



ADMINISTRATION GUIDE

Cisco Small Business
Version 3.1
Continuous Data Protection for Files



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

About This Guide	vi
Chapter 1: Product Overview	1
Introducing Continuous Data Protection for Files	1
Types of Protection	3
Enhancements for Version 3.1	5
Chapter 2: Installing Continuous Data Protection for Files	7
Basic Installation	7
System Requirements	7
Install Continuous Data Protection for Files	8
Initial Configuration Wizard	13
Uninstalling Continuous Data Protection for Files	28
Advanced Installation	28
Installing the Product Silently on a Single Local Computer	29
Pushing the Product to Other Computers	33
Providing a Configuration File for the Product	36
Chapter 3: Changing Protection Settings	38
Settings Notebook	38
General	40
Files to Protect	43
Folders and Files	43
Applications	50
Vault	52
E-mail Protection	56
Remote Storage	58
Advanced	63
Changing Protection Settings Tasks	68

Specify Which Files and Applications are Protected	69
Specify Which Files and Applications are Continuously Protected	69
Specify Which Files and Applications are Protected on a Schedule	71
Specify Which E-mail Applications are Protected	73
Specify Which Files and Applications are Vaulted	74
Specify the Period for Scheduled Protection	75
Specify Storage for Backup Copies	76
Specify the Remote Storage Area for Backup Copies	77
Force a Backup	78
Backup All Protected Files	79
Force a Scheduled Backup	80
Stopping a Backup or Restore Activity	81

Chapter 4: Monitoring Your Protection **84**

Popup Messages	84
Continuous Data Protection for Files Icon in the System Tray	85
Monitoring Protection with the User Interface	85
Continuous Data Protection for Files Status Page	85
Continuous Protection Activity Report	86
Scheduled Backup Report	88
Status Page	88
Menu Links	89
Graphic Icons	89
My Files	90
Status Panel	92
View Continuous Protection Activity Report	92
View Report of Scheduled Backups	93

Chapter 5: Restoring Files	94
Restore Wizard	95
Welcome	96
Files to Restore	97
Restore Location	100
Restore Data To	100
Summary	101
Chapter 6: Storage Areas	102
Format of Backup Copies	102
Versioning of Backup Copies	103
Modifying Backup Copies	104
Chapter 7: Central Management Considerations	105
Configuring Manageable Clients	105
An Example Configuration	106
Managing a Group	108
Managing a Single Client in a Group	110
Managing Clients Using Native File System Tools	111
Administration Folders	112
Example of Administration Subfolder Names	113
Central Administration Settings Window	114
Publishing a Configuration Template	114
Using the Backup Reports Table	116
Chapter 8: Protecting a Server	117
Managing a Server That Stores Backup Files	117
Run Continuous Data Protection for Files as a Service	117

Chapter 9: Problem Determination Guide	119
Files Are Not Backed Up	119
Storage for Backup Copies Has Not Been Correctly Specified	119
Files to Protect are Incorrectly Specified	119
Files are not Backed Up to IBM Tivoli Storage Manager Server	120
User Interface Contains No File Data	123
Restart Continuous Data Protection for Files Daemon	124
The Number of Backup Copy Versions is Greater than Configured	124

About This Guide

Purpose

This guide describes the concepts and tasks necessary to protect your files using the Continuous Data Protection for Files software solution.

Organization

This table describes the contents of each chapter in this document.

Chapter	Title	Description
Chapter 1	Product Overview	Introduces Continuous Data Protection for Files and briefly describes enhancements for this version
Chapter 2	Installing Continuous Data Protection for Files	Describes how to install and configure Continuous Data Protection for Files
Chapter 3	Changing Protection Settings	Describes how to change protection settings
Chapter 4	Monitoring Your Protection	Describes how to monitor file data protection
Chapter 5	Restoring Files	Describes how to restore files
Chapter 6	Storage Areas	Describes how to access backup copies

Chapter	Title	Description
Chapter 7	Central Management Considerations	Describes concepts, examples, and steps for centrally managing Continuous Data Protection for Files clients
Chapter 8	Protecting a Server	Describes issues you need to consider to protect a server
Chapter 9	Problem Determination Guide	Lists some common problems and suggests possible solutions.

Document Style Conventions

The following style conventions are used in this document.

- **Menus, Tabs, and Buttons:** Bold type is used to indicate the name of a button, menu, or tab in an application.

Example: Click **Submit All Changes** to save your entries.

- **Screens, Page Areas, and Fields:** Italic type is used to indicate the name of screens, page areas, and fields.

Example: Scroll down to the *PBX Parameters* area of the screen.

- **Data Input:** The `courier` font is used to indicate characters that you should type into a field exactly as printed in this guide.

Example: In the *Mailbox Subscribe Expires* field, type 30.

In this example, you would type the number 30 in the field.

- **Parameters:** Angle brackets and italic type indicate parameters that you must replace with the appropriate data.

Example: Type `800@<IP address of device>:5090`

In this example, you would type the characters 800@, followed by the IP address of your device, followed by a colon and the number 5090.

Finding Information in Your PDF Documents

The PDF Find/Search tool lets you find information quickly and easily online. You can:

- Search an individual PDF
- Search multiple PDFs at once (for example, all PDFs in a specific folder or disk drive)
- Perform advanced searches

Finding Text in a PDF

By default, the Find toolbar is open. If it has been closed, choose **Edit > Find**.

Use Find to search for text in an open PDF:

-
- STEP 1** Enter your search terms in the *Find* box on the toolbar.
- STEP 2** Optionally click the arrow next to the Find text box to refine your search (such as Whole words only).
- STEP 3** Press **Enter**. Acrobat jumps to the first instance of the search term. Pressing **Enter** again continues to more instances of the term.
-

Finding Text in Multiple PDFs

The *Search* window lets you search for terms in multiple PDFs. The PDFs do not need to be open. Either:

- Choose **Edit > Search**
or
- Click the arrow next to the *Find* box and choose Open Full Acrobat Search. The *Search* window appears.

In the *Search* window:

-
- STEP 1** Enter the text you want to find.
 - STEP 2** Choose **All PDF Documents** in.
 - STEP 3** From the drop-down box, choose **Browse for Location**.
 - STEP 4** Choose the location you want to search, either on your computer or on a network, then click **OK**.
 - STEP 5** If you want to specify additional search criteria, click **Advanced Search Options**, and choose the options you want.
 - STEP 6** Click **Search**.
-

For more information about the Find and Search functions, see the Adobe Acrobat online help.

Additional Information

Regulatory Compliance and Safety Information

Regulatory Compliance and Safety Information (RCSI) for this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

Warranty

Warranty information that applies to this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

End User License Agreement (EULA)

Licensing information that applies to this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

Product Overview

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

Introducing Continuous Data Protection for Files

Continuous Data Protection for Files is a flexible, easy to use file protection software system.

Using this system, you can provide continuous protection for your most important files and protect the less important files at scheduled intervals to save time and storage space.

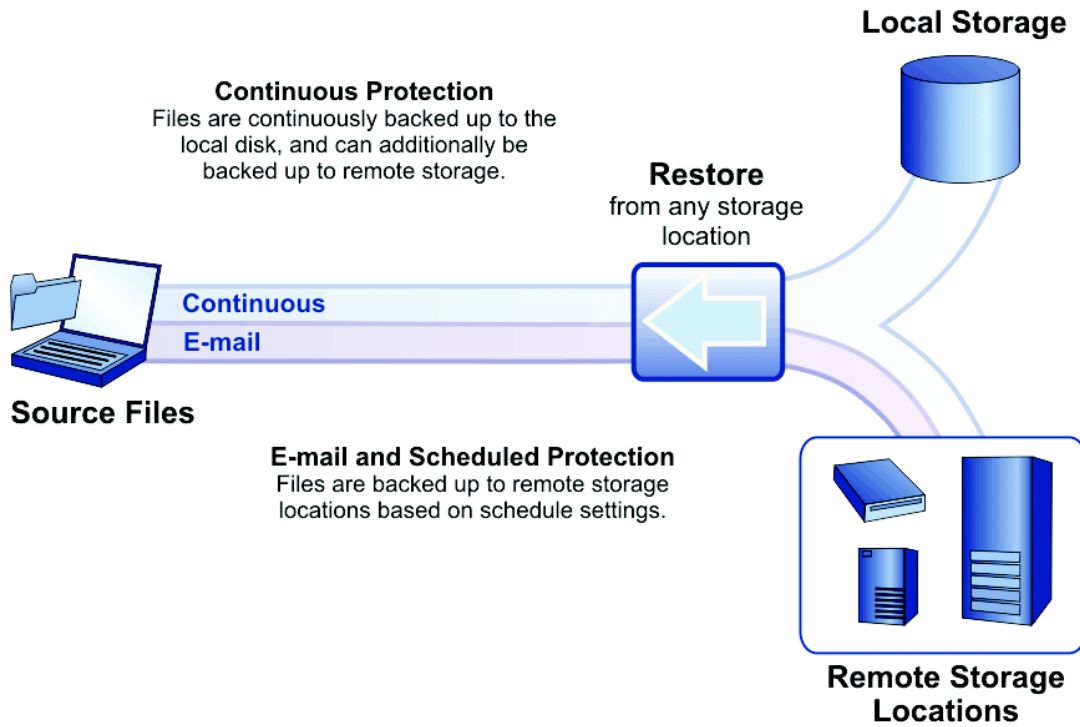
Continuously protected files are backed up to a local drive, ensuring that backup copies are created even when network conditions prevent storage on remote locations. Continuously protected backup copies can also be stored on remote storage locations, when network connections allow.

If a remote location is not available when you change a continuously protected file, Continuous Data Protection for Files makes a backup copy on the remote device as soon as it becomes available.

Scheduled backup copies are created at specified intervals (hourly, weekly, daily, or monthly). If a remote device a scheduled backup is not available, Continuous Data Protection for Files stores the backup file to the remote device as soon as it becomes available.

The following diagram provides an overview of Continuous Data Protection for Files.

Figure 1 Overview of Continuous Data Protection for Files



After installation, Continuous Data Protection for Files immediately provides continuous protection for a pre-configured list of files. You can see the backup copies in the \RealTimeBackup\ folder in the root of your primary drive, and in the list of files that you can restore via the Restore Wizard (see [“Restore Wizard,” on page 95](#)). The default space allocated for your backup copies is **500 MB**.

You can configure other lists of files to protect, other storage areas, scheduled protection, and other protection options, using the Continuous Data Protection for Files user interface (see [“Settings Notebook,” on page 38](#)).

Types of Protection

Continuous Data Protection for files offers three types of protection:

- Continuous Protection** Every time a file is saved, a backup copy is created. The backup copy exactly matches the original file as you last saved it. If you choose to save more than one version of a backup copy, the previous backup copies will match the previous versions of your file.
- Scheduled Protection** Files are backed up at specified intervals (hourly, daily, weekly, or monthly). The files are not backed up every time you save them as are continuously protected files. Hence, scheduled protection yields fewer backup copies. If a file is lost between the time it is saved and the time it is backed up, you will be able to restore only a previous version of the file.

E-mail files can be protected only on a schedule, not continuously.

If the storage area is unavailable when a protected file is saved, Continuous Data Protection for files will maintain an internal copy, and will create the backup copy on the remote storage area when the storage area becomes available.

- Vaulted** Vaulted files and folders cannot be modified or deleted, so this option should only be used for files that you do not want changed or deleted. Vaulted files are not backed up.

The attributes of each type of protection are compared in the following table:

Attribute	Continuous Protection	Scheduled Protection (includes e-mail)	Vaulting
Recommended for what files	Recommended for your most important files. Not recommended for large dynamic files like e-mail files.	Recommended for large, dynamic files like e-mail.	Recommended for files that you want to prevent being modified or deleted.

Attribute	Continuous Protection	Scheduled Protection (includes e-mail)	Vaulting
How protected	Backup copies are created on specified storage areas.	Backup copies are created on a single storage area.	Vaulted files and folders cannot be modified nor deleted.
Frequency of backups	File is backed up whenever it is saved.	File is backed up only at the scheduled time, and only if it has been saved since the previous schedule.	No backups
Backup copy storage area	Local or remote	Remote only	Not applicable
Files protected	Files selected in the Folders and Files box and the Applications box of the Files to Protect page of the Settings Notebook.	Files selected in the E-mail Protection page of the Settings Notebook. Files selected in the Folders and Files dialog of the Advanced page of the Settings Notebook.	Files selected in the Vault box of the Files to Protect page of the Settings Notebook.

Enhancements for Version 3.1

Continuous Data Protection for Files is updated this release with the following enhancements:

Updated Interface Information is reorganized to provide the right information when you need it. The Status window provides summary information about your protection, and quick links to help you do the following tasks:

- Monitor details about protection activity on your computer or computers that you administer
- Investigate potential problems
- Change your protection settings
- Restore protected files

Configuration and Restore Wizards These wizards greatly simplify two common tasks:

- **Configuration Wizard** When you initially install Continuous Data Protection for Files, a wizard guides you to configure the protection that meets your needs. You initiate protection quickly and easily.
- **Restore Wizard** When you want to restore a file, a wizard helps you choose the version of the file you want, and allows you to choose where to restore it.

Enhanced integration with IBM Lotus Notes® e-mail client Continuous Data Protection for Files works closely with IBM Lotus Notes e-mail client to efficiently provide protection for your email files. This protection allows you to easily restore your e-mail files in the event they are lost or damaged.

Versioning of data level changes for e-mail files Continuous Data Protection for Files tracks data level changes on e-mail files. This allows you to restore local copies of your IBM Lotus Notes and Microsoft® Outlook files from the point in time of your choosing.

MSI installation package Continuous Data Protection for Files has a Microsoft System Installer (MSI) installation package and uses Windows® Installer. You can use Microsoft Systems Management Server to deploy Continuous Data Protection for Files MSI package to computers that you administer.

Microsoft Vista operating system support Continuous Data Protection for Files is supported on 32-bit Windows Vista (Basic, Home Premium, Business, Ultimate, and Enterprise editions) and the following operating systems:

-
- 32-bit Windows 2000 Server, Advanced Server, SP2 and up (x86-32)
 - 32-bit Windows XP Professional, SP1 and up (x86-32)
 - 32-bit Windows 2003 Server–Standard Edition and Enterprise Edition (x86-32)

Installing Continuous Data Protection for Files

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

Basic Installation

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

For installation to a remote computer, installation without user interaction (silent), or installation for multiple computers, see [“Advanced Installation,” on page 28](#).

System Requirements

Continuous Data Protection for Files requires a Windows server or workstation with specific hardware and software.

Hardware

Minimum hardware is an Intel® Pentium® III machine with the following specifications:

- 500 MHz CPU
- 384 MB RAM
- 21 MB of available disk space for install footprint, additional space to store local backup copies



NOTE You must configure as much space as is needed to store at least one backup copy of every file that you protect. See [“Maximum Space for Backups,” on page 41](#).

The hardware configuration must also support the Windows operating system, as specified by Microsoft.

Software

The following Windows operating systems are supported:

- 32-bit Windows 2000 Server, Advanced Server, SP2 and up (x86-32)
- 32-bit Windows XP Professional, SP1 and up (x86-32)
- 32-bit Windows 2003 Server–Standard Edition and Enterprise Edition (x86-32)
- 32-bit Windows Vista (Basic, Home Premium, Business, Ultimate, and Enterprise editions)

The Continuous Data Protection for Files user interface supports the following browsers:

- Internet Explorer, Version 6.0 and above
- Mozilla Firefox 1.5.0.7 and above

Continuous Data Protection for Files supports IBM Tivoli Storage Manager server version 5.3.3 and higher.

Install Continuous Data Protection for Files

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

This section describes interactive installation on a single computer and configuration using a wizard. To do a silent installation (without user interaction) and to push Continuous Data Protection for Files to other computers, see [“Advanced Installation,” on page 28](#).

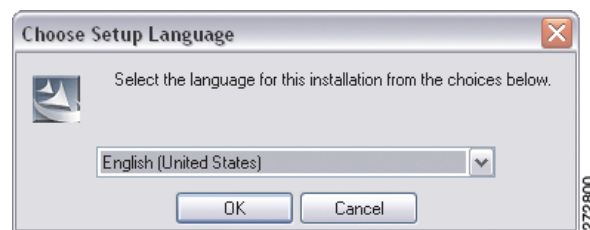
If you are upgrading from a previous version, see “[Considerations for Upgrading Continuous Data Protection for Files](#),” on page 32.

- You must have administrative rights to install Continuous Data Protection for Files.
- Your computer must have the necessary hardware and software. See “[System Requirements](#),” on page 7.
- If you are reinstalling or upgrading from a previous version of Continuous Data Protection for Files, close all other applications (especially e-mail programs) before you install. You must reboot immediately after the installation is complete.

Follow the steps below to interactively install on a single computer.

STEP 1 Insert the CD-ROM. The installer should launch automatically. The *Choose Setup Language* window appears. Select the appropriate language and click **OK**.

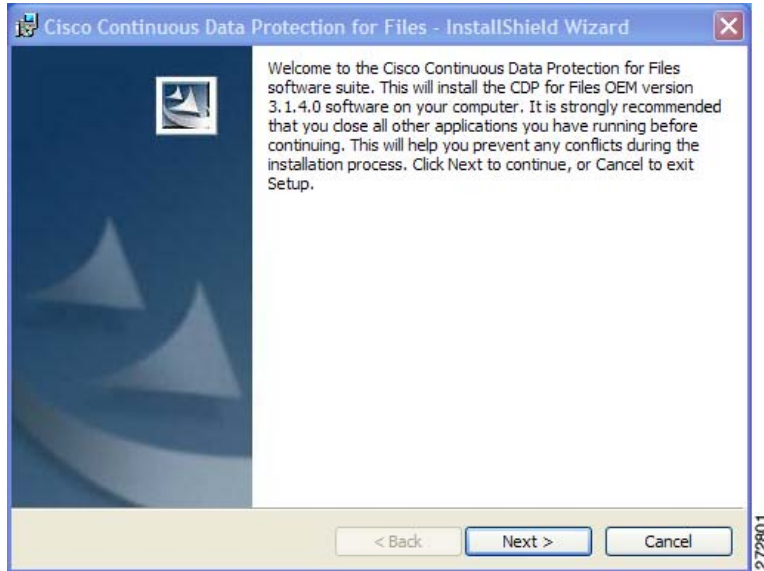
Figure 2 Choose Setup Language



NOTE If the CD-ROM doesn't start automatically, go to **My Computer**. Double-click the **CD drive**. Double-click the .exe file:
Cisco_CDP_<version_number>.exe.

STEP 2 When the InstallShield Wizard starts; click **Next**.

Figure 3 InstallShield Wizard



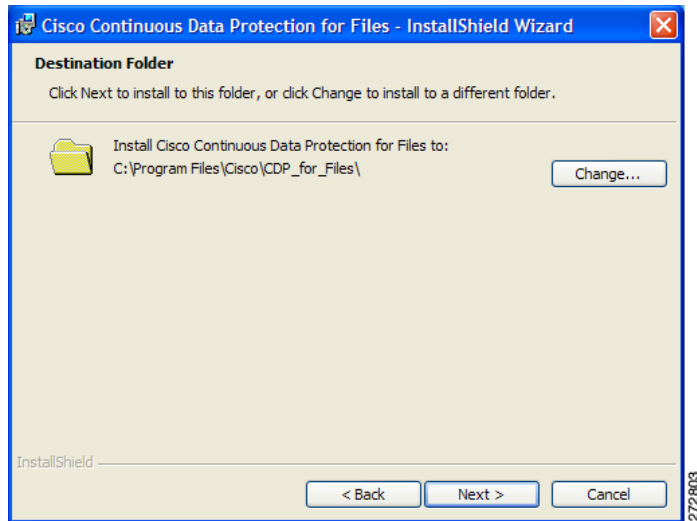
STEP 3 Read the Software License Agreement. If you accept the terms of the agreement, select **I accept the terms in the license agreement**, and click **Next**.

Figure 4 Software License Agreement



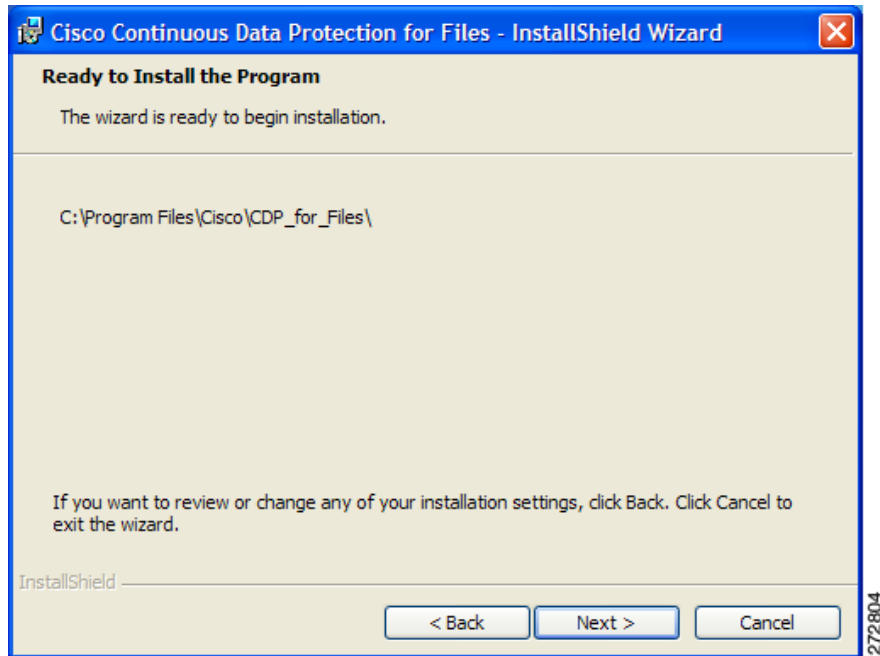
STEP 4 Accept the default install location, or click **Change** to specify another location. The default installation location is recommended. Click **Next**.

Figure 5 Destination Folder



STEP 5 Confirm that the information is correct and click **Next**.

Figure 6 Ready to install Program



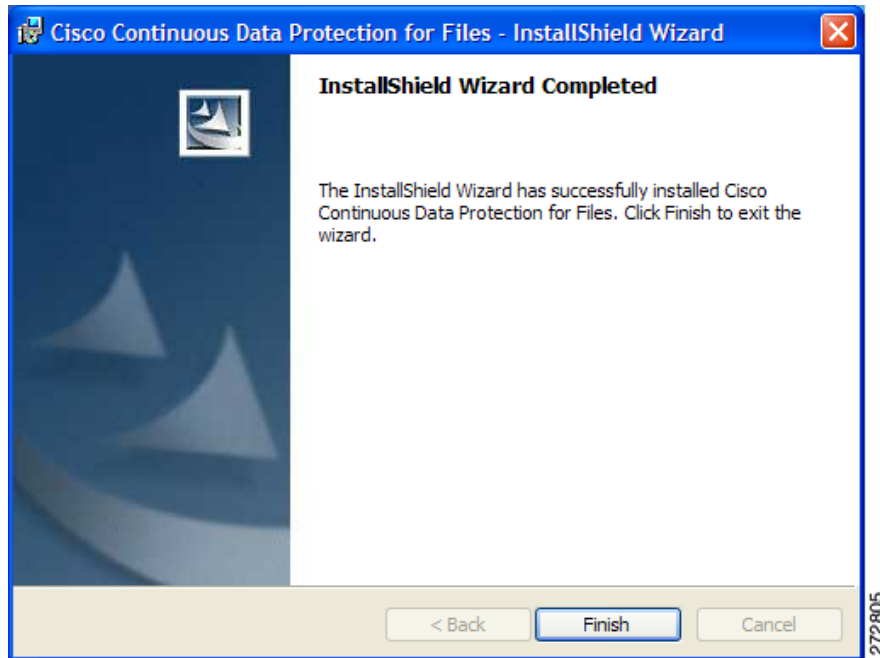
The installation window displays a progress bar indicating that the necessary files are being installed on your computer. You may also see a command prompt window as the installer runs several scripts.

If you are installing on Windows Vista, and there is an existing Continuous Data Protection for Files client, the *Files in Use* window appears. Click **OK**. A warning also appears informing you that setup was unable to automatically close all requested applications. Click **OK**.

If this is your first installation of Continuous Data Protection for Files on this computer, a configuration wizard helps you choose your protection settings. See [“Initial Configuration Wizard,” on page 13.](#)

STEP 6 Click **Finish** to complete the installation.

Figure 7 InstallShield Wizard Completed



The installer indicates that you must reboot in the following situations:

- You are reinstalling or upgrading Continuous Data Protection for Files.
- A product that uses the IBM Tivoli Storage Manager API is installed and running. The IBM Tivoli Storage Manager Backup-Archive client is such a product.

After installation (and reboot, if required), Continuous Data Protection for Files immediately starts protecting your files.

If you want to change your protection settings, see [“Settings Notebook,” on page 38.](#)

Initial Configuration Wizard

The first time you install the software, a wizard helps you choose your protection settings.

Use the navigation buttons at the bottom of each wizard page to navigate to all pages. When you have chosen all settings, click **Finish**.

If you cancel the wizard before finishing, any changes you made are cancelled. Continuous Data Protection for Files protects your files according to the configuration settings that were defined during installation. You can view and change your settings at a later time with the Settings Notebook.

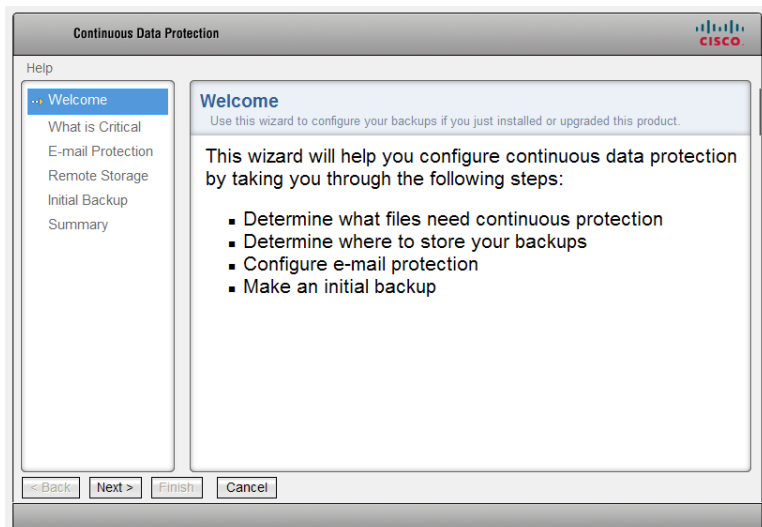
The wizard has six pages:

- Welcome
- What is Critical
- E-mail Protection
- Remote Storage
- Initial Backup
- Summary

Welcome

The *Welcome* page lists the steps to initially set your protection settings.

Figure 8 Welcome

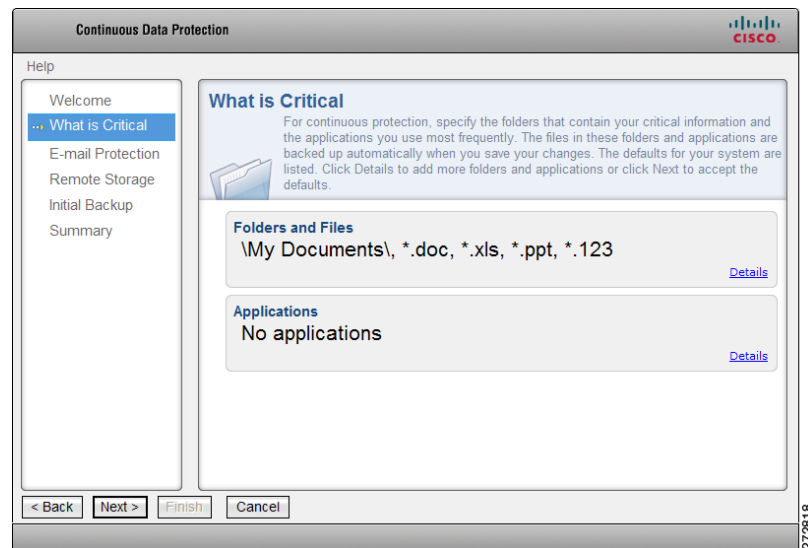


Click **Next** to advance to the next page of the wizard. Click **Cancel** to exit the wizard without changing the initial protection settings.

What is Critical

The *What is Critical* page is used to specify the files and folders that you want to protect. The specified files, folders and applications are continuously protected, which means Continuous Data Protection for Files creates backup copies on a storage area as soon as the files are changed.

Figure 9 What is Critical



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

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

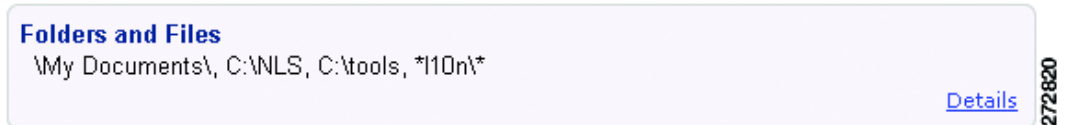
If you prefer viewing the file paths, names, and extensions that are protected, use the *Folders and Files* box. This option allows you to use a file tree to specify what to protect.

If you prefer viewing the applications that are protected, use the *Applications* box. This option allows you to specify applications from a list. Files that are created by the listed applications are protected. The file extensions associated with the application are automatically added to the Folders and Files list.



NOTE E-mail applications are specified in the *E-mail Protection* page. Because these files are often very large, their protection settings are configured separately.

Figure 10 Folders and Files box

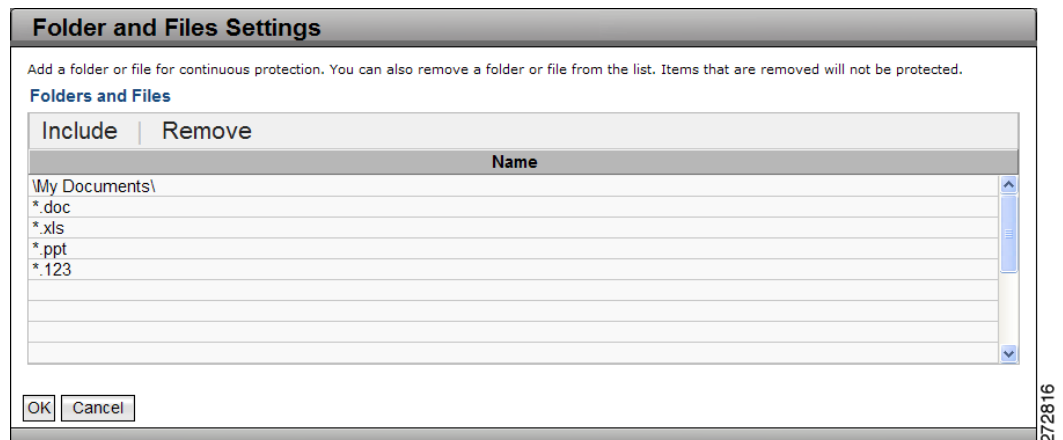


This box gives a summary of the folders and files that are continuously protected. The number of items protected refers to the items in the list of folders and files. A single list item can specify more than one file. Click the **Details** link to view all items in the list and modify the list. The *Folders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

Folders and Files Settings

Specify folders and files to protect by adding or removing items from the list.

Figure 11 List of Protect Folders and Files



The top of the list box has two menu buttons. Click the buttons to include or remove items from the list.

Include Click **Include** to add files and folders that you want to protect. The *Select folders* dialog appears.

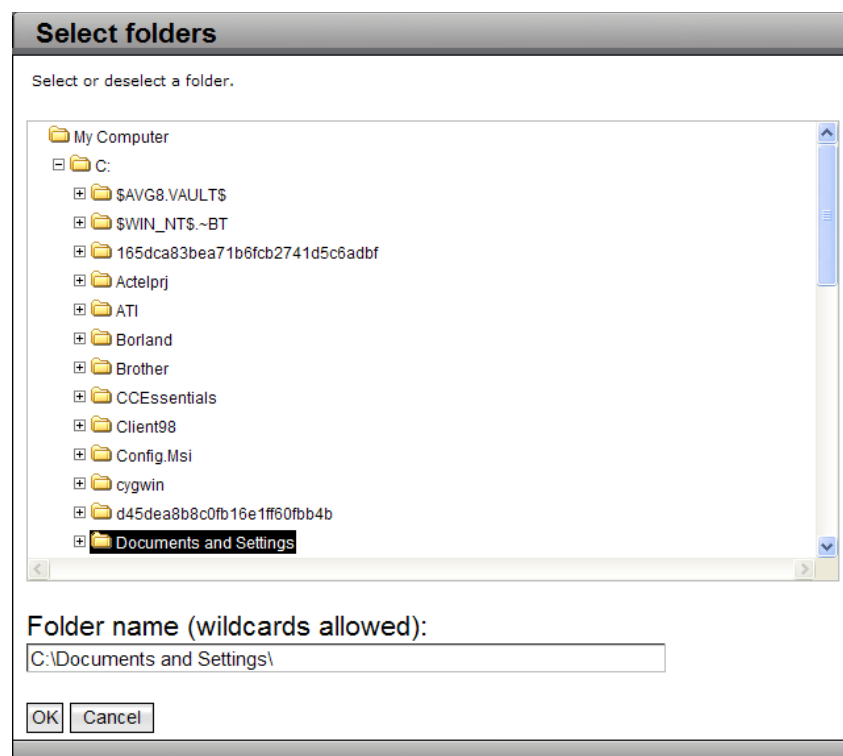
Remove Select one or more list items, then click **Remove** to remove those items.

Each row in the list has one column:

Name Patterns in the Name column specify one or more files or folders. See “[Interpreting File and Folder Patterns](#),” on [page 18](#) to determine what files and folders match a Name pattern with blanks or wildcards. When a folder is protected, all of its files and sub-folders are protected.

Select Folders

Figure 12 Select folders dialog



The *Select folders* dialog allows you to specify files and folders. You can browse to choose a folder, or type the name of a file or folder in the *Folder name* text field. If you browse and choose a file or folder, you can modify its path in the *Folder name* text field.



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

Interpreting File and Folder Patterns

Protection settings use patterns to specify what files and folders to protect. You can enter the complete path of a file that you want to protect.

For example, `C:\Documents and Settings\Administrator\My Documents\Soccer\2005AYSO\Parent Info U8B.doc`. The complete path unambiguously matches a single file. But to specify all files this way would be quite time-consuming. Use asterisks and blanks as wildcards in the pattern to specify several files. The files and folders that are protected depend on blanks before and after a pattern, and asterisks in the pattern.

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

If there are no asterisks in the pattern, then blank spaces before and after the pattern are interpreted as asterisks. Hence, `\myDocs\` and `*\myDocs*` yield the same matches. If there are asterisks in the pattern, then blank spaces before or after the pattern match no characters. Hence, `\myDir\`, `*\myDir\`, and `\myDir*` could yield three different matches, as in the table of examples below.

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

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

Examples of File and Folder Pattern Matches

Pattern	Matching Folders and Files
<code>\myDir\</code> or <code>\mYdiR\</code> or <code>*\myDir*</code> or <code>*\mydir*</code>	<code>c:\myDir\</code> <code>c:\myDir\Contacts\</code> <code>c:\myDir\Contacts\contacts.txt</code> <code>c:\Projects\myDir\</code> <code>c:\Projects\myDir\myThings\</code> <code>c:\Projects\myDir\myThings\things.doc</code> <code>c:\Projects\myDir\myThings\myPhoto.jpg</code> <code>d:\Notes\myDir\</code>
<code>*\myDir\</code>	<code>c:\myDir\</code> <code>c:\Projects\myDir\</code> <code>d:\Notes\myDir\</code>

Examples of File and Folder Pattern Matches (Continued)

Pattern	Matching Folders and Files
\myDir*	\myDir\ \myDir\Contacts\ \myDir\Contacts\contacts.txt \myDir\myThings\ \myDir\myThings\things.doc
d:*mydir*	d:\Notes\myDir\
\my best	c:\Books\My Best.doc c:\Photos.jpg\My Best Photo\ c:\Photos.jpg\My Best Photo\Best.jpg f:\Projects\My Best Project\ f:\Projects\My Best Project\Dream.xls
.jpg	c:\Photos.jpg\ c:\Photos.jpg\myHouse.bmp c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
*.jpg	c:\Photos.jpg\ c:\Photos.jpg\My Best Photo\Best.jpg c:\Projects\myDir\myThings\myPhoto.jpg
E:\ E:*	All files and folders on the E: drive.

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

Figure 13 Applications Box

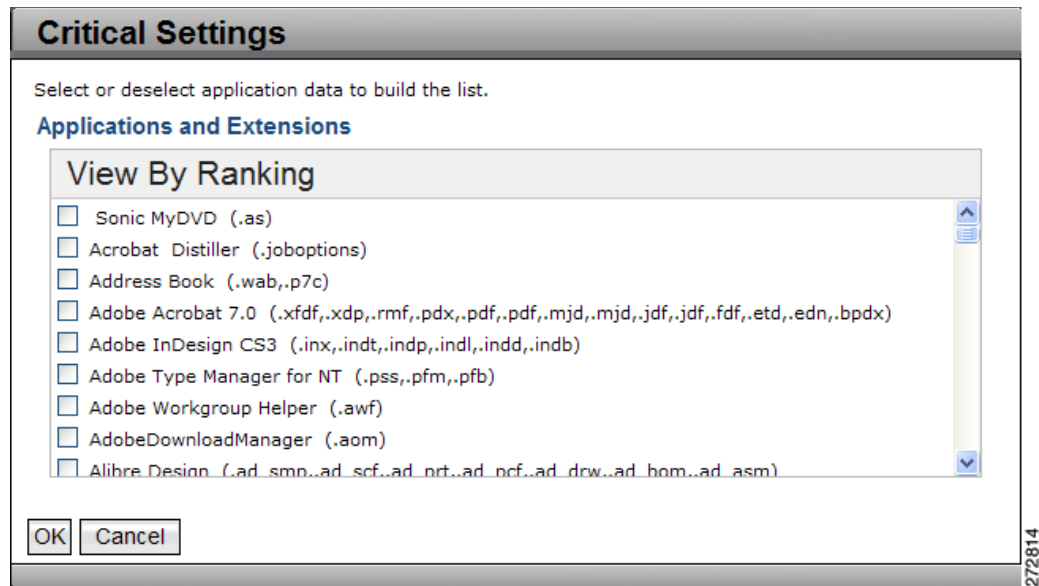
Applications
 Lotus Organizer, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Software DVD Player

[Details](#)

272810

To see the complete list of the applications that are protected, click **Details**. The *Critical Settings* window are displayed.

Figure 14 Critical Settings > Applications and Extensions



Specify a list of critical applications to protect.

The *Applications and Extensions* box presents a list of applications and their associated file extensions. Applications that are checked are continuously protected. You can check and uncheck applications to suit your protection needs.

The list of applications has two views. Each view orders the applications in a different way. Click the menu item at the top of the box to change the view.

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

View Alphabetically The applications are presented in alphabetical order.

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

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

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

You can add files to be protected in the *Critical Settings* dialog, but these applications are protected only if the files are not explicitly excluded. See [“Including and Excluding Files from Protection,” on page 45](#) for more information.

E-mail Protection

Select the e-mail applications that you want to protect. Select a schedule for protecting the e-mail applications.

Figure 15 E-Mail Protection



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

E-mail files are backed up only to remote storage. If the remote storage is not available at the scheduled backup time, Continuous Data Protection for Files queues the backup copies for later transmission. When the remote storage area becomes available, Continuous Data Protection for Files creates the backup copies on the remote storage area.

E-mail Application Select one of the popular e-mail applications in the list. If your application is not listed, select Other.

E-mail Application Data Folder If you choose your e-mail application from the E-mail Application list, the default file type for that application appears in this box, and you will not be able to update the file specification. You can update this field only if you select Other in the E-mail Application list.

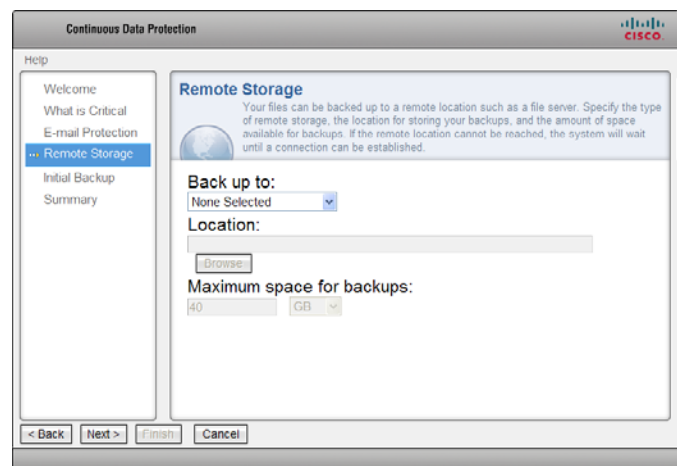
How often to protect your e-mail You can schedule e-mail protection at one of several intervals:

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

Remote Storage

Specify the remote storage location for the backups of your protected files.

Figure 16 Remote Storage



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

Back up to Specify the remote storage device type where your backup copies are stored. You can specify a file server or removable disk to store the backup copies. The remote device can be another computer (such as a NAS or file server), or a remote disk, or a removable disk.

Location Specify the location of your storage device. What you select from the *Back up to* list affects what you enter in the *Location* field.

- If you choose a remote server, it is recommended that you use Universal Naming Convention (UNC) specification for the file server instead of drive letters. Drive letters can change after rebooting and often do not reconnect automatically.
- If you choose a USB external device, you can select the driver letter. However, removable external device drive letters can change.

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

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

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

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

WebDAV Server

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

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

When using WebDAV, Continuous Data Protection for Files only supports the Basic Authentication method described in the HTTP 1.0 RFC. Because this authentication method sends the password as clear text over the network, it is also recommended that the Web server be configured to use secure sockets.

IBM Tivoli Storage Manager or IBM Tivoli Storage Manager Express

Continuous Data Protection for Files can store backup copies on an IBM Tivoli Storage Manager server. You do not need to install the IBM Tivoli Storage Manager backup-archive client. If you install the IBM Tivoli Storage Manager backup-archive client, it functions independently from Continuous Data Protection for Files.

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

You are prompted to enter a valid password for your IBM Tivoli Storage Manager server.

Continuous Data Protection for Files supports IBM Tivoli Storage Manager server version 5.3.3 or later.

Configure your IBM Tivoli Storage Manager server before trying to connect from Continuous Data Protection for Files. Register your computer as an IBM Tivoli Storage Manager node. Continuous Data Protection for Files uses the password assigned at registration to connect to the IBM Tivoli Storage Manager server. For more information about registering an IBM Tivoli Storage Manager node for your computer, see the *IBM Tivoli Storage Manager for Windows Administrator's Guide*.

In order to manage storage space, the IBM Tivoli Storage Manager administrator must grant authority to the IBM Tivoli Storage Manager client node to delete backup copies. For steps to assign authority to delete backup copies, see [“IBM Tivoli Storage Manager Client Node Lacks Authority to Delete Backup Copies,” on page 121](#).

To avoid problems when using the IBM Tivoli Storage Manager server, see [“Files are not Backed Up to IBM Tivoli Storage Manager Server,” on page 120](#).

You can restore backup copies from the IBM Tivoli Storage Manager server only with the Continuous Data Protection for Files GUI. You cannot use the IBM Tivoli Storage Manager Backup-Archive client to restore backup copies created by Continuous Data Protection for Files.

Maximum space for backups Specify how much space to use for all backup copies on remote storage.

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

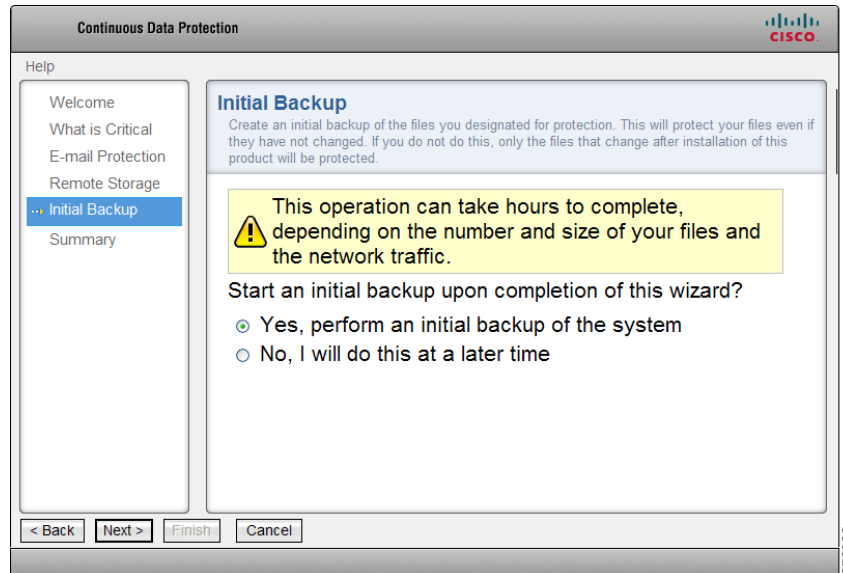
When the storage space becomes full, Continuous Data Protection for Files deletes older backup copies of files that have several backup copies. After deleting the versioned backup copies, if more space is needed for new backup copies, Continuous Data Protection for Files deletes the last remaining backup copies of enough files to make room for the newest backup copy.

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

Initial Backup

On the *Initial Backup* page, choose if you want to back up all your files when you finish the wizard.

Figure 17 Initial Backup



When you first install Continuous Data Protection for Files, it is highly recommended that you immediately back up all files that you configured for protection. Without the initial backup, only files that change are protected. The initial backup protects all of the existing files that you designated for protection.

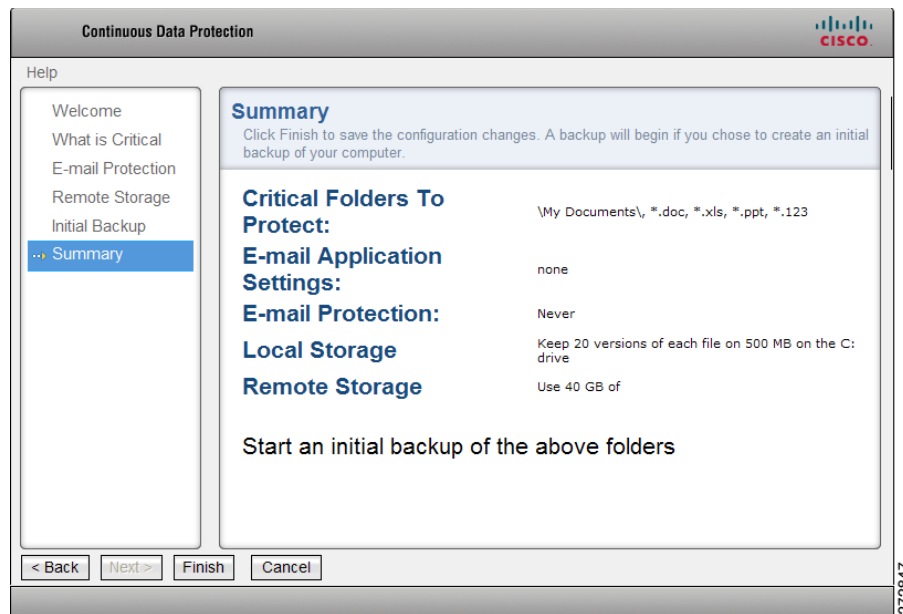
The initial backup scans all of your local drives for files that you designated for protection. All files that meet your specifications are backed up to the specified storage areas. This process can take a long time and can slow down your computer. Start this initial backup when you are not using your computer for other applications.

If you choose not to back up by the installation wizard, you can force a complete backup at a later time. At that time, use the *Files to Protect* page of the *Settings Notebook* ("**Files to Protect**," on page 43).

Summary

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

Figure 18 Summary



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

Choose **Finish** to apply your configuration choices. Continuous Data Protection for Files continues to run in the background and protect your files using the configuration choices you made.

Choose **Cancel** to exit the wizard without applying your configuration choices. Continuous Data Protection for Files continues to run in the background and protect your files using the pre-configured settings.

Uninstalling Continuous Data Protection for Files

Uninstall Continuous Data Protection for Files with the following steps.

-
- STEP 1** From the Windows *Start* menu, choose **Control Panel**.
 - STEP 2** Choose **Add or Remove Programs**. A list becomes populated with currently installed programs.
 - STEP 3** Scroll down and choose **Cisco Continuous Data Protection for Files**.
 - STEP 4** Click **Remove**.
 - STEP 5** Click **Yes** when prompted to confirm that you want to remove the product.
 - STEP 6** If you are uninstalling on Windows Vista, the *Files in Use* window appears. Click **OK**. You also see a warning that the setup was unable to automatically close all requested applications. Click **OK**.
 - STEP 7** A window confirming successful removal appears and prompts you to reboot now. Click **Yes** to reboot your system to remove file system filters.
 - STEP 8** Click **Finish** to exit the uninstall wizard.
-

Advanced Installation

“**Basic Installation,**” on page 7 describes an installation that requires user interaction, and installs Continuous Data Protection for Files on a single machine. There are more options for installing, upgrading, and re-configuring Continuous Data Protection for Files.

There are several ways to install or upgrade Continuous Data Protection for Files without user interaction.

Silent installation on a local computer You can install Continuous Data Protection for Files on your local computer silently without interacting with the installer wizard and the Continuous Data Protection for Files initial configuration wizard.

Silent product upgrades and configuration updates on a local or remote computer You can upgrade the product level and change protection settings on a local or remote computer silently. When you put a new product installer file or a new configuration file in the appropriate folder, Continuous Data Protection for Files pulls the information. Continuous Data Protection for Files adopts the new product level from the installer file or the new protection settings from the configuration file.

Silent installation pushed to a remote computer Using silent installation, an administrator can push Continuous Data Protection for Files to remote computers.

After Continuous Data Protection for Files is installed, it pulls product upgrades and configuration information. You can use this feature to upgrade your local Continuous Data Protection for Files client or Continuous Data Protection for Files on other computers.

Silent local upgrade You can upgrade the product level on your local computer by putting the upgraded installer in the appropriate folder. Continuous Data Protection for Files pulls in the new code. After a reboot, the product protects your files at the new level.

Silent installation pushed to another computer An administrator can push Continuous Data Protection for Files to other computers.

Installing the Product Silently on a Single Local Computer

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

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

- Invoke the installer with appropriate parameters.
- Optionally, you can provide a configuration file for the Continuous Data Protection for Files client. See **“Providing a Configuration File for the Product,” on page 36**. If you do not provide a configuration file, the initial configuration wizard does not start after installation.

Silent Installation Command

Invoke the installer for a silent installation. The installer is an executable file with a name like `Cisco_CDP_3.1.0.0.exe`. The installer name must include CDP and must be file type `.exe`. The version infix of the file name (3.1.0.0) can change from one version to the next.

For example:

`Cisco_CDP_3.1.0.0.exe /S "/v /qn options "`

There must be a blank space before each parameter. No space is allowed between `"` and `/v`.

Parameters

/S Install silently. Without this parameter, you install interactively via the installation wizard and (if necessary) the initial configuration wizard.

Options The following options are allowed:

- **INSTALLDIR=folder** The default installation folder is `C:\Program Files\Cisco\CDP_for_Files`. If you want to install to another folder, use this option and specify the folder.
- **REBOOT=ReallySuppress** Suppress system reboot after installation. This option is recommended when you are pushing installation to a remote computer (see [“FpPushInst.exe \(Push Install Command\),” on page 33](#)) because rebooting after installation could be disruptive to users on the remote system. This option is not recommended for a local installation when a previous version of Continuous Data Protection for Files exists.
- **/!*v log file path** Specify a file to log the installation activities.

Example: Install with Default Options

To install with default settings, including reboot after installation if Continuous Data Protection for Files was previously installed (this is recommended), use this syntax:

`Cisco_CDP_3.1.0.0.exe /S "/v /qn "`

Note that no blank space is permitted between the double-quote delimiter and the parameter `(/v)`.

Example: Install with Specific Options

To install to non-default folder (c:\newdir); and to log the installation activities to c:\temp\msi.log; and to suppress a reboot after installation, use this syntax:

```
Cisco_CDP_3.1.0.0.exe /S "/v /qn INSTALLDIR=c:\newdir /l*v c:\temp\msi.log REBOOT=ReallySuppress "
```

Upgrade Silently: Pull Upgrades and Configurations

After Continuous Data Protection for Files is installed, you can silently upgrade the product or silently change the configuration. Put an installer executable file or a configuration file in the appropriate folder and Continuous Data Protection for Files pulls the information.

Upgrade the Product Level

To upgrade the product, put a new installer in the downloads folder. For information on the downloads folder, see [“Administration Folders,” on page 112](#). Continuous Data Protection for Files pulls the new product code and prompts you to reboot the computer.

The new installer file name must contain the string CDP and end with .exe. For example, a typical name is **Cisco_CDP_3.1.1.0.exe**.

Continuous Data Protection for Files checks for new installer and configuration files every 10 to 20 minutes. If the date of an installer file is more recent than the file used for the current product level, Continuous Data Protection for Files adopts the new product level.

When Continuous Data Protection for Files detects a new installer file, a message pops up from the system tray indicating that a new version of the software is being installed.

When the installation is complete, a message pops up from the system tray indicating that the new software has been loaded, and you must reboot to resume data protection.

Between the time that Continuous Data Protection for Files pulls the upgrade and until the computer is rebooted, Continuous Data Protection for Files stops protecting your files.

After the reboot, Continuous Data Protection for Files continues protecting your files. Your protection settings are the same as in the previous version of the product.



NOTE Until you reboot, Continuous Data Protection for Files does not back up any file. You do not lose any existing backup copies, but any changes you make are not protected. If there is a long delay between install and reboot, consider forcing a backup of all protected files to protect any files that were changed during that time.

Change Protection Settings

To change the protection settings, put a new configuration file in the downloads folder. To create a configuration file, see [“Providing a Configuration File for the Product,” on page 36](#). If the modification date of a configuration file is more recent than the file used for the current configuration, Continuous Data Protection for Files adopts the new configuration.

You can use central administration features to manage the configuration of several Continuous Data Protection for Files clients. See [Chapter 7, “Central Management Considerations,” page 105](#), for instructions to set up and manage your clients.

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

Considerations for Upgrading Continuous Data Protection for Files

After you have installed Continuous Data Protection for Files, you can upgrade to a new product version by simply running the standard installer. You can upgrade from previous releases as well as from a previous build of the current release.

Upgrade a single machine to a new product version by installing the product as described in [“Install Continuous Data Protection for Files,” on page 8](#). Note that after upgrading to a new product version, you must reboot your computer. If the new version is significantly different from the previous version, you are prompted to choose protection settings. Otherwise, your current protection settings continues in the new product version.

Installing After Uninstallation

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

After uninstallation, and before installing again, remove the following folders:

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

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

The installation folder For Windows XP and Vista:

C:\Program Files\Cisco\CDP_for_Files

The application data folder

- **For Windows XP:** C:\Documents and Settings\All Users\Application Data\Cisco\CDP_for_Files
- **For Windows Vista:** C:\Program Data\Cisco\CDP_for_Files

Pushing the Product to Other Computers

There are several ways to push initial installation of Continuous Data Protection for Files to other computers.

- Use Microsoft Systems Management Server to install the Continuous Data Protection for Files.msi package. Please refer to Microsoft Systems Management Server documentation.
- Use IBM Tivoli Provisioning Manager Express. Please refer to the *IBM Tivoli Provisioning Manager Express* documentation.
- Place the installer on a file server and ask end users to invoke the installer at their leisure.
- Use the Continuous Data Protection for Files FpPushInst.exe executable.

FpPushInst.exe (Push Install Command)

The FpPushInst.exe executable pushes a local installer executable to another computer.

The FpPushInst.exe executable file can be found at the root of the installation folder. The default installation root folder is **C:\Program Files\Cisco\CDP_for_Files**.

The FpPushInst.exe executable pushes the Continuous Data Protection for Files local installer executable to the ADMIN\$ share on the target computer (see [“Windows Installation Folder,” on page 37](#)). The FpPushInst.exe executable can also copy a local configuration file fpa.txt, to \System32\ in the Windows installation folder. FpPushInst.exe executable then starts a service on the remote computer to invoke a silent installation. Due to firewall and other system settings, the FpPushInst.exe executable does not work in some environments.

Syntax

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

There must be a blank space before each parameter. Blank space is optional between most parameters and their values. No space is allowed between “ and /S. No space is allowed between “ and /v.

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

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

/c:local path and file name of configuration file The path and file name of a Continuous Data Protection for Files configuration file on the local computer. See [“Providing a Configuration File for the Product,” on page 36](#). The FpPushInst.exe executable copies the local configuration file to the \System32\ folder in the Windows installation folder of the remote computer. This parameter is optional. If not specified, the configuration of the remote Continuous Data Protection for Files client becomes the default configuration.



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

/r local path and file name of installer file The path and file name of Continuous Data Protection for Files installer file on local computer. The installer file name must contain the string CDP and end with .exe. For example, a valid path and name is Cisco_CDP_3.1.0.0.exe. Separate the parameter and the value with a blank space.

/S The /S parameter indicates silent installation.

Options

The FpPushInst.exe executable passes these options to the installer. The options for a push installation are the following:

- **DONT_LAUNCH_FILEPATHSRV=1** This option is required for push installation. A pushed installation runs in the system context. It is not recommended that you launch Continuous Data Protection for Files in the system context after installation. Running Continuous Data Protection for Files in the system context can lead to failures when backing up files, or failures later when a user tries to restore files. Use this option to suppress launching Continuous Data Protection for Files in the system context immediately after installation.
- **REBOOT=ReallySuppress** Suppress system reboot after installation. If users are logged on to the remote system, rebooting can be disruptive.
- **INSTALLDIR=folder** The default installation folder is C:\Program Files\Cisco\CDP_for_Files. If you want to install to another folder, use this option and specify the folder. The path corresponds to the remote computer.
- **/!*v log file path** Specify a file to log the installation activities. The path corresponds to the remote computer.

Example

This example pushes the installer file (Cisco_CDP_3.1.0.0.exe) to the remote computer (Computer1). It also pushes a local configuration file c:\fpa.txt to the remote computer's Windows installation folder as \System32\fpa.txt. The /user and /pwd values are used to log on to the remote computer for this operation. FpPushInst.exe then starts a service on the remote computer to invoke the installer, passing to it the parameters: /S, REBOOT=ReallySuppress, DONT_LAUNCH_FILEPATHSRV=1. This tells the installer to install silently; do not reboot after installation, and do not launch Continuous Data Protection for Files in the system context immediately after installation. The installer adopts the protection settings in the configuration file in the Windows installation folder \System32\fpa.txt.

```
FpPushInst.exe \\Computer1 /user:Administrator /pwd:secret /c:c:\fpa.txt /r
C:\Program Files\Cisco\Cisco_CDP_3.1.0.0.exe "/S \"/v /qn
REBOOT=ReallySuppress DONT_LAUNCH_FILEPATHSRV=1 \""
```

Providing a Configuration File for the Product

When Continuous Data Protection for Files is initially installed, the installer can get configuration data from a file `\System32\fp.txt` in the Windows installation folder. (See “Windows Installation Folder” on the right). If this file does not exist, the installer installs Continuous Data Protection for Files with default configuration.

After the initial installation, Continuous Data Protection for Files pulls future configuration settings from configuration files placed in a downloads folder in the central administration area (see “Administration Folders,” on page 112 and Chapter 7, “Central Management Considerations,” page 105). Continuous Data Protection for Files adopts new configurations within 10 to 20 minutes after being placed in the downloads folder.

Create a configuration file from an existing client:

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

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

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

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

If you use the configuration file for a push installation, do not configure a forced backup. If you force a backup on a pushed installation, Continuous Data Protection for Files attempts to back up files in the system context. These backups can fail, and when a logged on user later attempts to restore these files the restore can fail.

To avoid a forced backup, do not check the Run ‘Scan Now’ on other computers check box in the Central Administration Settings window.

Windows Installation Folder

Continuous Data Protection for Files references the Windows installation folder during installation of Continuous Data Protection for Files. During installation, Continuous Data Protection for Files can get configuration information from a file named `fpa.txt` in the `\System32\` sub-folder in the Windows installation folder.

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

Changing Protection Settings

When you initially install Continuous Data Protection for Files, the Initial Configuration Wizard guides you to set your protection settings. After installation, you can change your protection settings with the Settings Notebook.

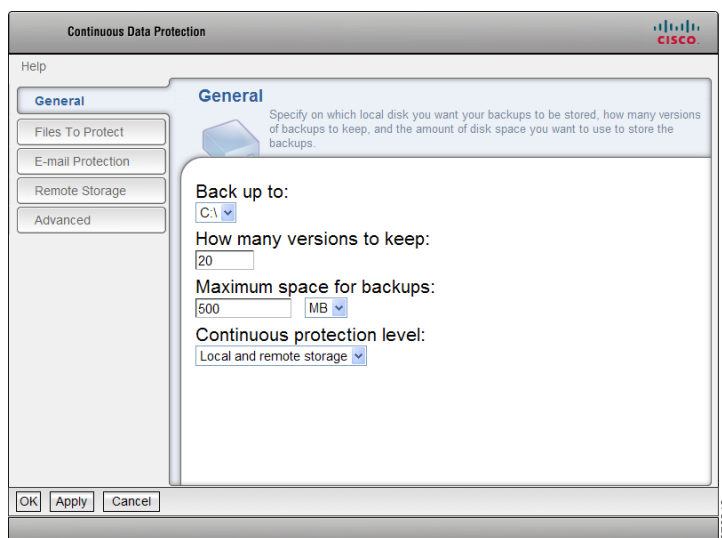
If you are managing other Continuous Data Protection for Files clients, see also [Chapter 7, “Central Management Considerations,” page 105](#).

If you are managing a server, see also [Chapter 8, “Protecting a Server,” page 117](#).

Settings Notebook

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

Figure 19 General



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

Use the control buttons at the bottom of each page to navigate to a page with settings you want to change. Click **OK** to apply your new settings and return to the *Continuous Data Protection for Files Status Page*. Click **Apply** to apply your new settings and stay in the Settings Notebook. Click **Cancel** to exit the Settings Notebook without applying your changes.

The Settings Notebook has 5 options:

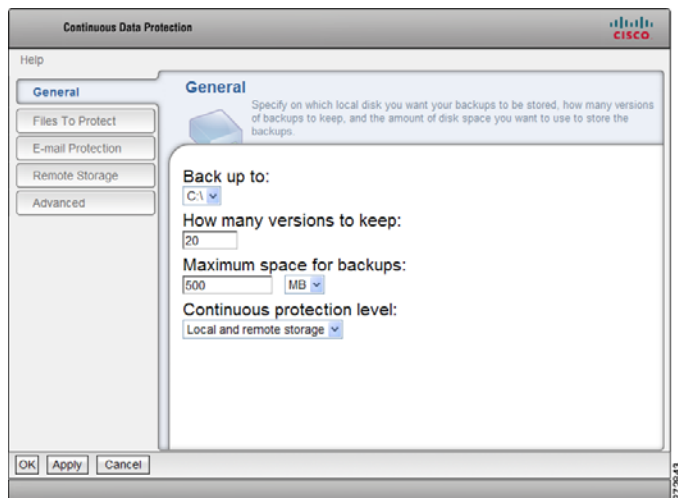
- **General** Use the General page for the following settings:
 - Which drive to use for your local storage area
 - How many versions of protected files to keep on local storage area
 - The maximum size of your local storage area
 - Whether you want to store backup copies on local storage area, remote storage area, neither, or both
- **Files to Protect** Refer to “**Files to Protect,**” on page 43 for these settings:
 - Which folders and files to continuously protect
 - Which folders to vault
 - Force a backup of all protected files when you change which files are continuously protected
- **E-mail Protection** Refer to “**E-mail Protection,**” on page 56 for your e-mail protection settings, including the schedule to protect your e-mail and all files that are backed up on a schedule.
- **Remote Storage** Refer to “**Remote Storage,**” on page 58 for these settings:
 - Your remote storage area
 - How many versions of protected files to keep on remote storage area
 - The maximum size of your remote storage area
 - Whether to encrypt, compress, or use sub-file copy for backup copies stored on remote storage area

- **Advanced** Refer to “Advanced,” on page 63 for these settings:
 - Whether to allow program messages to pop up
 - Performance settings, including the following:
 - Maximum size file to protect on local storage area
 - Maximum size file to protect on remote storage area
 - Maximum speed for transfer to remote storage area
 - The *Advanced* page also contains a link to set your scheduled backups. Follow the link to do these tasks:
 - Choose which files to back up on a schedule
 - Start a backup of your scheduled files immediately
 - View reports of your scheduled backups

General

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

Figure 20 General



Back Up To Choose the location where your local backup copies will be stored. Local backup copies will be stored in a folder on one of your local drives. The default configuration is the non-removable local drive which has the most free space.



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

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



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

How many versions to keep Continuous Data Protection for Files can save more than 1 backup version of each file. When you restore a file, you can choose which version of the file you want to restore. When the configured number of versions is reached, older versions of a file are deleted. Keeping more versions requires more storage space, but allows you more choices when restoring a file.

Maximum Space for Backups

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



NOTE No warning message appears when the maximum space is reached.

The default space for local backups is **500 MB**.

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



NOTE If you try to back up a file which is larger than the space you have allocated for your storage area, Continuous Data Protection for Files will purge all older versions of your files, and then will fail to back up the file. Make sure that the maximum space for your storage areas is greater than the file size limit in the *Advanced* page of the *Settings Notebook*.

Continuous protection level Continuous Data Protection for Files offers two levels of protection for your files: continuous protection and scheduled protection. See “Types of Protection,” on page 3 for a discussion of these two types of protection.

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

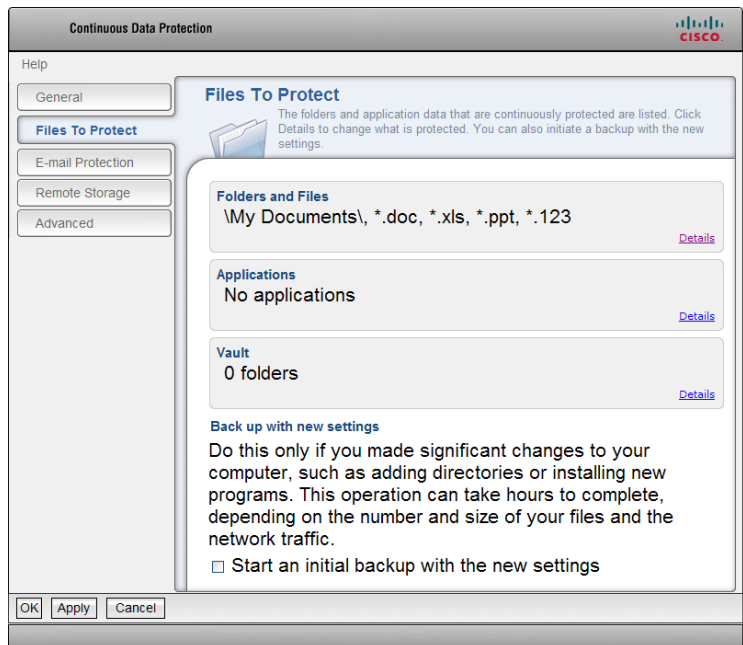
- **None** Files will not be protected.
- **Local storage only** Continuous Data Protection for Files will create backup copies only on the local storage area.
- **Remote storage only** Continuous Data Protection for Files will create backup copies only on the remote storage area.
- **Local and remote storage** Continuous Data Protection for Files will create backup copies on both the local and remote storage areas. This option provides the most protection for your files, and is the default.

Files to Protect

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

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

Figure 21 Files To Protect



Folders and Files

Figure 22 Files To Protect > Folders and Files

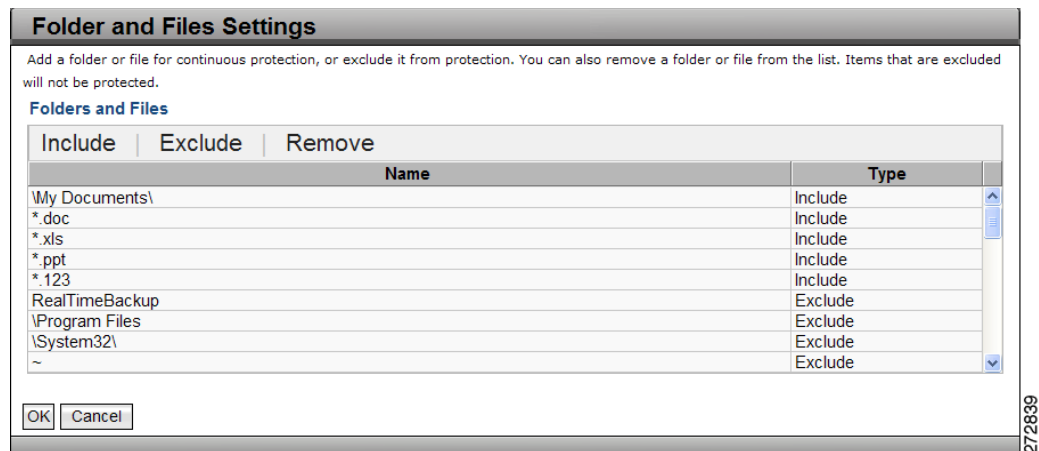


This box gives a summary of the folders and files that are continuously protected. The number of items protected refers to the items in the list of folders and files. A single list item can specify more than one file. Click the **Details** link to view all items in the list and modify the list. The *Folders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

Folders and Files Settings Dialog for Continuous Protection

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

Figure 23 Folders and Files Settings



The top of the list box has three menu buttons. Click the buttons to add and remove items from the list.

Include Click Include to add files/folders that you want to continuously protect. The Select folders dialog will open.

Exclude Click Exclude to add files/folders that you want to exclude from continuous and scheduled protection. The Select folders dialog will open.

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

Each row in the list has two columns:

Name Patterns in the Name column specify one or more files or folders. See **“Interpreting File and Folder Patterns,” on page 18** to determine what files and folders will match a Name pattern with blanks or wildcards. When a folder is protected, all of its files and sub-folders are protected.

Type Values in the Type column indicates if the files and folders should be included or excluded from protection. Files and folders of type Exclude will be explicitly excluded from continuous and scheduled protection. Files of type Include will be protected. Exclude has precedence over Include, so any file or folder that matches an Exclude pattern will not be protected, even if the same file or folder matches an Include pattern. (See **“Including and Excluding Files from Protection,” on page 45.**)



NOTE This Folders and Files Settings list looks similar to the list displayed in the Initial Configuration Wizard. However, the Initial Configuration Wizard only allows file additions (all of type Include). The Initial Configuration Wizard is intended to get Continuous Data Protection for Files started quickly and easily. Any Exclude patterns exclude files from protection as soon as Continuous Data Protection for Files is installed, but they are hidden from view during installation. Although the installed Exclude patterns are recommended for most users, the Exclude patterns are exposed in the Settings Notebook to allow advanced users more robust configuration options.

Protected Drives

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

In some cases, an external USB drive looks like an internal drive, and Continuous Data Protection for Files tries to protect the files on that drive. In this case, add the drive letter to the exclusion list so that all files on the USB drive are excluded from protection. For example, if your E: drive is a USB drive, add E:\ to the list of excluded items.

Including and Excluding Files from Protection

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

Continuous and Scheduled Protection (Not Vaulted)

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

A file is on the include list if it is defined in the Folders and Files list by a pattern with Type Include. Similarly, a file is on the exclude list if it is defined by a pattern of Type Exclude. It is possible that a file can be on both the include list and the exclude list.

If a file (or folder) is on the exclude list, it will not be protected, neither by continuous protection nor by scheduled protection. Even if the file (or folder) is also on an include list, it will not be protected.

If a file is on an include list and not on the exclude list, it will be protected.

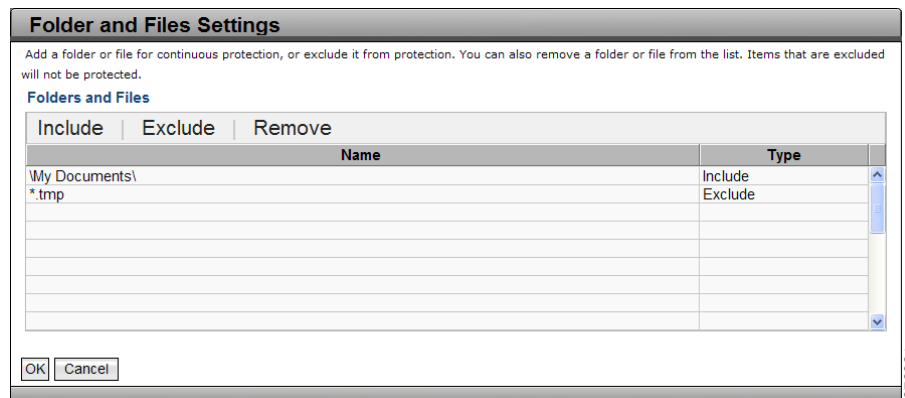
If a file is not on an include list, it will not be protected.

The table below summarizes the interaction of inclusion and exclusion. The two left columns indicate if a file is included or excluded, and the right column indicates if the inclusion and exclusion yield protection for the file.

File is specified on Include list	Files is specified on Exclude list	Is file protected?
No	No	No
No	Yes	No
Yes	No	Yes
Yes	Yes	No

You add items to the include list in several places where settings are configured. You add items to the exclude list in only one place: the *Folders and Files Settings* dialog of the *Files to protect* page of the *Settings Notebook*.

Figure 24 Folders and Files Settings



For example, assume the list above, which includes only \My Documents\, and explicitly excludes only *.tmp. The result is that any files with .tmp file extension in \My Documents\ folder will not be protected. All other files in \My Documents\ folder and its sub-folders will be protected.

As another example, assume the same list as above. If you choose an application (see **“Application Settings,” on page 51**) that typically creates files with extension .tmp, those .tmp files will not be protected.

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

Be very careful when excluding items. Because the patterns in your list can match more than one folder or file, be careful that you do not exclude some files by mistake. See [“Interpreting File and Folder Patterns,” on page 18](#) for an explanation of how patterns match file and folder names.

For example, consider a small variation to an excluded pattern: `\Temp\`. If you used instead `\temp` (without the closing folder delimiter), this would have a very different effect. Even though this may seem like a small change, it has a potentially large impact. All files which have `\temple`, `\temptation\`, `\temperature\`, `\template\`, and other variations of `\temp*`, would be excluded from protection.

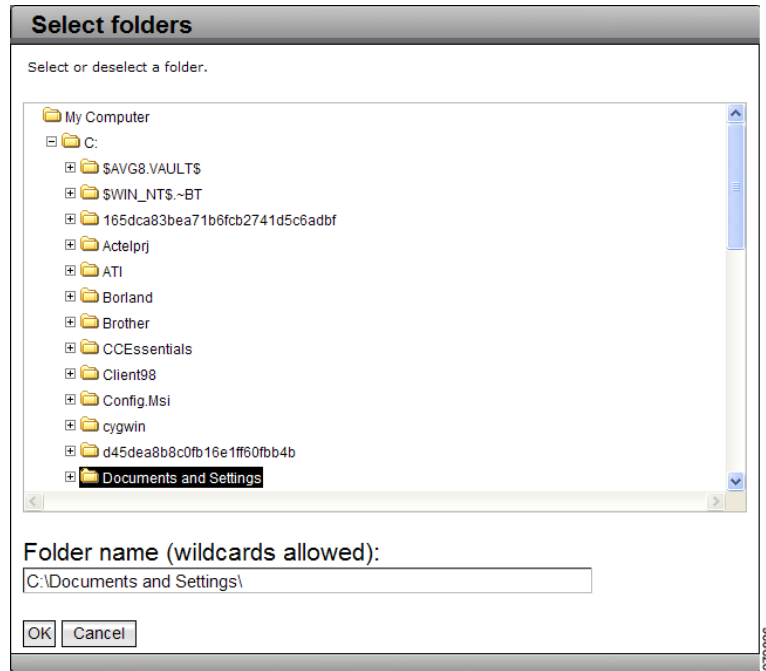
Consider another example. You choose to exclude `*.gif` so you can avoid backing up files saved by your browser when you open different web sites. This pattern will also exclude all `.gif` files in `\My Pictures\` folder.

Vaulted Folders

Vaulted folders, and the files in them, are not affected by the exclude list, nor by the lists of files that are specified for continuous or scheduled protection. All files that you select in the *Vault settings* dialog of the *Files to protect* page of the *Settings Notebook* will be vaulted.

Select Folders

Figure 25 Select Folders



The *Select Folders* dialog allows you to specify files and folders. You can browse to choose a folder, or type the name of a file or folder in the *Folder Name* text field. If you browse and choose a file or folder, you can modify its path in the *Folder Name* text field.



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

Interpreting File and Folder Patterns:

Protection settings use patterns to specify what files and folders to protect. The files and folders that are protected depend on blanks before and after a pattern, and asterisks in the pattern.

You can enter the complete path of a file that you want to protect. For example, C:\Documents and Settings\Administrator\My Documents\Soccer\2005AYSO\Parent Info U8B.doc. The complete path unambiguously matches a single file. But to specify all files this way would be quite time-consuming. Use asterisks and blanks as wildcards in the pattern to specify several files.

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

If there are no asterisks in the pattern, then blank spaces before and after the pattern are interpreted as asterisks. Hence, `\myDocs\` and `*\myDocs*` yield the same matches. If there are asterisks in the pattern, then blank spaces before or after the pattern match no characters. Hence, `\myDir\`, `*\myDir\`, and `\myDir*` could yield three different matches, as in the table of examples below.

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

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

Examples of File and Folder Pattern Matches

Pattern	Matching Folders and Files
<code>\myDir\</code> or <code>\myDir\</code> or <code>*\myDir*</code> or <code>*\mydir*</code>	c:\myDir\ c:\myDir\Contacts\ c:\myDir\Contacts\contacts.txt c:\Projects\myDir\ c:\Projects\myDir\myThings\ c:\Projects\myDir\myThings\things.doc c:\Projects\myDir\myThings\myPhoto.jpg d:\Notes\myDir\
<code>*\myDir\</code>	c:\myDir\ c:\Projects\myDir\ d:\Notes\myDir\
<code>\myDir*</code>	\myDir\ \myDir\Contacts\ \myDir\Contacts\contacts.txt \myDir\myThings\ \myDir\myThings\things.doc

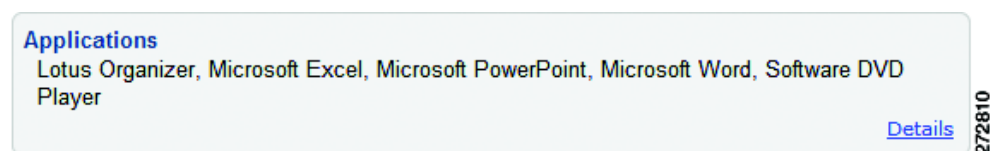
Examples of File and Folder Pattern Matches (Continued)

Pattern	Matching Folders and Files
d:*\\mydir	*d:\\Notes\\myDir\\
\\my best	c:\\Books\\My Best.doc c:\\Photos.jpg\\My Best Photo\\ c:\\Photos.jpg\\My Best Photo\\Best.jpg f:\\Projects\\My Best Project\\ f:\\Projects\\My Best Project\\Dream.xls
.jpg	c:\\Photos.jpg\\ c:\\Photos.jpg\\myHouse.bmp c:\\Photos.jpg\\My Best Photo\\Best.jpg c:\\Projects\\myDir\\myThings\\myPhoto.jpg
*.jpg	c:\\Photos.jpg\\ c:\\Photos.jpg\\My Best Photo\\Best.jpg c:\\Projects\\myDir\\myThings\\myPhoto.jpg
E:\\ E:*	All files and folders on the E: drive.

Applications

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

Figure 26 Applications Box

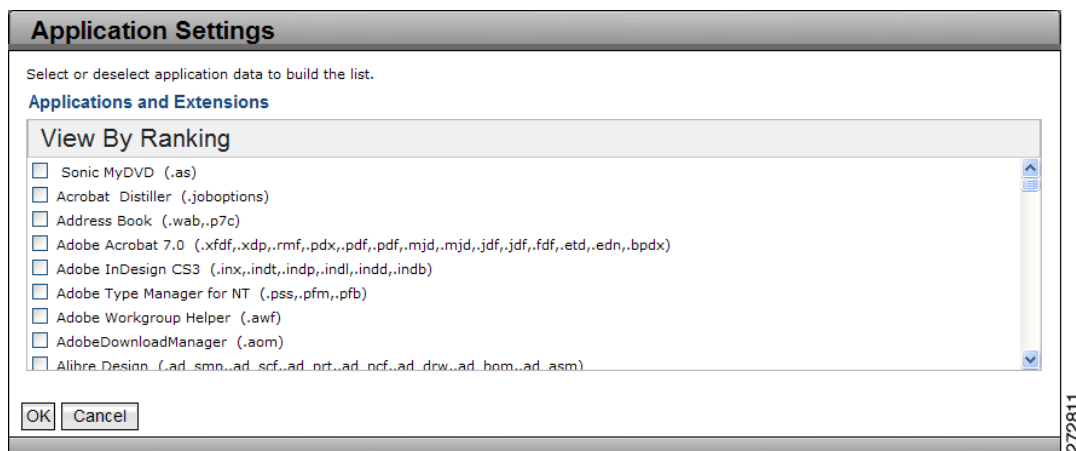


To see the complete list of the applications that are protected, click **Details**. The Application Settings dialog will be displayed.

Application Settings

Specify a list of applications to protect.

Figure 27 Application Settings



The Applications and Extensions box presents a list of applications and their associated file extensions. When an application is checked, all files with the associated extensions will be protected. For example, when Adobe Acrobat® is checked, all files with extension .xaf, .rdm, .pdx, .pdf, and .bpdf will be protected. You can check and uncheck applications to suit your protection needs.

The list of applications has two views. Each view orders the applications in a different way. Click the menu item at the top of the box to change the view.

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

View Alphabetically The applications are presented in alphabetical order.

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

If you uncheck a box, all files with that extension will be removed from the list of protected files. Note that removing file extensions from the list of protected files does not add those files to the list of files that are explicitly excluded from protection.

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

You can add files to be protected in the Application Settings dialog, but these applications will be protected only if the files are not explicitly excluded. See [“Including and Excluding Files from Protection,” on page 45.](#)

Vault

Displays a summary of vaulted folders.

Figure 28 Vault Box

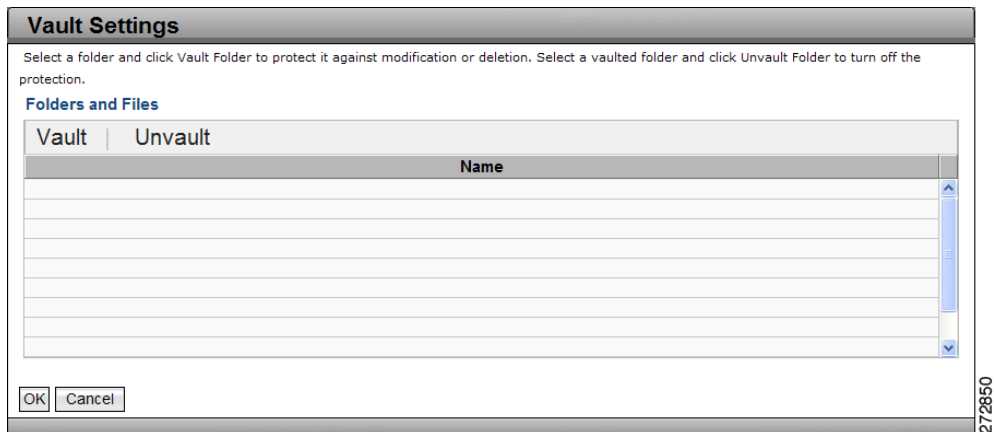


To change the folders that are protected, click **Details**.

Vault Settings

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

Figure 29 Vault Settings



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

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

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

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

Neither the Exclude nor Include items from other dialogs affect the list of vaulted folders. All folders in the *Vault settings* dialog, and only the folders in the *Vault settings* dialog, will be vaulted.

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



NOTE The configured settings will not be applied until you click Settings Notebook **OK** or **Apply** button.

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

Vault Duration

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

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

- **\KeepSafe\RetainForever** Files in this folder will be vaulted forever. Such material can never be moved to another folder with shorter vaulting duration. Material can be moved within the folder tree and to other folders of the same duration.
- **\KeepSafe\Retain Duration** Specify exact vaulting periods using English terminology. Duration is specified by a combination of the following time units:
 - Years
 - Days
 - Hours
 - Minutes
 - Seconds

Use one or more time units. Each time unit you use must be preceded by a number up to 5 digits long. You may include spaces or underlines or dashes and mix case in the folder name. The following are valid examples:

`\Retain23days4hours\`

`\Retain 3years\`

`\Retain_3years\`

`\Retain-23DAYS_4minutes\`

`\Retain 1000 days\`

- **\KeepSafe\RetainUntil Date** Specify a date after which the vaulting will expire. The date must include year, month, and day in the following format: `yyyymmddhhmmss`. The hours, minutes and seconds are optional. The default time is **00:00:00**. The following are valid examples:

`\RetainUntil20191231235959\`

`\RetainUntil 20200101\`

`\RetainUntil20200101\`

`\RetainUntil_20200101\`

**NOTE**

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

Back Up with New Settings

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

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

During a forced backup of all protected files, Continuous Data Protection for Files can use more space than you configured for local storage. (A forced backup of all files occurs during the initial backup when you install Continuous Data Protection for Files, and when you check the **Back up with new settings** box in the Settings

Notebook). The excessive space condition is only temporary. After the forced backup of all files is complete, the first time you change a protected file, Continuous Data Protection for Files purges files from the local storage area, if necessary, to meet the space you configured.

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

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

When to Back Up All Files

When you first install Continuous Data Protection for Files, it is highly recommended that you immediately back up all files that you configured for protection. Without the initial backup, only files that change will be protected. The initial backup will protect all of the existing files that you designated for protection.

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

After the initial backup, the typical rate of file changes do not require that you again back up all files at once. If you change the specifications for Folders and Files or Applications to include files that were not previously protected, the new files need to be backed up. If you extend protection to new e-mail files or other files that are included in scheduled backups, the new files need to be backed up. Until you change these files, and without a forced backup, Continuous Data Protection for Files will not back up these files. To protect these files, you must force a backup of all files.

If you don't change your configuration but suddenly make a big change to the files that are configured for protection, you should also force a backup of all files. Consider this if you add a new drive whose files are configured for protection.

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

After this scan and backup is complete, Continuous Data Protection for Files will continue to operate in the background without any significant impact on your regular computing activities.

Changing the Vault settings does not require a forced backup.

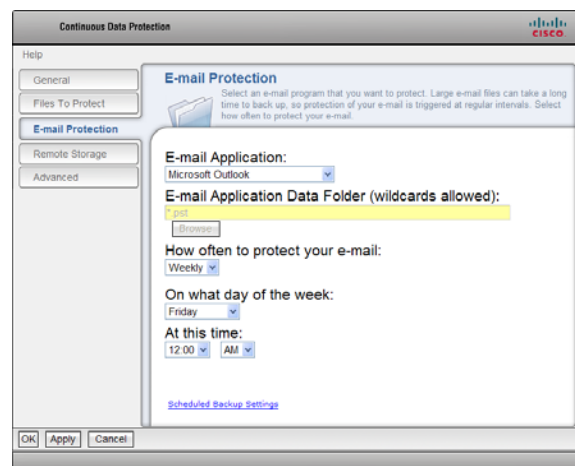
You can force a backup of your continuously protected files in two places:

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

E-mail Protection

Select the e-mail applications that you want to protect. Select a schedule for protecting the e-mail applications.

Figure 30 E-mail Protection



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

E-mail files are backed up only to remote storage. If the remote storage is not available at the scheduled backup time, Continuous Data Protection for Files will queue the backup copies for later transmission. When the remote storage area becomes available, Continuous Data Protection for Files will create the backup copies on the remote storage area.

E-mail Application Select one of the popular e-mail applications in the list. If your application is not listed, select **Other**.

E-mail Application Data Folder If you choose your e-mail application from the *E-mail Application* list, the default file type for that application will appear in this box, and you will not be able to update the file specification. You can update this field only if you select **Other** in the E-mail Application list.

How often to protect your e-mail You can schedule e-mail protection at one of several intervals:

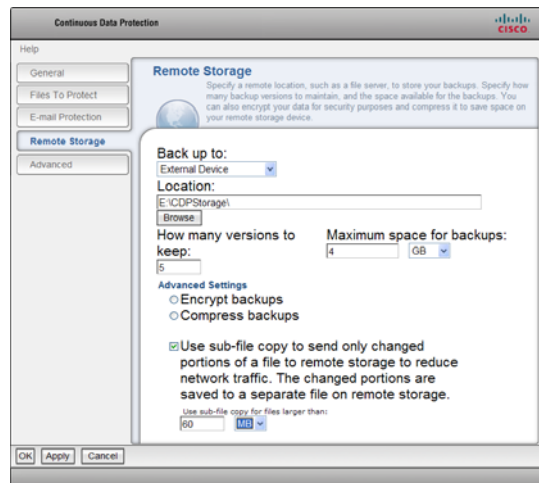
- **Never** E-mail will not be protected.
- **Hourly** E-mail files will be backed up every hour, just after the hour.
- **Daily** E-mail will be backed up once a day. If you choose this interval, also select the time for the backup.
- **Weekly** E-mail will be backed up once a week. If you choose this interval, also select the day and time for the backup.
- **Monthly** E-mail will be back up once a month. If you choose this interval, also select the day of the month and time for the backup.

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

Remote Storage

Specify the remote storage for the backups of your protected files.

Figure 31 Remote Storage



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

Back up to Specify the remote storage device type where your backup copies will be stored. You can specify a file server or removable disk to store the backup copies. The remote device can be another computer (such as a NAS or file server), or a remote disk, or a removable disk.

Location Specify the location of your storage device. What you select from the *Back up to* list affects what you enter in the *Location* field.

In the *Location:* field, if you choose a remote server, it is recommended that you use Universal Naming Convention (UNC) specification for the file server instead of drive letters. Drive letters can change after rebooting and often do not reconnect automatically.

If you choose a USB external device, you can select the driver letter. However, removable external device drive letters can change.

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

Continuous Data Protection for Files will create backup copies in a subfolder named `\RealTimeBackup\computer name`. For example, if a computer name is `Computer1`, and the remote storage location is configured with the value `\remote\share`, backup copies will be stored in `\remote\share\RealTimeBackup\Computer1\`.

If you log in to your computer with a user name and password that is valid also on your remote storage location, Continuous Data Protection for Files will authenticate transparently into that network location. If you do not log in to your computer with a user name and password that is valid also on your remote storage location, you will need to log into the network interactively using another account with regular privileges. You can log in interactively by using the *Net Use* command.

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

WebDAV Server

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

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

When using WebDAV, Continuous Data Protection for Files only supports the Basic Authentication method described in the HTTP 1.0 RFC. Because this authentication method sends the password as clear text over the network, it is also recommended that the Web server be configured to use secure sockets.

IBM Tivoli Storage Manager or IBM Tivoli Storage Manager Express

Continuous Data Protection for Files can store backup copies on an IBM Tivoli Storage Manager server. You do not need to install the IBM Tivoli Storage Manager backup-archive client. If you install the IBM Tivoli Storage Manager backup-archive client, it functions independently from Continuous Data Protection for Files.

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

You will be prompted to enter a valid password for your IBM Tivoli Storage Manager server.

Continuous Data Protection for Files supports IBM Tivoli Storage Manager server version 5.3.3 or later.

Configure your IBM Tivoli Storage Manager server before trying to connect from Continuous Data Protection for Files. Register your computer as an IBM Tivoli Storage Manager node. Continuous Data Protection for Files will use the password assigned at registration to connect to the IBM Tivoli Storage Manager server. For more information about registering an IBM Tivoli Storage Manager node for your computer, see the *IBM Tivoli Storage Manager for Windows Administrator's Guide*.

In order to manage storage space, the IBM Tivoli Storage Manager administrator must grant authority to the IBM Tivoli Storage Manager client node to delete backup copies. For steps to assign authority to delete backup copies, see [“IBM Tivoli Storage Manager Client Node Lacks Authority to Delete Backup Copies,” on page 121](#).

To avoid problems when using the IBM Tivoli Storage Manager server, see [“Files are not Backed Up to IBM Tivoli Storage Manager Server,” on page 120](#).

You can restore backup copies from the IBM Tivoli Storage Manager server only with the Continuous Data Protection for Files GUI. You cannot use the IBM Tivoli Storage Manager Backup-Archive client to restore backup copies created by Continuous Data Protection for Files.

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

Maximum space for backups Specify how much space to use for all backup copies on remote storage.

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

When the storage space becomes full, Continuous Data Protection for Files deletes older backup copy versions of files that have several backup copy versions. After deleting the versioned backup copies, if more space is needed for new backup copies, Continuous Data Protection for Files deletes the last remaining backup copies of enough files to make room for the newest backup copy.

If you try to remotely back up a file which is larger than the space you have allocated for your remote storage area, Continuous Data Protection for Files will purge all older versions of your files, and then may fail to back up the file. Make sure that the maximum space for your remote storage areas is greater than the maximum file size for remote backup in the *Advanced* page of the *Settings Notebook*. For example, if you decrease your maximum space for backups to 1 GB, you should decrease the maximum file size for remote backup from the default of **1 GB**.

Encrypt backups Set encryption for remote backup copies.

The encryption feature provides extra security on your remote location. This can be useful if multiple people have access to the remote server location, and you need to ensure that each user's data is protected from other users, or anyone else who has access to the remote server.

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

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

Continuous Data Protection for Files does not support prompted encryption. Hence, if you specify the IBM Tivoli Storage Manager server as your remote storage area, you must configure non-prompted encryption in the IBM Tivoli Storage Manager `dsm.opt` options file. In the `dsm.opt` file, use the statement: `encryptkey save`. See the IBM Tivoli Storage Manager for Windows Backup-

Archive Client Installation and User's Guide for information about setting encryption options in the IBM Tivoli Storage Manager dsm.opt file. Continuous Data Protection for Files supports AES128 encryption but does not support AES56 encryption.

The dsm.opt file is in this folder:

Microsoft Windows XP, new installation of version 3.1

C:\Documents and Settings\All Users\Application
Data\Cisco\CDP_for_Files\dsm.opt



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

Microsoft Windows Vista, new installation of version 3.1

C:\ProgramData\Cisco\CDP_for_Files\dsm.opt



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

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

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

Compress backups Set compression for remote backup copies.

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

If you enable both compression and sub-file copy, sub-file copy has precedence. This means that a file which has a size larger than the minimum for sub-file copy will not be compressed, since it is subject to sub-file copy activity. Only files smaller than the minimum size for sub-file copy will be compressed.

Use sub-file copy Set sub-file copy for remote backup copies.

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

Sub-file copy can significantly reduce the amount of network traffic. However, sub-file copy consumes more processing resource on your computer. The default setting is to use sub-file copy for files larger than 50 MB. If you need to conserve more network resources, you can reduce the size setting so sub-file copy will be used on even smaller files.

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

Advanced

The *Advanced* page allows you to control popup messages and tune performance.

Allow program messages to pop up For certain types of activities or notifications, Continuous Data Protection for Files pops up messages from the icon in the system tray. To prevent the messages from popping up, select **disabled**.



NOTE If messaging is disabled, important program messages regarding the failure of Continuous Data Protection for Files operations will be suppressed, which could lead to potential loss of data.

Performance Settings

Do not locally back up files larger than Limit the size of files that are backed up to your local storage area. If you try to back up a file which is larger than the space you have allocated for your storage area, Continuous Data Protection for Files will purge all older versions of your files, and then will fail to back up the file. Make sure that the file size limit in this field, and the size limit for files backed up to remote storage, is less than the maximum space for your storage areas.

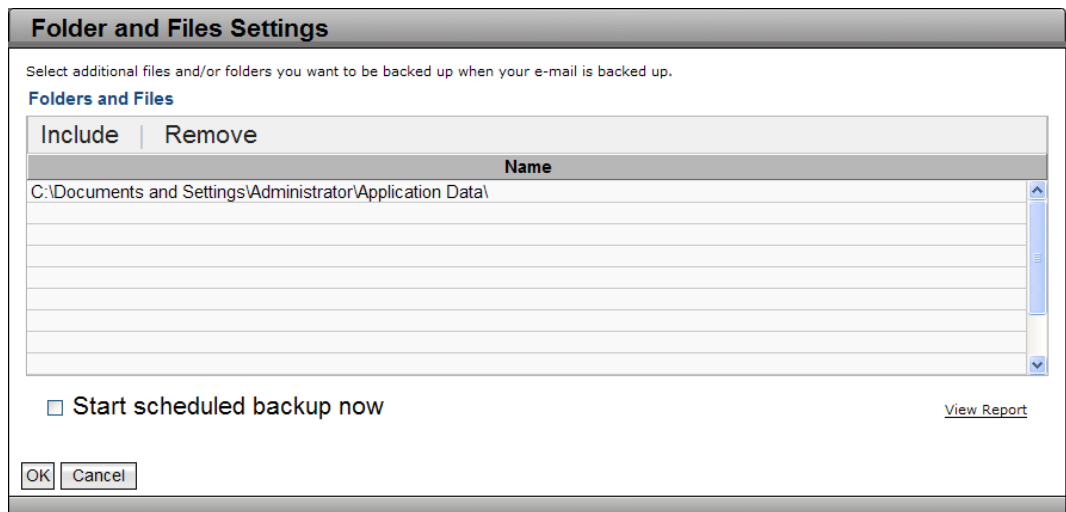
Do not remotely back up files larger than Limit the size of files that are backed up to your remote storage area.

Maximum remote transfer rate You can set a limit on the volume of data that Continuous Data Protection for Files transfers to remote storage. Consider limiting the transfer rate if you need to ease the burden on your network.

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

Folders and Files Settings dialog for scheduled backups Specify folders and files to back up on the same schedule as e-mail files are backed up.

Figure 32 Folders and Files Settings



When considering what files to protect on a schedule, see “Types of Protection,” on page 3, and “Considerations for Scheduled Backups,” on page 66.

The scheduled backup reports table gives a summary of scheduled backups to remote storage areas for all computers that share a common central administration folder. For more information on central administration folders, see [“Administration Folders,” on page 112.](#)

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

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

Version The version of Continuous Data Protection for Files.

Last Backup The last completed scheduled backup.

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

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

Failures This column indicates how many errors there were during the backup. Click the number to display a report of the errors during scheduled backup.

History Click the link to display a list of the historical backup and failure logs. After this list is displayed, you are able to click on logs to display more information. Only reports which had actual files backed up will show as active links.

Considerations for Scheduled Backups

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

Files That Are Appropriate to Protect on a Schedule

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

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

The files you select for scheduled protection will be backed up only at the scheduled time, and only if they change during the scheduled interval. This can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but offer fewer backup versions to choose from when you want to restore a file.

Closing Applications Before a Scheduled Backup

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

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

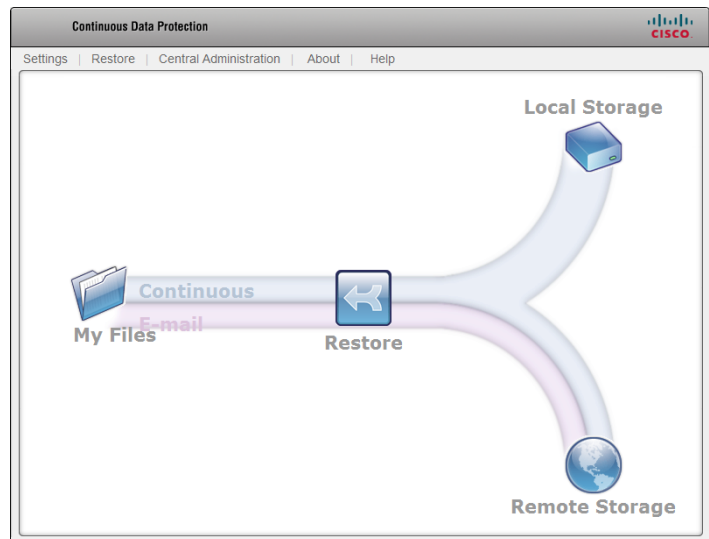
Changing Protection Settings Tasks

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

These tasks assume that you have installed Continuous Data Protection for Files. If you are setting which files are protected during product installation, please see [“Initial Configuration Wizard,” on page 13.](#)

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

Figure 34 Status Page




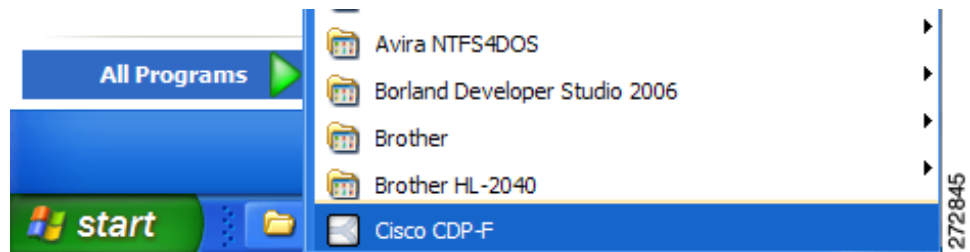
The *Status* page displays when you double-click the **Continuous Data Protection for Files**  icon in the system tray or start Continuous Data Protection for Files from *Start > All Programs > Cisco*.

Figure 35 Start > Programs > Cisco



Specify Which Files and Applications are Protected

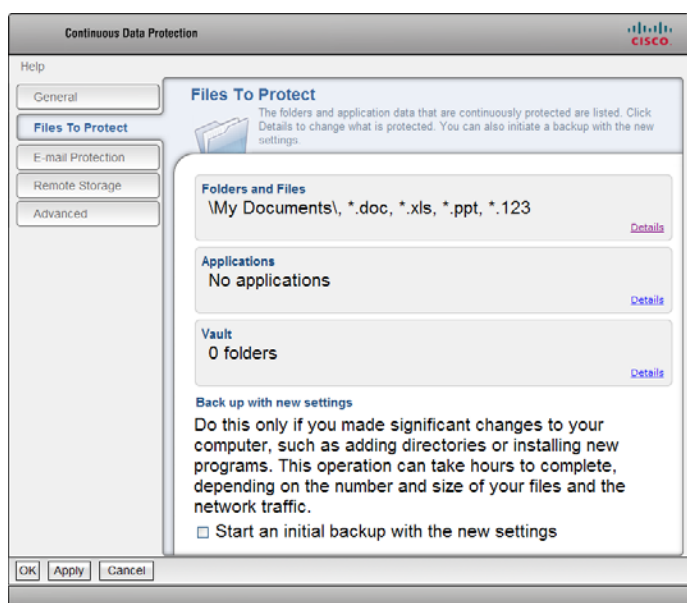
You can specify which files are continuously protected, which files are protected on a schedule, and which files are vaulted. For an explanation of the different kinds of protection, see “Types of Protection,” on page 3.

Specify Which Files and Applications are Continuously Protected

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

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The Settings Notebook will be displayed.
- STEP 3** In the *Settings Notebook*, click the **Files to Protect** tab on the left side of the notebook. The *Files to Protect* page displays. The page has three summary boxes: *Folders and Files*, *Applications*, and *Vault*.

Figure 36 Files To Protect



-
- STEP 4** In the *Applications* box, click the **Details** link. The *Applications Settings* dialog will be displayed and the *Files to Protect* page becomes inactive.
 - STEP 5** Check the applications whose files you want to protect. Uncheck those applications whose files you do not want to protect.
 - STEP 6** Click **OK**. The *Applications Settings* dialog will close and the *Files to Protect* page becomes active.
 - STEP 7** If you want to add or exclude files and folders by specifying file path, in the *Folders and Files* box, click the **Details** link. The *Folder and Files Settings* dialog appears, and the *Files to Protect* page becomes inactive. For an explanation of how to include and exclude files in this dialog, see [“Folders and Files Settings Dialog for Continuous Protection,” on page 44](#).
 - STEP 8** If you added applications or file specifications, you should now force a backup to ensure that all the new files are immediately protected. See [“When to Back Up All Files,” on page 55](#) for an explanation. Check the **Back up with new settings** check box.
 - STEP 9** Click **OK**. The *Settings Notebook* will close and your new settings are applied.
-

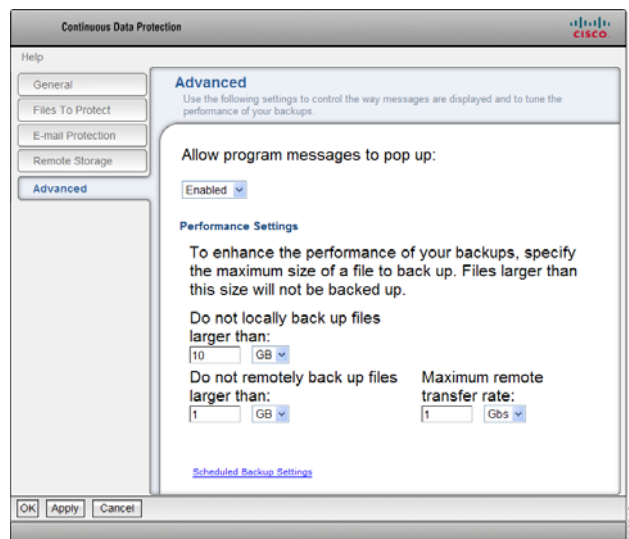
If you forced a backup, your system performance will become slower during the extensive scan of your protected drives.

Specify Which Files and Applications are Protected on a Schedule

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

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The *Settings Notebook* will be displayed.
- STEP 3** In the *Settings Notebook*, click the **Advanced** tab on the left side of the notebook. The *Advanced* page will be displayed.

Figure 37 Advanced



- STEP 4** Click the **Scheduled Backup Settings** link. The *Folders and Files Settings* dialog for scheduled backups will be displayed, and the *Advanced* page becomes inactive.
- STEP 5** Click the **Include** menu item. The *Select Folders* dialog will be displayed and the *Folders and Files Settings* dialog becomes inactive.
- STEP 6** Choose a folder in the folders tree, or specify a folder in the *Folder name* (wildcards allowed) field. You can specify individual files or folders. With wildcards, you can specify all files and folders that match your pattern. See [“Interpreting File and Folder Patterns,” on page 18](#) for details.

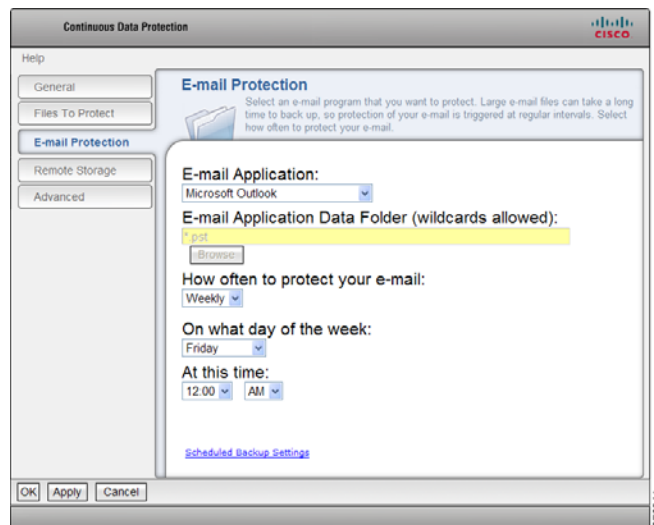
-
- STEP 7** Click **OK**. The *Select Folders* dialog exits, and the *Folders and Files Settings* dialog for scheduled backups again becomes active. The file or folder that you specified is added to the list.
 - STEP 8** Repeat the above three steps to specify more folders to protect.
 - STEP 9** In the *Folders and Files Settings* dialog, select the files and folders that you no longer want protected on a schedule, and click the **Remove** menu item. The files and folders are removed from the list.
 - STEP 10** Click **OK**. The *Folders and Files Settings* dialog exits, and the *Advanced* page in the *Settings Notebook* again becomes active.
 - STEP 11** Click **OK**. The *Settings Notebook* exits and your new settings are applied.
-

Specify Which E-mail Applications are Protected

E-mail applications have their own page in the Settings Notebook.

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The *Settings Notebook* will be displayed.
- STEP 3** In the *Settings Notebook*, click the **E-mail Protection** tab on the left side of the notebook. The *E-mail Protection* page will be displayed.

Figure 38 E-mail Protection

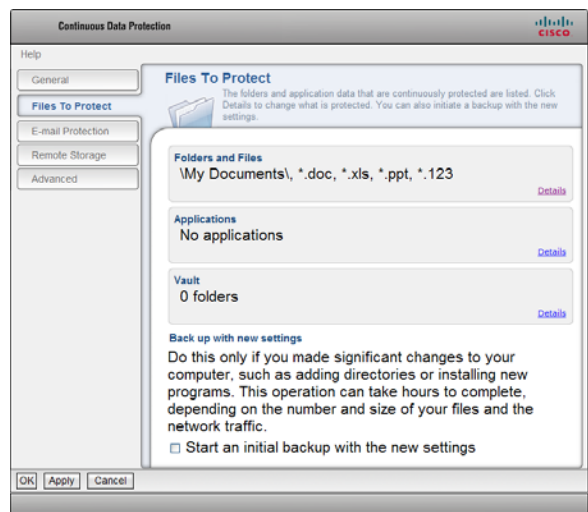


- STEP 4** Choose your e-mail application from the *E-mail Application* drop-down list. If your application is not listed in the drop-down list, choose **Other**. If you chose **Other**, the *E-mail Application Data Folder (wildcards allowed)* field will become active.
- STEP 5** If you chose *Other*, enter a file specification in the *E-mail Application Data Folder (wildcards allowed)* field. You can type the specification or browse for the folder.
- STEP 6** Click **OK**. The Settings Notebook closes and your new settings are applied.

Specify Which Files and Applications are Vaulted

- STEP 1** Click the **Settings** menu item. The *Settings Notebook* will be displayed.
- STEP 2** In the *Settings Notebook*, click the **Files to Protect** tab on the left side of the notebook. The *Files to Protect* page will be displayed. The page has three summary boxes: *Folders and Files*, *Applications*, and *Vault*.

Figure 39 Files To Protect



- STEP 3** In the *Vault* box, click the **Details** link. The *Vault Settings* dialog displays, and the *Files to Protect* page becomes inactive.
- STEP 4** Click the **Vault** menu item. The *Select Folders* dialog will be displayed, and the *Vault Settings* dialog becomes inactive.
- STEP 5** Choose a folder in the folders tree, or specify a folder in the *Folder name* (wildcards allowed) field. You cannot specify individual files. With wildcards, you can specify all folders that match your pattern. See **“Interpreting File and Folder Patterns;” on page 48** for details.
- STEP 6** Click **OK**. The *Select Folders* dialog exits, and the *Vault Settings* dialog again becomes active. The folder that you specified is added to the list.
- STEP 7** Repeat the above three steps to specify more folders to vault.
- STEP 8** In the *Vault Settings* dialog, select the folders that you no longer want vaulted, and click the **Unvault** menu item. The folders that you specified are removed from the list.

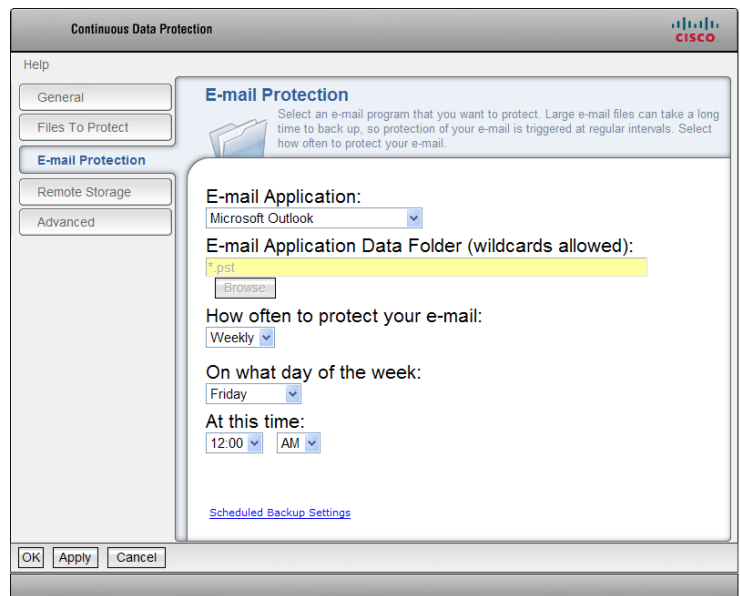
- STEP 9** Click **OK**. The *Vault Settings* dialog exits, and the *Files to Protect* page in the *Settings Notebook* again becomes active.
- STEP 10** Click **OK**. The *Settings Notebook* exits, and your folders become vaulted.

Specify the Period for Scheduled Protection

Schedule Protection occurs at the interval that is configured in the *E-mail Protection* page in the *Settings Notebook*. When you change the schedule for e-mail files, it affects all files that are protected on a schedule.

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The *Settings Notebook* will be displayed.
- STEP 3** In the *Settings Notebook*, click the **E-mail Protection** tab on the left side of the notebook. The *E-mail Protection* page will be displayed.

Figure 40 E-mail Protection



- STEP 4** Choose the schedule period in the *How often to protect your e-mail* drop-down list. Day or time fields will be displayed depending upon the scheduled period that are selected.

- STEP 5** If applicable for the scheduled period, choose the day and time to perform the backup.
- STEP 6** Click **OK**. The *Settings Notebook* exits and your new settings are applied.

Specify Storage for Backup Copies

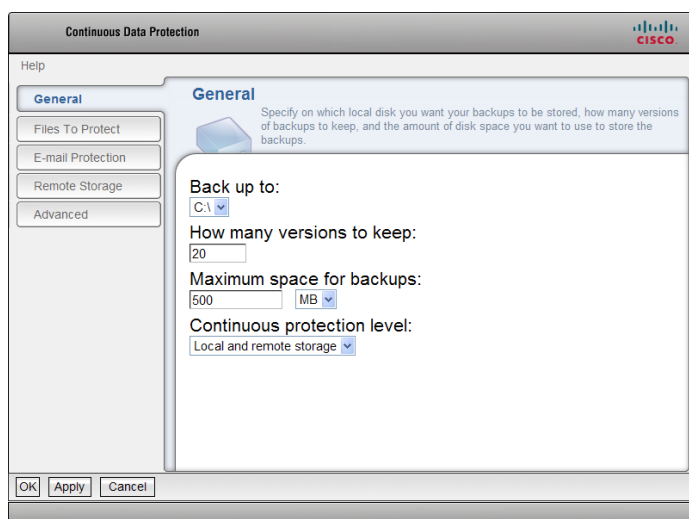
You can specify local storage areas, remote storage, and on which storage areas to store backup copies.

Specify the Local Storage Area for Backup Copies

You can specify where to store the backup copies. You can specify how many versions to keep, and the maximum space for backup copies. Also specify whether to use local storage, remote storage, both, or neither.

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The *General* page of the *Settings Notebook* will be displayed.

Figure 41 General



- STEP 3** Choose the location, number of versions, and space for local backup copies. For explanations of the fields on this page, see **“General,” on page 40**.

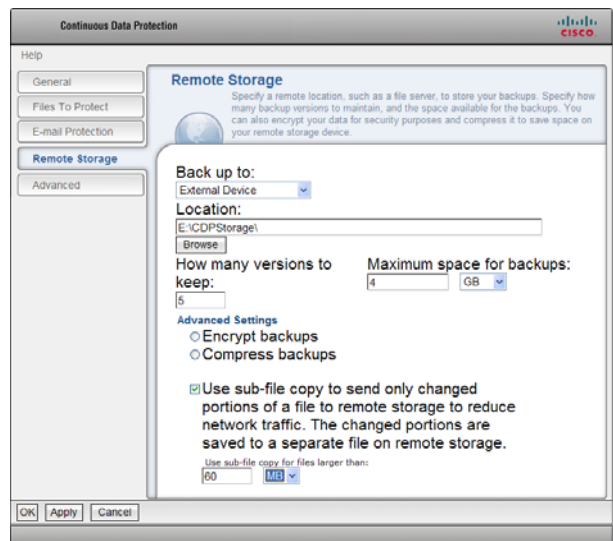
- STEP 4** Click **OK**. The *Settings Notebook* closes and your new settings are applied.

Specify the Remote Storage Area for Backup Copies

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

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The *Settings Notebook* will be displayed.
- STEP 3** In the *Settings Notebook*, click the **Remote Storage** tab on the left side of the notebook. The *Remote Storage* page will be displayed.

Figure 42 Remote Storage



- STEP 4** Choose appropriate values for the remote storage area fields. For explanations of the fields on this page, see **“Remote Storage,” on page 58**.
- STEP 5** Click **OK**. The *Settings Notebook* closes and your new settings are applied.

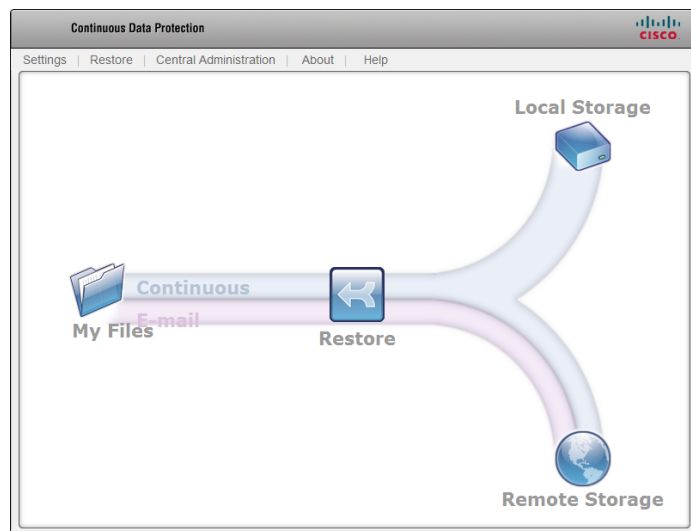
Force a Backup

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

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

These tasks assume that you start from the *Continuous Data Protection for Files Status* page.

Figure 43 Status Page




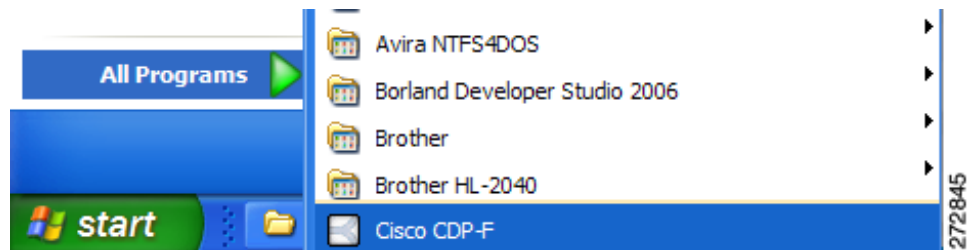
The *Status* page displays when you double-click the **Continuous Data Protection for Files**  icon in the system tray or start Continuous Data Protection for Files from *Start > All Programs > Cisco*.

Figure 44 Start > Programs > Cisco



Backup All Protected Files

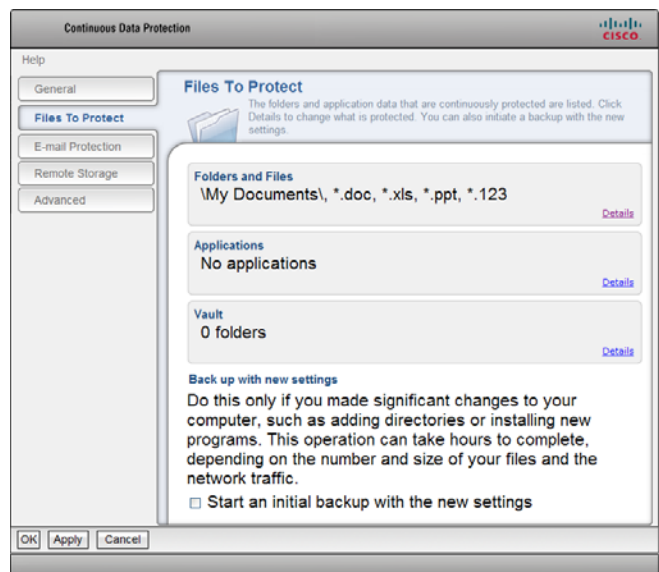
When you change your configuration to extend continuous or scheduled protection to more files, it is recommended that you back up all protected files. Failing to back up all protected files will yield protection only for those files that you change.

For an explanation of when to back up all files, see [“When to Back Up All Files,” on page 55](#).

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

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The *Settings Notebook* will be displayed.
- STEP 3** In the *Settings Notebook*, click the **Files to Protect** tab on the left side of the notebook. The *Files to Protect* page will be displayed.

Figure 45 Files To Protect



- STEP 4** Check the **Back up with new settings** check box.

- STEP 5** Click **OK**. The *Settings Notebook* will close and Continuous Data Protection for Files begins to scan your protected drives and back up all files that you designated for continuous or scheduled protection. Your system performance will become slower during the extensive scan of your protected drives.

Force a Scheduled Backup

You can force a scheduled backup before the schedule period. All files that have changed since the last scheduled backup will be backed up.

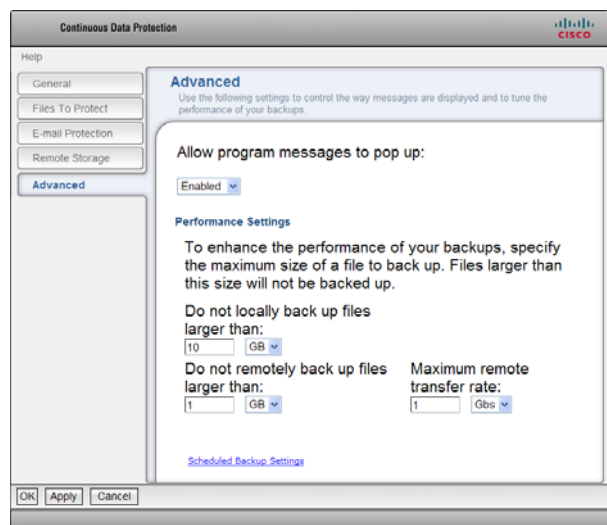


NOTE You will not back up all files that are designated for scheduled protection, but only those files that have changed since the last scheduled backup.

To force a scheduled backup, start at the *Status* page.

- STEP 1** Open the *Continuous Data Protection for Files Status* page.
- STEP 2** Click the **Settings** menu item. The *Settings Notebook* will be displayed.
- STEP 3** In the *Settings Notebook*, click the **Advanced** tab on the left side of the notebook. The *Advanced* page will be displayed.

Figure 46 Advanced



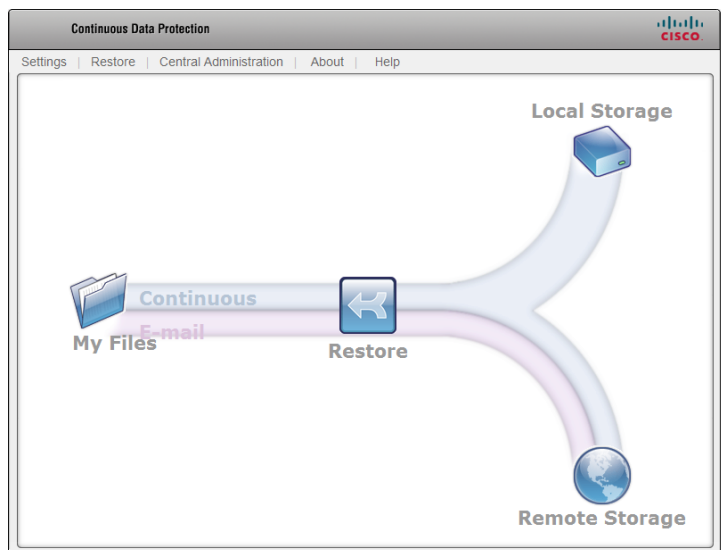
- STEP 4** Click the **Scheduled Backup Settings** link. The *Folders and Files Settings* dialog for scheduled backups displays, and the *Advanced* page becomes inactive.
- STEP 5** Check the *Start scheduled backup now* check box.
- STEP 6** Click **OK**. The *Folders and Files Settings* dialog closes and the *Advanced* page in the *Settings Notebook* becomes active.
- STEP 7** Click **OK**. The *Settings Notebook* will close and Continuous Data Protection for Files begins to back up all files that have changed since the last scheduled backup.

Stopping a Backup or Restore Activity

You can stop any backup or restore activity.

This task assumes that you start from the *Continuous Data Protection for Files Status* page.

Figure 47 Status Page




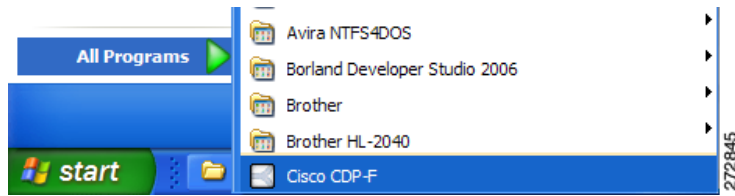
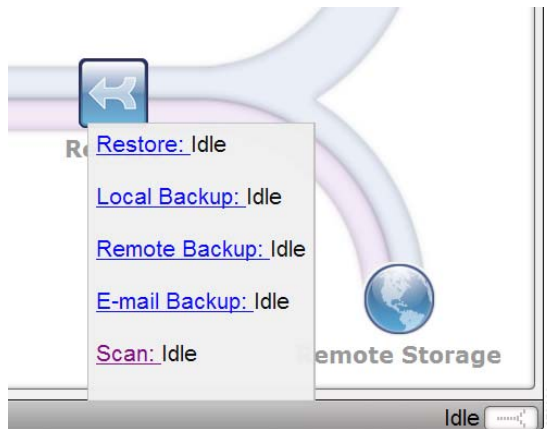
The *Status* page will be displayed when you double-click the **Continuous Data Protection for Files**  icon in the system tray or start Continuous Data Protection for Files from *Start > All Programs > Cisco*.

Figure 48 Start > Programs > Cisco



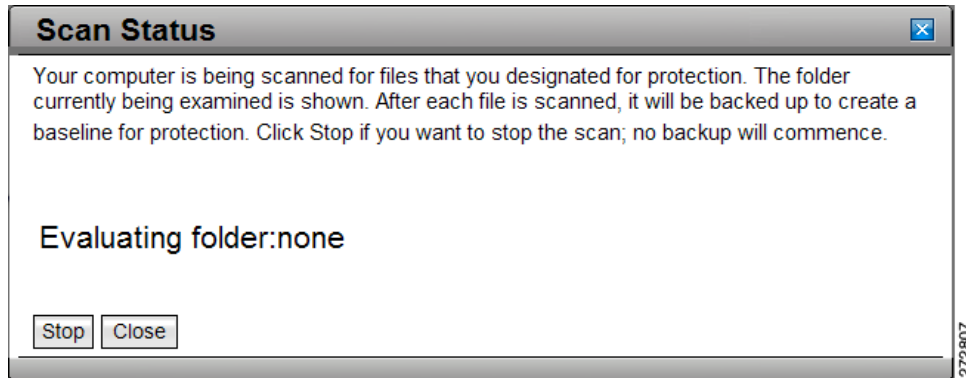
- STEP 1** The bar at the bottom of the *Status* page displays a brief text message of the status of backup and restore activities. Let your cursor hover over the text. A summary of activities will pop up. The summary lists five activities. For each activity, there is a link to a detailed status dialog, and a brief text that indicates the status of the activity.

Figure 49 Status Page Details



- STEP 2** Click the link for the activity you want to stop. The detailed status dialog for that activity displays, and the *Status* page becomes inactive.

Figure 50 Scan Status



- STEP 3** Click **Stop**. The *Detailed Status* dialog closes, and the *Status* page becomes active again. Within a short time, the activity will stop.

Monitoring Your Protection

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

If you determine that Continuous Data Protection for Files is not protecting your files as you intended, often the solution will be suggested by the data available from Continuous Data Protection for Files reports or configuration settings. If the solution is not clear, consider the information in [Chapter 9, “Problem Determination Guide,” page 119](#). The following monitoring opportunities are available.

Popup Messages

After you install and configure Continuous Data Protection for Files, it will work unobtrusively in the background. Chances are good that you can forget about Continuous Data Protection for Files until you want to restore a file. Unless you will do some active monitoring of Continuous Data Protection for Files, it is recommended that you allow Continuous Data Protection for Files to warn you those few times that you might need to pay attention to your protection system. For example, if you are running out of space in your storage area, Continuous Data Protection for Files can warn you with a message.

By default, Continuous Data Protection for Files sends you messages. However, if you disable this setting and need to re-enable it, configure this setting in the *Allow program messages to pop up* drop-down list in the *Advanced* page of the *Settings Notebook*.

Continuous Data Protection for Files Icon in the System Tray

When the Continuous Data Protection for Files daemon is protecting your files, the **Continuous Data Protection for Files**  icon appears in your desktop system tray. If you do not see the icon in your system tray, you must restart the daemon. See [“Restart Continuous Data Protection for Files Daemon,” on page 124.](#)

Monitoring Protection with the User Interface


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


Continuous Data Protection for Files Status Page

The *Status* page provides status information at a glance. The items below help you monitor the status of your protection. For an explanation of all fields on the page, see [“Status Page,” on page 88.](#)

Icon Color

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

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

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

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

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

Icon Data and Links

Let your pointer hover over an icon to display summary information and links to detailed information. The summary information for each icon gives clues about your protection status, and the links provide details.

My Files Icon

Files under protection If the number of files under protection is not reasonable given the changes you've made and the list of files that you've configured, you should investigate further. Verify that you accurately configured the list of files to protect. Click the **Settings** link below *Files under protection* to configure the files to protect.

View Report The *View Report* link opens a detailed list of recent protection activity. The top of the list contains failed activities and messages describing the failures.

E-mail protection If the *Last successful backup on field* does not indicate a recent successful backup, verify the configuration of your e-mail application and the schedule for your e-mail backups. Click the **Settings** link below E-mail protection to configure your e-mail protection.

Local Storage Icon

If the *Usage* bar indicates that your local storage is full, you should investigate further. You can re-configure your local storage area. Click the **Settings** link to configure your local storage area.

Remote Storage Icon

Usage If the *Usage* bar indicates that your remote storage is full, you should investigate further. You can re-configure your remote storage area.

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

Continuous Protection Activity Report

A report of continuous protection activity is available from a link in the *Status* page. The report is called Activity Report. To navigate to the Activity Report, see "[View Continuous Protection Activity Report,](#)" on page 92.

Figure 51 Activity Report

Activity Report		Monday, October 06, 2008 11:58:45 PM	
Failures	The following lists the operations that failed. Look for repeated failures as a basis for troubleshooting. For information on how to correct issues, see Troubleshooting .		
Date and Time	File Name	Activity	Reason for Failure
Successful			
The following is a list of recent successful operations.			
Date and Time	File Name	Activity	
10/06/2008 18:49:53	README.DOC	Backup (Local)	
10/06/2008 18:49:52	manual.doc	Backup (Local)	
10/06/2008 18:49:51	manual.doc	Backup (Local)	
10/06/2008 18:49:50	zoomTol_doc.doc	Backup (Local)	
10/06/2008 18:49:49	viewBimap_doc.doc	Backup (Local)	
10/06/2008 18:49:49	UMClpObj_doc.doc	Backup (Local)	
10/06/2008 18:49:49	Text_doc.doc	Backup (Local)	
10/06/2008 18:49:49	TerpPant_doc.doc	Backup (Local)	
10/06/2008 18:49:49	TerpPantFileFilter_doc.doc	Backup (Local)	
10/06/2008 18:49:48	TerpPantContainer_doc.doc	Backup (Local)	
10/06/2008 18:49:48	TerpOfficeAppInterface_doc.doc	Backup (Local)	

272806

The Activity Report lists failed activities (if any) at the top of the report. The failed activity is accompanied by a reason for the failure. Successful activities are listed below.

The list does not include all activities; only the most recent activities appear.

The activity can be one of the following:

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

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

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

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

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

Scheduled Backup Report

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

When managing Continuous Data Protection for Files clients, you can view the reports to see when the last successful scheduled backups took place. If it has been an extended period of time, this could indicate a problem with the Continuous Data Protection for Files client.

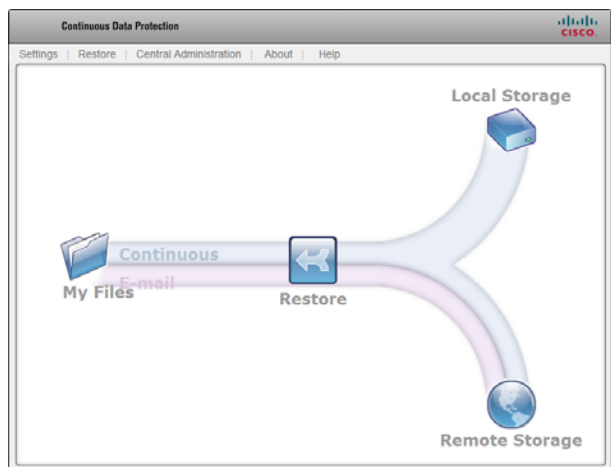
For an explanation of the scheduled backup reports table, see [“Scheduled Backup Reports Table,” on page 65.](#)

To navigate to the scheduled backup reports table, see [“View Report of Scheduled Backups,” on page 93.](#)

Status Page

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

Figure 52 Status Page




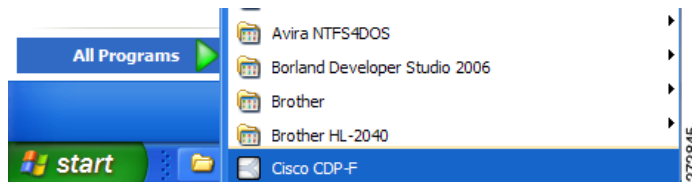
The *Status* page displays when you double-click the **Continuous Data Protection for Files**  icon in the system tray or start Continuous Data Protection for Files from *Start > All Programs > Cisco*.

Figure 53 Start > Programs > Cisco



Menu Links

The top of the page has five links:

- **Settings** Links to “**Settings Notebook,**” on page 38. Use the *Settings Notebook* to change your protection settings.
- **Restore** Links to “**Restore Wizard,**” on page 95. Use the *Restore Wizard* to restore a file from a backup copy.
- **Central Administration** Links to “**Central Administration Settings Window,**” on page 114. Use the *Central Administration* page to manage Continuous Data Protection for Files on other computers.



NOTE The Central Management feature is available with PC Edition and Server Edition.

- **About** Provides information about the product, including version level.
- **Help** Links to the online help documentation.

Graphic Icons

The center of the page contains a graphic representation of Continuous Data Protection for Files protection. Let your pointer hover over an icon to display summary information and links to detailed information.

My Files

Figure 54 My Files



Files Under Protection

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

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

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

For an explanation of the Activity Report, see “**Continuous Protection Activity Report,**” on page 86.

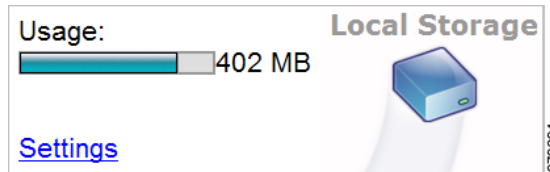
E-Mail Protection

Settings Links to the *E-mail* page of the *Settings Notebook*. Use this link to change the e-mail application that is protected.

Restore Links to the *Restore Wizard*, which helps you restore files from backup copies.

Local Storage

Figure 55 Local Storage

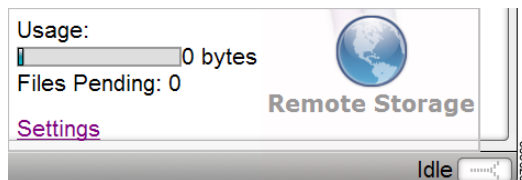


Usage Shows how much space is being used by backup copies on local storage. The bar graph indicates what portion of the storage is being used. The text indicates the usage in bytes.

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

Remote Storage

Figure 56 Remote Storage



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

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

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

Status Panel

The bar at the bottom of the page displays a brief text message of the status of backup and restore activities. Let your cursor hover over the text to display the status of five activities and links to detailed status reports.

The status of the activities can be one of the following:

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

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

Active The activity is active.

Paused The activity was paused by the user.

Disconnected The storage area is unavailable.

Disabled The storage area is not configured.

View Continuous Protection Activity Report

You can see a detailed report of recent backup activities. The report shows successful activities, and failed activities with messages.

-
- STEP 1** Open the *Continuous Data Protection for Files Status* page.
 - STEP 2** Let your pointer hover over the *My Files* icon. Summary information and links will be displayed.
 - STEP 3** Click the **View Report** link. The *Activity Report* will be displayed.
-

View Report of Scheduled Backups

You can see a detailed report of scheduled backup activities. Choose from a list of backup reports. The report shows successful activities, and failed activities with messages.

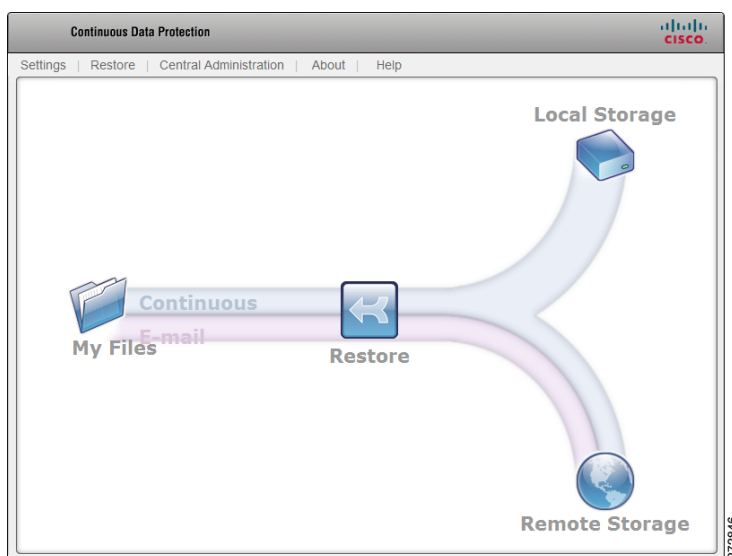
-
- STEP 1** Open the *Continuous Data Protection for Files Status* page.
 - STEP 2** Let your pointer hover over the *Remote Storage* icon. The summary information and links will be displayed.
 - STEP 3** Click the **Settings** link. The *Settings Notebook* will be displayed; the *Remote Storage* page is selected.
 - STEP 4** On the left side of the notebook, select the **Advanced** page.
 - STEP 5** Click the **Scheduled Backup Settings** link. The *Folders and Files Settings* dialog for scheduled backup will be displayed.
 - STEP 6** Click the **View Report** link.
-

Restoring Files

Continuous Data Protection for Files makes backup copies of your files so that when the time comes, you can restore your files. You can restore a file that you deleted, and you can restore an earlier version of a file that does not have your recent changes. A wizard guides you to find the file; choose the right version, and choose the location to restore your file.

Start from the *Continuous Data Protection for Files Status* page.

Figure 57 Continuous Data Protection for Files Status Page




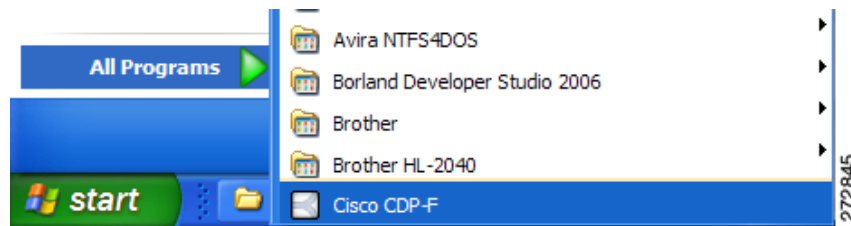

The *Status* page will be displayed when you double-click the **Continuous Data Protection for Files**  icon in the system tray or start Continuous Data Protection for Files from *Start > All Programs > Cisco*.

Figure 58 Start > Programs > Cisco



Click the **Restore**  icon in the middle of the page. The Restore Wizard will guide you to restore your file.

Restore Wizard

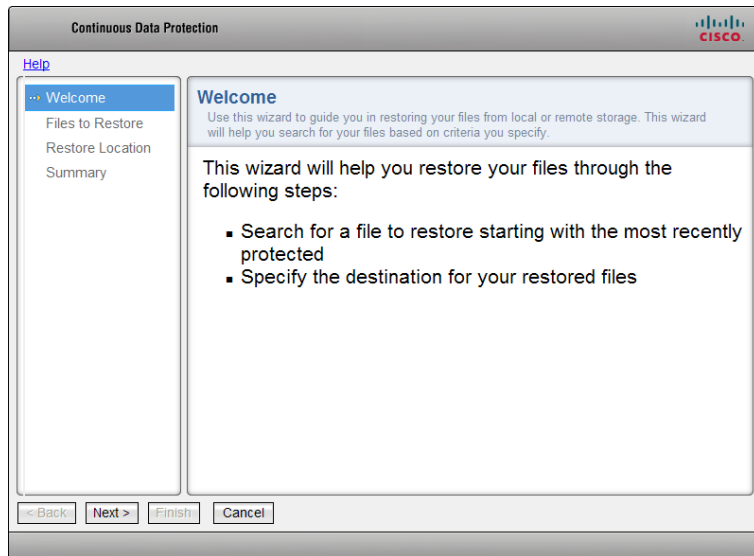
Restore a protected file Use the control buttons at the bottom of each Wizard page to navigate to all pages. When you reach the final page, click **Finish** to restore your files. The wizard has four pages:

- Welcome
- Files to Restore
- Restore Location
- Summary

Welcome

The *Welcome* page lists the steps to restore your files.

Figure 59 Welcome

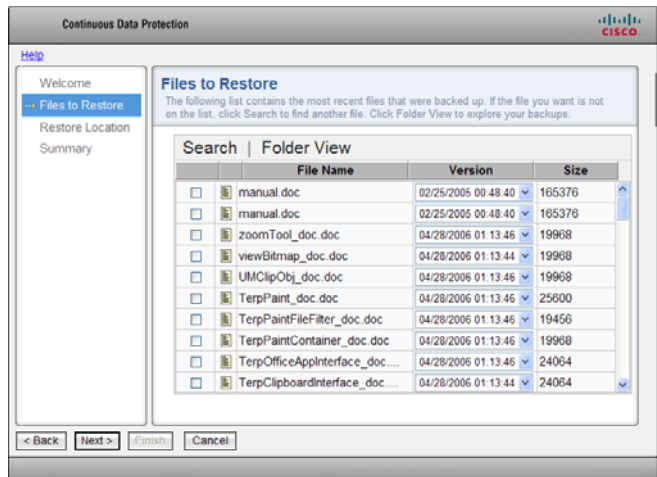


Click **Next** to advance to the next page of the wizard. Click **Cancel** to exit the wizard without restoring any files.

Files to Restore

This page contains a list of the most recent files that were backed up.

Figure 60 Files To Restore



Each row contains the following fields:

Select Check the box if you want to restore the file.

File Name The name of the file that you can restore. Let your pointer hover over the file name to pop up the full path of the file.

Version The drop-down box lists the dates and times that this file was backed up. Choose the version that you want to restore.

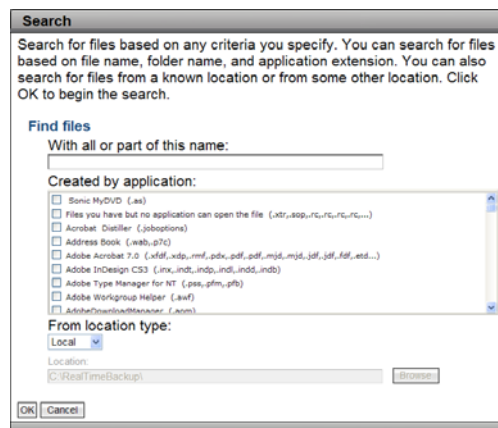
Size The size of the file.

The list initially contains the last 20 files that were backed up. Change the list of files by clicking the **Search** or **Folder View** menu items at the top of the box.

Search

Presents a dialog that allows you to search for backup copies to add to the list.

Figure 61 Search



The *Search* dialog has several fields. The fields are combined to narrow the search criteria. Leaving any field blank increases the chances of finding more files.

Find Files

With all or part of this name Use this field if you know the name or part of the name of the file you want to restore. You can enter a partial file name or folder and use an asterisk as wildcard. If you enter nothing, the search can yield files from any folder with any name.

Created by application Use this list if you know the application that created the file you want to restore. Check as many applications as you want. If you enter nothing, the search can yield files from any application.

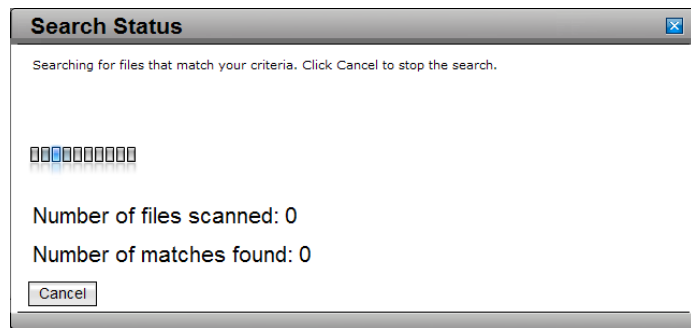
From location type Choose the location of the backup copy. You can choose from three locations:

- **Local** The local storage area that is currently configured.
- **Remote** The remote storage area that is currently configured.
- **Other** Any folder of your choosing. If you previously configured your local or remote storage areas differently than your current configurations, you can search in those previously configured areas. When you choose this option, the *Location* text entry field becomes active. Type the location to search or click **Browse** to browse for the folder.

Click **OK** to begin searching.

Click **Cancel** to exit the Search dialog without searching.

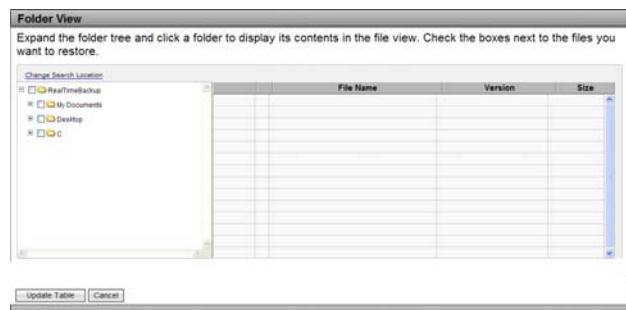
Figure 62 Search Status



The *Search Status* window will show the progress of your search. The *Cancel* button will stop the search and return to the list of files without adding the files in your search criteria. If the search completes without being cancelled, the *Files to Restore* list will contain the results of your search.

Folder View

Figure 63 Folder View



Presents a dialog that allows you to browse folders to find your files. The *Folder View* dialog has the following fields:

Folder tree Browse the tree to find a folder. Click a folder and the files in that folder will display in the file view to the right of the folder tree.

File view Displays the files in a folder that you chose. Check the box in the *Select* column to select a file. The *Version* drop-down list shows the dates that the file was backed up. Choose the version that you want to restore.

Click **Update Table** to add the selected files to the list of files.

Click **Cancel** to exit the dialog without adding any files to the list of files.

Restore Location

Choose the location to restore your files.

Figure 64 Restore Location



You can restore your files to their original location, or to a different location.

Restore Data To

Its original location Check the button if you want to restore the files you chose to their original locations. The original location is the full path that pops up when you let your pointer hover over the file name in the *Files to Restore* page.

The following location If you want to restore the files to a different location, check the button and enter the new location in the field. You can use the **Browse** button to select the location. All files that you choose will be restored to the path that you specify. No part of the original path will be appended to the path that you specify.

For example, assume the original file's full path is C:\Documents and Settings\Administrator\My Documents\My Pictures\Vacation2006\Family.jpg. Assume also that you want to restore the file to a folder called D:\BestPhotos. In the *Restore data to:* field, you must provide the folder name and a file name. Assume that you specify D:\BestPhotos\Family2006.jpg. Continuous Data Protection for Files will restore the file to this path: D:\BestPhotos\Family2006.jpg.

Summary

Use the *Summary* page to view a summary of your choices, and decide if you want to restore your files.

The *Summary* page displays the locations and number of files that you specified in the previous pages of the wizard.

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

Choose **Finish** to restore your files. If popup messages are enabled, you see a message when your restore is complete.

Choose **Cancel** to exit the wizard without restoring your files.

Storage Areas

Continuous Data Protection for Files stores many backup copies in the native file format. The exceptions are backup copies that were created using sub-file copy, compression, or encryption. You can access the backup copies by using native file system commands.

Format of Backup Copies

Continuous Data Protection for Files keeps most backup copies in the same format as the original file.

Although Continuous Data Protection for Files provides tools and views to see the backup copies and to restore them, in many cases it is not necessary to use Continuous Data Protection for Files to access, restore, or manipulate those backup copies. They are simply files, with contents exactly like the originals, in a directory tree structure that simulates the original tree.

Some backup copies are not in the same format as the original files, and must be restored using Continuous Data Protection for Files:

- Backup copies stored on the IBM Tivoli Storage Manager server
- Backup copies that were encrypted
- Backup copies that were compressed
- Large files that were backed up with sub-file copy. In the storage area, the sub-file copies have -FPdelta file name suffix
- Versioned bit map backups. In the storage area, these backup copies have -TPdelta file name suffix

Versioning of Backup Copies

As you change a file, Continuous Data Protection for Files keeps backup copies of each version of the original file.

To track versions of a file, Continuous Data Protection for Files adds a version suffix to the file name of the backup copy. On the local storage area, all backup copies contain a version suffix. On the remote storage area, all backup copies except the most recent backup copy contain a version suffix. When a file is deleted on your computer, Continuous Data Protection for Files adds a version identifier to the file name of the most recent backup copy on the remote storage area.

The version suffix is “-FP” followed by a number. For example, a file named data.xls could be stored as versioned backup copy data.xls-FP1168376676.xls.

The most recent backup copy of a file is the “active” backup copy. Older backup copies of that file are “inactive” backup copies. If storage space is approaching the limit, Continuous Data Protection for Files will delete inactive backup copies of a file before deleting active backup copies.



NOTE Backup copies that were created by scheduled backup will not be deleted in this way. Scheduled backup files must be deleted manually.

A file that is protected by schedule could change several times during the schedule interval. Only the last version of the file prior to the end of the schedule will be backed up. A continuously protected file (one that is protected, but not protected by schedule) is backed up after every change.

Continuous Data Protection for Files keeps as many versions of a file on local storage as you configure in the *Versions to keep* field of the *General* page of the Settings Notebook, and as space allows.

Continuous Data Protection for Files keeps as many versions of a file on remote storage as you configure in the *Versions to keep* field of the *Remote Storage* page of the Settings Notebook, and as space allows.

Modifying Backup Copies

You can modify the contents of backup copies with native file system tools. Continuous Data Protection for Files is able to restore with backup copies that you have modified.

You can move directories around within the backup area's top level directory. If you move backup copies, Continuous Data Protection for Files will have no record of their original location. If you move inactive backup copies, Continuous Data Protection for Files will not delete them when the backup area reaches the size limit. However, Continuous Data Protection for Files will subtract the file size from its calculated total for the storage area. This could result in Continuous Data Protection for Files allowing the backup area size to exceed the configured limit by the size of the files that have been moved.

Central Management Considerations

This chapter describes how to centrally manage Continuous Data Protection for Files clients.



NOTE The Central Management feature is available with PC Edition and Server Edition.

Configuring Manageable Clients

Continuous Data Protection for Files has features that allow an administrator to manage the configuration of other Continuous Data Protection for Files clients. You can manage the installed product level and configuration of other Continuous Data Protection for Files clients. The administrator can also monitor the activity reports of the other clients. To use the central management features, you must configure your Continuous Data Protection for Files clients to work together.

Several features allow central management:

Continuous Data Protection for Files clients pull upgrade and configuration information After Continuous Data Protection for Files is installed, you can update the product level and configuration by putting the installer and configuration file in the appropriate downloads folder for the consuming clients. See **“Advanced Installation,”** on page 28 for details on silent installation.

An executable pushes product installation to other computers The product includes an executable that will push Continuous Data Protection for Files to other computers. You can push a configuration at the time of the installation. See **“FpPushInst.exe (Push Install Command),”** on page 33 for details.

You can configure the folders that Continuous Data Protection for Files clients use to share configuration data You can configure the downloads and reports folders of the managed clients, and the central administration folder of the managing client. You must configure each so that so that the managed clients consume the configuration and information exported by the managing client. The same configuration allows the managing client to view the activity reports of the managed clients. You can change the administration folder of the managing client to communicate with different groups of managed clients. See **“Administration Folders,” on page 112** for details about the central administration folder, and the downloads and reports sub-folders.

An Example Configuration

The key to configuring the clients to be managed is in defining the central administration folders. Let's assume that there is one managing (administrator) client and two groups of clients to be managed.

In this example, the managed clients in group A do not explicitly configure the Central administration folder: field in the Central Administration Settings window, so their central administration folder defaults to the \RealTimeBackup\ folder on the remote storage location. Both computers have the same central administration folder.

Further, this example assumes that the managed clients in group B have different remote storage locations (or, in one case, no remote storage). Two clients with different remote storage locations would have different default central administration folders, and one client without remote storage would have no central administration folder. These three could not be managed as a group unless they have a common central administration folder. You want to manage them as a group, so you must specify a common central administration folder. Configure a common central administration folder in the *Central administration folder:* field in the *Central Administration Settings* window.

The configurations of the clients are illustrated by the following table.

Central Administration folder configurations for managing clients

Computer Name	Group	Remote storage location (configured in Settings Notebook, Remote Storage page)	Central Administration Settings window, Central administration folder: field value	The settings in the two columns to the left yield the central administration folder
BrightStar	Administrator	Not applicable for managing other clients		
Mercury	Managed group A	\\MyServer\ MyShare\	Not configured	\\MyServer\ MyShare\ RealTimeBackup
Venus	Managed group A	\\MyServer\ MyShare\	Not configured	\\MyServer\ MyShare\ RealTimeBackup
Neptune	Managed group B	\\SpaceMan\ CDPstorage\	\\SpaceMan\ CDPadmin\	\\SpaceMan\ CDPadmin\
Uranus	Managed group B	https://MyISP.com/ MyAcct	\\SpaceMan\ CDPadmin\	\\SpaceMan\ CDPadmin\
Pluto	Managed group B	Not configured	\\SpaceMan\ CDPadmin\	\\SpaceMan\ CDPadmin\

Managing a Group

When you want to manage group A, configure BrightStar’s central administration folder to be the same as the central administration folder for group A.

BrightStar Central Administration folder for managing group A

Computer Name	Group	Remote storage location (configured in Settings Notebook, Remote Storage page)	Central Administration Settings window, Central administration folder: field value	The settings in the two columns to the left yield the central administration folder
BrightStar	Administrator	Not applicable for managing other clients	\\MyServer\ MyShare\ RealTimeBackup	\\MyServer\ MyShare\ RealTimeBackup

For example, to manage the configuration of the clients in group A, do the following:

- STEP 1** Use the *Settings Notebook* to update the configuration of BrightStar. Configure the values that you want to export to group A.
- STEP 2** Click **Apply** on any page of the *Settings Notebook*.
- STEP 3** Open the *Central Administration Settings* window.
- STEP 4** In the Central administration folder: enter (or browse for) \\MyServer\MyShare\RealTimeBackup.
- STEP 5** Click **OK**. The window will close.
- STEP 6** Open the *Central Administration Settings* window again.
- STEP 7** Check the **Publish this computer’s settings as the configuration template for other computers to use** option.

At this point, consider if you want BrightStar to operate with this configuration, or if you want to return to the Settings Notebook and restore BrightStar’s previous configuration.

When you want to manage group B, configure BrightStar’s central administration folder to be the same as the central administration folder for group B.

BrightStar Central Administration folder for managing group B

Computer Name	Group	Remote storage location (configured in Settings Notebook, Remote Storage page)	Central Administration Settings window, Central administration folder: field value	The settings in the two columns to the left yield the central administration folder
BrightStar	Administrator	Not applicable for managing other clients	\\MyServer\ MyShare\ RealTimeBackup\ Mercury\	\\MyServer\ MyShare\ RealTimeBackup\ Mercury\

For example, to view the backup reports of the clients in group B, do the following:

1. Open the *Central Administration Settings* window.
2. In the Central administration folder: enter (or browse for) **\\SpaceMan\CDPadmin**.
3. Click **OK**. The window will close.
4. Open the *Central Administration Settings* window again.
5. Click the **View Report** link. The remote storage reports table will open. The remote storage reports table gives a summary of scheduled backup activity for the group B computers.

At this point, consider if you want BrightStar to operate with this central administration folder, or if you want to restore BrightStar’s previous central administration folder.

Managing a Single Client in a Group

When you want to manage Mercury, configure BrightStar’s central administration folder to be the same as the central administration sub-folder that is unique for Mercury.

BrightStar Central Administration folder for managing Mercury

Computer Name	Group	Remote storage location (configured in Settings Notebook, Remote Storage page)	Central Administration Settings window, Central administration folder: field value	The settings in the two columns to the left yield the central administration folder
BrightStar	Administrator	Not applicable for managing other clients	\\SpaceMan\CDPadmin\	\\SpaceMan\CDPadmin\

For example, to manage the configuration of the client on Mercury, do the following:

- STEP 1** Use the *Settings Notebook* to update the configuration of BrightStar. Configure the values that you want to export to Mercury.
- STEP 2** Click **Apply** on any page of the *Settings Notebook*.
- STEP 3** Open the *Central Administration Settings* window.
- STEP 4** In the Central administration folder: enter (or browse) **\\MyServer\MyShare\RealTimeBackup\Mercury**
- STEP 5** Click **OK**. The window will close.
- STEP 6** Open the *Central Administration Settings* window again.
- STEP 7** Check the **Publish this computer’s settings as the configuration template for other computers to use** option.

At this point, consider if you want BrightStar to operate with this configuration, or if you want to return to the Settings Notebook and restore BrightStar’s previous configuration.

Managing Clients Using Native File System Tools

The examples above assume that you use the Continuous Data Protection for Files feature (Publish this computer’s settings as the configuration template for other computers to use) to distribute configurations to the managed clients. You can also use native file system tools to distribute configuration files to the managed clients. You can use native file system tools to copy a configuration file to the downloads folder for a single client or for a group of clients. Assume that the managed clients have been configured as above, so that they may be managed individually or managed as a group. The table below indicates the appropriate downloads folder for configuring the group or the individual computer.

Computer Name	Group	Copy a configuration file to this folder to manage the group	Copy a configuration file to this folder to manage the individual computer
BrightStar	Administrator	Not applicable for the administrator computer	
Mercury	Managed group A	\\MyServer\MyShare\RealTimeBackup\BackupAdmin\Downloads	\\MyServer\MyShare\RealTimeBackup\Mercury\BackupAdmin\Downloads
Venus	Managed group A		\\MyServer\MyShare\RealTimeBackup\Venus\BackupAdmin\Downloads
Neptune	Managed group B	\\SpaceMan\CDPadmin\BackupAdmin\Downloads	\\SpaceMan\CDPadmin\Neptune\BackupAdmin\Downloads
Uranus	Managed group B		\\SpaceMan\CDPadmin\Uranus\BackupAdmin\Downloads
Pluto	Managed group B		\\SpaceMan\CDPadmin\Pluto\BackupAdmin\Downloads

Administration Folders

Continuous Data Protection for Files uses special folders to manage configuration settings and product level. Continuous Data Protection for Files clients consume configuration information and new product code from these folders. Continuous Data Protection for Files clients store their status reports on these folders, and can push their configuration information to these folders for other clients to consume.

The central administration folder is specified in the *Central Administration Folder:* field in the *Central Administration Settings* window. If the *Central Administration Folder:* field is not configured, then the central administration folder defaults to the `\RealTimeBackup\` folder in the remote storage area. If neither the *Central Administration Folder:* field nor a remote storage area is configured, then there is no central administration folder.



NOTE There is no central administration folder on IBM Tivoli Storage Manager server remote storage. If you use IBM Tivoli Storage Manager server remote storage and you want to use central administration folders, you must configure the *Central Administration Folder:* field in the *Central Administration Settings* window.

The central administration folder contains two levels of administrative sub-folders.

Group administrative sub-folders These folders apply to all computers that share this central administration folder.

Computer-specific sub-folders These folders apply to only 1 computer.

In each level of administrative sub-folders, there are two folders:

The Reports folder Continuous Data Protection for Files stores status reports in the Reports folder. You can view the reports in the graphical user interface. The full path is `<central administration folder>\BackupAdmin\Reports\`.

The Downloads folder When you put product upgrades or configuration files in this folder, Continuous Data Protection for Files will automatically adopt the product upgrades or configuration. For more information about this process, see [“Upgrade Silently: Pull Upgrades and Configurations,” on page 31](#). The full path is `<central administration folder>\BackupAdmin\Downloads\`.



NOTE The consuming computers must have read access to the administration folders.

Example of Administration Subfolder Names

Here is an example of administration subfolder names, given two specifications of the central administration folder. In one column, assume that the central administration folder is configured in the *Central Administration Folder:* field in the *Central Administration Settings* window as \\MyServer\MyShare\CDPadmin\. In another column, assume that the central administration folder is not configured in the *Central Administration Folder:* field in the *Central Administration Settings* window, but defaults to the remote storage location. Assume that the remote storage location is configured as \\MyServer\MyShare\. For both specifications, assume that your computer name is Computer1.

Central Administration Folder Names

	Central Administration area is configured in the Central administration folder: field in the Central Administration Settings window as \\MyServer\MyShare\CDPadmin\	Central Administration area is not configured in the Central administration folder: field in the Central Administration Settings window, but defaults to a subfolder of the remote storage location: \\MyServer\MyShare\
Central administration folder	\\MyServer\MyShare\CDPadmin\	\\MyServer\MyShare\RealTimeBackup\
Reports folder name for single computer:	\\MyServer\MyShare\CDPadmin\BackupAdmin\Reports\	\\MyServer\MyShare\RealTimeBackup\Computer1\BackupAdmin\Reports\
Reports folder name for all computers that share the central administration folder:	\\MyServer\MyShare\CDPadmin\BackupAdmin\Reports\	\\MyServer\MyShare\RealTimeBackup\BackupAdmin\Reports\
Downloads folder name for single computer:	\\MyServer\MyShare\CDPadmin\BackupAdmin\Downloads\	\\MyServer\MyShare\RealTimeBackup\Computer1\BackupAdmin\Downloads\
Downloads folder name for all computers that share the central administration folder:	\\MyServer\MyShare\CDPadmin\BackupAdmin\Downloads\	\\MyServer\MyShare\RealTimeBackup\BackupAdmin\Downloads\

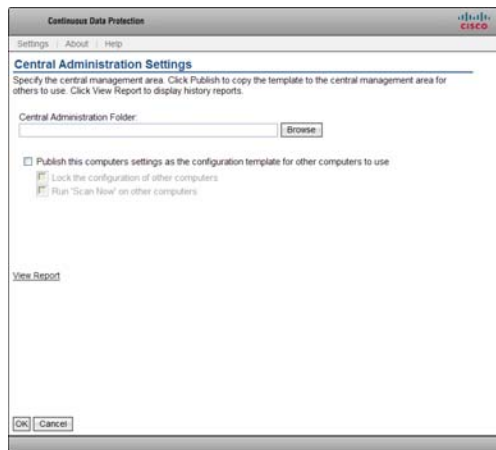
Central Administration Settings Window

Use the *Central Administration Settings* window to identify administration folders for this computer, and to manage the configuration settings on other computers.



NOTE The Central Management feature is available with PC Edition and Server Edition.

Figure 65 Central Administration Folder field



Type or browse for a folder that will be the central administration folder for this computer. The administrative tasks on the *Central Administration Settings* window are limited to only those computers that are centrally managed from this folder. If you type the name of a folder that does not exist, Continuous Data Protection for Files will create the folder.

The central administration folder is used for several purposes. You can change the folder depending on your purpose. See a discussion of central administration folder uses in [“Administration Folders,” on page 112](#).

Publishing a Configuration Template

When managing Continuous Data Protection for Files on a group of computers, it is customary to configure one computer as the template for all computers in the group. If you have configured other computers to share the central administration folder of this computer, they can be centrally managed by this computer.

Check this box to use this computer's settings to configure the other computers. When you click **OK**, this computer's configuration settings file will be copied to the downloads subfolder of the central administration folder that is shared by the group of computers. All computers that share the central administration folder will adopt the *Continuous Data Protection for Files* settings that you publish.

If you publish this computer's settings, your management of the group can be further extended:

Lock the configuration of other computers Check this box to prevent any of the centrally managed computers from changing their settings.



NOTE If you will be using the published configuration file to push installation to another computer, all Continuous Data Protection for Files clients that share the central administration folder with the new client will be prevented from updating their configurations.

:Run "Scan Now" on other computers When you change a configuration to protect files and folders that were not previously protected, you should back up all files, see **"When to Back Up All Files," on page 55**. Check this box to force the centrally managed computers to back up all protected files.



NOTE Publishing to managed computers a configuration file with this setting can put a large burden on the network and the computing resources of the managed computers.



NOTE If you will use the published configuration file to push installation to another computer, do not check this box. If you use this configuration setting in a push install, the push-installed Continuous Data Protection for Files client will create backup copies in the system context. When you later run Continuous Data Protection for Files in the user context, you can have problems restoring these files.

View Report

Click the **View Report** link to display a table of scheduled backup reports for the computers that are centrally managed.

Protecting a Server

Consider the following issues when you protect a server.

Managing a Server That Stores Backup Files

If you are protecting a server that contains remote storage areas for several Continuous Data Protection for Files clients, you can avoid protecting all versioned backup copies. Because all versioned backup copies on a remote storage area contain an -FP suffix, you can exclude versioned backup copies from protection by excluding -FP. This way you will protect only the most recent backup copies.

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

Run Continuous Data Protection for Files as a Service

If Continuous Data Protection for Files runs on a server, it needs to run as a service instead of as a logged-in application. The product provides this capability.

In the Continuous Data Protection for Files install directory there is a program called FpForServers.js. If you invoke this exec, Continuous Data Protection for Files runs as a service instead of as a logged-in application.

The default account for services on Microsoft Windows has no privilege for accessing folders shared via a network. The FpForServers.js exec launches the Microsoft Windows services configuration panel so that you may update the FilePathSrv service. Specify a valid account name and password that can access your remote backup locations. It is recommended that this account have full permissions, and read/write permissions as a minimum.

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



NOTE

Continuous Data Protection for Files installation directory and tree allows full access by all users on the system during installation. This feature ensures that non-privileged users (users without administration rights) can still be protected by the software and use the GUI. This is probably not a desirable setting for multi-user file servers. This is also not desirable because on the installation tree there are log files and programs whose contents and use should not be available to all users. Consider setting more restrictive ACLs on the installation directory and tree.

Problem Determination Guide

This section contains some common problems and suggested solutions. More assistance with problem determination is available via technical notes online. The technical notes are updated as issues arise, throughout the life of the product.

Files Are Not Backed Up

Files can fail backup for several reasons. Some common reasons are discussed below.

Storage for Backup Copies Has Not Been Correctly Specified

If the area to store backup copies of your protected files is not properly specified, Continuous Data Protection for Files can not back up files.

Verify that you have correctly specified local or remote storage areas in the *Settings Notebook*. Local storage and which location (local or remote) is specified in **“General,” on page 40** of the *Settings Notebook*. Remote storage is specified in **“Remote Storage,” on page 58**.

Files to Protect are Incorrectly Specified

The files that Continuous Data Protection for Files protects are configurable. If you have configured your list of protected files incorrectly, Continuous Data Protection for Files does not back up the files. Continuous Data Protection for Files backs up only those files that are configured for protection. The list of continuously protected files is configured in **“Files to Protect,” on page 43** of the *Settings Notebook*. Note that exclusions from protection have priority over inclusions. If an application or file path is explicitly included for protection, verify that no list items exclude the file from protection. See **“Including and Excluding Files from Protection,” on page 45**.

Files are not Backed Up to IBM Tivoli Storage Manager Server

These topics discuss problems backing up files to the IBM Tivoli Storage Manager server.

IBM Tivoli Storage Manager Node Name Does Not Match Hostname

Continuous Data Protection for Files uses the IBM Tivoli Storage Manager API. By default, the IBM Tivoli Storage Manager API uses the client's hostname as the IBM Tivoli Storage Manager node name when identifying itself to the IBM Tivoli Storage Manager server.

If the node name differs from the Continuous Data Protection for Files client's hostname, the backup to the IBM Tivoli Storage Manager server fails. The Continuous Data Protection for Files cannot identify itself properly to the IBM Tivoli Storage Manager server.

The following error message may be displayed:

```
FilePath ERROR ANS1353E (RC53) Session rejected: Unknown or incorrect ID
entered node:<node name> rc=53 reason=65535 tsm_init_api_session tsmInitEx
failed
```

When a backup failure occurs for this reason, you must configure the IBM Tivoli Storage Manager API to use the appropriate node name when logging on to the IBM Tivoli Storage Manager server. You can correct this problem by doing the following:

STEP 1 Edit the `dsm.opt` file. This file can be in one of three places, depending on the type of installation:

- New installation Continuous Data Protection for Files on Windows XP:

*C:\Documents and Settings\All Users\Application
Data\Cisco\CDP_for_Files*



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

- New installation on Windows Vista:

C:\Program Data\Cisco\CDP_for_Files



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

STEP 2 Add the node name to the **dsm.opt** file. To do this, go to the end of the file, and on a new line add the NODENAME parameter followed by the node name. For example:
NODENAME TSMclientnode1

STEP 3 Save the **dsm.opt** file.

The next time Continuous Data Protection for Files connects to the IBM Tivoli Storage Manager server, it uses the node name you specified. Continuous Data Protection for Files prompts you for the password, if necessary.

IBM Tivoli Storage Manager Client Node Lacks Authority to Delete Backup Copies

If Continuous Data Protection for Files does not have delete backup permission on the IBM Tivoli Storage Manager server, it cannot successfully purge older files when the designated storage space is getting full.

The following error is displayed in the replication.log file:

```
FilePath ERROR ANS1126E (RC27)
```

The file space cannot be deleted because this node does not have permission to delete archived or backed up data.

The following error is displayed in a popup window:

Target file system can only handle sequential I/Os.

Remote backup can be suspended because the backup storage space cannot be purged to make room for new files.

Continuous Data Protection for Files requires permission to manage space on the IBM Tivoli Storage Manager server and to create file versions. The registered node which is used by the Continuous Data Protection for Files client to access the IBM Tivoli Storage Manager server must have the permission to delete the backups it creates. This function is required when Continuous Data Protection for Files needs to purge files when the backup storage space is full.

Enable permission to delete backup copies for the IBM Tivoli Storage Manager Enterprise server as below. This sample assumes node name of TSMclientnode1; replace the node name appropriately when you enter the command:

-
- STEP 1** Log into the IBM Tivoli Storage Manager server and bring up the IBM Tivoli Storage Manager administrative command line.
- STEP 2** Enter this command to the IBM Tivoli Storage Manager server: **update node TSMclientnode1 backdel=y**.

Enable permission to delete backup copies for IBM Tivoli Storage Manager Express server as follows:

-
- STEP 1** Open the DOS command prompt.
- STEP 2** Enter this command: **cd "C:\Program Files\Cisco\TSM\server"**.
- STEP 3** Enter this command: **net stop "TSM Express Backup Server"**.
- STEP 4** Enter this command: **dsmserv.exe**.
- STEP 5** Enter this command to the IBM Tivoli Storage Manager server: **update node TSMclientnode1 backdel=y**.
- STEP 6** Enter this command to the IBM Tivoli Storage Manager server: **halt**.
- STEP 7** At the DOS command prompt, restart the Express server by entering this command: **net start "TSM Express Backup Server"**.

Non-System Accounts Do Not Have Appropriate User Security Rights to Use IBM Tivoli Storage Manager

In order to back up files to an IBM Tivoli Storage Manager server, the proper user security rights must be given to the non-system user account to use the IBM Tivoli Storage Manager client. Any non-system account (local or domain) must have the following rights:

- Back up files and directories
- Restore files and directories
- Manage auditing and security logs

If a non-system account does not have appropriate user security rights, and Continuous Data Protection for Files is configured to back up files to the IBM Tivoli Storage Manager server, files modified by the non-system account are not backed up.

User Interface Contains No File Data

If the Continuous Data Protection for Files daemon is not running, or if your browser is in offline mode, the Continuous Data Protection for Files user interface contains no file data. This condition is accompanied by an error message which begins like this: FPA_getNamedObject: Could not find:. There are two possible causes for this problem.

- **Your browser is offline** Your browser must be in online mode to see file data. Internet Explorer and Firefox browsers are turned on- or off- line by checking or unchecking **File > Work Offline** from the browser menu. Confirm that this menu item is not checked.
- **The Continuous Data Protection for Files daemon is not running** To determine if the Continuous Data Protection for Files daemon is running, and restart if necessary, see [“Restart Continuous Data Protection for Files Daemon,” on page 124](#) below.

Restart Continuous Data Protection for Files Daemon

To determine if the Continuous Data Protection for Files daemon is running, look for the FilePathSrv.exe process in Task Manager. If you cannot see this process, the daemon is not running. To restart the daemon on a DOS command line, do the following:

-
- STEP 1** Open a DOS command prompt.
 - STEP 2** Navigate to the Continuous Data Protection for Files installation folder. The default installation folder is: C:\Program Files\Cisco\CDP_for_Files.
 - STEP 3** Type the following:

filepathsrv -d

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

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

The Number of Backup Copy Versions is Greater than Configured

The number of backup copy versions exceeds the *How many versions to keep* configuration setting.

The problem occurs when versions are not tracked properly.

The problem can occur because data folders were not removed between an uninstall and a new install. The new install does not have a record of the backup copies created from the previous install and use of the product. This can occur on local storage, remote storage, or both. For a list of folders to remove after uninstall, and before installing again, see [“Installing After Uninstallation,” on page 32](#).

The problem can also be caused, on remote storage only, because of changes to the encryption or compression settings.

When encryption or compression settings are turned on or off, the versions counter is reset to 0, even if some backup copies exist. This behavior results because Continuous Data Protection for Files tracks file versions without encryption/compression differently than file versions with encryption/compression.

As an example, assume that a file file.txt is continuously protected, and has reached its five-version limit (five is the default version limit). The backup copies were neither encrypted nor compressed. The user then enables compression. Continuous Data Protection for Files then creates up to five new backup copy versions of the file. The restore view will show five versions of the file having name file.txt (corresponding to the original five versions backed up without compression), and five versions of the file named file.txt.cdp (corresponding to the new five versions backed up with compression enabled).