Tivoli Continuous Data Protection for Files Version 2.1

Installation and User's Guide

GC32-1783-00

Note: Before using this information and the product it supports read the general information under the "Notices" chapter in the back of the book.

First Edition (September, 2005)

This edition applies to the IBM Tivoli Continuous Data Protection for Files Version 2.1 (program number 5608-APF) and to any subsequent releases until otherwise indicated in new editions or technical newsletters.

Requests for copies of this publication and for technical information about IBM products should be made to your sales office or the IBM Branch Office serving your locality.

Your feedback is important in helping to provide the most accurate and high-quality information. If you have comments about this book or any other IBM Tivoli documentation, please visit http://www.ibm.com/software/tivoli/contacts.html

© Copyright International Business Machines Corporation 2005. All rights reserved.

Contents

About this Guide

Who should read this guide

This publication is for the system administrator or system programmer who installs and configures user access to the disk drives. The user should be knowledgeable with the operating system and networking on: Windows® or UNIX® computers. For more information on these operating systems, see the documentation that came with the computer.

Conventions used in this publication

This publication uses the following typographical conventions:

Example	Description
bold	Boldface type indicates a command, directory name, or file name. For the GUI, boldface type indicates a window name, button, menu item, option, icon, or field. Bold type is also used for emphasis in the text.
`example`	Monospaced type represents fragments of a program, an example, or information as it would appear on a display screen.
italics	Italicized type indicates the name of an optional parameter or a new term.

Related publications

The following publications are referenced in this guide.

Title	Order Number
IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients Installation and User's Guide	GC32-0789
IBM Tivoli Storage Manager for Macintosh Backup-Archive Clients Installation and User's Guide	GC32-0787
IBM Tivoli Storage Manager for Windows Backup-Archive Clients Installation and User's Guide	GC32-0788

Downloading or ordering publications

IBM posts publications for this and all other Tivoli® products, as they become available and whenever they are updated, to the Tivoli software information center Web site at the following Web address:

http://publib.boulder.ibm.com/tividd/td/tdprodlist.html

You can order many Tivoli publications online at the following Web site:

www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

Contacting Customer Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM® software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus, and Rational products, as well as DB2 and WebSphere products that run on Windows or UNIX operating systems), enroll in Passport Advantage in one of the following ways:
    - Online: Go to the Passport Advantage Web page www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home and click How to Enroll
    - By phone: For the phone number to call in your country, go to the IBM Software Support Web site (http://techsupport.services.ibm.com/guides/contacts.html) and click the name of your geographic region.
- For IBM eServer software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), 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 eServer software products, go to the IBM Technical Support Advantage Web page (http://www.ibm.com/servers/eserver/techsupport.html).

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 or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (http://techsupport.services.ibm.com/guides/contacts.html) and click the name of your geographic region for phone numbers of people who provide support for your location.

Reporting a problem

Follow the steps in this topic to contact IBM Software Support:
1. Determine the business impact of your problem.
2. Describe your problem and gather background information.
3. Submit your problem to IBM Software Support.

Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

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.

Describe your problem and gather background information

When explaining a problem to IBM, 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 currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- Online: Go to the "Submit and track problems" page on the IBM Software Support site (http://www.ibm.com/software/support/probsub.html). Enter your information into the appropriate problem submission tool.
- By phone: For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web (http://techsupport.services.ibm.com/guides/contacts.html) and click
- the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support web site:

1. Go to the IBM Software Support Web site (http://www.ibm.com/software/support).
2. Under Products A - Z, select your product name. This opens a product-specific support site.
3. Under Self help, follow the link to All Updates, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click Search tips.
4. Click the name of a fix to read the description and optionally download the fix.

Chapter 1. Introduction

Tivoli Continuous Data Protection for Files family and history

Tivoli Continuous Data Protection for Files was previously released on IBM Alphaworks site under the name VitalFile. The core component of the software is an IBM technology known as FilePath which is a general purpose real-time file system extender. Some files and programs included in Tivoli Continuous Data Protection for Files will include the name "filepath" (or "fp").

Tivoli Continuous Data Protection for Files

Tivoli Continuous Data Protection for Files is specifically targeted at end user computers such as laptops and workstations as well as file servers. It provides continuous data protection of files, providing the highest level of protection possible, yet is simple to use and administer. When files change, Tivoli Continuous Data Protection for Files will make up to three copies of the file (or queue copies to be made later). Tivoli Continuous Data Protection for Files is a replacement for traditional approaches to backup and focuses on exploiting affordable disk technology as the backup repository.

Comparison to traditional backup

Let's compare Tivoli CDP (Continuous Data Protection for Files) to traditional backup approaches:

	Tivoli CDP for Files	**Traditional**
When protected	Continuous for High importance files, Scheduled for others	Scheduled, full system
How detected	Journal-based on *all* file systems	Journal-based only on some file systems
Where copies are stored	On-disk, locally and remote; Tivoli Storage Manager	Typically on tape
Storage format	Left "native", on-line as files.	Wrapped into a propriety format.
Management / administration	Simplified per-client administration only	Client-server; server component typically more expensive/complex.

No server involved

Tivoli Continuous Data Protection for Files is a single end-point backup solution. Whereas typical backup solutions require client side software *and* a server running backup-server software, Tivoli Continuous Data Protection for Files only requires software on the client computer (the machines to be protected). Yet, Tivoli Continuous Data Protection for Files provides many of the important features typically found in client-server data protection products, such as:

- Centralized reports of all machines protected
- Global configuration changes and management
- Push-install for easily upgrading all computers running Tivoli Continuous Data Protection for Files
- Delta-block transmission (to reduce the number of bits moved)
- Multiple versions per file for restore based on a point in time
- Archiving (locking down coherent groups of files from any future alteration)

How are files stored?

Unlike traditional backup approaches, Tivoli Continuous Data Protection for Files keeps the protected instances of files in their natural form. That is, they are kept as files and kept directly accessible and available by any application. Although Tivoli Continuous Data Protection for Files provides tools and views to see the saved instances (and to restore them), it is not necessary to use the Tivoli Continuous Data Protection for Files product for accessing, restoring, or manipulating those instances. They are simply files, exactly like the originals, and kept in a directory tree structure that parallels the original tree. This is in contrast to traditional backup packages which typically re-package the protected files into conglomerates that are managed more like a database.

The Tivoli Continuous Data Protection for Files vision is biased towards exploiting disks and natural file systems as the backup targets and the file systems on those disks as a sort of repository manager. The computer world is rich with tools that know how to manage file system trees and can provide many features that would normally have to be custom built for a backup application. Those features include:

- Indexing of material (files) *content* of the backup repository
- Finding material based on name or age or other meta-data attributes
- Moving backed-up material around (re-arranging for administration reasons)
- System resource management features for understanding how much space is being used for various aspects of the backed-up material (by user, size, type, etc).
- Encryption of the backed up material
- Compression of the backed up material

Tivoli Continuous Data Protection for Files is able to provide all of the above features without actually providing any of them…because these are native capabilities of most computers and file systems or can easily be added on separately.

Modes of protection

Tivoli Continuous Data Protection for Files has two main data protection strategies:

1. Real-time backups for your most importance files
2. Scheduled protection (e.g. nightly or hourly) for all files

We refer to the first mode as the continuous protection and the second one as the scheduled protection.

Backup target

In general, Tivoli Continuous Data Protection for Files is designed to copy material onto any file system target. The target could be a local disk, a SAN disk, a removable disk, a disk at the end of a SAN extender, a NAS device, or any exported file system from another workstation or file server.

> NOTE: Tivoli Continuous Data Protection for Files also has special support for storing files into an IBM Tivoli Storage Manager application (TSM). TSM is a traditional data protection product often used in larger enterprises. Some enterprises need a real-time client solution for laptops and workstations and might find Tivoli Continuous Data Protection for Files useful for such clients, yet still want most of the protected data to ultimately be managed by the TSM server. To use the TSM feature of Tivoli Continuous Data Protection for Files, you must have first purchased and installed the TSM client on the computer and also have a TSM server running in the network.

Tivoli Continuous Data Protection for Files supports two main file-system target areas: Local Disk and Remote File Server (which can also be a disk; anything that responds to normal file system commands for creating and writing files will work). Tivoli Continuous Data Protection for Files has a rather unique view of data protection. For decades, proper data protection meant getting copies of the changed files *off* of the current system to protect against the system being fully compromised (destroyed, unbootable, or stolen). However, having the material off of the computer typically means that the restore process is more cumbersome and only works if the backup-server is available on the network (many times portable computers are detached from a network).

Tivoli Continuous Data Protection for Files is a bit of a hybrid solution in that it attempts to keep backup copies both locally and off-machine for your most important files. In this way, you are more likely to restore backed up files while not attached to the network (perhaps while on an airplane or in a hotel room). Whenever a file is changed, Tivoli Continuous Data Protection for Files notices. If a file is tagged as a high priority continuous type, a backup copy is made immediately on your local disk in a separate directory tree (to avoid cluttering the natural location for the file). Tivoli Continuous Data Protection for Files will store many backup versions of each file (typically up to 20) subject to a "pool size" that you configure. When the pool is full, the oldest copies (versions) are removed to make room for newer ones.

The same file is also copied to a remote file server (if you've configured this behavior) for off-machine protection. If the remote file server is not currently available (perhaps due to not being on the network at the time), then the changed file is remembered and sent as soon as the network appears to be functioning. The files sent to the remote file server in this mode will have only a single instance stored (that is, not versioned), since they are versioned locally.

If you have enabled Scheduled Protection, then all other changing files will be noticed by Tivoli Continuous Data Protection for Files and queued for transmission to the remote file server based on the interval you have selected. When the interval expires, Tivoli Continuous Data Protection for Files will copy all of the changed files to the remote file server, or wait if the file server is not currently available. Similar to the local disk versioning, files moved as a result of this scheduled protection mode *will* have versions created on the target (including files that are your high priority ones; so, you *will* get versions of say your Word files, but only per the frequency of scheduled backup and not necessarily every time you hit "save" in Word). The versioned files are currently kept along side of the base file at the target (with a special suffix added to the file name). The amount of space allowed to be consumed by the versions is configurable. When space runs out, the oldest versions are removed to make room for the new ones.

IMPORTANT: Tivoli Continuous Data Protection for Files never removes the "top" or "active" copy of a file, only a versioned instance.

Versioning on the remote file server

When a file is first copied to the remote file server, it is stored as its natural name (e.g. "test.doc") and its space is *not* tabulated against the configured pool size for the target. When the source file changes again, another copy is sent to the remote file server. Tivoli Continuous Data Protection for Files first renames the last copy placed there to be a versioned instance of the file, and adds the last copy's file size to the total for the pool. Then, Tivoli Continuous Data Protection for Files makes a new copy of the recently changed file and stores it on the remote file server with the natural name (e.g. "test.doc"). Thus, the most recent ("active") version of a file is stored using the file's original and natural file name. When a file is deleted on your computer, Tivoli Continuous Data Protection for Files will convert the last "active" file on the backup file server (if one exists) to a versioned instance (so that you can potentially restore it later). Once converted to a versioned instance, it may be reclaimed later as part of pool-space management.

Chapter 2. Installation

System requirements

Windows systems

A Windows server and workstation require the following hardware and software:

Machine: An Intel Pentium(R) processor

Operating system (one of the following):

Windows 2000 Server and Advanced Server, Version 5.0, SP2 and up
Windows XP Professional
Windows 2003 Advanced Server

Browser (to use the Tivoli Continuous Data Protection for Files GUI)

Internet Explorer, Version 5.0 and up (Recommended)
Firefox/Mozilla

Installing Tivoli Continuous Data Protection for Files (Windows)

1. Double-click on the Tivoli Continuous Data Protection for Files installer icon. InstallShield starts by loading Java™ VM and then displays the Language Selection dialog. The default is English.
2. Click OK. The Tivoli Continuous Data Protection for Files Information window will display with the build number.
3. Click Next. The License Agreement window will display.
4. Read the License Agreement, select the radio box to accept the terms and click Next. The Installation Location window will display.
   (NOTE: Presently it is not advised to select a different install location.)
5. Click Next. The Installation Confirmation window will display.
6. Confirm that the information is correct and click Next. The Installing Tivoli Continuous Data Protection for Files window will display a progress bar indicating that the necessary files are being installed on your system. You will also see a command prompt window open as the Installer runs several scripts.
7. The Tivoli Continuous Data Protection for Files Main configuration screen will open in a browser window to display the default settings. You can change the settings at this time, or close the browser window.
8. The Installation Complete window will display. Click Finish.

NOTE: You do not need to reboot your system after a normal install. However, if you are re-installing Tivoli Continuous Data Protection for Files or upgrading, you must reboot at the end of the installation.

Once you have completed the installation, Tivoli Continuous Data Protection for Files is up and running in the background with the default settings. If you want to change the settings or restore a file, see “Chapter 3. Configuring Tivoli Continuous Data Protection for Files.”

Uninstalling Tivoli Continuous Data Protection for Files

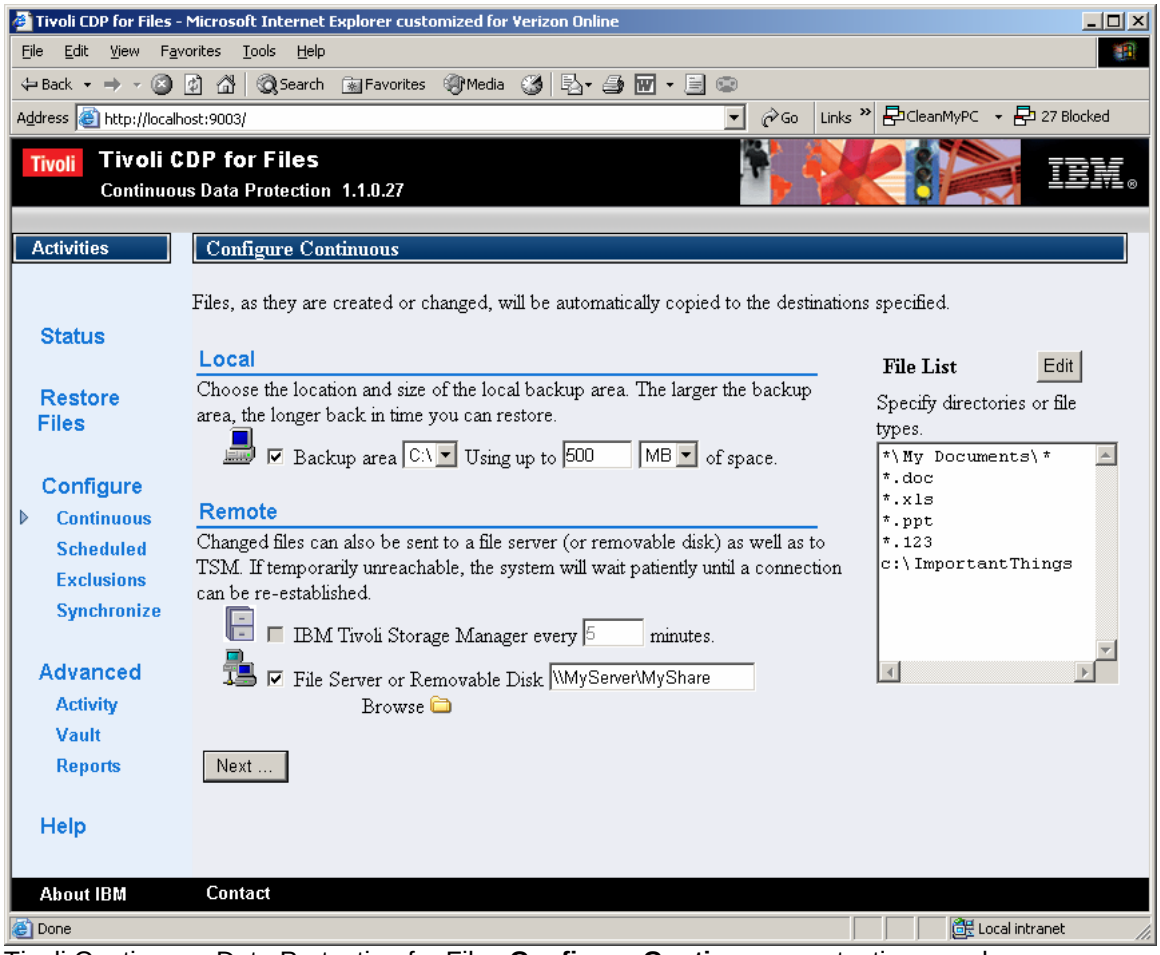
1. Navigate to Add/Remove Programs.
2. Select the Tivoli Continuous Data Protection for Files program and click Change/Remove. InstallShield will start by loading JVM and will then display the Language Selection dialog. The default is English.
3. Click OK. InstallShield will initialize and then display the Welcome window.
4. Click Next. The file location window displays.
5. Click Next. Tivoli Continuous Data Protection for Files will be removed from your system and the uninstall success window will display.
6. Click Finish.
7. Reboot your system.

NOTE: You must reboot your system after uninstalling.

Chapter 3. Configuring Tivoli Continuous Data Protection for Files

Introduction

Configuring Tivoli Continuous Data Protection for Files is simple. The web-based user interface is designed to be easy to use. There are two main configuration panels: **Configure Continuous** and **Configure Scheduled**. Continuously protect your most important files in the **Configure Continuous** panel. Protect all other files in the **Configure Scheduled** panel. Files that you designate for continuous protection will be protected in real-time (as soon as they are saved). All other changing files will be protected as part of the scheduled protection and will be copied on prescribed intervals.



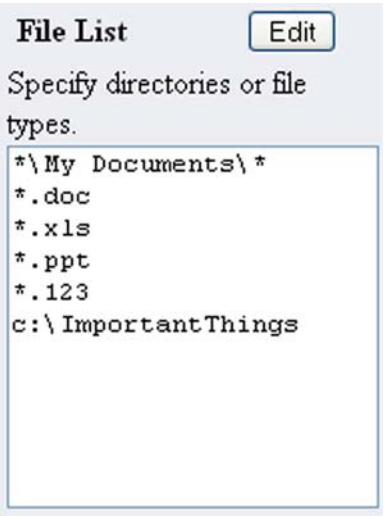
Tivoli Continuous Data Protection for Files **Configure Continuous** protection panel

Continuous protection configuration

Files that are continuously protected will be copied for protection as soon as the files are saved. Continuous protection is appropriate for files that you work on during the day, such as word processing documents or presentations. You can configure continuous protection to save files on a network-connected machine or storage device, to prevent loss of the files in case your local machine fails. A continuously protected file is saved in the backup area as a distinct version every time you save the changed file. The versioned copies are stored locally so that you can restore a previous version of the document even when you are not connected to a network. You may also configure to save the most recent, or "active", version of the file on a remote device.

File List

The default configuration includes typical Microsoft Office files and the files in your **My Documents** directory tree in the list of continuously protected files. You can change the list of files in the **File List** box by clicking the **Edit** button and entering new items, one per line:



Pattern matching

Tivoli Continuous Data Protection for Files supports pattern matching in the **File List**. Use asterisk as a wildcard for any number of characters. If there are no wildcards on a given item (e.g. **soup**) then Tivoli Continuous Data Protection for Files will match any file whose fully expanded pathname has that exact phrase anywhere in the path or filename. If there are wildcards, then the pattern matching is a stricter positional matching.

Examples:

- **.jpg** will match: **c:\dir\picture.jpg** and **c:\dir\pictures.jpg\myhouse**
- ***.jpg** will only match files that *end* with **.jpg**
- **C:*\test.jpg** will match files in any directory on **C:** drive that are named **test.jpg**
- ***\mydir*** will match any file that has a parent directory called **mydir** on any disk.

Multiple locations for backup copies

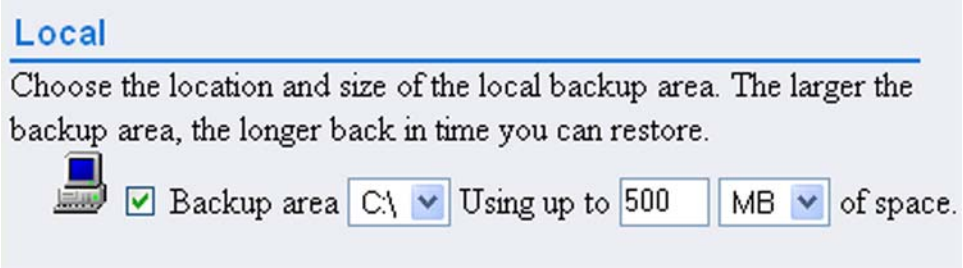
When a document is changed, Tivoli Continuous Data Protection for Files will save up to three copies of that document. Copies may be saved in any of the following locations:

- Local backup area: on a local drive.
- Remote backup area: on an IBM TSM (Tivoli Storage Manager) server
- Remote backup area: on a network-attached file server or removable disk

An important distinction between files saved in the local backup area and files saved to a remote device is backup versioning. Files that are saved to a local drive are saved as a different backup version each time you change the original file. Files that are saved to a remote device are saved as only the most recent, or "active", backup copy.

Local backup area

The first place a copy can be saved is another area of your local disk. If you configure this style of protection, Tivoli Continuous Data Protection for Files retains multiple versions of each document. On the **Configure Continuous** panel, in the **Local** section, select the **Backup area** check-box. Specify which local disk you want to receive the backup versions, and how much space to allow for the backup versions. When the space limit is reached, older backup versions will be deleted. The space is *not* pre-allocated.



NOTE: The disk selected in **Backup area** specifies the *target* disk where the backup versions are saved. The **Backup area** does *not* specify the disk to protect.

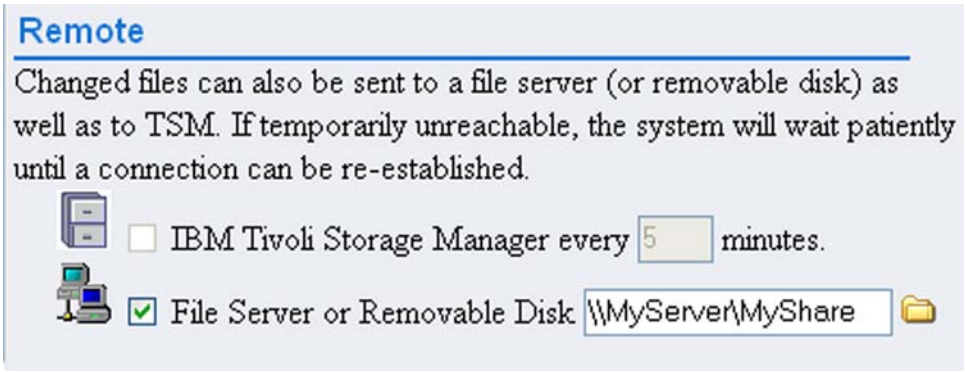
Remote backup area: IBM Tivoli Storage Manager server

You can also specify that your continuously protected files be sent to a TSM (Tivoli Storage Manager) server. You need to have the Tivoli Storage Manager Backup-Archive client software installed on this computer in order to use this option. You can specify the interval for sending the backup version to TSM. Typical backup intervals are 30 or 60 minutes.

NOTE: If you check the box for **IBM Tivoli Storage Manager**, ensure that the TSM option **passwordaccess** is set to **generate**. For details on setting the TSM passwordaccess option, see the option description in the IBM Tivoli Storage Manager Backup-Archive Clients User's Guide.

Remote backup area: File Server or Removable Disk

Lastly, you can specify a file server or removable disk to receive the backup versions as soon as a file changes. Typically the remote device is another computer (such as a NAS or file server) but you are allowed to specify simply another disk (which might be a WAN-attached remote disk or removable disk). The goal of this feature is to preserve the file in case local copies are lost. Backup copies on the remote device are not versioned; only the most recent backup copy is retained. However, files protected by schedule are saved as versions (see the next chapter). Tivoli Continuous Data Protection for Files is very tolerant of intermittently available networks. If the connection to the remote device is not available, you will receive a message that changed files are queuing for transmission to the remote device. Once the connection resumes, Tivoli Continuous Data Protection for Files will transmit the changed files.

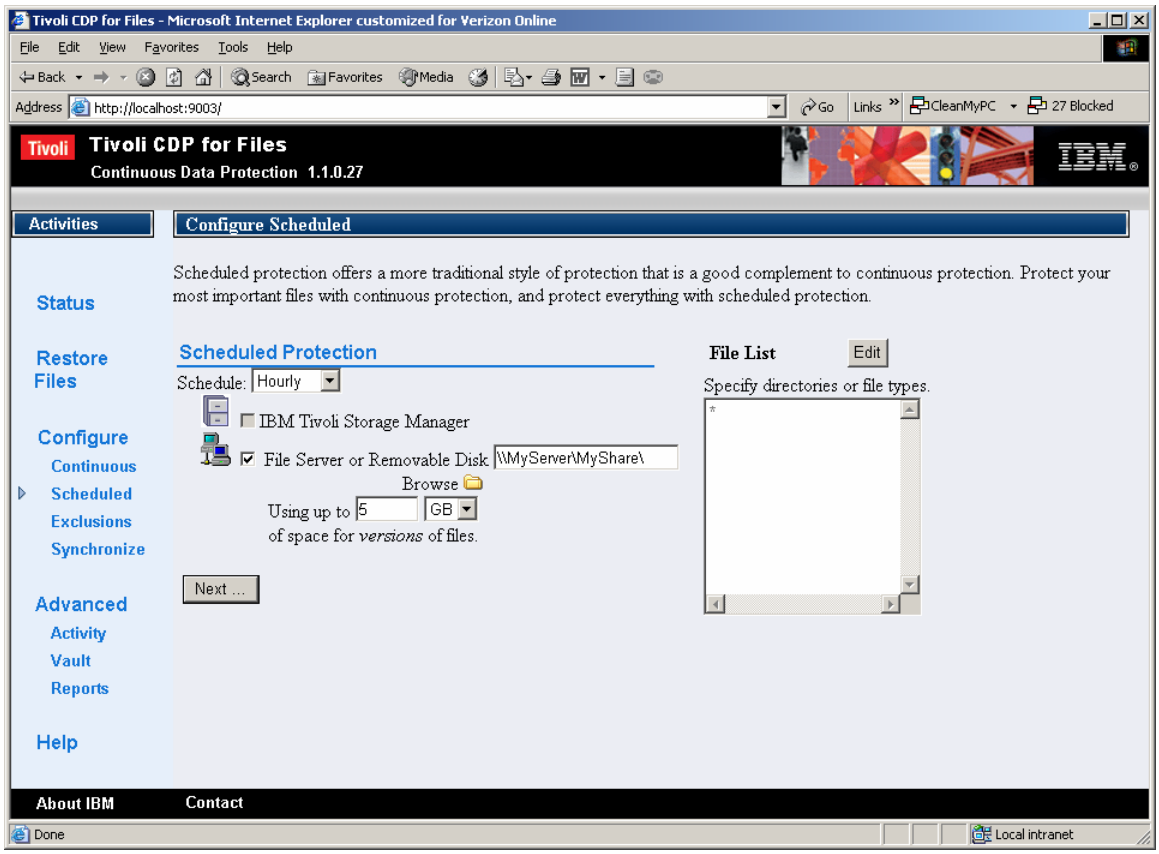


NOTES:

1. Use UNC naming specification of the file server instead of drive letters since drive letters can change after rebooting and many times do not reconnect automatically.
2. Log in to your machine with a username and password which Tivoli Continuous Data Protection for Files can use to authenticate transparently into the network location you have specified. If not, you can alternatively log into the network using another account with regular privileges interactively (i.e., by using the Net Use command).
3. Some versions of Windows have a concept of simplified file sharing, which allows one computer to network-attach to another with very little difficulty. The resulting connection allows only limited file system capabilities. If possible, disable simplified file sharing on the target system as it limits how well Tivoli Continuous Data Protection for Files can produce an identical copy of your files. If simplified file sharing is not disabled, some information such as access control lists or file streams may not get copied correctly. See your administrator if you have questions.
4. Clicking the **folder** icon will present a directory browse dialog box. If this dialog becomes hidden behind other windows, click on the task bar to bring it to the front.

Scheduled protection configuration

Files that are protected by schedule are copied to a remote device on a regular schedule. Only a file that changes is copied at the schedule; and each scheduled copy is retained as a distinct backup version. Whereas the **Configure Continuous** panel allows you to specify your most important files for continuous protection, this panel allows you to protect **all** files on your system at configured intervals.



When to Use Scheduled Protection

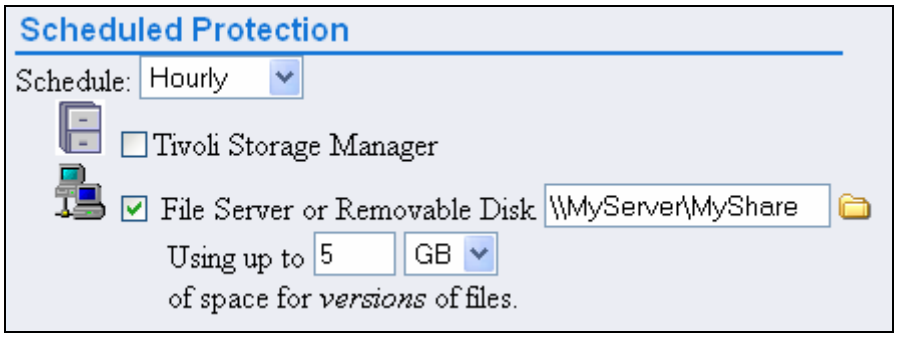
The continuous protection of important files that you specify could be sufficient for your needs. Consider that there may be other files on your system that are important, but you have not included them in the file list for continuous protection. This could be the case if you created a new directory tree for a project and forgot to update the list of continuously protected files, or you installed a new program that uses a different file extension than the ones you currently have in your file list. Also, there are often project files or other files that are necessary for correct operation of some application that you may not know about, and that would be sufficiently protected by schedule. For these reasons, it is useful to have a more comprehensive backup available. Scheduled protection provides this comprehensive backup.

Scheduled protection vs. traditional backup

Tivoli Continuous Data Protection for Files' scheduled protection is different than traditional backup for the following reasons:

- Tivoli Continuous Data Protection for Files never has to scan your file system trees to find new or changed files; it always knows exactly what is changed and this greatly speeds up the backup process.
- Tivoli Continuous Data Protection for Files offers both continuous and scheduled protection. Your most important files are saved as versions locally, in addition to being saved to a remote target.
- Except for files saved to the TSM server, backup copies are in their native format, as files on the backup device, with their original form. This makes maintenance of the backup device as simple as maintaining an ordinary file server.

Scheduled Protection schedule and backup location



To configure scheduled protection, select the interval you want in the **schedule** drop-down box in the **Scheduled Protection** panel. Next, select the location(s) to store your backups: **IBM Tivoli Storage Manager**, or **File Server or Removable Disk**.

Backup location: Tivoli Storage Manager

The space available for backups via Tivoli Storage Manager is configured by your TSM administrator. The location of your TSM server is configured in your TSM options file. For more information, see IBM Tivoli Storage Manager Backup-Archive Clients User's Guide.

Backup location: File Server or Removable Disk

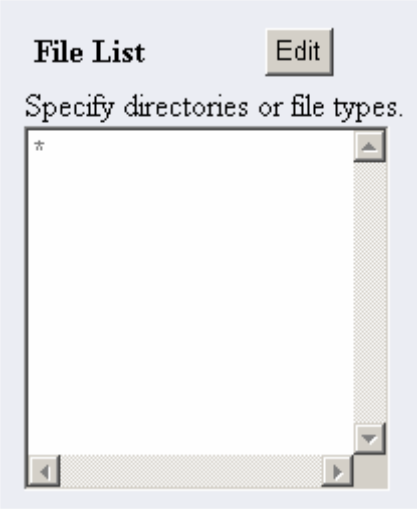
If you choose **File Server or Removable Disk**, you also specify the device location and the space for versioned backup copies. The space in the **Using up to** fields limits how much space Tivoli Continuous Data Protection for Files consumes for versioned backup copies of files. A versioned backup copy is a backup copy that has been replaced by a more recent backup copy. If the versioned backup copies reach the limit, Tivoli Continuous Data Protection for Files removes the oldest backup versions of files until there is enough room to complete the backup. Tivoli Continuous Data Protection for Files never removes the most recent backup copy of any file.

> NOTE: If you specify a space value of zero, then Tivoli Continuous Data Protection for Files does *not* make versioned instances of the protected files. Thus, the backup area will effectively match your computer. Some users may choose to back up the target file server using a conventional backup program and thus may not need versions.
>
> NOTE: The file server (or disk) specified in this panel is also the file server (or disk) specified in the **Configure Continuous** panel; a change made here changes that panel as well. The product does not support more than one remote target.

It is imperative that you have enough disk space at the specified backup location to hold at least one backup copy of all changing files from your list of files. If the backup location runs out of disk space, Tivoli Continuous Data Protection for Files will pause and notify you with a message, until you make more space available.

File List

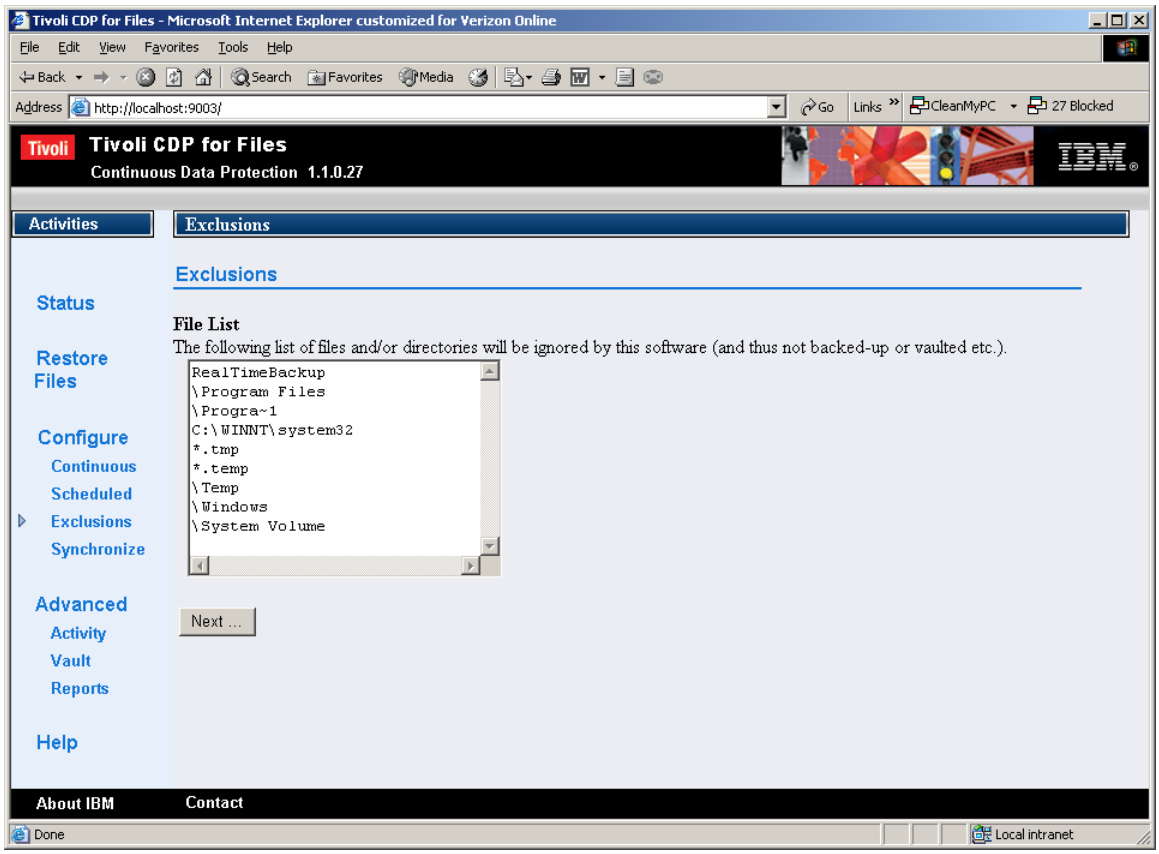
Next, configure the File List as desired.



By default, all changing files on your computer will be monitored by this feature, except for files and directories specifically excluded on the **Exclusions** panel. Click “Edit” to change the list following the same syntax rules described for the **Configure Continuous** panel.

Configuring exclusions

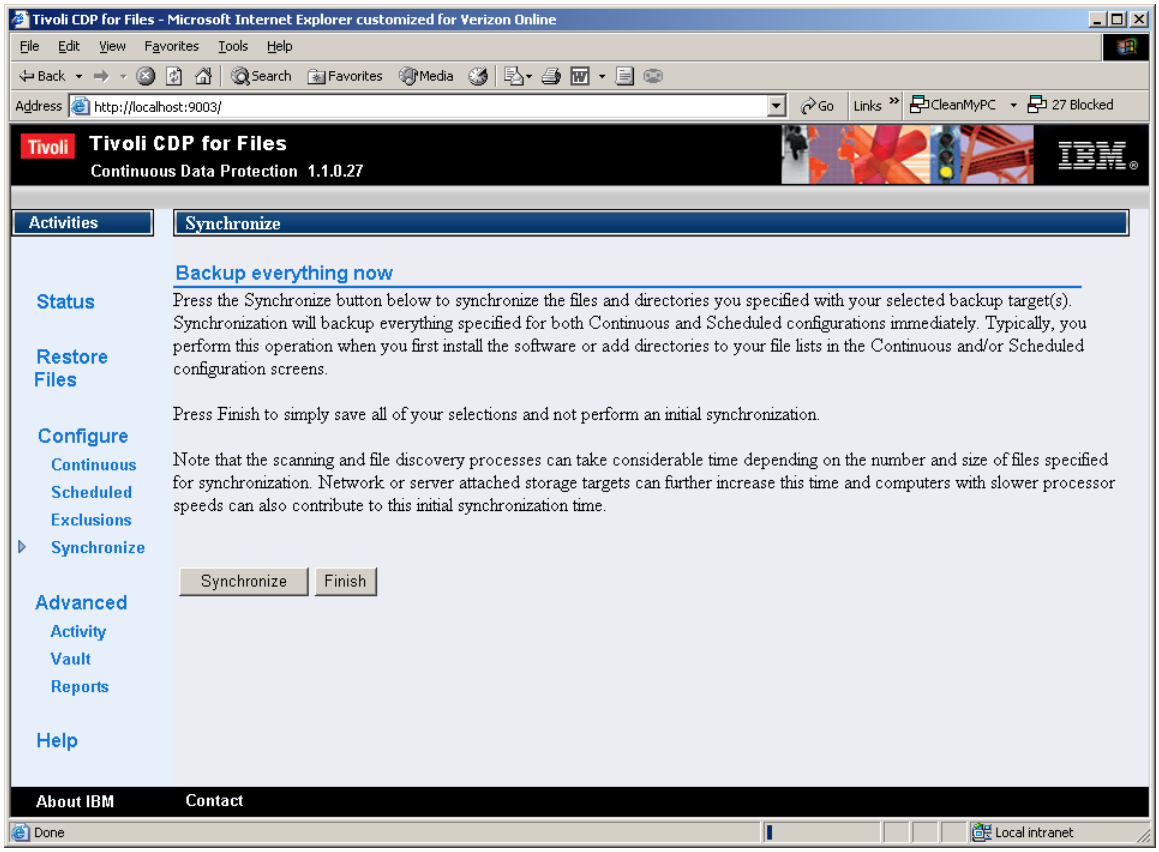
Use the **Exclusions** panel to configure which files and directories you don't want to protect. Exclusions are processed before the **File Lists** on the other configuration panels. By default, you will exclude the various Windows operating system and Program Files as well temporary files.



Synchronize

The **Synchronize** button in the **Synchronize** panel allows you to backup all files immediately. Synchronize soon after you first install Tivoli Continuous Data Protection for Files. Synchronizing protects all *existing* files on your machine, and doesn't leave unchanged files without protection. If you do not synchronize, only files that change after the product installation will be protected. Synchronize also when you change target remote servers so that the new server contains backup copies of all your files.

Synchronizing will cause all of your local disks to be processed. This means that every file in every directory will be investigated and scheduled for protection (unless the files are in an excluded directory). This can take a very long time. The scan process could take an hour or more, and depending on how much data it finds and how fast your network is, the actual transfer operation could take a very long time.



Versioning and expiration

As you make changes to files, either directly by saving or copying files, or by an application creating or altering support files, Tivoli Continuous Data Protection for Files will be aware of the changes. When the scheduled backup operation takes place, Tivoli Continuous Data Protection for Files copies the changed file to the remote device.

Versioning and expiration: Tivoli Storage Manager

Versioning and expiration of files on the TSM server are determined by the TSM management classes associated with your files. For more information, see the discussion of management policies in IBM Tivoli Storage Manager Backup-Archive Clients User's Guide.

Versioning and expiration: File server or remote device

The most recent backup copy becomes the active backup copy. If there is an older backup copy, it will be renamed with a *version* identifier suffix. Versioned backup copies can be restored through the Tivoli Continuous Data Protection for Files **Restore** panel.

When the space for versioned backup copies reached on the backup device, older versions will be deleted. The most recent backup copy of a file will never be deleted.

If you delete files from your local drive, Tivoli Continuous Data Protection for Files will expire all but the most recent backup copy on the remote server. Expired backup versions can be restored through the Tivoli Continuous Data Protection for Files **Restore** panel. They are subject to deletion if space is needed for active backup versions.

Chapter 4: Restoring Files

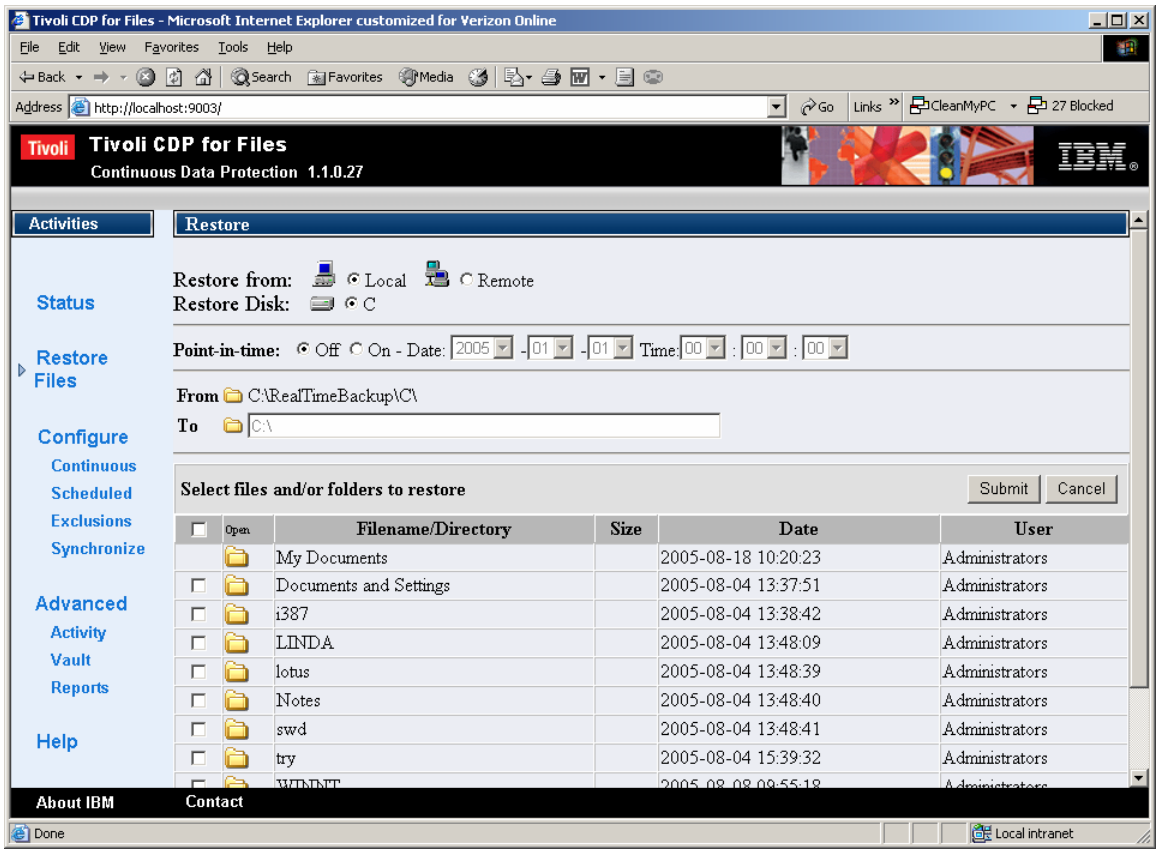
Introduction

If you restore from the TSM server, you must use the TSM Backup-Archive Client.

If you restore from the local Backup area or the location you configured in the remote File Server or Removable Disk, use the Tivoli Continuous Data Protection for Files **Restore** panel. You can restore individual files, groups, and directory trees. You can restore them to their original location or to a new location. If a file has several backup versions, you can select which version you desire, or by default take the most recent version.

> NOTE: You can also restore files yourself using your own file system tools. Tivoli Continuous Data Protection for Files stores backup copies with the same format, name, and directory path as the source file. Older backup versions have a suffix added to the file name. You are free to copy (restore) these files yourself at any time.

The actual restore process is done by the replication engine and does not tie up your session or application. You can view the status of a restore in the **Status** panel.



The Restore From section

First, select which location you want to restore *from.* Depending on how you configured your protection, you could have backup copies in two locations--one local and one remote. In the following example, both

local and remote backups are listed. Choose which backup location you wish to restore from by selecting the radio button next to the location. Then select which drive you want to restore from. Your local computer may have more than one drive, perhaps a C: and a D: drive, and each drive will have backup copies in the backup location(s) you configured. In this example, there is only one drive to restore from – C. If you have more drives available, they will also be listed here with radio buttons to select them. Click a radio button to refresh the data below.

Point-in-Time

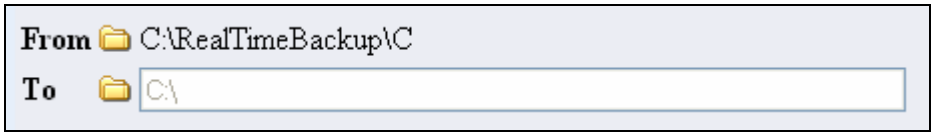
Tivoli Continuous Data Protection for Files has the ability to restore files and directories back to a specific point in time, provided the backup version for that time exists.

To use point-in-time recovery, click the **On** radio button and then select the date and time of the version you wish to restore. If you select a directory or a file that has versions, the system will restore the version of the file(s) that is closest *before* the date/time you select. If you do not restore by point-in-time, you will by default restore the latest version of a file.

Adjusting the From/To locations

The From/To section allows you to specify the target ("to") location of the file(s) you will restore. By default, files will be restored to their original location. If you would like them restored elsewhere, perhaps to a temporary directory, click the **To** folder icon and select a location.

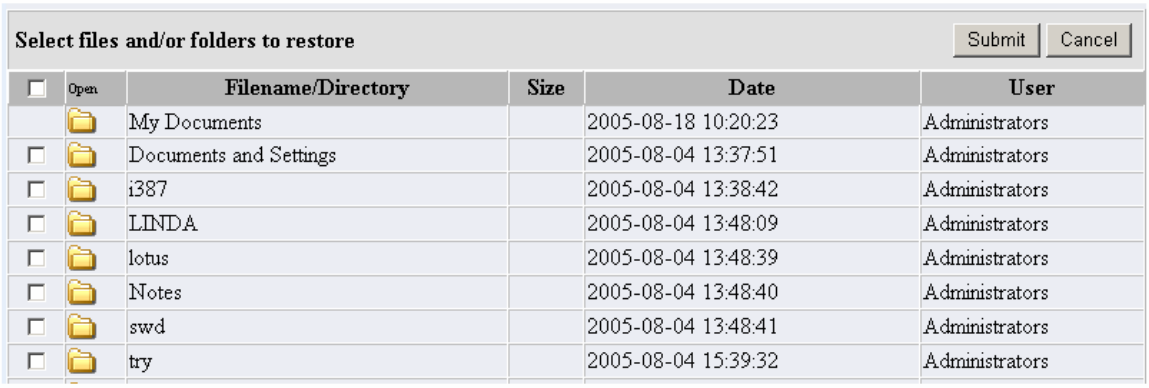
If you are restoring a single file, you can type a file name in the text box, e.g. "C:\restore\myfile_temp.doc". If you are restoring a directory tree, then you must specify a directory.



In certain circumstances, you might need to change the **From** location. In general, clicking the various radio buttons at the top will be sufficient. One case is if you are an administrator and need to navigate to a different part of the backup-file-server to restore from a different user's backup area.

File Selection

The last section shows you the files and directories discovered at the “From” location.

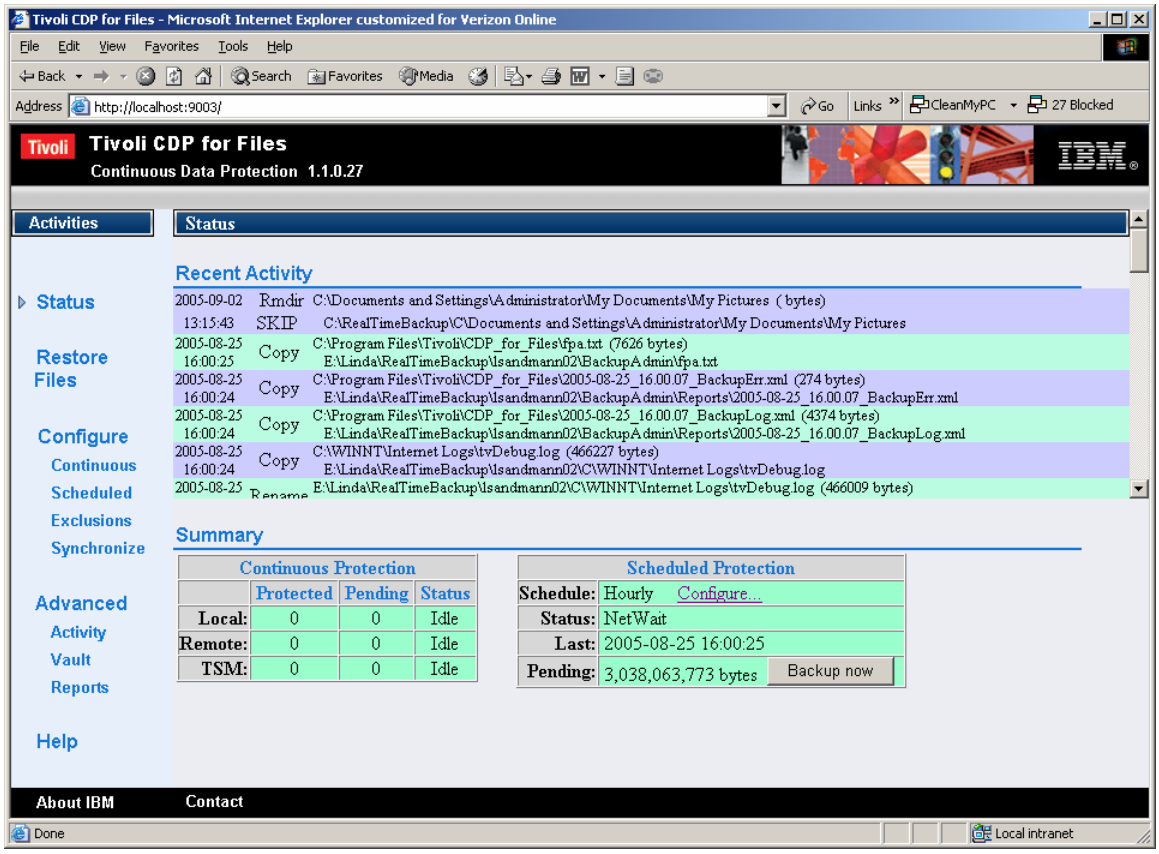


On this panel click the check box(es) next to the files or directory trees you wish to restore. You can also drill-down into a directory tree by clicking on the folder icon next to the directory name. Similarly, for files, if there are multiple versions available, you can click on the icon next to the file name to drill down into the individual versions. Once you have your files or directories selected, click **Submit** to restore your files.

Chapter 5: Status Panel

Introduction

Click on the **Status** link to display the **Status** panel:



This Status panel displays when you first start Tivoli Continuous Data Protection for Files. The panel shows various summary status information. The top section lists the most recent file protection activity. The top items in the list are the most recent.

The bottom left panel shows summary information regarding how many files have been protected since boot-up or log-in to the various targets. “Pending” indicates how many files are queued for transmission and “Status” indicates if that activity is in-process, idle, or waiting for a network connection.

The bottom right panel shows summary information about the Scheduled Protection feature. In general, the scheduled protection feature will operate at the interval you configured (e.g. daily or hourly). You can, however, press the **Backup Now** button to force the backup to take place right now.

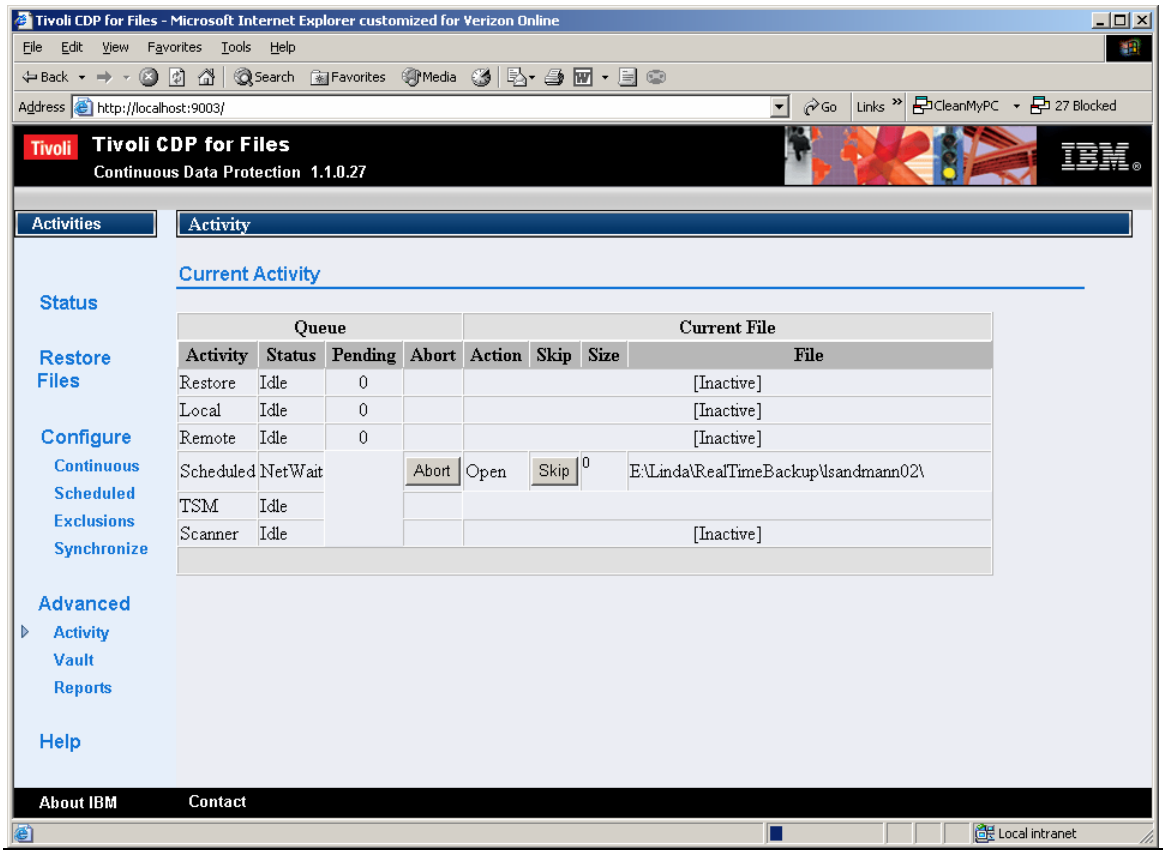
Chapter 6: Advanced Panels

Introduction

There are three Advanced Panels: **Activity**, **Vault**, and **Reports**.

Activity Panel

Click on the **Advanced/Activity** link to display the **Activity** panel:

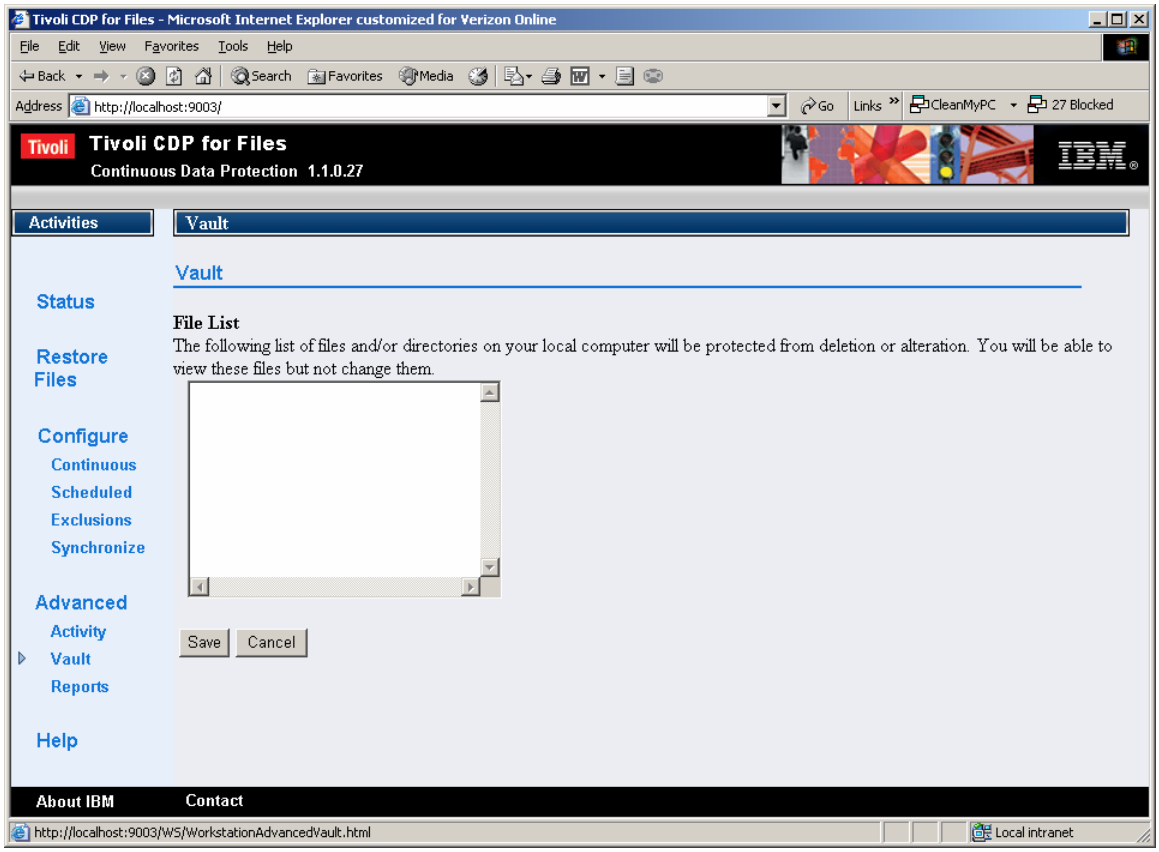


This panel shows summary information of the software's main worker activities (threads). This is a live display that changes as activity occurs. If a worker thread is active, the display will reflect how many items are pending and the current file being worked on (along with its size). Under the **Abort** and the **Skip** columns, a button will appear to allow you to abort all transactions for that thread or skip just the current file.

Notes:
The row for **Scheduled** will not show a pending count.
The **TSM** row does not support Abort or Skip in this release.
The **Scanner** row is active when you synchronize, and can be aborted.

Additional protection of source files with vaulting

Click on the **Advanced/Vault** link to display the **Vault** panel:



Vaulting is a unique concept that locks-down files tighter than normal file protection mechanisms such as Access Control Lists or permissions. Files that match any element in the vaulting list are prohibited from being deleted or altered. Vaulting should provide added protection against accidental or malicious deletions of important file.

Click inside the **File List** box to add or change which items you wish to have vaulted.

This feature can be used as a type of archiving. Perhaps you have a directory tree that has some stable set of files and you want to protect and version it. Either copy the tree to a new name (e.g. “c:\MyPictures\July”) and put the directory in the vault list or simply put the current location of that tree in the vault list.

You can use wildcards to essentially protect material that does not yet exist. For example, if you have “*.jpg” in your vault list, any current or future-created .jpg file will be vaulted. Perhaps you only want to vault .jpg files under a certain tree. To do so, use a syntax such as: C:\MyTree*.jpg

If you need to manipulate or delete a vaulted file, temporarily remove the corresponding item from the vault list while you do your maintenance and add it back to the list when you are through.

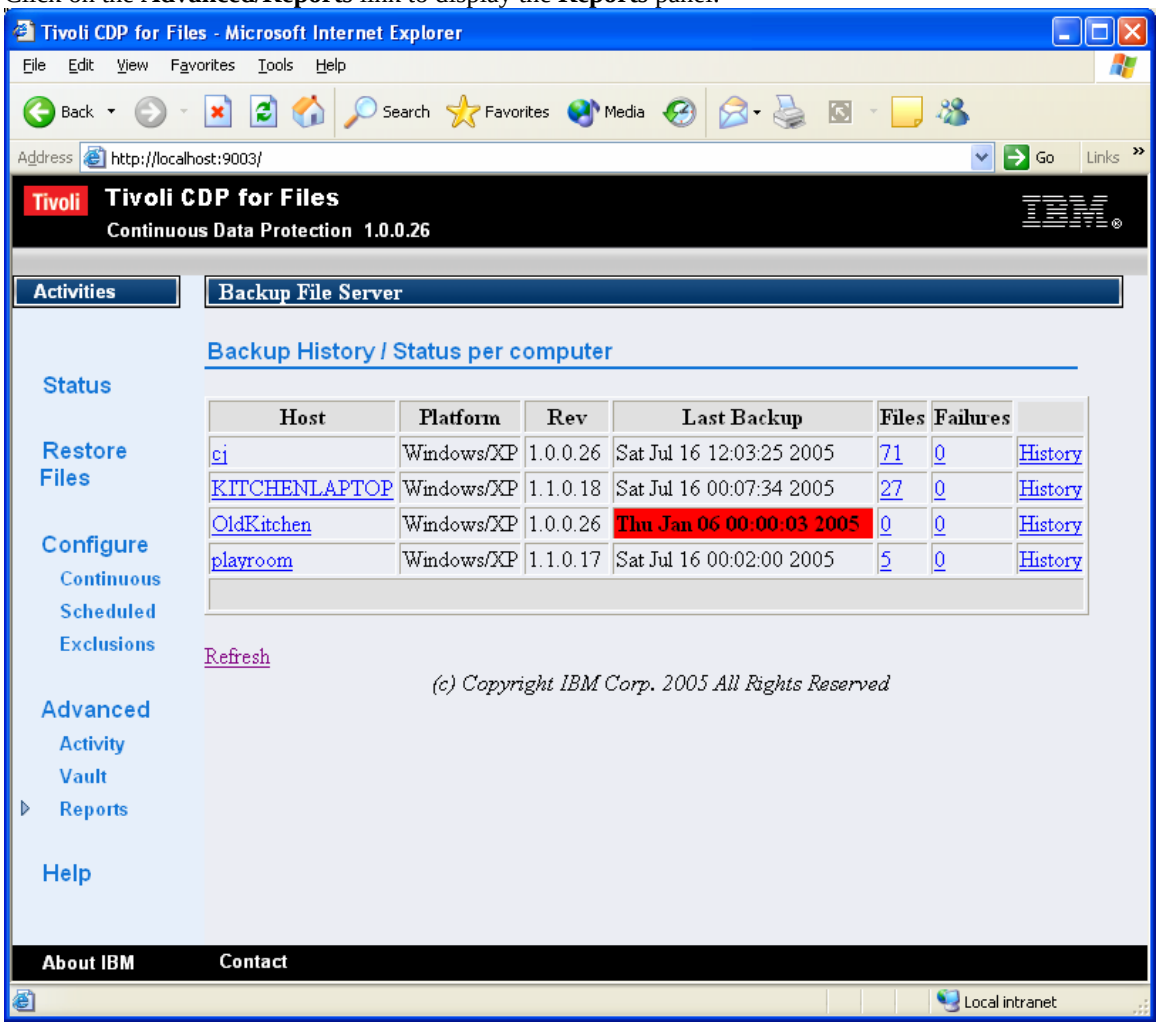
Retention

The vaulting feature includes a special additional feature called Retention. You can specify that some files be vaulted for a specific period of time and after that time elapses the material is *allowed* to be deleted.

To activate this capability, simply name a directory “KeepSafe” under any vaulted area. Files stored under the KeepSafe part of the tree have special rules. Namely, they must be stored within folders that indicate the retention holding period. For example, “C:\MyImportantDir\KeepSafe\Retain 3 years\”. Any file created in that directory will be prevented from alteration or deletion for three years. After the expiration time, the file may be deleted successfully. Tivoli Continuous Data Protection for Files does not automatically remove the material after the retention period. However, you can create a script that attempts to remove all items in a top level tree, and all the un-expired items will be protected from deletion by Tivoli Continuous Data Protection for Files.

Reports

Click on the **Advanced/Reports** link to display the **Reports** panel:



If you have a remote file server (or disk) configured as a backup target, then this display will show summary information of all the Tivoli Continuous Data Protection for Files users connected to that device. A row will be present for each computer that is using that backup target. Clicking on the link under the **Host** column will display an XML summary of the specifics of that computer (computer type, name, configuration settings, and so forth).

The **Last Backup** column states the time of the last completed backup. The date will be colored yellow if it has been several days since a backup and red if longer than week. The links under **Files** and **Failures** will display an XML file detailing each transaction.

Chapter 7: Administering Tivoli Continuous Data Protection for Files

Introduction

Tivoli Continuous Data Protection for Files is equally well suited to protect large numbers of computers in an organization as it is to protect a single laptop or homeowner's machine. When used to protect more than one machine, there are some administration features and deployment styles to consider.

Part of the charm of Tivoli Continuous Data Protection for Files is that it is a "single end-point" architecture. That is, you only load the Tivoli Continuous Data Protection for Files software on the machines you are protecting and there is no "Tivoli Continuous Data Protection for Files *server*" per se. Tivoli Continuous Data Protection for Files is able to be viable in large organizations, even without having a centralized server component, for two reasons:

1. It exploits the "server nature" of natural file servers
2. It performs what would be centralized work in a decentralized fashion via the client end-points.

Multiple machines

If you have multiple machines in your organization that need protection, it is recommended that you configure each one to use the same backup file server device. When Tivoli Continuous Data Protection for Files stores the backed up data on the file server, it puts the data into a sub-directory named "RealTimeBackup" and then under a directory named after the client's machine name. For example, if my computer is known to the network as "Smith", and my Tivoli Continuous Data Protection for Files is configured to store data on the remote file server "\\remote\share", files will actually be created in "\\remote\share\RealTimeBackup\Smith\" .

This is convenient in a multi-machine arrangement since every client can be configured the same. That is, pointing to the same file server and the same 'share' there, yet have a distinct tree of their own ultimately. In practice, it is quite common to have dozens to hundreds of clients pointing to the same backup file server (and share). Each installation is different with regard to the amount of data that is expected to move, so an exact limit can not be given.

While there is no "backup file server administration" (because there is no component for Tivoli Continuous Data Protection for Files on the file server), Tivoli Continuous Data Protection for Files still offers many common and important administration management features, including centralized reporting, global software update, global configuration updates, and other capabilities described in the following sections.

Changing the reporting/administration area

By default, Tivoli Continuous Data Protection for Files uses a special directory tree at the configured remote location for storing various reports and for learning of updates or other activities. The default location is:

\\Server\share\RealTimeBackup\BackupAdmin

Where "\\Server\share" is whatever you have configured for the remote target in your configuration panels, thus, the "BackupAdmin" tree is at the same tree-layer as each machine starting point. Some times this is not convenient for certain sites and an administrator may desire to have the reporting area be at a completely different location. To change the location, execute the command-line configuration utility "fpa" in the following manner:

>> fpa config-set GlobalManagementArea="\\AnotherComputer\AnotherShare\MyDir"

Reporting

Tivoli Continuous Data Protection for Files creates a couple of special folders on the remote target (or the configured GlobalManagementArea) to use for various administration purposes such as reporting. Under the "machine" directory (e.g. "\\remote\share\RealTimeBackup\Smith") Tivoli Continuous Data Protection for Files creates a "BackupAdmin" directory. Within the BackupAdmin directory, Tivoli Continuous Data Protection for Files creates a "LastBackupSummary.xml" file and another directory, "Reports", which holds a variety of reports from each backup operation. After each scheduled backup session, two files will be created in this directory. One file will list all of the transactions performed or attempted, and the other will list only failure items (to make it easier to see and deal with failures). The files are named by using the current date of the backup to aid in organizing the directory.

The Advanced Reports tool scans each machine's reports directory to produce the Reports display.

Closing applications during scheduled backup

Tivoli Continuous Data Protection for Files has an ability to send various programs a "close" signal before starting the scheduled backup. This is useful if an application holds various 'locks' on a file that would prevent a successful backup. Outlook holds its mail files open with special range-locks on the mail files which would cause the backup of those files to fail, for example.

Tivoli Continuous Data Protection for Files looks for a text file called "closeapps.txt" in the installation directory. If the file exists, then each line in the file is interpreted as a program name that should be found and sent a close command. To learn of the correct program names, use Windows Task Manager and view the "Image Name" column. (Outlook and Outlook Express have program names OUTLOOK.EXE and MSIMN.EXE respectively.)

Scaling

It is typically easier and more straightforward to scale a Tivoli Continuous Data Protection for Files network than a traditional backup system. Scaling a Tivoli Continuous Data Protection for Files backup file server is no different than scaling a typical file server and each installation has to understand the amount of data that is expected to move and when. You can scale a file server by:

- Adding more CPUs
- Adding more memory
- Adding more network interfaces

Similarly, to scale the storage you can add more disks or LUNs and grow your file system onto the new disk space. On occasion, you may need to do some intensive directory or system re-organization (perhaps migrating data from one share/LUN to another or even to another machine). It would be best to disable backups during this period and the easiest way to do that is to prohibit machines from connecting to your backup file server (using any of a variety of network administration tools you already have); Tivoli Continuous Data Protection for Files clients will patiently wait for the server to become available again.

If your backup file server can not be further upgraded, you may need to replace it or *add* additional backup file servers. If the storage repositories were on external disks (such as on a SAN), you can simply move the disks over to a new computer (presumably with the same network name so that the clients do not need to change). If not, first disable the current machine from performing any additional backups (per the directions above), copy the RealTimeBackup folder to the new machine (using any natural file and folder copy tools you have available), and then activate the new machine.

You may choose to add additional backup file servers to your network. When adding a new Tivoli Continuous Data Protection for Files client, you can "point" any clients at the new server. You may also

desire to split the backup load of a running backup file server among other servers. To do so, you should first move the effected computer's backup tree from the current machine to the new one, and then update those clients to reference the new machine. Again, you can accomplish this by using tools you have naturally available to you outside of Tivoli Continuous Data Protection for Files.

Purging and Removing Material

From time to time, you may need to remove unnecessary files from your backup file server. One common reason is due to client systems that are no longer active (and presumably there is no value in retaining their old backup data). You can simply remove their corresponding backup tree from the backup file server; there is nothing special to tell Tivoli Continuous Data Protection for Files.

You may also choose to run some SRM package and scan your backup trees looking for candidate material to delete. You might decide to remove files of a certain size or age (or both). You might target removing versioned-instances first (rather than delete the active instance of any file). If you do delete versioned instances, Tivoli Continuous Data Protection for Files will operate properly but its bookkeeping on the client will be somewhat off. This will auto-correct. When Tivoli Continuous Data Protection for Files purges its versions on its own due to the pool appearing full, it correctly understands that a missing versioned file should have it's space allocation deducted from the pool "in use" metric.

You can delete any file or directory you desire from the backup file server. Or move directories around within the machine's top level directory, all without telling Tivoli Continuous Data Protection for Files anything special. Tivoli Continuous Data Protection for Files "walks" the directory structure when presenting the "restore" interface. Obviously, if you delete a file from the backup file server, it can not be restored. The point is that there is no special knowledge of what's been backed up or where it has been backed up to, unlike in a traditional backup product.

> NOTE: If you do re-arrange or move trees on the backup file server, and those trees contain file *versions*, Tivoli Continuous Data Protection for files will be unaware of their movement for the purpose of purging them when the pool becomes full (it will, however, be aware of them for purposes of Restore presentation and selection as that logic simply walks the directory trees and presents what it finds). When the purge logic runs and attempts to delete a versioned instance from the previously known location, that delete will fail and Tivoli Continuous Data Protection for Files will down-count the pool metric as if the delete succeeded. The caveat is that the file is not truly deleted and thus consuming file system space.

Backing-up the backup file server

Some customers have the need to also "backup" (or protect) their backup data and machinery. The most typical reason is to get copies of the material off-site in case of some sort of site disaster. Historically, customers execute a typical backup application to tape and then hand carry the tapes to some archive service location.

Certainly, there is nothing preventing an administrator from running a conventional tape-type backup application on their backup file server and a particularly good choice is Tivoli Storage Manager.

In the modern world, it is possible to replicate the data to another more distant machine. Wide area networking is getting faster and more affordable every year. DSL and cable are viable alternatives to expensive T1 lines. Keep in mind, when replicating a backup file server to another backup file server, the "backup window" is typically much longer, perhaps upwards of 20 hours. Whereas you might need your client systems to complete all of their backups within a few hours so that the process doesn't interfere with normal work-hours operation, the backup file server replication can use the rest of the regular day to matriculate its material over the slower WAN link.

There are many different deployment models and each has merit. Consider the following options:

- Hardware. Consider using some asynchronous hardware solution. Perhaps your storage device has a controller that provides this capability or perhaps you can add a mirroring device to your SAN.
- Software. You could use a number of off-the-shelf software packages to replicate data at either the file or block level.
- Tivoli Continuous Data Protection for Files. You could run Tivoli Continuous Data Protection for Files on the backup file server and have it re-back-up material to the final target.
- Wide area file system device. (described below).

If you choose to use Tivoli Continuous Data Protection for Files, there are several different ways to configure and deploy it. One choice is related to how and where to do versioning. You may elect to disable versioning of the Tivoli Continuous Data Protection for Files clients on your LAN (by setting their pool size to zero) and allow the final backup file server to do versioning. In this way, you need less disk space at your primary site and have off-site protection of active and versioned files. The opposite configuration is to have versions locally but only the "active" copy at the final remote site. To achieve that, you need to add "-FP" to the exclude list of the backup file server so that it does not "backup" the version instances.

The last choice, using a Wide Area File System (WAFS) device, bears some explanation. The goal of a WAFS is to have a file server at a remote site "feel" like it is local with regard to speed and performance. Typically two pieces of hardware are used: one at each site. The hardware sits on the LAN and WAN at both sites. At one site the device attaches to a real file server (typically at a corporate headquarters location) and at the other site (typically a branch office) it presents itself on the LAN as a local file server. In the background, the device at the branch office packs and transmits changes to the corporate location and keeps a large "cache" locally so that the attached LAN clients have higher response than a WAN would typically provide. When used with Tivoli Continuous Data Protection for Files, the LAN clients are configured to use the corporate file server as their backup file server yet the performance is as if the backup file server was local.

There are many other solutions for protecting the backup file server that will work well in a Tivoli Continuous Data Protection for Files architecture.

Distributed installs and configuration updates

Tivoli Continuous Data Protection for Files is designed to allow for easy distribution of upgrades and configuration changes. On the backup file server (or the configured GlobalManagementArea), there are special directories where Tivoli Continuous Data Protection for Files clients will periodically check for work items. These directories occur at two levels in the tree: one is at the top (that is, directly under the RealTimeBackup directory) and then there is one for *each* machine.

The special directory is called "Downloads" and lives under the "BackupAdmin" directory (in either location). Tivoli Continuous Data Protection for Files periodically scans that directory for new Tivoli Continuous Data Protection for Files installers as well as for a "commands" file. There is a special flavor of installer provided with Tivoli Continuous Data Protection for Files that performs a quiet install (no windows and no prompts) and Tivoli Continuous Data Protection for Files knows how to invoke that installer if it is present in one of those two directories.

The other special file must be named "fpcommands.xml" and contain valid Tivoli Continuous Data Protection for Files XML command statements. At the time of this writing, those commands are *not* published, but under special circumstances can be made available to customers. All aspects of Tivoli Continuous Data Protection for Files (all settings and configuration values) can be set through this command syntax (for example, you could globally change the exclusion list for all clients).

The main configuration file for Tivoli Continuous Data Protection for Files is an XML text file called "fpa.txt" which lives in each client's install directory. All of the various settings configured in the UI result in changes to that text file. An administrator could copy one such fpa.txt file to the appropriate Download area (either the top global area or one specific for a machine) and name it "fpcommands.xml" to have each client absorb that file.

Any file processed from the Downloads directory will be processed only once. Each client that processes a file makes a local record of this in their install directory and knows not to re-process the same file in the future (based on name *and* date of the file; thus, if an administrator places a new 'fpcommands.xml' file in the download area, for example, it *will* be processed since it is newer).

If you wish to have *all* machines attached to that backup file server process a given file, place it in the upper directory's Downloads folder. If you want only certain machines to process a file, put the file in each machine's folder instead. To control *when* the file gets processed, simply place it in the folder near the time you wish for it to be processed (you could create a script, for example, that runs at 3am and puts the material into position).

Push-installs

For typical Windows networks, Tivoli Continuous Data Protection for Files has a method of "pushing" its installer out to machines that currently have no Tivoli Continuous Data Protection for Files software loaded. Your installation may or may not include all of the programs and files for this feature (contact support if necessary).

There are two programs that work together to achieve this push-install feature:

- TivoliCDPconsole.exe; a special version of the Tivoli Continuous Data Protection for Files installer that does not result in windows appearing and is essentially a "quiet" console-type of installer.
- FpPushInst.exe; a program that is capable of pushing other programs out to a target computer and executing them.

First, let's describe the console installer and its parameters. With no parameters, the console installer will simply install quietly on the current machine using all the defaults. Alternatively, the program can be passed the following parameters:

/d:*InstallPath*
/f:*ConfigurationFile*

The "/d" parameter allows you to overrule the default installation location, for example:

TivoliCDPconsole /d:c:\MyInstallArea

The "/f" parameter forces the installer to copy the specified file into the installation area at the end of the installation. Typically this will be the "fpa.txt" file (the main configuration database) to force the system to use a pre-configured one.

The FpPushInst.exe program makes a connection to a remote server (based on parameters you specify) and the copies an executable to a planned location, along with an additional file, and then executes that executable with parameters that you specify. The syntax for the command is:

FpPushInst \\computer [/USER:user] [/PWD:pwd|*] [/C:filename] /R program [arguments]

"/USER" and "/PWD" are used to specify the username and associated password respectively of an account on the target system that will be used to make the connection.

"/C:" specifies a file on the *current* computer that you want pushed to the temporary area on the target presumably to be consumed by the program that you're pushing there (e.g. the 'fpa.txt' file).

"/R" is the start of the program and parameters section. The item after "/R" is the program you want sent to the remote computer and all the remaining arguments will be sent to the program when it is started. The default directory on the target when the program is running is the Windows system32 directory.

Example:
Assuming in your current default directory you have the console installer and an 'fpa.txt' file:
FpPushInst \\Computer /user:administrator /pwd:admin /c:fpa.txt /r TivoliCDPconsole.exe /f:c:\windows\system32\fpa.txt

Using Tivoli Continuous Data Protection for Files on servers

Tivoli Continuous Data Protection for Files works very well on file servers (in addition to end user workstations). There are some caveats, however. Tivoli Continuous Data Protection for Files has two main components: a kernel extension that watches your file system and a "daemon" that performs the file duplication tasks. The part that does the duplication needs to be "authenticated" by the target computer. Tivoli Continuous Data Protection for Files is able to have this component run as either an operating system service or as an interactive application. This product, as shipped, launches the component each time someone logs into the computer. Thus, the authentication will happen under the current logged-in user's credentials. However, if no one logs in, the daemon isn't running, which wont be effective for server type configurations.

If you plan on Tivoli Continuous Data Protection for Files running on a server (that is, a machine without logged-in users), you need to change the default behavior. In the Tivoli Continuous Data Protection for Files install directory there is a program called "FpForServers.js" which you need to execute. This will register changes so that Tivoli Continuous Data Protection for Files runs as a service instead of as a logged-in application.

You may then need to configure the service (with regard to the account that it uses) in the services control panel. The default account for Services (on Windows) has no privilege for accessing network file shares. Most likely you'll need to update the service ("filepathsrv") and specify a valid account name and password that is able to access your Remote targets. The "FpForServers.js" application launches the Windows services configuration pane.

Note: Tivoli Continuous Data Protection for Files installation directory and tree is set for full access to all users on the system during installation. This is done so that non-privileged users (users without Administration rights) can still be protected by the software and use the user interface. This is probably *not* a desirable setting for multi-user file servers. Consider re-setting the ACL's on the installation directory and tree to something more restrictive as there are log files and programs whose contents and use should not be available to all users.

Sequencing backup times

By default, Tivoli Continuous Data Protection for Files will start the "scheduled backup" at 6 seconds after the specified interval. If you select hourly, Tivoli Continuous Data Protection for Files will start 6 seconds after the start of the hour. If you select daily, it will start 6 seconds after midnight. If you select weekly, it will start 6 seconds after Sunday morning.

In larger installations, you may need to have more control over the start time (perhaps to better stage many machines attacking the backup file server). Internally, there is a configuration parameter called "targetBackupTime". You can set this parameter on a machine by executing the "fpa" program (in the Tivoli Continuous Data Protection for Files install directory) as follows:

fpa config-set targetbackupTime="6"

Or, you can put the command "<config-set targetBackupTime="6"/>" into an fpcommands.xml file and deposit that into the "Downloads" directory as mentioned earlier.

The value specified is interpreted as "seconds after the natural boundary". If you specify hourly as your interval, then this value indicates "seconds after the next hour". If you specify "daily", then this value indicates "seconds after midnight". Often administrators will desire to stage various client clients to backup at various starting times throughout the night or week.

Encryption and security

Tivoli Continuous Data Protection for Files will work correctly with any number of layered security and encryption tools. Some sites desire to have their "backup data" encrypted so that it is of little value to unauthorized people. Windows has built-in encryption capability that can be activated simply by right-clicking on the upper backup tree folder. Or, use any other 3rd party encryption product.

Security and access in general is a concern to many shops. The backup file server is truly a "file server" and can be protected by any means suitable for a file server. Typically administrators create user groups with various privileges and control access to directories through ACLs (capabilities built natively into Windows and all operating systems). An administrator may desire to place various ACLs on certain machine backup directories (or even all of them) to prevent one user from seeing into another user's area.

Tivoli Continuous Data Protection for Files also works well over corporate VPN links.

Tivoli Continuous Data Protection for Files will work with other file-sharing protocols that might have better security features for various customers. NFS or WebDAV or anything that presents the target as a "mounted file system" to the client computer should work fine.

Delta replication

Many replication products offer a special mode that results in fewer bits being transmitted when a given file changes multiple times. The technique involves examining the file on the source as well as the last copy sent to the destination and learning of which sub-areas have changed.

Such techniques require the replication software to be installed at both end points. Tivoli Continuous Data Protection for Files, by contrast, is a single-endpoint solution.

That said, Tivoli Continuous Data Protection for Files has abstracted the "data movement" component and allows for other programs or agents to move the actual bits of a file. Rsync is a commonly available application (freeware) that is a capable of moving only the sub-portions of a file and it would be useful if Tivoli Continuous Data Protection for Files could exploit rsync (or any other similar application) if they are available on both the client and server.

Tivoli Continuous Data Protection for Files checks its install directory for the presence of a file named "rcopy.js" or "rcopy.bat" (or "rcopy" on unix). If this file is present, and the current file to be replicated exceeds a particular size, Tivoli Continuous Data Protection for Files will invoke this program to perform the file copy. (Typically, the processing logic to calculate and determine the changed-blocks is very CPU intensive on both end points and it is probably not worth the overhead of launching a separate and intensive program for files under a certain threshold size).

There are three parameters passed to this program: file-to-be-copied, target, and backup-file-name. The third parameter, the backup-file-name (if present), instructs the data mover to rename any existing file at the target to this name (presumably to version that instance).

Tivoli Continuous Data Protection for Files provides a sample script, rcopy.js.example, that shows one way to invoke rsync (assuming rsync is available on both the source and target).

Tivoli Continuous Data Protection for Files will interrogate the presence of the rcopy.js just one time, when it first starts. You may need to reboot or re-activate the Tivoli Continuous Data Protection for Files daemon if you change the disposition of this file.

The Tivoli Continuous Data Protection for Files parameter that controls the minimum size for this to be activated is "ExternalCopyMinimum" and can be set by the following:

fpa config-set ExternalCopyMinimum="1000000"

Typically values below a few hundred kilobytes are not worth the overhead of launching the external program. Certainly files larger can benefit greatly.

LAN-Free backup

Tivoli Continuous Data Protection for Files will work with a variety of LAN-free networking solutions such as SANergy®. Products like SANergy transparently move data to a file server directly over SAN channels rather than the slower LAN ones. If you have the requisite software installed (on both client and server) it should work correctly with Tivoli Continuous Data Protection for Files.

SnapShots, open files, and application quiescing

The "scheduled" backup capability in Tivoli Continuous Data Protection for Files allows for support of SnapShots, Open Files, and Quiescing. When a scheduled backup is about to start, Tivoli Continuous Data Protection for Files will look for and launch a customer-provided script in the install directory named either "synchronizer.js" or "synchronizer.bat" (or "sychronizer" on Unix) and passes it a single parameter, "starting". This is the opportunity for the user to call special functions to quiesce their system and applications. When the backup is finished, Tivoli Continuous Data Protection for Files will call the same program with "finished" as the parameter.

Many platforms today support some sort of "SnapShot" capability (either through software at the volume level or hardware externally). Tivoli Continuous Data Protection for Files can exploit SnapShots which greatly increases the coherency and accuracy of a data protection operation. Tivoli Continuous Data Protection for Files provides a "synchronizer.js" script for Windows that attempts to create volume snapshots of all the local hard drives (if it can not, perhaps because the version of Windows does not support snapshotting, then the script does nothing). For any snapshots that are created, Tivoli Continuous Data Protection for Files has to know of the association of the old (source) mount point and the new snapshot-view one. There is a special "fpa" command for setting this association:

fpa "<SnapShotSubstituteList list="s1|d1||s2|d2…"/>

The syntax for "list" is pairs of source-and-targets where the source and target are separated by vertical bars and double-bars between entries.

When Tivoli Continuous Data Protection for Files performs the scheduled backup, for each source file in its change journal, it will first perform any substitutions per this substitution list. Thus, the "synchronizer" script/program needs to inject this information per use of the "fpa" command above. The supplied "synchronizer.js" does the proper injecting.

The purpose of calling the "synchronizer" program at the completion is to allow the user to unfreeze any applications or reclaim snapshot resources. The provided "synchronizer" program will delete any snapshots it created.

Open files. Typically, Tivoli Continuous Data Protection for Files "journals" (records that a file has changed) when a file has been written and *closed.* Thus, files that are held open would not have an entry in the Tivoli Continuous Data Protection for Files journal log. Prior to the start of a scheduled backup, Tivoli Continuous Data Protection for Files will flush-out any such files so that they in fact have an entry in the change journal. Tivoli Continuous Data Protection for Files is able to access the contents of files, even if they are held open; HOWEVER, Tivoli Continuous Data Protection for Files can not assure coherency of a file that is still in use by an application.

System directories and registry backup and recovery

By default, Tivoli Continuous Data Protection for Files excludes backing up the "\Windows" and "\Program Files" directories. You can remove those from the exclusion list and then the contents will get backed-up. However, much of the material in those directories is not desirable to back up. The recommended suggestion is:

- Leave the exclusion list excluding those system areas.
- Periodically make a copy of those directories yourself to some location, preferably after installing new programs or drivers and once you believe the system to be stable (typically this is as infrequent as once or twice a year).
- Backup the "registry" and system object using the built-in Windows utility "ntbackup". Typically this is found in "Start Programs -> Accessories -> System Tools -> Backup" but can also be invoked on the command line as follows:

  >> ntbackup backup systemstate /f c:\MySystemState.bck

If you have to completely restore your system (perhaps after physical loss, disk loss, or damage), the recommended steps are:

- Get your system bootable (recovery disk, new Windows installation, Windows recovery installation, etc).
- Copy the saved "\Windows" and "\Program Files" trees that you created above.
- Use ntbackup to restore the systemstate object you created above.

Non-privileged users

Tivoli Continuous Data Protection for Files will work correctly for users with limited privileges (that is, users with administration rights). However, it requires administrations rights to *install* the software (as there are driver components and registry updates). Additionally, it is quite likely that the install directory tree will need its permissions opened up to wider access (this all depends on your default configuration). Use caution when making any directory more accessible. If you do believe you need to have the install tree opened for complete access by any user, you can a command similar to this:

>> cacls "c:\program files*installDir*" /T /G users:F

The "/T" means do the specified directory and all of its sub-directories.
The "/G" means "grant the following users the specified privilege" and the "F" means full access.

Appendix: Frequently Asked Questions

Include / Exclude and File Lists

Which has higher precedence, Include or Exclude?
Excludes are processed first

How do I include some parts of a directory but not others?
This "workstation" version is designed to be extremely simplistic to use and thus such capabilities are not exposed. The underlying architecture supports very complex selection/exclusion abilities. A future version might allow for more complex include/exclude capabilities.

Why is there a file list for both the continuous and the scheduled panels?
Most people want different protection for different types of files. While you *could* protect all your changing files with continuous protection, it is probably more sensible to only protect the most important files (files that you change and save directly). So the continuous file protection file list is likely a sub-set of the scheduled protection.

Should my scheduled protection file list include the same files as my continuous protection list?
Yes, in most cases. Even if you have elected to have "remote protection" on your continuous panel, you will probably want to re-capture those files on the scheduled screen as the scheduled protection will make versioned instances on the remote (and the continuous feature will *not*).

Replication Features

Does Tivoli Continuous Data Protection for Files do sub-file copying?
No. It's currently disabled, and a new method is forthcoming. (You can also use an external data mover such as rsync; see the User's Guide for details).

Is the data encrypted in-flight and/or on-target?
No, but you can use off-the-shelf tools and layers such as VPN's or Windows encryption as desired.

Is my data put into some sort of proprietary format that I need a tool to decompose or for recovery?
No. Your data is stored as ordinary files exactly like the originals. You can navigate to the folders yourself to restore a file or use the interface provided.

Does this add a lot of overhead to my system?
No. Our overhead only occurs when files are "saved" and statistically that is a very small percent of the overall operation of your system. Plus, our overhead (for continuous protection) is simply an additional "file copy", tantamount to you hitting Control-S twice in a row in your application.

File Versions

How many versions will it store?
On the local cache, 20, and this number can be changed/increased by a special command (see the User's Guide). On remote, we don't limit versions per-file (yet) and so its strictly by total pool space.

How do I know what files have been backed-up?
The History panel shows you the most recent 100 or so transactions.

Where are my files stored?
Your files are stored in a directory structure that mirrors their original location. There is a sub-directory named RealTimeBackup created on one of your local disks (if you've selected local protection) and similarly on the remote file server. You can navigate through those trees using Explorer or other tools. For the local/pool files, they are stored in their original format but have a unique-identifier added to their name so that several can be stored simultaneously. You can copy or move those files if you do not want to use the built-in Restore capability. If you do so, you probably want to change the filename back to a normal style.

Why do my backed-up files have funny names?
In the local save pool area Tivoli Continuous Data Protection for Files adds a unique tail to each file it copies so that several of the same name can be stored (for separate versions). Those funny numbers are a sort of timestamp and thus when sorted are in creation-order. When you use the built-in restore capability, Tivoli Continuous Data Protection for Files automatically removes the special part of the name.

Can I do some hand-pruning of the local version pool?
I would like to get rid of some large and unneeded files in the local version pool. Is that okay?
Yes, that is okay. The space will be immediately available for Tivoli Continuous Data Protection for files to use and the only impact will be that the file can not be restored from the local storage.
Probably need to clarify that if the filename pattern is not excluded it will be recopied after the next change.

Can I hand-prune the remote version pool?
Yes, but we wont realize that those files have been removed until we attempt to delete them ourselves. (Thus, they're contribution to the current pool size will be unchanged until we attempt to delete them and thus could cause a pool-purge event sooner than expected).

Tivoli Storage Manager (TSM) Questions

How do I use the TSM feature?
TSM is IBM/Tivoli's Enterprise class backup product. If you system already has the TSM "client" code loaded, Tivoli Continuous Data Protection for Files can exploit the TSM agent and send changed files directly to a remote TSM server for even higher protection.

How do I restore from TSM?
If you have TSM installed and have activated Tivoli Continuous Data Protection for Files to push data into TSM, you can retrieve that data using the normal TSM Client GUI. Currently, Tivoli Continuous Data Protection for Files does not provide an interface for restoring from TSM but a future version might.

Network Questions

If I change my remote target while not on the network and there are already files pending to the old one, what happens?
An attempt is made to send the pending ones to the new target.

What if I'm not always connected to a network?

Tivoli Continuous Data Protection for Files will queue-up the list of files that need to be moved to either the remote file server and/or the TSM server. Once you are reconnected, it will automatically send the most current version of the file(s) to the save area.

Removable Disk questions

Can I use a removable disk instead of a network target?

Yes. Be sure to have it hooked-up and available when you do your configuration and hit 'save' (or, visit the configuration panel later and hit 'save' again). At 'save' time we plant a signature on the disk so that we wont mistakenly send data into another removable device (such as your digital camera) when it is plugged-in instead.

I want to use a removable disk but not on a schedule.

Set the schedule to monthly (or longer) and whenever you desire to sync-up with your removable device simply plug it in and press the "send now" button on the status page.

Miscellaneous

I *really* want to stop Tivoli Continuous Data Protection from doing its thing for a while, but I don't want to uninstall.

Kill "filepathsrv" from task manager; no accumulation or monitoring will take place. Then simply log-out and log-in to have to start again.
I want to see more history than the status screen shows.
Examine the file 'replication.log' file for the last 1.3MB's of transactions.

If I save a large document 20 times while on an airplane, will it attempt to move 20 copies to my remote target when I reconnect?

No; only the most recently copy will move to the network.

What is this thing called FilePath?

The underlying technology of Tivoli Continuous Data Protection for Files is called FilePath. FilePath is real-time file system filter driver that wraps around any file system on any platform and extends the basicvfeatures of that file system.

What is fp?

"fp" is shorthand for FilePath. Some internal components are called "fp" and/or use "fp" as a prefix.

What about protecting databases and business applications?

The typical disk-to-disk approach for such applications is to use real-time synchronous or asynchronous replication. This Workstation version makes copies (or replications) of files when they are "closed" which is not ideal for database applications. Another version exists that has sync/async replication specifically for databases and higher business applications that typically run on servers. If demand exists, that version may be released as well.

Will this work with SANergy or similar software for LAN-free backup?

Yes. What is SANergy? SANergy allows LAN network connections to move the data payload over an overlaid SAN fabric if present, thus achieving very high data transfer rates.

I want to install a new rev. Do I have to uninstall?

No. You can "over install" and all of your data and configuration will be preserved.

If I uninstall will all my data be removed?

No. It is all left where it last was. As long as you do not remove the install directory (which contains special bookkeeping databases) you should be able to re-install later and the system will remember your settings and data.

Notices

This information was developed for products and services that are offered in the U.S.A.

IBM may not offer the products, services, or features that are 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 to cover subject matter that is described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the following address:

BM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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.

Trademarks

The following terms are trademarks or registered trademarks of Tivoli Systems Inc. and the IBM Corporation in the United States, or other countries, or both:

AIX	SANergy
IBM	SP2
PowerPC	FilePath
Redbooks	Tivoli

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Netscape, Netscape Navigator, and Netscape Communicator are trademarks or registered trademarks of the Netscape Communications Corporation in the United States and other countries.

Pentium is a trademark of Intel Corporation in the United States, other countries, or both.

Sun, Solaris, Java(TM), and all Java-based trademarks, and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of the Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.