. Contrast with *threshold migration* and *demand migration*.

selective recall
The process of copying user-selected files from Tivoli Storage Manager storage to a local file system. Contrast with *transparent recall*.

serialization
The process of handling files that are modified during backup or archive processing. See *dynamic serialization*, *static serialization*, *shared static serialization*, and *shared dynamic serialization*.

server
A software program or a computer that provides services to other software programs or other computers.

server options file
A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode
A client/server communication technique where the server contacts the client node when tasks must be done. Contrast with *client-polling scheduling mode*.

server storage
The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from space manager client nodes (space-managed files). See also *active-data pool*, *primary storage pool*, *copy storage pool*, *storage pool volume*, and *volume*.

session

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data.

session resource usage

The amount of wait time, processor time, and space that is used or retrieved during a client session.

shared dynamic serialization

A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. Tivoli Storage Manager retries the backup or archive operation a number of times; if the file is being modified during each attempt, Tivoli Storage Manager will back up or archive the file on its last try. See also *serialization*. Contrast with *dynamic serialization*, *shared static serialization*, and *static serialization*.

shared library

A library device that is used by multiple storage manager servers.

shared static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. Tivoli Storage Manager attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *static serialization*.

snapshot

An image backup type that consists of a point-in-time view of a volume.

space-managed file

A file that is migrated from a client node by the space manager client. The space manager client recalls the file to the client node on demand.

space management

The process of keeping sufficient free storage space available on a local file system for new data by migrating files to server storage. Synonymous with *hierarchical storage management*.

space manager client

A program that runs on a UNIX or Linux system to manage free space on the local file system by migrating files to server storage. The program can recall the files either automatically or selectively. Also called *hierarchical storage management (HSM) client*.

space monitor daemon

A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file

A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file

On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL See *Secure Sockets Layer*.

stabilized file space
A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Each stanza is identified by a name that occurs in the first line of the stanza. Depending on the type of file, a stanza is ended by the next occurrence of a stanza name in the file, or by an explicit end-of-stanza marker. A stanza can also be ended by the end of the file.

startup window
A time period during which a schedule must be initiated.

static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the storage manager cannot back up or archive the file. See also *serialization*. Contrast with *dynamic serialization*, *shared dynamic serialization*, and *shared static serialization*.

storage agent
A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)
A dedicated storage network that is tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy
(1) A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also *storage pool*.

(2) An arrangement of storage devices with different speeds and capacities. The levels of the storage hierarchy include: main storage, such as memory and direct-access storage device (DASD) cache; primary storage (DASD containing user-accessible data); migration level 1 (DASD containing data in a space-saving format); and migration level 2 (tape cartridges containing data in a space-saving format).

storage pool
A named set of storage volumes that are the destination that is used to store client data. A storage pool contains backup versions, archive copies, and files that are migrated from space manager client nodes. A primary storage pool is backed up to a copy storage pool. See also *primary storage pool*, *copy storage pool*, and *active-data pool*.

storage pool volume
A volume that has been assigned to a storage pool. See also *volume*, *active-data pool*, *copy storage pool*, and *primary storage pool*.

storage privilege class
A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also *privilege class*.

stub A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file
A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from Tivoli Storage Manager storage. It also contains additional information that can be used to eliminate the need to recall a migrated file.

stub file size
The size of a file that replaces the original file on a local file system when the file is migrated to Tivoli Storage Manager storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription
In a Tivoli environment, the process of identifying the subscribers that the profiles are distributed to. For Tivoli Storage Manager, a subscription is the process by which a managed server receives configuration information associated with a particular profile on a configuration manager. See also *managed server*, *configuration manager*, and *profile*.

system privilege class
A privilege class that gives an administrator the authority to issue all server commands. See also *privilege class*.

Systems Network Architecture (SNA)
The description of the logical structure, formats, protocols, and operational sequences for transmitting information through and controlling the configuration and operation of networks.

T

tape library
A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix
The high-level-qualifier of the file name or the data set name in the standard tape label.

target node
A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See *trusted communications agent*.

TCP/IP
See *Transmission Control Protocol/Internet Protocol*.

threshold migration
The process of moving files from a local file system to Tivoli Storage Manager storage based on the high and low thresholds that are defined for the file system. Contrast with *demand migration*, *selective migration*, and *migration job*.

throughput
In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout
A time interval that is allotted for an event to occur or complete before operation is interrupted.

timestamp control mode
A mode that determines whether commands preserve the access time for a file or set it to the current time.

Tivoli Storage Manager command script
A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic.

tombstone object
A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types.

transparent recall
The process that is used to automatically recall a file to a workstation or file server when the file is accessed. See also *recall mode*. Contrast with *selective recall*.

trusted communications agent (TCA)
A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See *Universal Naming Convention name*.

Unicode
A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus some classical and historical texts. The Unicode standard has a 16-bit character set defined by ISO 10646.

Unicode-enabled file space
Unicode file space names provide support for multilingual workstations without regard for the current locale.

Unicode transformation format 8
Unicode Transformation Format (UTF), 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208.

Universal Naming Convention (UNC) name
A name that is used to access a drive or directory containing files shared across a network. The UNC name includes the system name and a SharePoint name that represents the shared drive or directory.

Universally Unique Identifier (UUID)
The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier.

UTF-8 See *Unicode transformation format 8*.

UUID See *Universally Unique Identifier*.

V

validate
To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version
A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space
A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual volume
An archive file on a target server that represents a sequential media volume to a source server.

volume
A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also *scratch volume*, and *storage pool volume*.

volume history file
A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service
A set of Microsoft application-programming interfaces (APIs) that you can use to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See *Volume Shadow Copy Service*.

VSS Backup
A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

VSS Fast Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS)

software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on local shadow volumes.

VSS Instant Restore
A volume-level hardware-assisted Microsoft Volume Shadow Copy Service (VSS) function where target volumes that contain the snapshot are copied back to the original source volumes.

VSS offloaded backup
A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the Tivoli Storage Manager server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

W

wildcard character
A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workstation
A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name
A 64-bit, unsigned name identifier that is unique.

workload partition (WPAR)
A partition within a single operating system instance.

Product Number: 5608-APG 5724-S64 5641-FSE

Printed in USA

SC14-7653-00