IBM Spectrum Protect for Workstations
Version 8 Release 1

Client Installation and User's Guide

IBM Spectrum Protect for Workstations
Version 8 Release 1

Client Installation and User's Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 97.

This edition applies to Version 8 release 1 modification 0 of IBM Spectrum Protect for Workstations (product number 5725-X12) and to all subsequent releases and modification until otherwise indicated in new editions.

Contents

About this publication v
Who should read this publication v
Publications v
New for the client v

Chapter 1. Product overview 1
Product overview for the IBM Spectrum Protect for Workstations client 1
Types of protection 2
Administration folders 3

Chapter 2. Installing the IBM Spectrum Protect for Workstations client 7
Basic installation of the IBM Spectrum Protect for Workstations client 7
System requirements. 7
Installing the IBM Spectrum Protect for Workstations client 7
Uninstalling the IBM Spectrum Protect for Workstations client 18
Advanced installation of the client. 19
Install the IBM Spectrum Protect for Workstations client silently on a single local computer. . . . 19
Upgrade the IBM Spectrum Protect for Workstations client silently 21
Methods of deploying the client to other computers 23
Windows installation folder 23

Chapter 3. Changing protection settings 25
Settings Notebook 25
General panel of client Settings Notebook . . . 26
Files to Protect panel of client Settings Notebook 28
Email Protection panel of the client Settings Notebook 35
Remote Storage panel of client Settings Notebook 36
Expiration panel of client Settings Notebook . . 41
Advanced panel of client Settings Notebook . . 41
Changing protection settings for the client 45
Specifying which files and applications are protected by IBM Spectrum Protect for Workstations 45
Specifying storage for backup copies by IBM Spectrum Protect for Workstations. 49
Backup features 50

Chapter 4. Starting and stopping protection activity of the IBM Spectrum Protect for Workstations client 51
Methods to start the client GUI. 51
Starting and stopping client backups 51
When to back up all files 52
Backing up all files that are protected by IBM Spectrum Protect for Workstations. 53
Forcing a scheduled backup by IBM Spectrum Protect for Workstations 53
Stopping backup or restore activity by IBM Spectrum Protect for Workstations. 54
Restarting the client process 54
Run the IBM Spectrum Protect for Workstations client as a service 55

Chapter 5. Monitoring the protection state. 57
Monitoring protection with the IBM Spectrum Protect for Workstations client 58
Status panel of IBM Spectrum Protect for Workstations 60
Viewing reports by IBM Spectrum Protect for Workstations 62
Viewing the continuous protection activity report of a IBM Spectrum Protect for Workstations client 62

Chapter 6. Restoring files with the IBM Spectrum Protect for Workstations client 63
Restore Wizard of IBM Spectrum Protect for Workstations 63
Welcome panel (Restore Wizard) of IBM Spectrum Protect for Workstations. 63
Files to Restore page of IBM Spectrum Protect for Workstations 64
Restore Location panel of IBM Spectrum Protect for Workstations. 65
Restore wizard **Summary** panel 66

Chapter 7. Storage areas of IBM Spectrum Protect for Workstations . . 67
Format of backup copies 67
Version format of backup copies created by IBM Spectrum Protect for Workstations. 67
Tools restriction for modifying backup copies . . . 68

Chapter 8. Troubleshooting the IBM Spectrum Protect for Workstations client 69
Files are not backed up by IBM Spectrum Protect for Workstations 69
Storage for backup copies is not correctly configured in IBM Spectrum Protect for Workstations 69
Files to protect are incorrectly configured in IBM Spectrum Protect for Workstations. 69
Files in use are not backed up by IBM Spectrum Protect for Workstations 69

Files are not backed up to IBM Spectrum Protect server 70
IBM Spectrum Protect for Workstations user interface replaces existing browser session 72
IBM Spectrum Protect for Workstations user interface contains no file data 72
Restarting the client process 72
The number of backup copy versions is greater than configured in IBM Spectrum Protect for Workstations 73
Limit user access to files on a target file server . . 74
Restoring many files from a single directory IBM Spectrum Protect for Workstations 76
Backup fails after configuration because of insufficient IPV6 permissions 76
Frequently Asked Questions 76

Appendix A. Messages issued by IBM Spectrum Protect for Workstations . . 79
Format of messages issued by IBM Spectrum Protect for Workstations 79
Messages issued by the Central Administration Console. 79
Messages issued by the IBM Spectrum Protect for Workstations client 83

Appendix B. Accessibility features for IBM Spectrum Protect for Workstations 95

Notices 97

Glossary 101
A 101
B 103
C 104
D 105
E 107
F 108
G 108
H 109
I. 110
J. 110
K 110
L 111
M 112
N 113
O 114
P 114
Q 115
R 116
S 117
T 120
U 120
V 121
W 122

Index 123

About this publication

This publication contains information about how to install and use IBM® Spectrum Protect for Workstations on client systems. To administer activity on client systems, you must also install the IBM Spectrum Protect™ for Workstations Central Administration Console on an administrator system. This publication does not contain information about how to install and use the Central Administration Console. For information about setting up the Central Administration Console, see *IBM Spectrum Protect for Workstations Central Administration Console Installation and User's Guide*.

Who should read this publication

This publication is intended for users of IBM Spectrum Protect for Workstations clients.

Publications

The IBM Spectrum Protect for Workstations product family includes IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for databases, and several other storage management products from IBM.

For more IBM product documentation, see http://www.ibm.com/support/knowledgecenter.

You can view or download PDF versions of IBM publications from the IBM Publications Center (http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss).

New for the client

IBM Spectrum Protect for Workstations is updated for version 8.1.0 and includes new enhancements and features for the client.

Changes since the previous edition are marked with a vertical bar (|) in the left margin. Ensure that you are using the correct edition for the level of the product.

New Help system
Product integrated Help for the client is now created by using Eclipse tools. The Help system runs on all modern browsers.

Block level backups
IBM Spectrum Protect for Workstations backs up the email files with a new block level backup strategy. This feature reduces the number of full backups.

Chapter 1. Product overview

This release of IBM Spectrum Protect for Workstations provides several enhancements for monitoring and administering client systems.

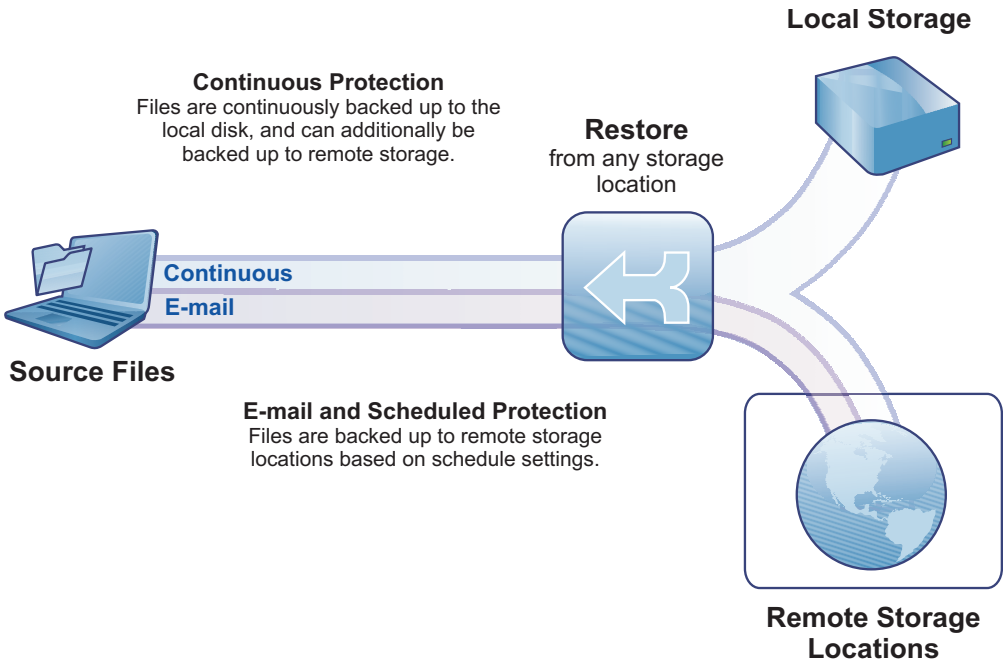
Product overview for the IBM Spectrum Protect for Workstations client

The IBM Spectrum Protect for Workstations client provides a flexible, easy to use file protection system. Your most important files can be continuously protected. Your less important files can be protected at scheduled intervals to save time and storage space. Email files can also be protected. You can also prevent any changes, including deletions, to files in folders that you designate as vaults.

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

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

This diagram provides an overview of how the IBM Spectrum Protect for Workstations client protects your data.



After installation of an IBM Spectrum Protect for Workstations client, the client immediately provides continuous protection for a pre-configured list of files. You can see the backup copies in the `\RealTimeBackup\` folder in the root of your primary drive. The backup copies can also be seen in the list of files that you can restore with the Restore Wizard of the client. The default space that is 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, by using the client or the Central Administration Console.

IBM Spectrum Protect for Workstations can store backup copies on an IBM Spectrum Protect server, but there is no requirement to use IBM Spectrum Protect. IBM Spectrum Protect for Workstations is a stand-alone product and has no dependencies on IBM Spectrum Protect or Spectrum Protect Snapshot.

Types of protection

The IBM Spectrum Protect for Workstations client offers three types of protection for your files: continuous protection, scheduled protection, and vaulting.

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

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

Email files are protected on a schedule.

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

Table 1. Comparison of the three types of protection

Type of Protection	Continuous Protection	Scheduled Protection (includes email)	Vaulting
Advised for what files	Advised for your most important files. Not advised for large dynamic files like email files.	Advised for large, dynamic files like email.	Advised for files that you do not want to be changed nor deleted.
How protected	Backup copies are created on storage areas.	Backup copies are created on a storage area.	Vaulted files and folders cannot be modified nor deleted.
Frequency of backups	File is backed up whenever it is saved.	File is backed up only at the scheduled time, and only if it was saved since the previous schedule.	No backups

Table 1. Comparison of the three types of protection (continued)

Type of Protection	Continuous Protection	Scheduled Protection (includes email)	Vaulting
Backup copy storage area	Local or remote	Remote only	Not applicable
Files protected	Files selected in the **Folders and Files** and **Applications** boxes in the **Files to Protect** panel in the Settings Notebook of the client. Files selected in the **Protected Folders and Files** field in the **Files to Protect** panel in the **Groups Configuration** notebook of the Central Administration Console.	Files selected in the **E-mail Protection** panel and by the **Scheduled Backup Settings** link in the **Advanced** panel in the Settings Notebook of the client. Files selected in the **E-mail Protection** panel of the **Groups Configuration** notebook of the Central Administration Console.	Files selected in the **Vault** box in the **Files to Protect** panel of the Settings Notebook of the client. Files selected in the **Vault** box in the **Protected Folders and Files** panel in the **Groups Configuration** notebook of the Central Administration Console.

For more information about scheduled backup, see "What to consider before you set up scheduled backups" on page 43.

Administration folders

Clients gather configuration information, commands, and software updates from administration folders. The Central Administration Console manages clients by sharing information with clients in administration folders.

Managing clients

When the client and the Central Administration Console access the same administration folder, they exchange information in the administration folder. The client sends reports to the folder. The Central Administration Console collects the reports and presents the information to the administrator. The Central Administration Console pushes software updates, configuration information, and command scripts to the administration folder. The client periodically pulls the updates, configuration, and command scripts.

If the Central Administration Console and a client are not configured to access the same administration folder, the Central Administration Console cannot manage that client.

By default, the Central Administration Console service uses a local system account to log on. A local system account can access administration folders on the Central Administration Console server, but cannot access administration folders on shared drives on other computers. If the clients use administration folders on remote computers, run the Central Administration Console service in an account that has access to the remote administration folders.

Determining administration folders for clients

Clients whose configuration files are created with the Central Administration Console access the administration folder that you identify in the Central Administration Console. The Central Administration Console periodically scans the administration folder for reports from new clients. When the client is installed, the client accesses this administration folder, and the Central Administration Console discovers the client. The Central Administration Console locks the value of the administration folder for the new client.

If a IBM Spectrum Protect for Workstations client is not discovered by the Central Administration Console, you can specify the administration folder with the client. In this case, the administration folder defaults to the `\RealTimeBackup\` subfolder of the remote storage area. When such a client is discovered by the Central Administration Console, the Central Administration Console sets and locks the value of the administration folder.

If a remote storage area is not configured, or if the client uses remote storage on a IBM Spectrum Protect server, there is no default administration folder.

IBM Spectrum Protect for Workstations OEM Edition clients have a **Central Administration Settings** panel that you can use to explicitly configure the administration folder location. If the **Central Administration Folder** field is configured, that value overrides the default administration folder location. The Central Administration Console can discover and manage the following clients:

- Clients that are configured with no remote storage
- Clients that are configured with remote storage on a IBM Spectrum Protect

However, you can change the administration folder to a location that is not known to the Central Administration Console. In this case, the Central Administration Console cannot manage the client.

Standard IBM Spectrum Protect for Workstations clients and Starter Edition clients do not have a **Central Administration Settings** panel where a user can explicitly configure the administration folder location. If these clients use IBM Spectrum Protect server remote storage, there is no administration folder. You can configure an administration folder for such a client only by using the **fpa config-set** command. If you use the **fpa config-set** command to identify a folder that is accessible to the client, the Central Administration Console discovers the client.

The **fpa config-set** command sets the administration folder for any client, even one that was discovered by the Central Administration Console. Start the command from a Command Prompt window at the installation directory, for example:

```
fpa config-set GlobalManagementArea="\\MyServer\MyShare\MyAdminFolder"
```

Replace `\\MyServer\MyShare\MyAdminFolder` with the CIFS (Common Internet File System) URL of a folder that is accessible to the client and the Central Administration Console.

Administration folder subfolders

The administration folder contains two levels of administrative subfolders.

Computer-specific subfolders
These folders apply to only one computer. The Central Administration

Console communicates with clients through the computer-specific subfolders. The following subfolders are in the computer-specific subfolder:

Reports

The client stores status reports in the Reports folder. You can view the reports in the Central Administration Console. The full path of the reports folder is *administration_folder_location**computer_name*\BackupAdmin\Reports\.

Downloads

When you put product upgrades or configuration files in the Downloads folder, the client automatically adopts the product upgrades or configuration. The full path is *administration_folder_location**computer_name*\BackupAdmin\Downloads\.

Group administrative subfolders

These folders apply to all computers that share this administration folder. In each group administrative subfolder, there is a Downloads subfolder. When you put product upgrades or configuration files in the Downloads subfolder, all clients that share this group administrative folder automatically adopt the upgrades or configuration.

Chapter 2. Installing the IBM Spectrum Protect for Workstations client

This chapter contains information for installing and initially configuring the IBM Spectrum Protect for Workstations client.

Basic installation of the IBM Spectrum Protect for Workstations client

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

System requirements

The IBM Spectrum Protect for Workstations client requires a Windows workstation with minimum levels of hardware and software.

For software and hardware requirements, see IBM Spectrum Protect for Workstations Hardware and Software Requirements (http://www.ibm.com/support/docview.wss?uid=swg21643334).

Installing the IBM Spectrum Protect for Workstations client

An InstallShield Wizard helps you to complete an interactive installation of the IBM Spectrum Protect for Workstations client on a single computer.

Before you begin

Ensure that the following conditions are met before you install the client on your computer.

- You must have administrator authority to install the client.
- Your computer must have the necessary hardware and software. For information about system requirements, see "System requirements."
- Before you reinstall or upgrade from a previous version of the client, close all other applications, especially email programs. For information about upgrading from a previous version of the client, see "Conditions for upgrading a client" on page 22.

Procedure

Complete the following steps to interactively install the client on a single computer.

1. Double-click the client installer and click **Run**.
2. Choose your preferred language and click **OK**.
3. In the welcome window of the InstallShield Wizard, click **Next** to begin the software installation.
4. Read the License Agreement, accept the terms of the agreement, and click **Next**.
5. Choose whether to install the following applications and click **Next**.
   - IBM Support Assistant Data Collection tool. This tool is used to collect data that can be provided to the support team.

- IBM Spectrum Protect API Runtime Files. The Application Program Interface (API) is necessary for running backups to a IBM Spectrum Protect server.

6. In the Destination Folder window, accept the default installation location or click **Change** to specify another location. Click **Next**.
7. In the Ready to Install the Program window, ensure that the information is correct and click **Next**.
8. To create a shortcut icon on your desktop for the client, click **Yes**.
9. In the InstallShield Wizard Completed window, click **Finish** to exit the wizard.
10. For first-time installations, a configuration wizard is displayed in your browser. Click **Next** and use the configuration wizard to choose your protection settings.

    For information about the configuration wizard, see "Navigating the Configuration Wizard" on page 9.
11. Click **Finish** to close the configuration wizard in your browser.

    For first-time installations, the client immediately starts protecting your files. In some cases, you must start the system again for the protection settings to take effect. Shut down and start the system again in the following situations:
    - You are reinstalling or upgrading the client.
    - A product that uses the IBM Spectrum Protect API is installed and running. IBM Spectrum Protect Backup-Archive client is such a product.

What to do next

If you upgrade a previous version of the client, you must start the computer again. The new settings become active and file protection continues after the system starts again. If you want to change your protection settings, see "Settings Notebook" on page 25.

Attention: You must configure the server Access Control List (ACL) settings before you can configure multiple clients to back up files to the same remote file server. Complete the configuration tasks that are described in "Limit user access to files on a target file server" on page 74.

Configuring clients by using the configuration wizard

After you install IBM Spectrum Protect for Workstations, you must configure the client. Use the Configuration wizard to step you through the configuration process.

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

Navigating the Configuration Wizard

After you install IBM Spectrum Protect for Workstations, the Configuration Wizard helps you to configure your protection settings.

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

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

- "**What is Critical** page."
- "**Email Protection** page" on page 13.
- "**Remote Storage** page" on page 13.
- "**Initial Backup** page" on page 17.
- "**Summary** page" on page 18.

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

- "**Specify Backup Server** page" on page 17.
- "**Identify the Backup** page" on page 17.
- "**Start Restore Wizard** page" on page 17.
- "**Summary** page" on page 18.

Configuration wizard Welcome page:

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

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

Select Setup Type page:

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

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

What is Critical page:

Specify the files and folders that you want to protect. The specified files and folders and applications will be continuously protected. IBM Spectrum Protect for Workstations creates backup copies on a storage area as soon as the files are changed.

When IBM Spectrum Protect for Workstations is installed, it is preconfigured with a list of files and folders to continuously protect. Use this page to confirm that the initial protection settings are correct for your system, or change the settings as appropriate.

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

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

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

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

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

Folders and Files Settings *page for continuous protection by IBM Spectrum Protect for Workstations:*

Use the Folders and Files Settings page to specify which folders and files to continuously protect by selecting the files to include and exclude.

List of Folders and Files to Include and Exclude

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

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

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

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

The list contains these columns:

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

Type Values in the **Type** column indicate whether the files and folders should be included or excluded from protection. Files and folders that are excluded from continuous and scheduled protection are not protected. Files that are included are protected. Files that are excluded have precedence over files that are included. As a result, any file or folder that matches an exclude pattern are not protected, even if the same file or folder matches an include pattern. (See "Including and excluding files from protection" on page 29).

Note: The Initial Configuration Wizard. However, the Initial Configuration Wizard only allows file additions (of type Include). Any exclude patterns exclude files

from protection as soon as IBM Spectrum Protect for Workstations is installed, but they are hidden from view during installation. Although exclude patterns are exposed in the Settings Notebook, you can specify advanced configuration options.

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

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

Wildcard characters in file specifications:

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

You can enter the complete path of a file that you want to protect. The complete path must match a single file. You can use asterisks and blanks as wildcard characters to specify several files.

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

Apply the following guidelines for using wildcard characters:

- If there are no asterisks, blank spaces are interpreted as asterisks before or after the pattern. For example, `\myDocs\` and `*\myDocs\*` yield the same matches. If there are asterisks in the pattern, blank spaces do not match any characters before or after the pattern. For example, `\myDir\`, `*\myDir\`, and `\myDir\*` can yield three different matches.

  For example, assume a pattern `fish`. This pattern matches the following files and folders:

  - `C:\dir\fish.doc`
  - `C:\fish\anyfile.doc`
  - `c:\Dirfishfood\something`
- If the file specification includes slashes, for example `\fish\`, the specification matches any object with `\fish\` somewhere in the path. For example, this pattern produces the following matches and non-matches:
  - Matches `C:\fish\anyfile.doc`
  - Does not match `C:\dir\fish.doc`
  - Does not match `c:\Dirfishfood\something`

The following table provides examples of how patterns match files and folders.

Table 2. File and folder pattern matches

Pattern	Matches for folders and files on your computer:

`\myDir\` or
`\mYdiR\` or
`*\myDir\*` or
`*\mydir\*`
	`c:\myDir\`
	`c:\myDir\Contacts\`
	`c:\myDir\Contacts\contacts.txt`
	`c:\Projects\myDir\`
	`c:\Projects\myDir\myThings\`
	`c:\Projects\myDir\myThings\things.doc`
	`c:\Projects\myDir\myThings\myPhoto.jpg`
	`d:\Notes\myDir\`

Table 2. File and folder pattern matches (continued)

Pattern	Matches for folders and files on your computer:

`*\myDir\`	`c:\myDir\`
	`c:\Projects\myDir\`
	`d:\Notes\myDir\`

`d:*\mydir\*`	`d:\Notes\myDir\`

`\my best`	`c:\Books\My Best.doc`
	`c:\Photos.jpg\My Best Photo\`
	`c:\Photos.jpg\My Best Photo\Best.jpg`
	`f:\Projects\My Best Project\`
	`f:\Projects\My Best Project\Dream.xls`

`.jpg`	`c:\Photos.jpg\`
	`c:\Photos.jpg\myHouse.bmp`
	`c:\Photos.jpg\My Best Photo\Best.jpg`
	`c:\Projects\myDir\myThings\myPhoto.jpg`

`*.jpg`	`c:\Photos.jpg\`
	`c:\Photos.jpg\My Best Photo\Best.jpg`
	`c:\Projects\myDir\myThings\myPhoto.jpg`

`E:\` `E:\*`	All files and folders on the E: drive.

Applications *pane of IBM Spectrum Protect for Workstations:*

The **Application** pane lists the applications that are protected.

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

Critical Settings *page:*

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

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

The list of applications has the following views:

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

View Alphabetically
The applications are presented in alphabetical order.

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

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

You can add files to be protected in the **Critical Settings** page, but these applications are protected only if the files are not explicitly excluded. For more information, see "Including and excluding files from protection" on page 29.

Email Protection page:

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

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

Email files are backed up only to remote storage. If the remote storage is not available at the scheduled backup time, IBM Spectrum Protect for Workstations backs up the email files when the remote storage area becomes available.

Email Application list

Select one of the email applications in the list.

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

Email Application Data Folder field

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

How Many Email Versions to Keep field

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

How often to protect your email list

You can schedule email protection at one of several intervals:

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

Remote Storage page:

Use the Remote Storage page of the configuration wizard to specify the remote storage for backups of your protected files.

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. IBM Spectrum Protect for Workstations is tolerant of intermittently available networks. If the remote storage area is temporarily unavailable, IBM Spectrum Protect for Workstations queues backup copies until the remote storage becomes available.

Remote Storage server or device name and location:

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

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

Backup Identifier

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

Location for the External Device or File Server

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

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

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

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

IBM Spectrum Protect for Workstations creates backup copies in a subfolder called `\RealTimeBackup\`*`computer name`*. For example, if a computer name is Computer1, and the remote storage location is configured with the value `\\remote\share`, backup copies are stored in `\\remote\share\RealTimeBackup\Computer1\`.

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

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

WebDAV Server storage location

Some Internet Service Providers (ISPs) provide Web-based Distributed Authoring and Versioning, or WebDAV. With the WebDAV protocol, you can create, change, and move documents on a remote server. The WebDAV protocol is useful for authoring the documents that a web server serves, but can also be used for general web file storage. If your ISP provides WebDAV functions, IBM Spectrum Protect for Workstations 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, IBM Spectrum Protect for Workstations can use the basic authentication method. Because this authentication method sends the password as clear text over the network, the web server is configured to use secure sockets.

IBM Spectrum Protect for Workstations storage location

IBM Spectrum Protect for Workstations can store backup copies on a IBM Spectrum Protect server.

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

You can use IBM Spectrum Protect server version 6.1 or later with IBM Spectrum Protect for Workstations.

Configure the IBM Spectrum Protect server before you connect from IBM Spectrum Protect for Workstations. Register the computer as a IBM Spectrum Protect node. IBM Spectrum Protect for Workstations prompts you for the password for this node in order to connect to the IBM Spectrum Protect server. For more information about registering a IBM Spectrum Protect node for your computer, see *IBM Spectrum Protect for Windows Administrator's Guide*.

If you specify a IBM Spectrum Protect server as the backup target and you want encryption or compression features applied to the backup, you must specify these options in the `dsm.opt` file in the IBM Spectrum Protect for Workstations subfolder of the "Accessing the program data folder" on page 40.

Restriction: You cannot use a subfile backup feature when the IBM Spectrum Protect server is the backup target.

In addition to backing up data directly to a IBM Spectrum Protect server, you can back up data using a two-stage method. First, use IBM Spectrum Protect for Workstations to create remote backups on a file server. Then, schedule a IBM Spectrum Protect backup-archive client on that file server to back up the files to a IBM Spectrum Protect server.

Restriction: If you use IBM Spectrum Protect for Workstations encryption, you cannot use IBM Spectrum Protect compression.

To manage storage space, the IBM Spectrum Protect administrator must grant authority to the IBM Spectrum Protect client node to delete backup copies. For

steps to assign authority to delete backup copies, see the topic in the problem determination section: " IBM Spectrum Protect client node lacks authority to delete backup copies" on page 70.

To avoid problems when using the IBM Spectrum Protect server, see "Files are not backed up to IBM Spectrum Protect server" on page 70.

Remote Storage advanced settings:

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

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

When the storage space becomes full, IBM Spectrum Protect for Workstations deletes older backup copy versions of files that have several backup copy versions. If more space is needed for new backup copies, IBM Spectrum Protect for Workstations deletes backup copies of files to make room for the newest backup copy.

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

Advanced settings

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

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

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

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

Initial Backup page:

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

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

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

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

Specify Backup Server page:

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

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

Identify the Backup page:

You must enter a IBM Spectrum Protect node name and password, or select a backup location from a list of backup identifiers.

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

Start Restore Wizard page:

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

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

Select the **Yes** option to start the Restore wizard when you click **Finish** on the Summary page. The Restore wizard steps you through the process of selecting the files you want to restore, and choosing the location to store the restored files, see "Restore Wizard of IBM Spectrum Protect for Workstations" on page 63. If you decide not to start the restore wizard, you can access it by selecting the Restore icon on the IBM Spectrum Protect for Workstations Status page.

Summary page:

Use the **Summary** page to view the summary information for your configuration of IBM Spectrum Protect for Workstations. When you click **Finish** the configuration is complete.

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

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

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

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

Depending on the configuration chosen, the summary lists:

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

If you cancel the configuration wizard, IBM Spectrum Protect for Workstations continues to run in the background and protect your files using the pre-configured settings.

Uninstalling the IBM Spectrum Protect for Workstations client

Uninstall the IBM Spectrum Protect for Workstations client by using the Windows uninstall feature.

Before you begin

Close the IBM Spectrum Protect for Workstations client before you uninstall the application.

Procedure

1. Click **Start** > **Control Panel**.
2. Click **Uninstall a program**.
3. In the Programs and Features window, choose IBM IBM Spectrum Protect for Workstations and click **Uninstall**.
4. Click **Yes** to start your system again and to remove file system filters.
5. Click **Finish** to exit the uninstall wizard.

Advanced installation of the client

You can use advanced options for installing, upgrading, and configuring the IBM Spectrum Protect for Workstations client. There are several ways to install or upgrade the client without user interaction.

Silent installation on a local computer
You can install the client on your local computer in silent mode. The installer wizard is not displayed if you supply the `fpa.txt` configuration file. Use Notebook settings to configure IBM Spectrum Protect for Workstations when the installation completes. You can either use the configuration wizard or the notebook to configure IBM Spectrum Protect for Workstations.

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

Silent installation that is pushed to a remote computer
Using the silent installation method, you can push the client to remote computers. When the client is installed, product upgrades and configuration information are pulled from the administration folder.

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

Silent installation that is pushed to another computer
An administrator can push the client to other computers.

Install the IBM Spectrum Protect for Workstations client silently on a single local computer

You can install the IBM Spectrum Protect for Workstations client on your local computer silently. In a silent installation, you do not interact with the installation wizard. If you provide a configuration file, you do not interact with the client initial configuration wizard.

To install the client silently, you must complete the following actions:

- Start the installer with appropriate parameters.
- Optionally, you can provide a configuration file for the client. You can generate a configuration file with the Central Administration Console. For information about how to create a configuration file, see the *IBM Spectrum Protect for Workstations Central Administration Console Installation and User's Guide*. If you do not provide a configuration file, the initial configuration wizard starts after installation.

Silent installation command for the IBM Spectrum Protect for Workstations client

You can use the /S parameter in the installation command to silently install the IBM Spectrum Protect for Workstations client.

The client installer is an executable file with a name similar to 8.1.0-IBM-SP4WKSTNS-*EDITION*-x86_windows.exe.

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

Parameters

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

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

/v Specifies whether to pass options that can be used by the Windows Installer to the MSI package. Do not insert a space between the parameter /v and the options list. You must enclose the options list in quotation marks if there are blank spaces in the options list. The following options are applicable:

/qn Specifies that everything except setup.exe is silent.

/l*v log file path
Specifies a file to log the installation activities.

CUSTOM_CONFIG_FILES_PATH=configuration file path
Specifies the path to the directory where the configuration files are stored. The configuration files include fpa.txt, dsm.opt, networks.xml, and machinename.txt.

DONT_LAUNCH_FILEPATHSRV=1
This option is required in the following cases:

- The client installation is pushed down to the computer.
- The client is installed by a user other than the user that the application is intended for.

For example, an administrator can use this option to install the software for another user.

INSTALLDIR=*folder*

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

Restriction: You cannot specify the root folder of a drive. For example, you cannot specify C:\.

REBOOT=ReallySuppress
Specifies to suppress system start after installation. This option is useful when you are pushing installation to a remote computer, because a system start after installation can be disruptive to users on the remote system. Do not use this option for a local installation when a previous version of the client exists.

Example of a silent installation with default options

To issue a silent installation with default settings, use the following syntax:

```
8.1.0-IBM-SP4WKSTNS-EDITION-x86_windows.exe /S /v"/qn "
```

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

For example, for the IBM Spectrum Protect for Workstations OEM Edition, use the following syntax:

```
8.1.0-IBM-SP4WKSTNS-OEM-x86_windows.exe /S /v"/qn option1 option2 "
```

Example of a silent installation with options

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

```
8.1.0-IBM-SP4WKSTNS-EDITION-x86_windows.exe /S /v
"/qn INSTALLDIR=c:\newdir /l*v c:\temp\msi.log REBOOT=ReallySuppress "
```

Upgrade the IBM Spectrum Protect for Workstations client silently

After you install the IBM Spectrum Protect for Workstations client, you can upgrade the product version by putting an installer executable file or a configuration file in the administration folder. The client pulls the software update or new configuration.

Upgrade the product level

To upgrade the product, put a new client installer in the downloads folder. For information about the downloads folder, see “Administration folders” on page 3. The client pulls the new product code and notifies you to start the computer again.

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

Tip: To view the program messages, open the Advanced page in the settings notebook and set **Allow program messages to pop up** to **Enabled**.

Restriction: The client does not back up any files until you start the system again. You do not lose any existing backup copies, but any changes you make are not protected. If there is a long delay before you start the system, you can force a backup to protect any files that were changed during that time. To force a backup, open the settings notebook and click **Files to Protect**. Select the **Start an initial backup with the new settings** check box and click **OK**.

Change protection settings

To change the protection settings, put a new configuration file in the downloads folder. You can generate a configuration file with the Central Administration Console. For information about how to create a configuration file, see the *IBM Spectrum Protect for Workstations Central Administration Console Installation and User's Guide*. If the modification date of a configuration file is more recent than the file that is used for the current configuration, IBM Spectrum Protect for Workstations adopts the new configuration.

Conditions for upgrading a client

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

The client installer file must have the following characteristics:

- The file name includes the string `SP4WKSTNS`.
- The file type is `exe`, for example: `8.1.0-IBM-SP4WKSTNS-x86_windows.exe`.
- The date of the new installer file must be more recent than the date of the installer file that was used for the current product level.

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

Removing old data files after uninstallation

If you uninstall the client, you must remove old data files before you install the client again. When the client is uninstalled, some files are not removed by the installer. The old files can cause problems when you reinstall the client.

Remove files in the following data folders:

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

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

Installation folder

The default installation location for the client is the `c:\Program Files\Tivoli\TSM\FastBack_for_Workstations` directory. If you upgraded from IBM Spectrum Protect Continuous Data Protection for Files, the default installation location is the `C:\Program Files\Tivoli\CDP_for_Files` directory.

The program data folder
The program data folder varies according to operating system and previously installed versions. The default program data folder for Windows 7 and Windows 8 is `C:\Programs\Tivoli\TSM\FastBack_for_Workstations`.

Upgrade from Continuous Data Protection for Files

If you upgrade from IBM Spectrum Protect Continuous Data Protection for Files, your IBM Spectrum Protect Continuous Data Protection for Files client must be at version 3.1 or later.

IBM Spectrum Protect Continuous Data Protection for Files clients that are older than version 3.1.5.9 accept client installer files with a name such as `TivoliCDP_CDPForFiles_3.1.8.0_windows.exe`. The installer name must include `CDP` and must be file type `exe`. IBM Spectrum Protect Continuous Data Protection for Files clients of version 3.1.5.9 and later accept client installer files with `CDP` or `SP4WKSTNS` in the file name. IBM Spectrum Protect for Workstations client installer files have a name such as `8.1.0-IBM-SP4WKSTNS-x86_windows.exe` for a full installation or `8.1.0-IBM-SP4WKSTNS-x86_windows-FP0000.exe` for a patch installation. The installer file name for a IBM Spectrum Protect for Workstations client must contain `SP4WKSTNS`.

Therefore, if you want a IBM Spectrum Protect Continuous Data Protection for Files client earlier than version 3.1.5.9 to pull an upgrade to IBM Spectrum Protect for Workstations, you have the following options:

- You can rename the IBM Spectrum Protect for Workstations installer file to include `CDP` in the file name.
- You can first upgrade the IBM Spectrum Protect Continuous Data Protection for Files client to version 3.1.5.9 or later. The client can then pull an installer file with `CDP` or `SP4WKSTNS` in the file name.

Methods of deploying the client to other computers

You can use several methods to deploy the initial installation of the IBM Spectrum Protect for Workstations client to other computers.

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

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

Restriction: If more than one client is backing up files to the same remote file server, you must configure the server Access Control List (ACL) settings. For more information about the configuration tasks, see “Limit user access to files on a target file server” on page 74.

Windows installation folder

The IBM Spectrum Protect for Workstations client references the Windows installation folder during installation. During the installation, the client can get configuration information from files in the `\System32\` subfolder in the Windows installation folder. The files are named `fpa.txt`, `dsm.opt`, `networks.xml`, and `machinename.txt`.

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

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

Chapter 3. Changing protection settings

When you initially install the IBM Spectrum Protect for Workstations client, the Initial Configuration Wizard guides you to set your protection settings. After installation, you can change your protection settings with the Settings Notebook.

Settings Notebook

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

Open the Settings Notebook by clicking **Settings** from the menu of the IBM Spectrum Protect for Workstations Status panel.

Use the tabs to navigate to any panel whose settings you want to change. Click the **OK** button to apply your new settings and return to the IBM Spectrum Protect for Workstations Status panel. Click the **Apply** button to apply your new settings and stay in the Settings Notebook. Click the **Cancel** button to exit the Settings Notebook without applying your changes.

The Settings Notebook has six panels:

- Use the "**General** panel of client Settings Notebook" on page 26 for these settings:
  - Which drive to use for your local storage area.
  - How many versions of protected files to keep on local storage area.
  - The maximum size of your local storage area.
  - Whether you want to store backup copies on local storage area, remote storage area, neither, or both.
- Use the "**Files to Protect** panel of client Settings Notebook" on page 28 to specify:
  - Which folders and files to continuously protect.
  - Which folders to vault.
  - A forced backup of all protected files when you change which files are continuously protected.
- Use the "**Email Protection** panel of the client Settings Notebook" on page 35 for your email protection settings, including the schedule to protect your email and all files that are backed up on a schedule. You can also specify how many versions of the email files to keep.
- Use the "**Remote Storage** panel of client Settings Notebook" on page 36 to specify:
  - A backup identifier name to help you find the backup on the remote server during the recovery process of an existing machine.
  - A remote storage area.
  - How many versions of protected files to keep on the remote storage area.
  - The maximum size of your remote storage area.
  - Whether to encrypt, compress, or use sub-file copy for backup copies stored on a remote storage area, depending on what type of remote storage is used.
- Use the "**Expiration** panel of client Settings Notebook" on page 41 to specify:

  - Whether to remove backups of files that were deleted from the backed up computer.
  - How long to keep copies of deleted files before they are removed from the remote storage.
  - How often to check for deleted files to be removed from the remote storage.
- Use the "**Advanced** panel of client Settings Notebook" on page 41 to specify:
  - Whether to allow program messages to display.
  - Performance settings include:
    - Maximum size of file to protect on local storage area.
    - Maximum size of file to protect on remote storage area.
  - The Advanced panel contains a link to set your scheduled backups. Follow the link to:
    - Choose which files to back up on a schedule.
    - Start a backup of your scheduled files immediately.
  - The Advanced panel also contains a link to manage the throttle settings. Follow the link to:
    - Manage the network rules settings.
    - Manage bandwidth usage.
    - Define throttle speed.

General panel of client Settings Notebook

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

Back up to: drop-down list

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

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

IBM Spectrum Protect for Workstations creates backup copies in a subfolder named `\RealTimeBackup\`. For example, if the local storage area is configured as the `C:\` drive, backup copies are stored in `C:\RealTimeBackup\`.

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

How many versions to keep: field

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

Maximum space for backups: field

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

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

The default space for local backups is 500 MB.

During a forced backup of all protected files, IBM Spectrum Protect for Workstations can use more space than you configured for local storage. (A forced backup of all files occurs during the initial backup when you install IBM Spectrum Protect for Workstations, 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, IBM Spectrum Protect for Workstations purges files from the local storage area, if necessary, to meet the space you configured.

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

Continuous protection level: drop-down list

IBM Spectrum Protect for Workstations offers two levels of protection for your files: continuous protection and scheduled protection. See “Types of protection” on page 2 for a discussion of these two types of protection.

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

None Files are not protected.

Local storage only
IBM Spectrum Protect for Workstations creates backup copies only on the local storage area.

Remote storage only
IBM Spectrum Protect for Workstations creates backup copies only on the remote storage area.

Local and remote storage
IBM Spectrum Protect for Workstations creates backup copies on both the local and remote storage areas. This provides the most protection for your files, and is the default choice.

Files to Protect panel of client Settings Notebook

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

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

Folders and Files box (Settings Notebook) of IBM Spectrum Protect for Workstations

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

Folders and Files Settings page for continuous protection by IBM Spectrum Protect for Workstations:

Use the Folders and Files Settings page to specify which folders and files to continuously protect by selecting the files to include and exclude.

List of Folders and Files to Include and Exclude

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

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

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

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

The list contains these columns:

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

Type Values in the **Type** column indicate whether the files and folders should be included or excluded from protection. Files and folders that are excluded from continuous and scheduled protection are not protected. Files that are included are protected. Files that are excluded have precedence over files that are included. As a result, any file or folder that matches an exclude pattern are not protected, even if the same file or folder matches an include pattern. (See "Including and excluding files from protection" on page 29).

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

Protected drives:

All files that meet the include and exclude specifications, and that appear to IBM Spectrum Protect for Workstations as internal drives, are protected.

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

Including and excluding files from protection:

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

Continuous and scheduled protection (not vaulted)

IBM Spectrum Protect for Workstations keeps a list of files that are included for protection, and a list of files that are explicitly excluded from protection. The list of included files is separated into those files that are included for continuous protection, and those files that are included for scheduled protection. If a file is excluded, it is excluded from both continuous and scheduled protection.

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

The following table summarizes the interaction of inclusion and exclusion.

Table 3. Inclusion and exclusion. File protection by Include list and Exclude list.

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

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

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

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

Vaulted folders

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

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

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

Wildcard characters in file specifications:

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

You can enter the complete path of a file that you want to protect. The complete path must match a single file. You can use asterisks and blanks as wildcard characters to specify several files.

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

Apply the following guidelines for using wildcard characters:

- If there are no asterisks, blank spaces are interpreted as asterisks before or after the pattern. For example, `\myDocs\` and `*\myDocs\*` yield the same matches. If there are asterisks in the pattern, blank spaces do not match any characters before or after the pattern. For example, `\myDir\`, `*\myDir\`, and `\myDir\*` can yield three different matches.

  For example, assume a pattern `fish`. This pattern matches the following files and folders:

  - `C:\dir\fish.doc`
  - `C:\fish\anyfile.doc`
  - `c:\Dirfishfood\something`

- If the file specification includes slashes, for example `\fish\`, the specification matches any object with `\fish\` somewhere in the path. For example, this pattern produces the following matches and non-matches:
  - Matches `C:\fish\anyfile.doc`
  - Does not match `C:\dir\fish.doc`
  - Does not match `c:\Dirfishfood\something`

The following table provides examples of how patterns match files and folders.

Table 4. File and folder pattern matches

Pattern	Matches for folders and files on your computer:

`\myDir\` or
`\mYdiR\` or
`*\myDir\*` or
`*\mydir\*`
	`c:\myDir\`
	`c:\myDir\Contacts\`
	`c:\myDir\Contacts\contacts.txt`
	`c:\Projects\myDir\`
	`c:\Projects\myDir\myThings\`
	`c:\Projects\myDir\myThings\things.doc`
	`c:\Projects\myDir\myThings\myPhoto.jpg`
	`d:\Notes\myDir\`

`*\myDir\`	`c:\myDir\`
	`c:\Projects\myDir\`
	`d:\Notes\myDir\`

`d:*\mydir\*`	`d:\Notes\myDir\`

`\my best`	`c:\Books\My Best.doc`
	`c:\Photos.jpg\My Best Photo\`
	`c:\Photos.jpg\My Best Photo\Best.jpg`
	`f:\Projects\My Best Project\`
	`f:\Projects\My Best Project\Dream.xls`

`.jpg`	`c:\Photos.jpg\`
	`c:\Photos.jpg\myHouse.bmp`
	`c:\Photos.jpg\My Best Photo\Best.jpg`
	`c:\Projects\myDir\myThings\myPhoto.jpg`

`*.jpg`	`c:\Photos.jpg\`
	`c:\Photos.jpg\My Best Photo\Best.jpg`
	`c:\Projects\myDir\myThings\myPhoto.jpg`

`E:\` `E:\*`	All files and folders on the E: drive.

Applications box (Settings Notebook) of IBM Spectrum Protect for Workstations

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

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

Application settings for IBM Spectrum Protect for Workstations:

Specify a list of applications to protect.

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

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

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

View Alphabetically
The applications are presented in alphabetical order.

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

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

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

You can add files to be protected in the **Application Settings** dialog, but these applications are protected only if the files are not explicitly excluded. For more information, see "Including and excluding files from protection" on page 29.

Vault box of IBM Spectrum Protect for Workstations

The **Vault** displays a summary of vaulted folders.

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

Vault Settings dialog of IBM Spectrum Protect for Workstations:

Use the **Vault Settings** dialog to specify a list of folders that are protected from being changed or deleted.

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

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

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

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

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

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

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

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

Vault duration:

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

To specify duration of vaulting, create a folder that is 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 files that are created in that folder are prevented from alteration or deletion for three years. After the expiration time, the file is no longer vaulted. There are three ways to indicate the vaulting period. Each way requires that you use a keyword in the folder name.

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

   Use 1 or more time units. Each time unit that you use must be preceded by a number up to 5 digits long. You can include spaces or underlines or dashes and mix case in the folder name. The following are valid examples:

   ```
   \Retain23days4hours\
   \Retain 3years\
   \Retain_3years\
   \Retain-23DAYS_4minutes\
   \Retain 1000 days\
   ```
3. **`\KeepSafe\RetainUntil Date\`**
   Specify a date after which the vaulting expires. The date must include year, month, and day in the following format: `yyyymmddhhmmss`. The hours, minutes, and seconds are optional. The default time is 00:00:00. The following examples specify valid dates:

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

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

Back up with new settings check box of IBM Spectrum Protect for Workstations

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

If you change the specifications for **Folders and Files** or **Applications** to include files that were not previously protected, back up those files immediately. 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, IBM Spectrum Protect for Workstations can use more space than you configured for local storage. (A forced backup of all files occurs during the initial backup when you install IBM Spectrum Protect for Workstations, 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, IBM Spectrum Protect for Workstations 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 installation, the backup copies are created in the system context. When you later run IBM Spectrum Protect for Workstations in the user context, you might have problems to restore these files.

When to back up all files:

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

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

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

After the initial backup, the typical rate of file changes does not require that you again back up all files immediately. If you change the protection settings to include files that were not previously protected, the files need to be backed up. Until you

change these files, and without a forced backup, IBM Spectrum Protect for Workstations does not back up these files. To protect these files, you must force a backup of all files.

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

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

When the scan and backup complete, IBM Spectrum Protect for Workstations continues to operate in the background without any significant impact on your regular computing activities.

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

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

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

You can force an initial backup of a newly installed client by setting this option when you identify an administration folder with the Central Administration Console. Then create a configuration file and deploy a client with the created configuration file.

You can force a complete backup at any time by sending to the client a script that includes the command to back up all files.

Email Protection panel of the client Settings Notebook

Use the **Email Protection** panel of the client Settings Notebook to select the email applications that you want to protect. Select a schedule for protecting the email applications.

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

Email files are backed up only to remote storage. If the remote storage is not available at the scheduled backup time, IBM Spectrum Protect for Workstations backs up the email files when the remote storage area becomes available.

Email Application list

Select one of the email applications in the list.

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

Email Application Data Folder field

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

How Many Email Versions to keep field

You use this field to specify how many versions of the Email file you want to keep on the remote storage.

How often to protect your email list

You can schedule email protection at one of several intervals:

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

Scheduled Backup Settings

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

Remote Storage panel of client Settings Notebook

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

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. IBM Spectrum Protect for Workstations is tolerant of intermittently available networks. If the remote storage area is temporarily unavailable, IBM Spectrum Protect for Workstations queues backup copies until the remote storage becomes available.

Remote Storage server or device name and location

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

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

Backup Identifier

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

Location for the External Device or File Server

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

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

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

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

IBM Spectrum Protect for Workstations creates backup copies in a subfolder called `\RealTimeBackup\`*`computer name`*. For example, if a computer name is Computer1, and the remote storage location is configured with the value `\\remote\share`, backup copies are stored in `\\remote\share\RealTimeBackup\Computer1\`.

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

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

WebDAV Server storage location

Some Internet Service Providers (ISPs) provide Web-based Distributed Authoring and Versioning, or WebDAV. With the WebDAV protocol, you can create, change, and move documents on a remote server. The WebDAV protocol is useful for authoring the documents that a web server serves, but can also be used for general web file storage. If your ISP provides WebDAV functions, IBM Spectrum Protect for Workstations 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, IBM Spectrum Protect for Workstations can use the basic authentication method. Because this authentication method sends the password as clear text over the network, the web server is configured to use secure sockets.

IBM Spectrum Protect for Workstations storage location

IBM Spectrum Protect for Workstations can store backup copies on a IBM Spectrum Protect server.

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

You can use IBM Spectrum Protect server version 6.1 or later with IBM Spectrum Protect for Workstations.

Configure the IBM Spectrum Protect server before you connect from IBM Spectrum Protect for Workstations. Register the computer as a IBM Spectrum Protect node. IBM Spectrum Protect for Workstations prompts you for the password for this node in order to connect to the IBM Spectrum Protect server. For more information about registering a IBM Spectrum Protect node for your computer, see *IBM Spectrum Protect for Windows Administrator's Guide*.

If you specify a IBM Spectrum Protect server as the backup target and you want encryption or compression features applied to the backup, you must specify these options in the `dsm.opt` file in the IBM Spectrum Protect for Workstations subfolder of the "Accessing the program data folder" on page 40.

Restriction: You cannot use a subfile backup feature when the IBM Spectrum Protect server is the backup target.

In addition to backing up data directly to a IBM Spectrum Protect server, you can back up data using a two-stage method. First, use IBM Spectrum Protect for Workstations to create remote backups on a file server. Then, schedule a IBM Spectrum Protect backup-archive client on that file server to back up the files to a IBM Spectrum Protect server.

Restriction: If you use IBM Spectrum Protect for Workstations encryption, you cannot use IBM Spectrum Protect compression.

To manage storage space, the IBM Spectrum Protect administrator must grant authority to the IBM Spectrum Protect client node to delete backup copies. For steps to assign authority to delete backup copies, see the topic in the problem determination section: " IBM Spectrum Protect client node lacks authority to delete backup copies" on page 70.

To avoid problems when using the IBM Spectrum Protect server, see "Files are not backed up to IBM Spectrum Protect server" on page 70.

How many versions to keep

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

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

Remote Storage advanced settings

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

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

When the storage space becomes full, IBM Spectrum Protect for Workstations deletes older backup copy versions of files that have several backup copy versions. If more space is needed for new backup copies, IBM Spectrum Protect for Workstations deletes backup copies of files to make room for the newest backup copy.

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

Advanced settings

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

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

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

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

Encrypt backups feature

IBM Spectrum Protect for Workstations provides AES256 encryption for files that are stored on the remote server. The encryption feature for backups provides an extra layer of security for files in the remote storage area.

To set up encryption, click **Encrypt backups**. When the first file backup occurs, you are prompted to enter an encryption password. This password is cached and also saved in an encrypted file in the `ProgramData` folder. The password is required to restore files that are backed up by IBM Spectrum Protect for Workstations. If you disable encryption and enable encryption again, you are not prompted to create a new password.

Preserve your password: Ensure that you make a secure record of your password. If you lose your password, files might be unrecoverable.

The IBM Spectrum Protect product does not support prompted encryption. Therefore, if you specify the IBM Spectrum Protect server as your remote storage area, you must configure non-prompted encryption in the IBM Spectrum Protect `dsm.opt` options file. In the `dsm.opt` file, use the following statement to create the encryption key:

```
encryptkey generate
```

See *IBM Spectrum Protect for Windows Backup-Archive Client Installation and User's Guide* for information about how to set encryption options in the `dsm.opt` file. The `dsm.opt` file is stored in the `ProgramData` folder. For information about how to access the `ProgramData` folder, see "Accessing the program data folder."

The following usage rules apply to the encrypt backups feature:

- You cannot encrypt files that are stored in the local storage area.
- You cannot configure both encryption and compression.

IBM Spectrum Protect for Workstations cannot protect backup copies that are encrypted. In other words, you cannot create encrypted backup copies and then use IBM Spectrum Protect for Workstations to make backup copies of those backup copies. You can use IBM Spectrum Protect or another backup solution to protect the encrypted backup copies on the file server.

Accessing the program data folder:

Passwords for encrypted files are kept in the program data folder.

The following list indicates the location of the program data folder for Microsoft Windows 7 and Windows 8.

Tip: `\ProgramData\` is a hidden folder. To see the folder, modify your view preferences in Windows Explorer to show hidden files and folders.

- For a fresh installation of IBM Spectrum Protect for Workstations Version 8.1.0, the program data folder is in the following directory:

  ```
  C:\ProgramData\Tivoli\TSM\FastBack_for_Workstations
  ```

- For an upgrade from IBM Spectrum Protect Continuous Data Protection for Files to IBM Spectrum Protect for Workstations Version 8.1.0, the program data folder is in the following directory:

  ```
  C:\ProgramData\Tivoli\CDP_for_files
  ```

Compress backups option

Set compression for remote backup copies.

Use compression to save space on your remote storage location. The compression feature is not compatible with the encryption feature. You can use compression or encryption, but not both simultaneously. Files that are backed up using the compression function must be restored by using IBM Spectrum Protect for Workstations.

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

You can choose to select either encryption or compression.

Use sub-file copy option

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

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

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

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

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

Expiration panel of client Settings Notebook

Use the **Expiration** panel of the client Settings Notebook to specify whether deleted files are removed from the remote backup location.

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

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

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

Advanced panel of client Settings Notebook

Use the **Advanced** panel of the client Settings Notebook to allow messages to be displayed, and to tune performance.

Allow program messages to display

For certain types of activities or notifications, IBM Spectrum Protect for Workstations opens messages from the icon in the system tray. To prevent the messages from opening, select **disabled**.

Note: If messaging is disabled, important program messages regarding the failure of IBM Spectrum Protect for Workstations operations is suppressed, which may lead to potential loss of data.

Performance Settings

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

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

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

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

Folders and Files Settings dialog for scheduled backups by IBM Spectrum Protect for Workstations

Use the **Folders and Files Settings** dialog to specify folders and files to back up on the same schedule as email files are backed up.

When considering what files to protect on a schedule, see "Types of protection" on page 2 and "What to consider before you set up scheduled backups" on page 43.

List of folders and files to include

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

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

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

Each row in the list has one column.

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

Starting a scheduled backup

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

What to consider before you set up scheduled backups:

You configure IBM Spectrum Protect for Workstations to protect appropriate files on a schedule, and prepare the files for backup.

Files that are appropriate to protect on a schedule

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

Some files are not often closed and saved, but must be backed up periodically. Files that are protected by schedule are backed up even if they are open.

Scheduled backups can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but there are fewer versions to restore a file.

Conditions for a scheduled backup to occur

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

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

If the computer is shut down or IBM Spectrum Protect for Workstations is not running at the schedule time, the scheduled backup runs when the computer is powered on and IBM Spectrum Protect for Workstations is running.

If you shut down a computer or stop the IBM Spectrum Protect for Workstations client when a scheduled backup is running, the backup is suspended. The backup resumes when the client is started again and the remote storage is available. If you forced a backup of scheduled files during the 10 minutes before the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

IBM Spectrum Protect for Workstations backs up all files that changed during the schedule interval, including files that are open at the time of backup.

Tip: If a file is open during the backup, the copy of the file can be corrupted. To avoid this issue, close applications before a scheduled backup.

At the beginning of a scheduled backup, IBM Spectrum Protect for Workstations attempts to close all files that are listed in the file `closeapps.txt` in the installation directory. Each line in the file must be a program name, with name and extension, but no folder path. IBM Spectrum Protect for Workstations sends a close command to each instance of every program that is included in the `closeapps.txt` file. The IBM Spectrum Protect for Workstations does not send a start command to any of those programs when the scheduled backup is finished.

Throttle settings and network rules

You can modify or create policy rules that manage bandwidth usage in the networks that you specify for IBM Spectrum Protect for Workstations.

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

Using Network Rules

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

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

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

Move Up
Select a list item and click **Move Up** to increase the priority of this rule. When searching for rules to apply to a network, IBM Spectrum Protect for Workstations searches the list in order from highest to lowest.

Move Down
Select a list item and click **Move Down** to decrease the priority of this rule. When searching for rules to apply to a network, IBM Spectrum Protect for Workstations searches the list in order from highest to lowest.

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

Create a Network Rule

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

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

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

DNS Suffix
The Domain Name System information is displayed.

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

```
192.168.*
```

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

Throttle

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

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

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

Changing protection settings for the client

You can change which files and applications are protected by the IBM Spectrum Protect for Workstations client, and how they are protected.

The IBM Spectrum Protect for Workstations client must be already installed before you can change the protection settings. If you configure the client during product installation, see "Navigating the Configuration Wizard" on page 9.

To change the protection settings, start from the IBM Spectrum Protect for Workstations Status panel.

The Status panel is displayed when you twice click the  icon in the system tray. In Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Spectrum Protect > IBM Spectrum Protect for Workstations**.

Specifying which files and applications are protected by IBM Spectrum Protect for Workstations

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

Specifying which files and applications are continuously protected by IBM Spectrum Protect for Workstations

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

Procedure

Complete the following steps to specify applications and files to be backed up:

1. Open the IBM Spectrum Protect for Workstations Status panel and click **Settings**.
2. In the Settings Notebook, click **Files to Protect**.
3. In the **Applications** box, click the **details** link. The **Applications Settings** dialog is displayed, and the **Files to Protect** page becomes inactive.
4. Check the applications whose files you want to protect. Clear those applications whose files you do not want to protect.
5. Click **OK**. The **Applications Settings** dialog exits, and the **Files to Protect** page again becomes active.

6. Optional: If you want to add or exclude files and folders by specifying file paths, in the **Folders and Files** box, click the **details** link. The **Folder and Files Settings** dialog display is displayed, and the **Files to Protect** page becomes inactive. For an explanation about how to include and exclude files in this dialog, see "**Folders and Files Settings** page for continuous protection by IBM Spectrum Protect for Workstations" on page 10
7. If you added applications or file specifications, you must force a backup to ensure that all the new files are immediately protected. See "When to back up all files" on page 34 for an explanation. Check the **Start and initial backup with the new settings** check box.
8. Click **OK**.

Results

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

Specifying which files and applications are protected on a schedule by IBM Spectrum Protect for Workstations

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

Procedure

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

What to consider before you set up scheduled backups:

You configure IBM Spectrum Protect for Workstations to protect appropriate files on a schedule, and prepare the files for backup.

Files that are appropriate to protect on a schedule

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

Some files are not often closed and saved, but must be backed up periodically. Files that are protected by schedule are backed up even if they are open.

Scheduled backups can yield fewer backup versions than continuously protected files. Fewer backup versions use less storage space, but there are fewer versions to restore a file.

Conditions for a scheduled backup to occur

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

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

If the computer is shut down or IBM Spectrum Protect for Workstations is not running at the schedule time, the scheduled backup runs when the computer is powered on and IBM Spectrum Protect for Workstations is running.

If you shut down a computer or stop the IBM Spectrum Protect for Workstations client when a scheduled backup is running, the backup is suspended. The backup resumes when the client is started again and the remote storage is available. If you forced a backup of scheduled files during the 10 minutes before the scheduled time, the scheduled backup does not occur.

Closing applications before a scheduled backup

IBM Spectrum Protect for Workstations backs up all files that changed during the schedule interval, including files that are open at the time of backup.

Tip: If a file is open during the backup, the copy of the file can be corrupted. To avoid this issue, close applications before a scheduled backup.

At the beginning of a scheduled backup, IBM Spectrum Protect for Workstations attempts to close all files that are listed in the file `closeapps.txt` in the installation directory. Each line in the file must be a program name, with name and extension, but no folder path. IBM Spectrum Protect for Workstations sends a close command to each instance of every program that is included in the `closeapps.txt` file. The IBM Spectrum Protect for Workstations does not send a start command to any of those programs when the scheduled backup is finished.

Specifying which email applications are protected by IBM Spectrum Protect for Workstations

You use the Email Protection page of IBM Spectrum Protect for Workstations to specify an email application to protect.

Procedure

Complete the following steps to specify which email applications are to be protected:

1. Start IBM Spectrum Protect for Workstations Status panel and click **Settings**.
2. In the Settings Notebook, click **Email Protection**.
3. Choose your email application from the **Email Application** list. If your application is not listed in the list, choose **Other**. If you chose **Other**, the **Email Application Data Folder (wildcards allowed)** field becomes active.
4. If you chose **Other**, enter a file specification in the **Email Application Data Folder (wildcards allowed)** field. You can type the specification or browse for the folder.
5. Specify **How many Email versions to keep** on the remote storage.
6. Click **OK**.

Related tasks:

"Specifying the period for scheduled protection by IBM Spectrum Protect for Workstations" on page 49
All files that are protected on a schedule are protected on the schedule that is configured in the **E-mail Protection** page in the Settings Notebook. When you change the schedule for e-mail files, you change the schedule for all files that are protected on a schedule.

Specifying which files and applications are vaulted by IBM Spectrum Protect for Workstations

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

About this task

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

Procedure

1. Click the **Settings** menu item. The Settings Notebook displays.
2. In the Settings Notebook, click the **Files to Protect** tab. The **Files to Protect** page displays. The page has three summary boxes: **Folders and Files**, **Applications**, and **Vault**.
3. In the **Vault** box, click the **details** link. The **Vault Settings** dialog displays, and the **Files to Protect** page becomes inactive.
4. Click the **Vault** menu item. The **Select Folders** dialog displays, and the **Vault Settings** dialog becomes inactive.
5. Choose a folder in the folders tree, or specify a folder in the **Folder name (wildcards allowed)** field. You cannot specify individual files. With wildcards, you can specify all folders that match your pattern. See "Wildcard characters in file specifications" on page 11 for details.
6. Click the **OK** button. The **Select Folders** dialog exits, and the **Vault Settings** dialog again becomes active. The folder that you specified is added to the list.

7. Repeat the previous three steps to specify more folders to vault.
8. In the **Vault Settings** dialog, select the folders that you no longer want vaulted, and click the **Unvault** menu item. The folders that you specified are removed from the list.
9. Click **OK**. The **Vault Settings** dialog exits, and the **Files to Protect** page in the Settings Notebook again becomes active.
10. Click **OK**. The Settings Notebook exits, and your folders become vaulted.

Specifying the period for scheduled protection by IBM Spectrum Protect for Workstations

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

Procedure

1. Open the IBM Spectrum Protect for Workstations Status panel.
2. Click the **Settings** menu item. The Settings Notebook displays.
3. In the Settings Notebook, click the **E-mail Protection** tab. The **E-mail Protection** page displays.
4. Choose the schedule period in the **How often to protect your e-mail:** drop down list. Depending on the schedule period that you chose, day or time fields will display
5. If applicable for the scheduled period, choose the day and time to perform the backup.
6. Click the **OK** button. The Settings Notebook exits and your new settings are applied.

Specifying storage for backup copies by IBM Spectrum Protect for Workstations

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

Specifying the local storage area for backup copies by IBM Spectrum Protect for Workstations

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

Procedure

1. Open the IBM Spectrum Protect for Workstations Status panel.
2. Click the **Settings** menu item. The **General** page of the Settings Notebook displays.
3. Choose the location, number of versions, space for local backup copies, and level of continuous protection. For explanations of the fields on this page, see "**General** panel of client Settings Notebook" on page 26.
4. Click the **OK** button. The Settings Notebook exits and your new settings are applied.

Specifying the remote storage area for backup copies by IBM Spectrum Protect for Workstations

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

Procedure

1. Open the IBM Spectrum Protect for Workstations Status panel.
2. Click the **Settings** menu item. The Settings Notebook displays.
3. In the Settings Notebook, click the **Remote Storage** tab. The **Remote Storage** page displays.
4. Choose appropriate values for the remote storage area fields. For explanations of the fields on this page, see "**Remote Storage** panel of client Settings Notebook" on page 36.
5. Click the **OK** button. The Settings Notebook exits and your new settings are applied.

Backup features

IBM Spectrum Protect for Workstations has a number of backup features available that can impact how the backups are implemented.

The information on how the backup features impact one another when more than one feature is in use during a backup process is as follows.

1. Files defined eligible for continuous backups, scheduled backups, or both.

   If both compression and subfile copy are enabled for these files, then the files that are smaller than the subfile copy limit are backed up compressed. The files that exceed this limit are backed up using subfile copy (that is, not compressed).
2. Files defined eligible for email backups, which are specified in the **Email Application list** field of the Email Protection screen.

   These files are backed up using email bitmap backup, which doesn't have any tunable limit on file size. So, all specified files are backed up using this feature. The file size is disregarded. Compression and subfile copy are not used for these files.

Chapter 4. Starting and stopping protection activity of the IBM Spectrum Protect for Workstations client

How to administer the IBM Spectrum Protect for Workstations client. You can find out how to start, stop, and restart the client, how to force a backup, and how to run the client as a service.

Methods to start the client GUI

Start the client GUI to work with the IBM Spectrum Protect for Workstations client. From the Status panel of the GUI, you can modify data protection settings, restore files, and monitor protection activity.

The Status panel is displayed when you twice click the  icon in the system tray. In Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Spectrum Protect > IBM Spectrum Protect for Workstations**.

Starting and stopping client backups

When you change your configuration so that a new set of files is protected, ensure that you back up all protected files. If you do not back up all protected files, only those files that you change are protected.

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

To work with forced backups, start from the IBM Spectrum Protect for Workstations Status panel.

The Status panel is displayed when you twice click the  icon in the system tray. In Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Spectrum Protect > IBM Spectrum Protect for Workstations**.

When to back up all files

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

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

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

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

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

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

When the scan and backup complete, IBM Spectrum Protect for Workstations continues to operate in the background without any significant impact on your regular computing activities.

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

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

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

You can force an initial backup of a newly installed client by setting this option when you identify an administration folder with the Central Administration Console. Then create a configuration file and deploy a client with the created configuration file.

You can force a complete backup at any time by sending to the client a script that includes the command to back up all files.

Backing up all files that are protected by IBM Spectrum Protect for Workstations

When you change your configuration to extend continuous or scheduled protection to more files, back up all of the protected files. If you do not back up all protected files, only those files that you change are protected.

About this task

For an explanation of when to back up all files, see "When to back up all files" on page 34.

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

Procedure

1. Start the IBM Spectrum Protect for Workstations Status panel.
2. Click **Settings** to open the Settings Notebook.
3. In the Settings Notebook, click **Files to Protect**.
4. Click **Start an initial backup with the new settings**.
5. Click **OK**. Your protected drives are scanned and all of the files that you designated for continuous or scheduled protection are backed up. System performance is slower during the extensive scan of your protected drives.

Forcing a scheduled backup by IBM Spectrum Protect for Workstations

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

About this task

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

Procedure

Complete the following steps to back up all the files that changed since the last scheduled backup:

1. Open the IBM Spectrum Protect for Workstations Status panel and click **Settings**.
2. In the Settings Notebook, click **Advanced**.
3. Click **Scheduled Backup Settings**. The **Folders and Files Settings** dialog for scheduled backups is displayed and the **Advanced** page becomes inactive.
4. Check on **Start scheduled backup now**.
5. Click **OK**. The **Folders and Files Settings** dialog exits and the **Advanced** page in the Settings Notebook becomes active.
6. Click **OK**. Backing up starts for all of the files that changed since the last scheduled backup.

Stopping backup or restore activity by IBM Spectrum Protect for Workstations

You can stop any backup or restore activity that the IBM Spectrum Protect for Workstations client is running.

To stop backup or restore activity, start from the IBM Spectrum Protect for Workstations Status panel.

The Status panel is displayed when you twice click the  icon in the system tray. In Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Spectrum Protect > IBM Spectrum Protect for Workstations**.

1. The bar at the end of the Status panel displays a brief text message of the status of backup and restore activities. Hover your cursor over the icon next to the text. A summary of activities opens from the bar. The summary lists five activities. For each activity, there is a link to a detailed status dialog, and a brief text that indicates the status of the activity.
2. Click the link for the activity you want to skip or stop or close. The detailed status dialog for that activity is displayed, and the Status panel becomes inactive.
3. In the Status dialog, you can click **Skip** to skip a restore or backup operation, or **Stop** to stop a restore or backup operation. Click **Close** to exit, and the Status panel becomes active again.

Restarting the client process

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

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

To restart the process on a Command Prompt window, complete the following steps:

1. Open a Command Prompt window.
2. Navigate to the IBM Spectrum Protect for Workstations installation folder.
3. Enter the following command: `filepathsrv -d`.
4. Confirm that the process is running by checking the System Event log or Task Manager. If the process is running, an entry in the System Event log contains the following message: `HTML listener started successfully and listening on port 9003`. This process is event # 6049. In Task Manager, you can see **`FilePathSrv.exe`** process.

You can also restart the process from the **Start** menu. Choose **Start > All Programs > Startup > SP4WKSTNSSrv**.

Run the IBM Spectrum Protect for Workstations client as a service

You can run the IBM Spectrum Protect for Workstations client as a service instead of a logged-in application.

The default account for services on Microsoft Windows has no privilege for accessing folders that are shared on a network. To update the `FilePathSrv` service, open a command prompt with elevated privileges and run the `FpForFileServers.js` executable. This executable starts the Microsoft Windows services configuration panel. Specify a valid account name and password that can access your remote backup locations.

When you uninstall the IBM Spectrum Protect for Workstations client, the IBM Spectrum Protect for Workstations service is also uninstalled.

Tip: The IBM Spectrum Protect for Workstations client installation directory and tree provide full access for all users on the system during installation. This access is provided so that non-privileged users without administration rights can be protected by the software, and access the client. For multiuser workstations, you might want a more restrictive access control list (ACL) on the installation directory and tree.

Chapter 5. Monitoring the protection state

When IBM Spectrum Protect for Workstations is installed and configured, you can monitor the state of your protection. You can receive messages, check that the IBM Spectrum Protect for Workstations daemon is running, and use the IBM Spectrum Protect for Workstations user interface to check detailed status of your protection.

If you determine that IBM Spectrum Protect for Workstations is not protecting your files as you intended, often the solution is suggested by the data available from IBM Spectrum Protect for Workstations reports or configuration settings. If the solution is not clear, consider the information in Chapter 8, "Troubleshooting the IBM Spectrum Protect for Workstations client," on page 69. The following monitoring opportunities are available.

Messages

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

To receive messages from IBM Spectrum Protect for Workstations, you must configure IBM Spectrum Protect for Workstations to send you messages. By default, IBM Spectrum Protect for Workstations sends you messages. You configure this setting in the **Allow program messages to pop up** list in the **Advanced** page of the Settings Notebook.

IBM Spectrum Protect for Workstations Icon in the System Tray

When the IBM Spectrum Protect for Workstations daemon is protecting your files as a logged in application, the IBM Spectrum Protect for Workstations icon  is shown in the desktop system tray. (If IBM Spectrum Protect for Workstations is running as a service, the icon is not shown in the system tray). If you do not see the icon in your system tray, and IBM Spectrum Protect for Workstations is not running as a service, you must restart the process. See "Restarting the client process" on page 54.

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

Monitoring protection with the IBM Spectrum Protect for Workstations client

If you want to actively check the status of your protection, there are several checks you can do in the IBM Spectrum Protect for Workstations client user interface.

IBM Spectrum Protect for Workstations client Status page

The Status page provides status information at a glance. For an explanation of all fields on the page, see "Status panel of IBM Spectrum Protect for Workstations" on page 60

Icon color

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

The **Remote storage** icon becomes yellow when you are disconnected from your remote storage area. This is not necessarily cause for alarm. For example, if you know that you will connect to your remote storage location before long, you do not need to worry. IBM Spectrum Protect for Workstations 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 IBM Spectrum Protect for Workstations cannot access the local storage area.

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

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

Icon Displays Data and Links

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

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

My Files icon

Files under protection

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

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

View Report

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

Email protection

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

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

Local Storage icon

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

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

Remote Storage

Usage bar

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

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

Continuous Protection Activity Report

A report of continuous protection activity is available from a link in the Status panel. The report is called **Activity Report**. To go to the **Activity Report**, see "Viewing the continuous protection activity report of a IBM Spectrum Protect for Workstations client" on page 62

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

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

Backup

IBM Spectrum Protect for Workstations creates a backup copy on the storage area.

Delete IBM Spectrum Protect for Workstations deletes the most recent backup copy from the storage area.

Purge IBM Spectrum Protect for Workstations deletes a versioned backup copy because the storage area is full.

Report

IBM Spectrum Protect for Workstations sends a report of scheduled backup activity to the central management area.

Version

IBM Spectrum Protect for Workstations adds a version suffix to a backup copy. A backup copy becomes versioned when IBM Spectrum Protect for Workstations creates a newer backup copy of the same file.

Status panel of IBM Spectrum Protect for Workstations

The Status panel is the entry point to the IBM Spectrum Protect for Workstations user interface. You can view a summary of how your files are protected, and link to other panels to view details and change protection settings.

The Status panel is displayed when you twice click the  icon in the system tray. In Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Spectrum Protect > IBM Spectrum Protect for Workstations**.

Menu Links

The menu bar of the Status panel contains the following links:

Settings
Links to the "Settings Notebook" on page 25. Use the Settings Notebook to change your protection settings.

Restore
Links to the "Restore Wizard of IBM Spectrum Protect for Workstations" on page 63. Use the Restore wizard to restore a file from a backup copy.

About Provides information about the product, including the version level.

Help Links to the online help documentation.

Graphic Icons

The screen contains a graphic representation of IBM Spectrum Protect for Workstations protection. Hover over an icon to show summary information and links to detailed information.

My Files icon

Files under protection:

Number
An approximation of the total number of files that are protected.

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

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

For an explanation of the **Activity Report**, see "Continuous Protection Activity Report" on page 59.

Email Protection

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

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

Local Storage

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

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

Remote Storage

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

Files Pending
When remote storage is not available, IBM Spectrum Protect for Workstations queues backup copies that are destined for remote storage. When the remote storage becomes available, IBM Spectrum Protect for Workstations transmits the queued backup copies. This field indicates the number of files that are destined for remote storage but were not transmitted yet.

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

Status Panel

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

Activities can have the following statuses:

Idle The activity is idle. If you stop an activity, the activity can become idle before it is finished.

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

Active The activity is active.

Paused
The activity was paused by the user.

Disconnected
The storage area is unavailable.

Disabled
The storage area is not configured.

System tray

The icon for the IBM Spectrum Protect for Workstations client is displayed in the system tray. When you hover the cursor over this icon, the loaded version is

shown. In Microsoft Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

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

If errors occur, the icon changes to  .

Tips:

- The error icon disappears when you view the activity report. The error icon reappears when the error occurs again.
- If errors occur and the status is disconnected, only the error icon is shown.

Viewing reports by IBM Spectrum Protect for Workstations

You can view a report of continuous protection activities on the IBM Spectrum Protect for Workstations client.

To view reports, start from the IBM Spectrum Protect for Workstations Status panel.

The Status panel is displayed when you twice click the  icon in the system tray. In Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Spectrum Protect > IBM Spectrum Protect for Workstations**.

Viewing the continuous protection activity report of a IBM Spectrum Protect for Workstations client

You can see a detailed report of recent backup activities.

About this task

The report shows successful activities, and failed activities with messages.In the Central Administration Console, this same report is called the client activity log.

Procedure

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

Chapter 6. Restoring files with the IBM Spectrum Protect for Workstations client

The IBM Spectrum Protect for Workstations client makes backup copies of your files so that when the time comes, you can restore your files. You can restore a file that you deleted, and you can restore an earlier version of a file that does not have your recent changes. A wizard guides you to find the file; choose the correct version, and choose the location to restore your file.

Start from the IBM Spectrum Protect for Workstations client Status panel.

The Status panel is displayed when you twice click the  icon in the system tray. In Windows 7 and Windows 8, all icons are hidden by default. For information about how to hide and display icons in the system tray, see the Microsoft website.

You can also start the client GUI from the **Start** menu. Choose **Start > All Programs > Spectrum Protect > IBM Spectrum Protect for Workstations**.

Click the large arrow in the middle of the Status panel. The Restore Wizard guides you to restore your file. For explanations of the Restore Wizard fields, see "Restore Wizard of IBM Spectrum Protect for Workstations."

Restore Wizard of IBM Spectrum Protect for Workstations

Restore a protected file with this Restore Wizard.

Use the control buttons in each wizard page to navigate to all pages. When you reach the final page, click the **Finish** button to restore your files.

The wizard has 4 pages:

- "**Welcome** panel (Restore Wizard) of IBM Spectrum Protect for Workstations"
- "Files to Restore page of IBM Spectrum Protect for Workstations" on page 64
- "**Restore Location** panel of IBM Spectrum Protect for Workstations" on page 65
- "Restore wizard **Summary** panel" on page 66

Welcome panel (Restore Wizard) of IBM Spectrum Protect for Workstations

The **Welcome** panel lists the steps to restore your files. Click the **Next** button to advance to the next panel of the wizard. Click the **Cancel** button to exit the wizard without restoring any files.

Files to Restore page of IBM Spectrum Protect for Workstations

You use the Files to Restore page of IBM Spectrum Protect for Workstations to select the files that you want to restore.

Files to Restore

The box contains a list of files that you can choose to restore. Each row contains the following fields:

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

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

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

Size The size of the file.

The list initially contains approximately 20 of the files that were most recently backed up. Change the list of files by clicking the **Search** or **Folder View** menu items at the start of the box:

Search
Presents a dialog that you can use to search for backup copies to add to the list.

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

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

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

Find files From location type
Choose the location of the backup copy.

You can choose from three locations:

Local The local storage area that is configured.

Remote
The remote storage area that is configured.

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

Click the **Search** dialog **OK** to begin searching.

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

The **Search Status** window shows the progress of your search. The **Search Status** > **Cancel** button stops the search and returns to the list of files without adding the files in your search criteria. If the search is completed without being canceled, the **Files to Restore** list contains the results of your search.

Folder View

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

Folder tree
Browse the tree to find a folder. Click a folder to display files in the folder in the file view.

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

Click **Change search location** to specify the backup location to search for files to restore. The options are **Local**, **Remote**, or **Other**. The user can use the browse to a specific folder if they select **Other**.

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

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

Restore Location panel of IBM Spectrum Protect for Workstations

Use the **Restore Location** panel to specify a location to restore your files.

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

Restore data to its original location
Check this option if you want to restore the files you chose to their original locations. The original location is the full path that is displayed when you hover over the file name in the **Files to Restore** panel.

Restore data to a new location
If you want to restore the files to a different location, check this option and enter the new location in the field. Use **Browse** to find and select the location. All files that are chosen are restored to the path that you specify. No part of the original path is appended to the path that you specify.

For example, assume that the original file path is `C:\Documents and Settings\Administrator\My Documents\My Pictures\Vacation2006\Family.jpg`. Assume also that you want to restore the file to a folder called `D:\BestPhotos\`. In the **Restore data to** field, you must provide the folder name and a file name. Assume that you specify `D:\BestPhotos\Family2006.jpg`. IBM Spectrum Protect for Workstations restores the file to this path: `D:\BestPhotos\Family2006.jpg`.

If you are restoring data from the `My Documents` folder to another machine with a different user name, you cannot select to restore to the original location. Instead, specify a location such as `\\users\joanne\my documents\`.

Tip: When you restore data to a new folder, you must place a trailing \ after the folder name. Otherwise, the file that is restored is renamed to the folder that is specified. For example, if the user put `D:\BestPhotos`, that is the name of the restored file.

Restore wizard Summary panel

Use the **Summary** panel to view a summary of your choices, and to start the restore process.

The **Summary** panel displays the locations, and the number of files that you specified in the wizard.

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

Choose **Finish** to restore your files. The **Directory Restore** dialog opens. Use this dialog to specify whether to:

- Restore the latest version of the files in that directory, or to
- Automatically select the latest versions of the files in the folders from a specified date.

If messages are enabled, a message indicates when your restore operation is complete.

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

Chapter 7. Storage areas of IBM Spectrum Protect for Workstations

IBM Spectrum Protect for Workstations stores many backup copies in the native file format. You can restore the backup copies by using native file system commands. Some backup copies are created using sub-file copy, compression, or encryption. These must be restored with the IBM Spectrum Protect for Workstations client.

Format of backup copies

IBM Spectrum Protect for Workstations keeps most backup copies in the same format as the original file.

IBM Spectrum Protect for Workstations provides tools and views to see backup copies and restore the files. However, in many cases you do not have to use IBM Spectrum Protect for Workstations to restore backup copies. These files have the same content as the originals, in a directory tree structure that duplicates the original directory structure.

The following types of backup copy are not in the same format as the original files, and must be restored by using IBM Spectrum Protect for Workstations:

- Backup copies that are stored on IBM Spectrum Protect server.
- Backup copies that are encrypted.
- Backup copies that are compressed.
- Large files that are backed up with subfile copy. In the storage area, the subfile copies have a `-FPdelta` file name suffix.
- Versions of bitmap backups. In the storage area, these backup copies have a `-TPdelta` file name suffix.

Version format of backup copies created by IBM Spectrum Protect for Workstations

As you change a file, IBM Spectrum Protect for Workstations keeps backup copies of each version of the original file.

To track versions of a file, IBM Spectrum Protect for Workstations 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, IBM Spectrum Protect for Workstations 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` might 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, IBM Spectrum Protect for Workstations deletes inactive backup copies of a file before active backup copies are deleted.

A file that is protected by schedule might change several times during the schedule interval. Only the last version of the file prior to the end of the schedule is backed up. A continuously protected file is backed up after every saved change.

Configure the number of versions of backup copies to keep in the Settings Notebook. Depending on the storage type, enter the number of versions to keep in the following fields:

- Copies on local storage: the > **General** > **Versions to keep**.
- Copies on remote storage: **Remote Storage** > **Versions to keep**.
- Copies of an email file: **Email Protection** > **Versions to keep**.

Tools restriction for modifying backup copies

If you modify backup copies with native file system tools, the client ceases to function correctly and is not supported.

You can use native file system tools to copy backup copies to restore your original files. Do not use native file system tools to modify backup copies. Use native file system tools to remove backup copies only if you uninstall the client.

Chapter 8. Troubleshooting the IBM Spectrum Protect for Workstations client

Information and suggested solutions are provided for some common problems with IBM Spectrum Protect for Workstations clients.

Files are not backed up by IBM Spectrum Protect for Workstations

Files can fail backup for several reasons. Some common reasons are provided in this section.

Storage for backup copies is not correctly configured in IBM Spectrum Protect for Workstations

If the area to store backup copies of your protected files is not properly specified, IBM Spectrum Protect for Workstations can not back up files.

Verify that you have correctly specified local or remote storage areas in the Settings Notebook. Local storage and which location (local or remote) is specified in the "**General** panel of client Settings Notebook" on page 26 of the Settings Notebook. Remote storage is specified in the "**Remote Storage** panel of client Settings Notebook" on page 36.

Files to protect are incorrectly configured in IBM Spectrum Protect for Workstations

The files that IBM Spectrum Protect for Workstations protects are configurable. If you have configured your list of protected files incorrectly, IBM Spectrum Protect for Workstations does not back up the files.

IBM Spectrum Protect for Workstations backs up only those files that are configured for protection. The list of continuously protected files is configured in the "**Files to Protect** panel of client Settings Notebook" on page 28 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 29.

Files in use are not backed up by IBM Spectrum Protect for Workstations

Attempts to perform a local or remote backup of a file that is saved but not closed can fail. This can occur with Quicken Quick Books objects (files with an extension ending in .QBW).

The failure is indicated by the message in the Windows System Tray: `The software has experienced a problem. Check for details in the View Report link from the Status page. Also check the Windows System Event log and Application log.`

Details of the failure in the linked report and in `replication.log` can look like this:

```
<replication-status when="date/time" lastStatus="FAIL"
explanation="WinErr:32(creln)"
errValue="5081" errMnemonic="SRCFILE" action="COPY"
src="X:\path\to\filename.QBW"
dst="C:\RealTimeBackup\x\path\to\filename.QBW"
```

To protect such files, add the application type to the include list for scheduled backup, and select a time for scheduled backup when the application is not in use.

Files are not backed up to IBM Spectrum Protect server

These topics discuss problems encountered when backing up files to IBM Spectrum Protect server.

IBM Spectrum Protect node name does not match the host name

If the node name assigned by the IBM Spectrum Protect administrator is different from the IBM Spectrum Protect for Workstations client host name, back up to the IBM Spectrum Protect server fails. The reason is that the IBM Spectrum Protect for Workstations cannot identify itself properly to the IBM Spectrum Protect server.

The following error message displays:

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

IBM Spectrum Protect for Workstations uses IBM Spectrum Protect API. By default, the IBM Spectrum Protect API uses the client host name as the IBM Spectrum Protect node name when identifying itself to the IBM Spectrum Protect server. A IBM Spectrum Protect server administrator typically registers a node using the host name. In some cases, the IBM Spectrum Protect server administrator uses a name that is different from the client host name and causes the problem.

If it happens, you must configure the IBM Spectrum Protect API to use the appropriate node name when logging on to the IBM Spectrum Protect server. You can correct this problem by completing these steps:

1. Edit the `dsm.opt` file. This file is in the IBM Spectrum Protect for Workstations subfolder of the "Accessing the program data folder" on page 40.
2. Add the node name to the `dsm.opt` file. Go to the end of the file, and on a new line add the NODENAME parameter followed by the node name. For example: `NODENAME TSMclientnode1`.
3. Save the `dsm.opt` file.

The next time IBM Spectrum Protect for Workstations connects to the IBM Spectrum Protect server, it uses the node name you specified. IBM Spectrum Protect for Workstations prompts you for the password, if necessary.

IBM Spectrum Protect client node lacks authority to delete backup copies

If IBM Spectrum Protect for Workstations does not have delete backup permission on the IBM Spectrum Protect server, it cannot successfully purge older files when the designated storage space is getting full.

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

```
FilePath ERROR ANS1126E (RC27)
The file space cannot be deleted because
this node does not have permission to delete archived or backed up data.
```

The following error is displayed in a pop-up window:

```
Target file system can only handle sequential I/Os.
```

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

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

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

1. Log into the IBM Spectrum Protect server and bring up the IBM Spectrum Protect administrative command line.
2. Enter this command to the IBM Spectrum Protect server: **update node** TSMclientnode1 **backdel=y**.

Enable permission to delete backup copies for IBM Spectrum Protect Express server as follows:

1. Open an administrative command prompt.
2. Enter this command: `query session`. Note the session numbers for your client node.
3. Enter this command, where session_number is the session number you identified in the previous step: `cancel session session_number`. Repeat if there is more than one session for your client node.
4. Enter this command, where TSMclientnode1 is the name of your client node: `update node TSMnode backdel=y`

Non-system accounts do not have appropriate user security rights to use IBM Spectrum Protect

If a non-system account does not have appropriate user security rights, and IBM Spectrum Protect for Workstations is configured to back up files to IBM Spectrum Protect server, files modified by the non-system account are not backed up.

In order to back up files to a IBM Spectrum Protect server, the proper user security rights must be given to the non-system user account to use the IBM Spectrum Protect 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.

IBM Spectrum Protect for Workstations user interface replaces existing browser session

When the user interface is started, the interface replaces an existing browser session. You can modify this behavior by changing settings in Mozilla Firefox and Internet Explorer.

In Internet Explorer version 10 and later versions, modify the following browsing settings to change the browser behavior:

1. Click **Tools** > **Internet Options**.
2. In the **General** section of the **Internet Options** notebook, click **Tabs**.
3. In the section **Open links from other programs in**, click **A new window** and click **OK**.
4. In the **Internet Options** notebook, click **OK**.

In Mozilla Firefox version 24.5.0 and later versions, modify the following browsing settings to change the browser behavior:

1. Click **Tools** > **Options** > **Tabs**.
2. Click **Open new windows in a new tab instead**.
3. Click **OK**.

IBM Spectrum Protect for Workstations user interface contains no file data

If the IBM Spectrum Protect for Workstations daemon is not running, or if your browser is in offline mode, the IBM Spectrum Protect for Workstations 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 IBM Spectrum Protect for Workstations daemon is not running.

To determine if the IBM Spectrum Protect for Workstations daemon is running, and restart if necessary, see "Restarting the client process" on page 54.

Restarting the client process

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

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

To restart the process on a Command Prompt window, complete the following steps:

1. Open a Command Prompt window.

2. Navigate to the IBM Spectrum Protect for Workstations installation folder.
3. Enter the following command: `filepathsrv -d`.
4. Confirm that the process is running by checking the System Event log or Task Manager. If the process is running, an entry in the System Event log contains the following message: `HTML listener started successfully and listening on port 9003`. This process is event # 6049. In Task Manager, you can see **`FilePathSrv.exe`** process.

You can also restart the process from the **Start** menu. Choose **Start > All Programs > Startup > SP4WKSTNSSrv**.

The number of backup copy versions is greater than configured in IBM Spectrum Protect for Workstations

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

The problem occurs when file versions are not tracked properly.

The problem can occur because data folders were not removed between an uninstallation and a new installation. The new installation does not have a record of the backup copies that were created from the previous installation and use of the product. This problem can occur on local storage, remote storage, or both. For a list of folders to remove after uninstallation, and before you install IBM Spectrum Protect for Workstations again, see Removing old data files after uninstallation.

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 IBM Spectrum Protect for Workstations tracks file versions without encryption/compression differently than file versions with encryption/compression.

As an example, consider the following scenario as to how this problem can arise:

1. A file `file.txt` is continuously protected, and reaches the default version limit of five backup copies. These backup copies were not encrypted or compressed.
2. You enable compression.
3. IBM Spectrum Protect for Workstations creates up to five new backup versions of the file `file.txt`.

The restore view shows the following file versions:

- Five versions of the file that have the name `file.txt`, corresponding to the original five versions that were backed up without compression.
- Five versions of the file that have the name `file.txt.cdp`, corresponding to the new five versions that are backed up with compression enabled.

Limit user access to files on a target file server

Set up the security permissions on a target file server to make sure that users have access only to the files that they back up.

By default, the first client that connects to a specific server share creates the `RealTimeBackup` directory. Permissions that are assigned to the `RealTimeBackup` directory do not prevent users from reading files that they do not own.

The settings that are used in this example assume one primary user of IBM Spectrum Protect for Workstations on the client. This primary user is the first user that connects to the server and creates the subdirectory for files that are backed up from the client. If IBM Spectrum Protect for Workstations operates from other accounts on that client, failures might occur when copying files to the remote server. Error messages such as `Failed to open the destination file` are logged to the activity report.

Windows file server

This example assumes that the following conditions exist:

- The Windows server shares a directory named `c:\fileservertest`.
- The accounts that are used to access the server are members of the `Users` group.

Access Control List settings for the `RealTimeBackup` directory

Access Control List (ACL) settings enable client accounts to create directories that are only accessible by the account that creates the directories. As a result, the directory that contains data for a node is not created until that node connects to the server.

Using Windows Explorer, set the ACL for the `c:\fileservertest\RealTimeBackup` directory according to the settings in ACL settings for the `RealTimeBackup` directory.

Important condition for ACL settings: Do not select the check box **Apply these permissions to objects and/or containers within this container only**.

Table 5. ACL settings for the `RealTimeBackup` directory

Type	Name	Permission	Applies to
Allow	Administrators	Full Control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	This folder, subfolders, and files
Allow	Users	Special	This folder only
Allow	OWNER RIGHTS*	Full Control	This folder, subfolders, and files

*The OWNER RIGHTS object must be added for Windows 2008 Servers.

The ability for objects to inherit permissions from the parent is not set. As a result, set the `Special` access for the `Users` group to provide the following settings:

```
Traverse Folder / Execute Allow
List Folder / Read Data Allow
Read Attributes Allow
Read Extended Attributes Allow
```

```
Create Files / Write Data Allow
Create Folders / Append Data Allow
Delete subfolders and files Allow
Read Permission's Allow
```

To verify that the ACL settings are correct, run the following command:

```
Cacls
```

The following output for the `Cacls` command shows the correct ACL settings:

```
CREATOR OWNER:(OI)(CI)(IO)F
```

If the parameter `(NP)` is included in the command output, set the ACL settings again to exclude `(NP)`. To ensure that the `(NP)` is excluded, verify that the check box **Apply these permissions to objects and/or containers within this container only** is not selected.

ACL settings for the `RealTimeBackup\BackupAdmin` directory

The `RealTimeBackup\BackupAdmin` directory is used by the IBM Spectrum Protect for Workstations client to download revisions and configurations. Nodes require read-only access to these directories:

```
c:\fileservertest\RealTimeBackup\BackupAdmin
```

Table 6. ACL settings for the `RealTimeBackup\BackupAdmin` directory

Type	Name	Permission	Applies to
Allow	Users	Read, Execute	This folder, subfolders, and files
Allow	Administrators	Full Control	This folder, subfolders, and files

The ability for objects to inherit permissions from the parent is not set. As a result, set the `Special` access for the `Users` group to provide only these settings:

```
Traverse Folder / Execute Allow
List Folder / Read Data Allow
Read Attributes Allow
Read Extended Attributes Allow
Delete subfolders and files Allow
Delete Allow
Read Permission's Allow
```

UNIX file server that is running Samba

This example assumes that the Samba server is set up to share a directory that is named `/fileservertest`.

These settings enable users to create directories under the `RealTimeBackup` directory:

```
chmod o+wrxt /fileservertest/RealTimeBackup
chmod o+rx /fileservertest/RealTimeBackup/BackupAdmin
chown root /fileservertest/RealTimeBackup/BackupAdmin
```

In the Samba configuration file (`smb.conf`), set the `create mask` and `directory mask` parameters to each specify `0700`. For example:

```
[fileservertest]
path = /fileservertest
writable = yes
create mask = 0700
directory mask = 0700
```

Restoring many files from a single directory IBM Spectrum Protect for Workstations

When restoring many files from a single directory using the restore wizard, a message saying that the script is taking too long displays.

When using the restore wizard to list the contents of a directory containing over 3000 files, the browser issues a message saying that the script is taking too long. If you see this message, you can choose to allow the script to continue. Otherwise, you can also choose to customize the behavior of this dialog to avoid the message.

See the following links for details:

Firefox: http://support.mozilla.org/en-US/kb/Warning%20Unresponsive%20script?s=A+script+on+this+page&r=0&e=sph&as=s .

Microsoft Internet Explorer: http://support.microsoft.com/kb/175500.

Backup fails after configuration because of insufficient IPV6 permissions

If IBM Spectrum Protect for Workstations does not have IPv6 or the appropriate permissions to the IPv6 path, then reports cannot be sent to the Central Administration Console.

If you do not have IPv6, IBM Spectrum Protect for Workstations is not able to report to the Central Administration Console (CAC). After configuration, IBM Spectrum Protect for Workstations uses the IPv6 path to reach the administration folder. If the client was using an IPv4 path prior to this release, it switches to IPv6.

Configuration scripts created using the CAC use the IPv6 path in the configuration script field to denote the location of the administration folder. If the user does not have IPv6 or does not have the appropriate permissions to the IPv6 path, then IBM Spectrum Protect for Workstations will not be able to send reports to the CAC. To resolve the issue, set up IPv6 and ensure that the account running the client has the correct permissions to the IPv6 path.

Frequently Asked Questions

Here are some of the common questions that users have about how to use the product.

How to make sure changes to the include/exclude list are pushed to all clients on a group?

Sometimes changes made to the include/exclude list in the Central Administration Console might not be sent to all of the clients in a particular group. This omission might arise because the client cannot read the configuration file that is sent by the Central Administration Console.

Complete the following steps to ensure that the client can read the configuration file:

1. Open a Windows Explorer window and navigate to the administration folder.
2. Navigate to the `RealTimeBackup\COMPUTERNAME\BackupAdmin\Downloads` directory.
3. Try to open the files in this directory by using Notepad. If any of the files fail to open in Notepad, then there might be a problem with the permission levels on the administration folder.

What variables are supported for the include/exclude lists?

The following variables are supported through the central administration console.

- $(*USERNAME*): For example: Administrator `(getenv("USERNAME"))`
- $(*MYDESKTOP*): For example: `C:\Documents and Settings\Administrator\Desktop (CSIDL_DESKTOPDIRECTORY)`
- $(*MYFAVORITES*): For example: `C:\Documents and Settings\Administrator\Favorites (CSIDL_FAVORITES)`
- $(*MYPROFILE*): For example: `C:\Documents and Settings\Administrator (CSIDL_PROFILE)`
- $(*MYDOCUMENTS-SHORT*): For example: `My Documents (CSIDL_PERSONAL)`
- $(*MACHINE*): For example: `AdminLaptop (gethostname())`

How to identify an administration folder for clients that are backed up to a IBM Spectrum Protect server?

To deploy centrally managed clients that are backed up to a IBM Spectrum Protect server, you must configure the clients by using the IBM Spectrum Protect for Workstations Central Administration Console. The configuration specifies what IBM Spectrum Protect server to back up to and what central administration folder to use. You then copy the configuration file (`fpa.txt`) to the `%WINDIR%\system32` directory on the client machine before you install the client software.

How to create a configuration:

1. Create a group by using the Central Administration Console.
2. On the administration folder page, select the administration folder that the client reports to and assign that group to the folder.
3. Select the folder again and select the `Create a Configuration File` option.
4. Click **Get Configuration**. The text area is filled with data. Highlight the entire text area and copy it to a file named `fpa.txt`.

If the clients are already deployed, you can point them to an existing administration folder by running this command from the installation directory on the client: **`fpa config-set GlobalManagementArea="\\server\share"`**. Replace **`\\server\share`** with the address of the administration folder.

How to find out more information about error messages?

Detailed information on error messages can be found in the IBM Spectrum Protect for Workstations message guides. The message guides are available in PDF format and on the product information centers.

How to get more information on how to troubleshoot problems with IBM Spectrum Protect for Workstations?

More information about how to troubleshoot problems with IBM Spectrum Protect for Workstations is available in Chapter 5 of the IBM Redbook "Deployment Guide Series: Tivoli Continuous Data Protection for Files V3.1". To download the guide, go to http://www.redbooks.ibm.com/redbooks/SG247423/wwhelp/wwhimpl/js/html/wwhelp.htm.

A frequently asked questions tech note is available on the support site. For more information, see CDP for Files / IBM Spectrum Protect for Workstations FAQ Document

Are there any issues when you use IBM Spectrum Protect for Workstations and other applications that use GSKit8?

There is a known issue when you uninstall IBM Spectrum Protect for Workstations version 6.3.0 if other applications that use GSKit8 are also installed on the system, such as the IBM Spectrum Protect Backup Archive Client.

After you uninstall IBM Spectrum Protect for Workstations, you might see the following error message when you use the IBM Spectrum Protect Backup Archive Client:

- `ANS1463E Unexpected error in cryptography library`

For more information, see the technote Uninstallation issues with IBM Spectrum Protect for Workstations and other applications using GSKit8 on Windows 7 and Windows Vista, at http://www.ibm.com/support/docview.wss?rs=4199&tc=SS6PEB&uid=swg21584788.

Appendix A. Messages issued by IBM Spectrum Protect for Workstations

Messages are issued by the IBM Spectrum Protect for Workstations client and the Central Administration Console to provide you with activity information. All of these messages have the prefix FBW.

Format of messages issued by IBM Spectrum Protect for Workstations

Each element of a message that is issued by IBM Spectrum Protect for Workstations provides information that can help you to understand and fix a problem.

Messages consist of the following elements:

- A three-letter prefix.
- A number that identifies the message.
- A one-letter severity code, also called the message type.
- Message text that is displayed on screen and written to message logs.
- Explanation and User Response texts. These texts elaborate on the message text, and are accessible only in documentation.

The severity codes give an indication of the severity of the issue that generated the message. The severity codes have the following meanings:

S Severe error. Processing cannot continue.

E Error. Processing cannot continue.

W Warning. Processing can continue, but problems might occur later.

I Information. Processing continues. A user response is not necessary.

Message variables in the message text are formatted in italic font.

Messages issued by the Central Administration Console

FBW messages with a message number of less than 5000 are issued by the IBM Spectrum Protect for Workstations Central Administration Console.

FBW0201I The IBM Spectrum Protect for Workstations servlet is starting.

Explanation: Starting the IBM Spectrum Protect for Workstations servlet.

User response: No action is required.

FBW0202I The IBM Spectrum Protect for Workstations servlet has started.

Explanation: The IBM Spectrum Protect for Workstations servlet is now accepting requests from the web browser.

User response: No action is required.

FBW0203E The ajax command is invalid.

Explanation: This is an internal error.

User response: Stop and start the Central Administration Console service. If the problem persists, install the Central Administration Console again.

FBW0204I The client *client name* was updated with a new configuration from the group *group name*.

Explanation: The client is running with a new configuration.

User response: No action is required.

FBW0205I **A new client was discovered at** *client address***.**

Explanation: There was a scan of all the administration folders and a new client was discovered at the specified address.

User response: No action is required.

FBW0206I **A new administration folder was identified at** *folder address***.**

Explanation: An administration folder was identified and a scan for this folder will be performed to discover new clients.

User response: No action is required.

FBW0207I **The following administration folder was deleted from the database:** *folder address***.**

Explanation: An administration folder at the specified address was deleted.

User response: No action is required.

FBW0208I **The configuration for client** *client name* **has changed.**

Explanation: The specified client has accepted a new configuration.

User response: No action is required.

FBW0209I **Starting the audit log.**

Explanation: The audit log has started.

User response: No action is required.

FBW0210I **The IBM Spectrum Protect for Workstations servlet stops.**

Explanation: The IBM Spectrum Protect for Workstations servlet stops and no longer accepts requests from the web browser.

User response: Restart the Central Administration Console service.

FBW0211I **The administration folder address** *folder address* **must be in UNC format. For example: \\\\server\\share.**

Explanation: UNC is a Universal/Uniform Naming Convention. It describes the location of a volume, directory, or file on a local-area network (LAN). The format is \\\\server-name\\shared-resource-pathname.

User response: Enter a valid path for the administration folder and then retry the operation.

FBW0212I **The administration folder** *folder address* **already exists.**

Explanation: This administration folder has already been identified.

User response: Enter a different administration folder and then retry the operation.

FBW0213I **The group** *group name* **already exists.**

Explanation: This group name has already been defined.

User response: Enter a different group name and then retry the operation.

FBW0214I **The group** *group name* **was not found.**

Explanation: This is an internal error. The group specified is not in the database.

User response: Check the group name and then retry the operation.

FBW0215I **The client** *client name* **was not found.**

Explanation: This is an internal error. The client specified is not in the database.

User response: Check the client name and then retry the operation.

FBW0216I **The client configuration at** *filename* **was not found.**

Explanation: The file that contains the configuration has not been generated.

User response: Check if the client is online. Set the scan settings and the settings for how often the client checks for updates to a shorter interval. Then retry the operation.

FBW0217E **There was an error accessing the client configuration at** *filename***.**

Explanation: The administration console cannot read the contents of the file that contains the configuration.

User response: Check the permissions on the configuration file.

FBW0218I **The administration folder directory** *folder address* **was not found.**

Explanation: It is possible that the administrator does not have the permissions to create the administration folder on the remote server.

User response: Check the permissions of the remote location.

FBW0219I **The administration folder record** *folder address* **was not found.**

Explanation: The administration folder may have been deleted by another user.

User response: Refresh the administration folder view to get an updated list of folders.

FBW0220I **The configuration file for group** *group name* **was not found.**

Explanation: This is an internal error. The configuration file may have been deleted.

User response: Ensure that the administration console has correct permissions to access the database.

FBW0221E **There was an error accessing the configuration file** *config file* **for group** *group name***.**

Explanation: The administration console cannot read the content of the configuration file.

User response: Check the permissions on the configuration file. Verify that the service account has full access to the file.

FBW0222I **The folder for the client** *address* **is missing.**

Explanation: The folder for the client does not exist. It may have been deleted.

User response: No action is required.

FBW0223I **The administration folder name** *folder name* **already exists in the database.**

Explanation: The administration folder name has already been defined for another administration folder.

User response: Enter a different name for the administration folder and then retry the operation.

FBW0224I **The client activity report at** *directory* **was not found.**

Explanation: The file that contains the activities for this client has not been generated.

User response: Check if the client is online. Set the scan settings and the settings for how often the client checks for updates to a shorter interval. Then retry the operation.

FBW0225E **There was an error accessing the client activity report at** *filename***.**

Explanation: The administration console cannot read the content of the client activity report.

User response: Check the permissions on the client activity report file. Verify that the service account has full access to the file.

FBW0226E **The alert** *name* **was not found in the database.**

Explanation: The alert may have been deleted.

User response: Refresh the alerts table to get an updated list of alerts.

FBW0227E **The script** *name* **was not found in the database.**

Explanation: The script may have been deleted.

User response: Refresh the scripts table to get an updated list of scripts.

FBW0228E **An error was encountered when trying to send an email alert. Check the email settings.**

Explanation: The administration console was unable to send an email alert with the specified settings.

User response: Verify the email settings are correct and then retry the operation.

FBW0229E **An error was encountered when trying to send an email alert. No mail server is defined.**

Explanation: The mail server name is not provided.

User response: Enter a valid mail server name and then retry the operation.

FBW0230E **The request was denied because that alert name** *alert name* **already exists.**

Explanation: This alert name has already been defined.

User response: Enter a different alert name and then retry the operation.

FBW0231E **The request was denied because that script name** *script name* **already exists.**

Explanation: This script name has already been defined.

User response: Enter a different script name and then retry the operation.

FBW0232E **An unexpected error occurred while processing the request.**

Explanation: This is an internal error.

User response: No action is required.

FBW0233E **An error occurred while writing the script** *script name* **to the directory** *directory***.**

Explanation: The administration console cannot create the file for the script.

User response: Verify that the service account has full access to the directory and then retry the operation.

FBW0234W **The client** *client address* **did not accept the script** *script name* **from the directory** *directory***, in the specified time.**

Explanation: The client failed to accept the script within the acceptance timeout limit.

User response: Verify the client is up and running. Verify the connectivity between the client and the remote server. Ensure the acceptance timeout is long enough.

FBW0235I **The script** *script name* **was accepted for processing by client** *client address***.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0236I **The script** *script name* **has been sent to the client** *client address* **for processing.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0237E **Unable to delete group** *group name***. There are clients or administration folders that are still referencing this group.**

Explanation: There are clients assigned to this group or an administration folder is still referencing this group. This group cannot be deleted.

User response: Ensure that no clients or administration folders are using this group.

FBW0243E **Invalid condition value in condition** *condition name***.**

Explanation: The value for the alert condition is not valid.

User response: Correct the value and then retry the operation.

FBW0244E **Invalid address syntax in address** *address***.**

Explanation: An email address consists of a user name, followed by an @ sign then the domain name. For example: youremail@yourcompany.com

User response: Enter a valid email address.

FBW0245I **Package** *package name* **has been sent to client** *address***.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0246I **Package** *package name* **has been accepted by client** *address***.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0247E **An error occurred while deploying the package** *package name* **to client** *client name***. The package is missing.**

Explanation: An error occurred and the package is missing.

User response: Copy the package to the deployments directory or select another package.

FBW0248E **Unable to cancel the search operation. The search id was not found.**

Explanation: The search operation has already been cancelled.

User response: No action is required.

FBW0249I **The search operation was cancelled.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW0250I **There were no administration folders found.**

Explanation: The specified location does not have any administration folders.

User response: Enter a different location and then retry the operation.

FBW0251I **The location to search** *location address* **was not found.**

Explanation: The specified search path does not exist.

User response: Verify the remote location and then retry the operation.

FBW0252I **The location to search** *location address* **is not a directory.**

Explanation: The specified path is a file. The search location must be a directory.

User response: Correct the search location and then retry the operation.

FBW0253E **An error occurred when an attempt was made to insert a backup entry into the reporting database. The entry is discarded.**

Explanation: An error occurred when entries were read from a client activity log and an attempt was made to put the data into the report database.

User response: No action is required.

FBW0254E **Invalid referrer in the HTTP request header.**

Explanation: The request could be a cross-site request forgery. Request is denied.

User response: No action is required.

FBW0255E **Invalid password. Password cannot contain these special characters `@!%&()-|;'"<>` or the password cannot be encoded.**

Explanation: The password might contain one of these special characters `@!%&()-|;'"<>` or the user does not have administration privilege to encode the password.

User response: Verify that the user has administration privilege or change the password and try again.

FBW0256E **A read or write error was encountered. The password was not changed.**

Explanation: There was an error in reading or writing the password to file.

User response: Verify that the user has administration privilege and try again.

FBW1019E **Group name is reserved for internal use. Enter a different group name.**

Explanation: The group name that you specified is a reserved group name.

User response: Specify a different group name.

FBW1020E **Specify a number to indicate when to remove backups of deleted files.**

Explanation: In the Group Configuration page, you must specify a value in the **Remove backups of files deleted...** field before you click **Next**.

User response: Specify a number of days in the past in the **Remove backups of files deleted...** field. Backups of files that were deleted before this point in the past are removed.

Messages issued by the IBM Spectrum Protect for Workstations client

FBW messages with a message number of 5000 or greater are issued by the IBM Spectrum Protect for Workstations client.

FBW5001E **No memory available for operation**

Explanation: The program is low on memory. It is possible that there is a programming flaw that resulted in run-away memory usage, or that the system does not have enough memory.

User response: Open the Task Manager and ensure that the application is not using more memory over time. Then add more memory to the computer to resolve the issue.

FBW5003E **The device driver could not be opened.**

Explanation: In order for a user-mode program to talk to the kernel component driver, it must open a device node to communicate with the kernel. This error could be because the driver is not loaded, the device-node does not exist, or it has insufficient privileges.

User response: Reboot the system, if the problem persists contact support.

FBW5004E **Unknown IOCTL value**

Explanation: The user daemon program communicates with the kernel component by sending a binary value (an IOCTL) to the kernel. The kernel then interprets this value as a command. This error means that the kernel is unaware of the meaning of the specified value. This is likely to be caused by a mismatch of the kernel and daemon revision levels or by some non-authorized program sending arbitrary data.

User response: Ensure the driver Fp.sys and Filepathsrv.exe are the same version. You could also uninstall and reinstall the product.

FBW5010E The specified tracing level is not known.

Explanation: The specified tracing level is not known or incorrectly spelled.

User response: Ensure the specified tracing level is valid, in the correct format, and spelled correctly.

FBW5011E The specified logging device is unknown or unsupported on this platform.

Explanation: Typically, only the terms SCREEN and FILE are valid logging device key words. Not all platforms can support logging to a screen or terminal device.

User response: Ensure the specified device is valid and spelled correctly.

FBW5013E Error creating the HTML listener

Explanation: This is typically caused when the default port 9003 is already in use by another product.

User response: Change the default port used, refer to the technote: HOW TO MODIFY THE DEFAULT PORT 9003 IF ANOTHER APPLICATION IS CURRENTLY USING IT. This tech note is in the support portal.

FBW5018E The current operation is denied by the operating system due to permission.

Explanation: Some attempted operation such as a mkdir, is refused by the operating system due to insufficient privilege or permission.

User response: In a command window attempt the same operation that resulted in the error, this can sometimes give more information for the error. Ensure the user has the correct privledges for the particular directory or file.

FBW5019E Queue or queue transaction is corrupted

Explanation: The daemon is attempting to read or write to the kernel queue but the data does not validate as a known queue item.

User response: Internal error in the application, no action required.

FBW5022E Unable to access the specified file

Explanation: The file specified is unable to be accessed. Possibly spelled incorrectly, or bad path, or permissions.

User response: Ensure the user has the proper permissions for the file and directories involved and that the file and directory exist.

FBW5028E Specified named object does not exist

Explanation: An operation that is attempted to work on a database object, such as a rule or action, can not find the one specified.

User response: Ensure the rule or action name is correct and the database is configured properly.

FBW5029E The database query for the remote location returned an empty string or remote backup is disabled.

Explanation: The Group1Remote action was not found in the database or is disabled. The database was queried for the value before the initial configuration completed, a remote location was not specified in the GUI, or remote backup is disabled in the GUI.

User response: Ensure the remote backup is enabled and the remote location is specifed in the GUI.

FBW5037E Some items in the XML command were not recognized or consumed

Explanation: Not everything in the specified XML message was consumed. Possibly something is misspelled and thus not recognized or some other feature has been added in a newer release and is attempted but not known.

User response: No action required

FBW5040E The server does not have any space available.

Explanation: The storage pool on the server is full.

User response: Report to your system administrator to increase the storage pool on the server.

FBW5047E A system command such as mkdir, system, or unlink resulted in an error.

Explanation: Some intrinsic functions of the native operating system, such as mkdir, rm, or system, resulted in an error that was not anticipated.

User response: Ensure that the user has the correct permissions for the operation. Reboot the system if the problem persists.

FBW5053E File or path does not exist.

Explanation: Files have to be opened for reading or writing. For example database files or files for replication management. This error is because a file cannot be found.

User response: Ensure that the file exist, the pathname is valid, and is spelled correctly.

FBW5056E Value specified for an error value is either missing or invalid

Explanation: These error messages are processed. There must be a val= statement in the XML string. The value must be between 0 and 99999.

User response: The message file is corrupted and you need to reinstall the product. Contact support if the problem persists.

FBW5057E The xml paragraph does not contain the MsgText and /MsgText tags

Explanation: Incorrectly formed expression for an error-message.

User response: The message file is corrupted and you need to reinstall the product. Contact support if the problem persists.

FBW5077E The source file for the backup operation was not found.

Explanation: The file may have been deleted before the backup happened.

User response: Ensure that the file being backed up exists and that the path is correct.

FBW5078E The source file for backup has a permission problem.

Explanation: The permissions are not correct for the file.

User response: Ensure that the user has the proper access to the file and that the file exists.

FBW5079E The destination file for backup has a permission problem.

Explanation: The permissions are not correct for the file.

User response: Ensure the user has the proper access to the file.

FBW5080E An operating system error reported trying to open the destination file for backup.

Explanation: The permissions are not correct for the file.

User response: Ensure that the user permission on the file is correct and that the file is not in use by another application.

FBW5081E An operating system error occured when trying to open the source file for backup.

Explanation: The permissions are not correct for the file.

User response: Ensure that the user permissions on the file are correct and the file is not in use by another application at the time of the backup.

FBW5082E Backup failed due to the operating system reporting no space.

Explanation: Not enough space available for the backup.

User response: Increase the storage space available for the backup.

FBW5084I This replication item is being skipped because the file size or date of the source is different from when the operation was recorded.

Explanation: Replication events will be skipped if it appears that the event is older than the source file and thus there should be additional events forthcoming.

User response: Informational message no action required.

FBW5088E A Retention specification did not specify any categories.

Explanation: Retain commands must specify at least one category.

User response: Ensure that at least one category is used with Retain commands.

FBW5089E The supplied item is not a RETAIN item.

Explanation: A incorrectly formed retain command was given.

User response: Ensure that the retain command being used is valid.

FBW5090E The specified retention name is not known.

Explanation: An attempt to reference a given Retain is not known.

User response: Ensure the retain name being used is valid.

FBW5091E The replication.retain clause is missing and is required when doing generations.

Explanation: Replication actions that specify generations MUST have a Retain clause.

User response: Ensure the replication action is formatted correctly.

FBW5092E The duration value specified for a retention category must be greater than the previous duration value.

Explanation: Durations must be specified in increasing duration order.

User response: Change the duration for this category to be greater than the duration of the previous category.

FBW5095E The target file of a skip unset request is not currently in a skipped state.

Explanation: This is an internal error during an unset skip operation.

User response: No action is required.

FBW5101E The replication has failed and this may be because of an networking error, so it is possible to try again.

Explanation: This may be related to transient network or reliability issues.

User response: Make sure the network is connected or authenticate to the remote share.

FBW5103E The password is not correct for the specified user.

Explanation: An incorrect password has been supplied.

User response: Enter a correct password then retry the action.

FBW5105I This replication item is being skipped due to the source matching the target.

Explanation: The target file is identical to the one that is already at the target. This is based on the file size and the modification time.

User response: No action is required.

FBW5114E All backups in this queue have been cancelled by the user.

Explanation: The user has cancelled the operation.

User response: No action is required.

FBW5126I The current file backup was cancelled by the user.

Explanation: Backup operation for the file was cancelled.

User response: No action is required.

FBW5127I The backup directory cannot be deleted.

Explanation: You cannot delete the target directory because it is not empty.

User response: No action is required.

FBW5128I The backup item is being skipped because the destination does not exist.

Explanation: The backup cannot be carried out because the target does not exist.

User response: No action is required.

FBW5130E The file being deleted is a directory.

Explanation: Internal error. Attempted to delete a file but encountered a directory.

User response: No action is required.

FBW5132E The operating system is not currently supported.

Explanation: The operating system is not supported.

User response: See the System Requirements section at http://www.ibm.com/software/products/en/spectrum-protect-for-workstations

FBW5137I Data field for a rule in fpa.txt is too long and has been truncated.

Explanation: Internal error. A truncated data field is detected.

User response: No action is required.

FBW5138E The system configuration is locked against changes.

Explanation: Cannot change the system configuration because it is locked.

User response: Use the Central Administration Console to unlock the configuration.

FBW5139I The file is being skipped because it is larger than the configured maximum size for backup.

Explanation: The file size exceeds the maximum limit in the advanced setting tab.

User response: Change the maximum file size limit for this backup type.

FBW5140E Unexpected error with encryption. Detailed information maybe available in the event log or replication log.

Explanation: Internal error. Encryption failed with an error.

User response: No action is required.

FBW5143E The backup failed because the encryption library could not be loaded.

Explanation: The encryption library could not be found or was not the expected version.

User response: Download a new install image and reinstall the application.

FBW5144E The header in the encrypted or compressed file is corrupted.

Explanation: The header where all the file meta data is kept for the compressed or encrypted file has been corrupted.

User response: No action is required.

FBW6001I Last message repeated *number* **times.**

Explanation: Before the centralized logging system displays a message it checks to see if the message is the same as the previous message. If the messages are the same, the system does not display the new message. It counts the number of similar messages and displays information on how many times the message was repeated.

User response: No action is required.

FBW6002E Function: *function* **failed to open file: [***filename***] Reason:** *error***.**

Explanation: The error may occur if the permissions are incorrect, if file or path does not exist, or if the file is corrupted.

User response: No action is required.

FBW6003E Failed to start the *name* **thread. Reason:** *error***.**

Explanation: An unexpected error occured when a thread was created.

User response: Restart the daemon.

FBW6004E Command failed, result:(*retcode***)** *error***.**

Explanation: A command given to the fpa program or parse a configuration file has failed with the specified result-code and messages.

User response: Use the error code to troubleshoot the problem.

FBW6008E Socket *name* **operation failed; Reason:** *error***.**

Explanation: One of the socket operations between the daemon and the html has failed with the operating system error given. Typically this happens when more than one html listener has been started.

User response: No action is required.

FBW6009E General error during function *name***: (***retcode***)** *error***.**

Explanation: An unexpected error occurred from a specified mid-level function. The error and associated message is also specified.

User response: No action is required.

FBW6010E Memory allocation failed of *number* **bytes in function** *name***.**

Explanation: An attempt to allocate memory failed. Either the amount of memory was too high or there was a runaway process. The number of bytes desired and the function needing the memory are specified.

User response: No action is required.

FBW6011E Unknown or unsupported IOCTL value *number* **was given.**

Explanation: Internal error. It is possible that the driver and the daemon are out of sync.

User response: Restart the system or reinstall the software. Then retry the action.

FBW6012E Failed user exec-command [*command***] Result:** *retcode***.**

Explanation: An exec command resulted in an error. The full exec command is specified along with the operating system result value.

User response: No action is required.

FBW6013E Backup failed to open the log file: [*filename***] Reason:** *error***.**

Explanation: The log file for logging every backup transaction could not be opened. It is possible that this is related to a problem with the permissions or the pathname. The result is specified.

User response: No action is required.

FBW6018E **An unexpected error occured during driver read operation to get next item from work queue, error (***retcode***)** ***error*****.**

Explanation: Internal error. The kernel component failed to retrieve the next item from the queue.

User response: No action is required.

FBW6019E **User buffer is too small during driver read operation. User-buffer size:***maxsize* **is not big enough for** *size* **bytes.**

Explanation: This is an internal error. The daemon did not supply a large enough buffer to the driver. This should only occur if the driver and the daemon components are out of sync.

User response: Reinstall the software then retry the action.

FBW6020E **Data (0x%x) sent to the driver from the daemon does not match any addresses in the queue.**

Explanation: This is an internal error. Data relating to a write operation from the daemon to the kernel is invalid and could not be matched-up to a pending transaction.

User response: Reinstall the software then retry the action.

FBW6021E **Too much data (***total* **bytes) sent to the driver. The queue item can only hold** *maxsize***.**

Explanation: This is an internal error. A daemon write operation into the kernel provided too much data. This could be caused by incompatible versions.

User response: Reinstall the software then retry the action.

FBW6029I **Trying to unload the driver but some files still active. Waiting...**

Explanation: This is an informational message. When the driver is requested to unload, it tries to do so safely by waiting until all in-process file objects are complete. The driver will wait and periodically generate this message.

User response: No action is required.

FBW6030E **The kernel audit buffer overflowed and some audits are lost.**

Explanation: The kernel puts audit messages into a buffer that the user daemon must periodically drain. This error could be because the daemon is not running correctly, because too many messages are sent too quickly, or because the buffer is too small.

User response: Restart the daemon and start a full backup.

FBW6031E **The HTML daemon did not start. Consult system error log.**

Explanation: The HTML daemon was unable to start and the specific reason is shown in the system log. This could be because the intended port is in use. Another fpa daemon may be running, or some web-process is communicating with the port and keeping it in-use.

User response: Make sure that the port is not in use by other applications. Restart the system and retry the action. See the tech note at http://www-01.ibm.com/support/docview.wss?uid=swg21300055 for more information.

FBW6033I **Driver loaded and ready.**

Explanation: The driver has successfully completed all of its initialization and is ready to go to work.

User response: No action is required.

FBW6035I **Driver unloading.**

Explanation: The driver has started the processes of unloading. It can not log any messages.

User response: No action is required.

FBW6043E **Replication or mirroring resulted in the destination path matching the source file:***filename***. Action name** *action* **is disabled.**

Explanation: The destination can not have the same path as the source.

User response: No action is required.

FBW6045E ***filename*****, error:** *error***. The application will try again.**

Explanation: An internal error occurrred during an unlink. This happens after a file has been replicated.

User response: No action is required.

FBW6046I **The GUI messages file** *filename* **could not be opened, error:** *error*

Explanation: The message file may be corrupted or missing from the installation folder. The installation folder may also be corrupted.

User response: Look in the installation folder for the message file. If the file exists, verify that the file has

read permissions. You can also reinstall the product to fix this error.

FBW6047I The account must have the "Act as part of the operating system" privilege set.

Explanation: The service daemon needs to run with the "Act as part of the operating system" privilege or run as the local system account.

User response: Use the Windows Local Security Policy tool to set this privilege in the Local Policies->User Rights Assignment section. You can also change the service to run as the local system account.

FBW6048I Daemon started successfully.

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6049I HTML listener started successfully and is listening on port *number***.**

Explanation: This message is for informational purposes only. It indicates the port that the HTML listener is listening on.

User response: No action is required.

FBW6051I The `fpa` command syntax.

Explanation: This message is for informational purposes.

User response: For details about the syntax of the **fpa** command, see technical document 1638130 on the IBM support site: http://www-01.ibm.com/support/docview.wss?uid=swg21638130.

FBW6054I You can not start both the HTML listener and the daemon in interactive mode at the same time.

Explanation: This occurs when the user specifies the -d flag with fpa and also specifies to start both daemons.

User response: Start either the HTML listener or the daemon in interactive mode only.

FBW6057I A special HOLD directory created: *directory*

Explanation: A special HOLD directory created for WORM (Write Once Write Many) or Retention. This message is for informational purposes only.

User response: No action is required.

FBW6058E Special WORM/Retention SHRED directory has non-numeric tail: *directory***.**

Explanation: The path name must end with a number.

User response: Change the path name so that it ends with a number.

FBW6059I Special WORM/Retention SHRED directory created: *directory***.**

Explanation: A SHRED directory or subdirectory was created.

User response: No action is required.

FBW6060E Special WORM/Retention RETAIN directory has improper format: *directory*

Explanation: The format of a path name should be 'Retain[nDays nHours nSeconds]'. For example: Retain10Days

User response: Use path name in the correct format.

FBW6061I Special WORM/Retention RETAIN directory created:*directory* **(***number* **Years,** *number* **Days,** *number* **Hours,** *number* **Minutes,** *number* **Seconds)**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6062E You can not create a RETAIN within a RETAIN tree:*path*

Explanation: Nested RETAIN is not allowed.

User response: Create the directory path with one instance of a RETAIN directory only.

FBW6063I You can not change the base name of a file. Source:*source filename* **Destination:***dest filename*

Explanation: This is an internal error. The file name can not be changed.

User response: No action is required.

FBW6069I The daemon has detected a network error that may be resolved easily. The network may be temporarily unavailable or the current logon information is incorrect. Check access to the network. The application will retry the action. File attempted: *filename***.**

Explanation: The client can not connect to the remote server.

User response: Verify that there is network access and

that the logon information is correct.

FBW6070I **The network appears to be functioning again. Backup resumed for** *filename***.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6075E **The restore location,** *destination***, must be an absolute pathname.**

Explanation: The restore process requires a full path name to a file or to a directory.

User response: Modify the restore destination then retry the action.

FBW6076I **The remote target does not support the native Windows Backup-API for fully capturing file attributes. The application uses an alternative file-copy heuristic.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6077I **The application has detected the target backup device is full. This may be a temporary issue. Create some free space at the target location. The application will retry the action.**

Explanation: The backup target needs more storage.

User response: Delete some files to create free space at the target location. The remote storage state may be out of synch if you delete the backed up files.

FBW6085I **Completed restore request. The client restored** *number of* **files.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6086E **Fail to do** *action string* **file** *source filename* **to** *dest filename***. Error:** *error***. Extra information:** *additional error*

Explanation: File can not be backed up.

User response: No action is required.

FBW6087I **The application can not reach the network target. This may be a temporary issue. The application will retry the action.**

Explanation: There is no network connection to the remote server. The computer may not be logged on to the network. This issue may also occur if the remote target was changed and there are files in the queue for backups to the previous remote target.

User response: Verify that the remote server is running and that the computer can ping the server. You may need to authenticate through a firewall or to logon to the network. If files are queued to a remote target that is no longer valid, you need to clear the queue to resolve this error.

FBW6088I **The network appears to be functioning again. Backup resumes.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6089I **The application has experienced a problem. Check for details in the View Report link from the Status page. Also check the Windows System Event log and Application log.**

Explanation: An error occurred, check the error logs.

User response: If View Report link from the Status does not contain any details, check the Windows System Event log and the Application log.

FBW6091I **Password information is needed for backup. Acknowledge the prompt or launch the user interface.**

Explanation: The application requires password details to perform an action. The IBM Spectrum Protect server may need a password to perform backups. The WebDav server or the file server may need an encrytion password. The Lotus Notes® application may need a password.

User response: Enter the password when it is prompted.

FBW6092I **A new version of the product is being installed.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6094I **New software has been loaded and you must restart the machine to resume data protection.**

Explanation: The machine must be restarted to run the new software.

User response: Restart the machine.

FBW6095I **Your product trial evaluation period has expired.**

Explanation: The trial period has ended.

User response: Uninstall the product or install the full product.

FBW6096I **Driver was not loaded correctly. Data protection is not functioning.**

Explanation: A problem may have occurred during the installation and the driver was not loaded correctly.

User response: Uninstall the product then reinstall it.

FBW6097E **One or more delta files is missing or was not accessible during the restore operation.**

Explanation: The version of the file being restored was corrupted or manually deleted from the remote storage.

User response: Restore an earlier version of the file.

FBW6101I **The current version of Lotus Notes installed on this machine does not contain full support for this application. An upgrade of Lotus Notes is recommended. If you choose not to upgrade Lotus Notes, the application will still function, but it may need to wait and retry a Lotus Notes database backup if the files are being updated heavily while the backup is being performed.**

Explanation: The application does not support the current Lotus Notes version.

User response: Upgrade to Lotus Notes 7.0 or later.

FBW6102I **Warning: The My Documents folder in the include list does not match the location where the system stores your documents in. Add *folder*\ to the include list.**

Explanation: The system does not reference My Documents as your document folder. It might be called Documents.

User response: Add the specified folder to the include list.

FBW6103I *Product* **version** *product number* **is starting. The kernel driver version is** *kernel version number***.**

Explanation: This message is logged when the application starts the daemon and reads the version from the driver. This message is used for support purposes.

User response: No action is required.

FBW6104E **The driver received a command before the initial configuration was loaded.**

Explanation: Commands cannot be processed before the initial configuration is loaded.

User response: Wait until the initial configuration is loaded then retry the command.

FBW6105E **The connection to the daemon could not be established.**

Explanation: The commands are not processed.

User response: Ensure the daemon is running then retry the command.

FBW6107I **Network '***adapter GUID***' is disconnected.**

Explanation: The specified network is disconnected.

User response: No action is required.

FBW6108I **Setting the maximum backup speed to** *number* **Kbps.**

Explanation: This is an informational message showing the throttle value used.

User response: No action is required.

FBW6109W **This network rule already exists. Change the rule or click Cancel to exit this dialog.**

Explanation: The same network rule is already defined for the selected network adapter.

User response: Change the rule or click Cancel to exit this dialog.

FBW6111I **The throttle function was disabled because an internal error occurred. View the system error log for more details.**

Explanation: An internal error disabled the throttle function. As a result, network changes or network rules settings did not update the throttle value.

User response: No action is required.

FBW6113W **This network rule already exists or another network rule matches the same criteria. Modify the rule and issue the command again.**

Explanation: The same network rule or another network rule that matches the criteria is already defined.

User response: Modify the rule and issue the command again.

FBW6114I **The daemon has detected a local storage error condition. Check the local storage settings. The application will retry for file:** *filename*

Explanation: The local backup directory may have been deleted.

User response: Check the local storage settings and ensure that the local backup directory exist.

FBW6115I **The local storage is available. Backup resumed for file** *filename*

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6116I **The application can not access the local storage. Check the local settings and reapply the settings if necessary.**

Explanation: The local backup directory may have been deleted. The drive letter where the directory resided may have changed.

User response: Check the local storage settings and reapply the settings if necessary. Ensure that the local backup directory exist with write permissions.

FBW6117I **The local storage appears to be available again. Backup resumes.**

Explanation: This message is for informational purposes only.

User response: No action is required.

FBW6209E **Errors have occurred.**

Explanation: Errors have occurred since the last time the replication log was viewed.

User response: Check the replication log for errors.

FBW6210W **Warnings have occurred.**

Explanation: Warnings have occurred since the last time the replication log was viewed.

User response: Check the replication log for errors.

FBW6211I **The fpcommands.xml file has been copied to the local machine for processing.**

Explanation: When an administrator publishes a new configuration, the client machine will copy the fpcommands.xml file to the clients machines data directory to be processed.

User response: No action is required.

FBW6212W **Existing configuration can not be restored. Database 'fpa.txt' was not backed up to this remote location** *remote location***. The default configuration is used. Use the Settings Notebook to change the default configuration.**

Explanation: There was an attempt to restore a configuration that was not backed up.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6213W **Restoring database 'fpa.txt' from the remote location** *remote location* **failed. Error returned:** *error***. The default configuration is used. Use the Settings Notebook to change the default configuration.**

Explanation: Failed to restore the database from the remote location.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6214E **Reset database 'fpa.txt' before the import of the restored database failed. Error returned:** *error***. The product must be reinstalled.**

Explanation: An internal error occurred during the reset of the database. The machine can not be recovered from this error.

User response: Uninstall then reinstall the product.

FBW6215E **Import database 'fpa.txt.bk' failed. Error returned:** *error***. The default configuration failed ro load, error** *retcode***. The product must be reinstalled.**

Explanation: An internal error occurred during the import of the restored database. The second attempt to load the default configuration failed. The machine can not be recovered from this error.

User response: Uninstall then reinstall the product.

FBW6216W **Import database 'fpa.txt.bk' failed. Error returned:** *error***. The default configuration was loaded. Use the Settings Notebook to change the default configuration.**

Explanation: An internal error occurred during the import of the restored database. Loading of the default configuration was successful.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6217E **Import database 'fpa.txt.save' failed. Error returned:** *error***. The default configuration failed to load, error** *retcode***. The product must be reinstalled.**

Explanation: An internal error occurred during the import of the restored database. The second attempt to import the installed configuration database prior to recovery failed. The third attempt to load the default configuration also failed. The machine can not be recovered from this error.

User response: Uninstall then reinstall the product.

FBW6218W **Import database 'fpa.txt.save' failed. Error returned:** *error***. The default configuration was loaded. Use the Settings Notebook to change the default configuration.**

Explanation: An internal error occurred during the import of the restored database. The second attempt to import the installed configuration database prior to recovery failed. Loading of the default configuration was successful.

User response: Use the Settings Notebook to change the default configuration. Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6219W **Import database 'fpa.txt.bk' failed. The previous saved configuration is loaded instead.**

Explanation: An internal error occurred during the import of the restored database. The installed configuration saved before the import is now loaded.

User response: Use the Settings Notebook to change the default configuration.

FBW6220I **Restoring 'identifier.txt' from** *remote target* **failed. Error returned:** *error***. The default logon name is used as the identifier.**

Explanation: An internal error occurred during the restore.

User response: Use the Settings Notebook to change the identifier value.

FBW6221I **Restoring 'dsm.opt' from** *remote target* **failed. Error returned:** *error***. The default dsm.opt file is used.**

Explanation: An internal error occurred during the restore.

User response: Manually update the dsm.opt to add other IBM Spectrum Protect for Workstations client options.

FBW6222I **Host name was not specified on the restore command. The host name of the machine is used.**

Explanation: This is an internal error where the host name was not specified on the restore command. The 'machinename.txt' file is not created.

User response: If the intent is to back up with a different host name, manually create the 'machinename.txt' file in the data folder with the correct host name.

FBW6223I **Failed to create 'machinename.txt' to store the host name of the machine that the files ared recovered from. Host name of the current machine is used.**

Explanation: The host name of the machine is used as the backup folder for the client unless 'machinename.txt' file exists and contains a different host name.

User response: If the intent is to back up with a different host name, manually create the 'machinename.txt' file in the data folder with the correct host name.

FBW6224I **Synchronizing files with the remote server.**

Explanation: After the configuration files are recovered, the files are synchronized with the remote server.

User response: No action is required.

FBW6225I **Finished synchronizing files with the remote server.**

Explanation: This message is for informational purposes only.

User response: No action is required.

Appendix B. Accessibility features for IBM Spectrum Protect for Workstations

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. IBM Spectrum Protect for Workstations provides various accessibility features that you can use.

Accessibility features

The following list includes the major accessibility features in IBM Spectrum Protect for Workstations:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices
- User documentation that is provided in HTML and PDF format. Descriptive text is provided for all documentation images.

The IBM Spectrum Protect for Workstations Information Center, and its related publications, are accessibility-enabled.

Keyboard navigation

IBM Spectrum Protect for Workstations follows Microsoft conventions for most keyboard navigation and access. Drag and Drop support is managed by using the Microsoft Windows Accessibility option *MouseKeys*. For more information about MouseKeys and other Windows accessibility options, see the Windows Online Help. To open the Windows Online Help for accessibility options, click **Start** and enter `MouseKeys` in the search field.

The following access methods differ from Microsoft conventions.

In the IBM Spectrum Protect for Workstations client, there are several tasks in which you select files:

- Select files to include for continuous protection and to exclude from any protection.
- Select files to include for scheduled protection.
- Select files to vault

Each of these tasks presents a list of file specifications labeled **Folders and Files**. You can add file specifications to the list and remove file specifications. When you add a file specification, you can browse for files in a file tree. The file tree opens when you click **Include**, **Exclude**, or **Vault**. Navigate the file tree with the following method:

1. Press Tab and Shift+Tab to navigate to + (expand folder). Press Enter to expand the folder.
2. Press Down Arrow and Up Arrow to navigate among the objects in the folder.
3. On an expanded folder, press Enter to collapse the folder.

4. As you navigate the file tree, the object that has focus is displayed in the **Folder name (wildcards allowed)** field at the end of the panel.
5. Press Tab to navigate to the text field. Optionally, edit the text field.
6. Press Tab to navigate to **OK**. Click **OK** to add the file specification to the **Folders and Files** list.

To remove file specifications from the list, select a file specification and click **Remove**. Navigate the list of file specifications with this method:

1. Press Tab to move down to the next file specification and Shift+Tab to move up to the previous file specification.
2. Press Spacebar to select a file specification or to clear a selection.
3. Press Shift+Tab to navigate to **Remove**. Click **Remove** to remove the file specification from the **Folders and Files** list.

The **Folders and Files** list is displayed when you navigate the following paths:

- **Settings** > **Files to Protect** > **Folders and Files** box > **Details**
- **Settings** > **Files to Protect** > **Vault** box > **Details**
- **Settings** > **E-mail Protection** > **Scheduled Backup Settings**
- **Settings** > **Advanced** > **Scheduled Backup Settings**

You can also use the **Files to Restore** panel in the restore wizard to select files from a file tree, and add and remove files from a list. When you select **Folder View**, a panel with a file tree and a list of files is displayed. The restore file tree and files list is similar to other file trees and files lists. The restore controls are different in the following ways:

- The file tree folder items each have a check box.
- The items in the folders and files list each have a check box. If more than one version of a file exists, the row contains a list of versions in the **Version** column.

Press Spacebar to select or clear a check box. If more than one version of a file is available, select the version this way:

- Press Tab to navigate to the **Version** column.
- Use Up Arrow and Down Arrow to select a version.

Related accessibility information

You can view the publications for IBM Spectrum Protect for Workstations in Adobe Portable Document Format (PDF) by using the Adobe Acrobat Reader. You can access these files or any of the other documentation PDF files at IBM Publications Center at http://www.ibm.com/shop/publications/order/.

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center at http://www.ibm.com/able.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

SoftLayer® is a registered trademarks of SoftLayer, Inc., an IBM Company.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

This glossary provides terms and definitions for the IBM Spectrum Protect for Workstations software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website.

A

absolute mode
In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also mode, modified mode.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access mode
An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume.

ACK See acknowledgment.

acknowledgment (ACK)
The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See access control list.

activate
To validate the contents of a policy set and then make it the active policy set.

active-data pool
A named set of storage pool volumes that contain only active versions of client backup data. See also server storage, storage pool, storage pool volume.

active file system
A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. See also inactive file system.

active policy set
The activated policy set that contains the policy rules currently in use by all client nodes assigned to the policy domain. See also policy domain, policy set.

active version
The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. See also backup version, inactive version.

activity log
A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup
A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client
A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the server. See also backup-archive client.

administrative command schedule
A database record that describes the planned processing of an administrative command during a specific time period. See also central scheduler, client schedule, schedule.

administrative privilege class
See privilege class.

administrative session
A period of time during which an

administrator user ID communicates with a server to perform administrative tasks. See also client node session, session.

administrator
A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

agent node
A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate
An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also logical file, physical file.

aggregate data transfer rate
A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

application client
A program that is installed on a system to protect an application. The server provides backup services to an application client.

archive
To copy programs, data, or files to another storage media, usually for long-term storage or security. See also retrieve.

archive copy
A file or group of files that was archived to server storage

archive copy group
A policy object containing attributes that control the generation, destination, and expiration of archived files. See also copy group.

archive-retention grace period
The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also bind.

association
The defined relationship between a client node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

audit To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication rule
A specification that another user can use to either restore or retrieve files from storage.

authority
The permission level to access objects, resources, or functions. See also privilege class.

authorization rule
A specification that permits a user to either restore or retrieve files for another user from storage.

authorized user
A user who has administrative authority for the client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS
See automounted file system.

automatic detection
A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration
The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also demand migration, threshold migration.

automounted file system (AutoFS)
A file system that is managed by an automounter daemon. The automounter

daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client
A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. See also administrative client.

backup copy group
A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class. See also copy group.

backup retention grace period
The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set
A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection
A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version
A file or directory that a client node backed up to storage. More than one backup version can exist in storage, but only one backup version is the active version. See also active version, copy group, inactive version.

bind To associate a file with a management class name. See also archive-retention grace period, management class, rebind.

C

cache To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file
A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD See client acceptor daemon.

central scheduler
A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See also administrative command schedule, client schedule.

client A software program or computer that requests services from a server. See also server.

client acceptor
A service that serves the Java applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX, UNIX, and Linux systems, the client acceptor is run as a daemon.

client acceptor daemon (CAD)
See client acceptor.

client domain
The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node
A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session
A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. See also administrative session.

client option set
A group of options that are defined on the server and used on client nodes in conjunction with client options files.

client options file
An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client-polling scheduling mode
A method of operation in which the client queries the server for work. See also server-prompted scheduling mode.

client schedule
A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also administrative command schedule, central scheduler, schedule.

client/server
Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file
A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. See also client user-options file, options file.

client user-options file
A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also client system-options file. See also client system-options file, options file.

closed registration
A registration process in which only an administrator can register workstations as client nodes with the server. See also open registration.

collocation
The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool. Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group
A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point
A point in time when data is considered to be consistent.

communication method
The method by which a client and server exchange information. See also Transmission Control Protocol/Internet Protocol.

communication protocol
A set of defined interfaces that permit computers to communicate with each other.

compression
A function that removes repetitive characters, spaces, strings of characters, or binary data from the data being processed and replaces characters with control characters. Compression reduces the amount of storage space that is required for data.

configuration manager
A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also enterprise configuration, managed server, profile.

conversation
A connection between two programs over a session that allows them to communicate with each other while processing a transaction. See also session.

copy backup
A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted.

copy group
A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also archive copy group, backup copy group, backup version, management class.

copy storage pool
A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also destination, primary storage pool, server storage, storage pool, storage pool volume.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file
A physical file in which read errors have been detected.

database backup series
One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series. See also database snapshot, full backup.

database snapshot
A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also database backup series, full backup.

data center
In a virtualized environment, a container that holds hosts, clusters, networks, and data stores.

data deduplication
A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server
A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover
A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)
A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

data store
In a virtualized environment, the location where virtual machine data is stored.

deduplication
The process of creating representative records from a set of records that have been identified as representing the same entities.

default management class
A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

demand migration
The process that is used to respond to an out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated. See also automatic migration, selective migration, threshold migration.

desktop client
The group of backup-archive clients that includes clients on Microsoft Windows, Apple, and Novell NetWare operating systems.

destination
A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated. See also copy storage pool.

device class
A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file
1. For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.
2. For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

disaster recovery manager (DRM)
A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan
A file that is created by the disaster recover manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and

hardware that is used by the server, and the location of recovery media.

domain
A grouping of client nodes with one or more policy sets, which manage data or storage resources for the client nodes. See also policy domain.

DRM See disaster recovery manager.

DSMAPI
See data storage-management application-programming interface.

dynamic serialization
Copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive. See also shared dynamic serialization, shared static serialization, static serialization.

E

EA See extended attribute.

EB See exabyte.

EFS See Encrypted File System.

Encrypted File System (EFS)
A file system that uses file system-level encryption.

enterprise configuration
A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also configuration manager, managed server, profile, subscription.

enterprise logging
The process of sending events from a server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also event.

error log
A data set or file that is used to record error information about a product or system.

estimated capacity
The available space, in megabytes, of a storage pool.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process. See also enterprise logging, receiver.

event record
A database record that describes actual status and results for events.

event server
A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)
For processor, real and virtual storage capacities and channel volume, 2 to the power of 60 or 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude
The process of identifying files in an include-exclude list. This process prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup, from space management, or from both backup and space management.

exclude-include list
See include-exclude list.

expiration
The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file
A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend
To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)
Names or value pairs that are associated with files or directories. There are three

classes of extended attributes: user attributes, system attributes, and trusted attributes.

external library
A collection of drives that is managed by the media-management system other than the storage management server.

F

file access time
On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age
For migration prioritization purposes, the number of days since a file was last accessed.

file device type
A device type that specifies the use of sequential access files on disk storage as volumes.

file server
A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space
A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore, retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)
A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state
The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also migrated file, premigrated file, resident file.

file system migrator (FSM)
A kernel extension that intercepts all file system operations and provides any space management support that is required. If no space management support is required, the operation is passed to the operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state
The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency
A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See file space ID.

FSM See file system migrator.

full backup
The process of backing up the entire server database. A full backup begins a new database backup series. See also database backup series, database snapshot, incremental backup.

fuzzy backup
A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy
A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified.

G

GB See gigabyte.

General Parallel File System (GPFS)
A high-performance shared-disk file system that can provide data access from nodes in a clustered system environment. See also information lifecycle management.

gigabyte (GB)
For processor storage, real and virtual storage, and channel volume, 10 to the

power of nine or 1,073,741,824 bytes. For disk storage capacity and communications volume, 1,000,000,000 bytes.

global inactive state
The state of all file systems to which space management has been added when space management is globally deactivated for a client node.

Globally Unique Identifier (GUID)
An algorithmically determined number that uniquely identifies an entity within a system. See also Universally Unique Identifier.

GPFS See General Parallel File System.

GPFS node set
A mounted, defined group of GPFS file systems.

group backup
The backup of a group containing a list of files from one or more file space origins.

GUID See Globally Unique Identifier.

H

hierarchical storage management (HSM)
A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity. See also hierarchical storage management client, recall, storage hierarchy.

hierarchical storage management client (HSM client) A client program that works with the server to provide hierarchical storage management (HSM) for a system. See also hierarchical storage management, management class.

HSM See hierarchical storage management.

HSM client
See hierarchical storage management client.

I

ILM See information lifecycle management.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. See also active file system.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. See also active version, backup version.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also include-exclude list.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services. See also include-exclude file.

incremental backup
The process of backing up files or directories, or copying pages in the database, that are new or changed since the last full or incremental backup. See also selective backup.

individual mailbox restore
See mailbox restore.

information lifecycle management (ILM)
A policy-based file-management system for storage pools and file sets. See also General Parallel File System.

inode The internal structure that describes the individual files on AIX, UNIX, or Linux systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the Internet Protocol standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface. See also migration job.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

KB See kilobyte.

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 2 to the power of 10 or 1,024 bytes. For disk storage capacity and communications volume, 1,000 bytes.

L

LAN See local area network.

LAN-free data movement
The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network.

LAN-free data transfer
See LAN-free data movement.

leader data
Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library
1. A repository for demountable recorded media, such as magnetic disks and magnetic tapes.
2. A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client
A server that uses server-to-server communication to access a library that is managed by another storage management server. See also library manager.

library manager
A server that controls device operations when multiple storage management servers share a storage device. See also library client.

local
1. Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line. See also remote.
2. For hierarchical storage management products, pertaining to the destination of migrated files that are being moved. See also remote.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volume
Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See loopback virtual file system.

logical file
A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also aggregate, physical file, physical occupancy.

logical occupancy
The space that is used by logical files in a storage pool. This space does not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy. See also physical occupancy.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier used to differentiate devices, each of which is a logical unit (LU).

logical volume
A portion of a physical volume that contains a file system.

logical volume backup
A back up of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)
Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)
A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LUN See logical unit number.

LVSA See Logical Volume Snapshot Agent.

M

macro file
A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. See also IBM Spectrum Protect command script.

mailbox restore
A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object
A definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server.

managed server
A server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also configuration manager, enterprise configuration, profile, subscription.

management class
A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also bind, copy group, hierarchical storage management client, policy set, rebind.

maximum transmission unit (MTU)
The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See megabyte.

media server
In a z/OS environment, a program that provides access to z/OS disk and tape storage for IBM Spectrum Protect servers that run on operating systems other than z/OS.

megabyte (MB)
For processor storage, real and virtual storage, and channel volume, 2 to the 20th power or 1,048,576 bytes. For disk storage capacity and communications volume, 1,000,000 bytes.

metadata
Data that describes the characteristics of data; descriptive data.

migrate
To move data to another location, or an application to another computer system.

migrated file
A file that has been copied from a local file system to storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also file state, premigrated file, resident file, stub file.

migration
The process of moving data from one computer system to another, or an application to another computer system.

migration job
A specification of files to migrate, and actions to perform on the original files after migration. See also job file, threshold migration.

migration threshold
High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

mirroring
The process of writing the same data to multiple disks at the same time. The mirroring of data protects it against data loss within the database or within the recovery log.

mode A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See also absolute mode, modified mode.

modified mode
In storage management, a backup copy-group mode that specifies that a file

is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also absolute mode, mode.

mount limit
The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also mount point.

mount point
A logical drive through which volumes are accessed in a sequential access device class. For removable media device types, such as tape, a mount point is a logical drive associated with a physical drive. For the file device type, a mount point is a logical drive associated with an I/O stream. See also mount limit.

mount retention period
The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period
The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See maximum transmission unit.

N

Nagle algorithm
An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe
A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS file server
See network-attached storage file server.

NAS file server node
See NAS node.

NAS node
A client node that is a network-attached storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system
A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format
A format of data that is written to a storage pool directly by the server. See also non-native data format.

NDMP
See Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)
A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

network-attached storage file server (NAS file server)
A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System
See NetBIOS.

Network Data Management Protocol (NDMP)
A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate
A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the

backup-archive client program has been installed, and which has been registered to the server.

node name
A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class
A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also privilege class.

non-native data format
A format of data that is written to a storage pool that differs from the format that the server uses for operations. See also native format.

O

offline volume backup
A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup
A backup in which the volume is available to other system applications during the backup operation.

open registration
A registration process in which users can register their workstations as client nodes with the server. See also closed registration.

operator privilege class
A privilege class that gives an administrator the authority to disable or halt the server, enable the server, cancel server processes, and manage removable media. See also privilege class.

options file
A file that contains processing options. See also client system-options file, client user-options file.

originating file system
The file system from which a file was migrated. When a file is recalled, it is returned to its originating file system.

orphaned stub file
A file for which no migrated file can be found on the server that the client node is contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

P

packet In data communication, a sequence of binary digits, including data and control signals, that are transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode
A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation
A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character
See wildcard character.

physical file
A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also aggregate, logical file, physical occupancy.

physical occupancy
The amount of space that is used by physical files in a storage pool. This space includes the unused space that is created when logical files are deleted from aggregates. See also logical file, logical occupancy, physical file.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy domain
A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain. See also active policy set, domain.

policy privilege class
A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also privilege class.

policy set
A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also active policy set, management class.

premigrated file
A file that has been copied to server storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in server storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. See also file state, migrated file, resident file.

premigrated files database
A database that contains information about each file that has been premigrated to server storage.

premigration
The process of copying files that are eligible for migration to server storage, but leaving the original file intact on the local file system.

premigration percentage
A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary storage pool
A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also copy storage pool, server storage, storage pool, storage pool volume.

privilege class
A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also authority, node privilege class, operator privilege class, policy privilege class, storage privilege class, system privilege class.

profile
A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also configuration manager, enterprise configuration, managed server.

profile association
On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

Q

quota

1. For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.
2. For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization
The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume
A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

rebind
To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also bind, management class.

recall To copy a migrated file from server storage back to its originating file system using the hierarchical storage management client. See also selective recall.

receiver
A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the server console and activity log. See also event.

reclamation
The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold
The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recovery log
A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register
To define a client node or administrator ID that can access the server.

registry
A repository that contains access and configuration information for users, systems, and software.

remote
For hierarchical storage management products, pertaining to the origin of migrated files that are being moved. See also local.

resident file
On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in server storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from server storage and modified.

restore
To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention
The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve
To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool. See also archive.

root user
A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See storage area network.

schedule
A database record that describes client operations or administrative commands to be processed. See also administrative command schedule, client schedule.

scheduling mode
The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume
A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use. See also volume.

script A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. See also IBM Spectrum Protect command script.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup
The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. See also incremental backup.

selective migration
The process of copying user-selected files from a local file system to server storage and replacing the files with stub files on the local file system. See also demand migration, threshold migration.

selective recall
The process of copying user-selected files from server storage to a local file system. See also recall, transparent recall.

serialization
The process of handling files that are modified during backup or archive processing. See also shared dynamic serialization, shared static serialization, static serialization.

server A software program or a computer that provides services to other software programs or other computers. See also client.

server options file
A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode
A client/server communication technique where the server contacts the client node when tasks must be done. See also client-polling scheduling mode.

server storage
The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from hierarchical storage management client nodes (space-managed files). See also active-data pool, copy storage pool, primary storage pool, storage pool volume, volume.

session
A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data for the duration of the session. See also administrative session.

session resource usage
The amount of wait time, processor time, and space that is used or retrieved during a client session.

shadow copy
A snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shadow volume
The data stored from a snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shared dynamic serialization
A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. The backup-archive client retries the backup or archive operation a number of times; if the file is being modified during each attempt, the backup-archive client will back up or archive the file on its last try. See also dynamic serialization, serialization, shared static serialization, static serialization.

shared library
A library device that is used by multiple storage manager servers. See also library.

shared static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. The client attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also dynamic serialization, serialization, shared dynamic serialization, static serialization.

snapshot
An image backup type that consists of a point-in-time view of a volume.

space-managed file
A file that is migrated from a client node by the hierarchical storage management (HSM) client. The HSM client recalls the file to the client node on demand.

space management
See hierarchical storage management.

space monitor daemon
A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file
A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file
On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL See Secure Sockets Layer.

stabilized file space
A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Stanzas are usually separated by blank lines or colons, and each stanza has a name.

startup window
A time period during which a schedule must be initiated.

static serialization
A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the backup-archive client cannot back up or archive the file. See also dynamic serialization, serialization, shared dynamic serialization, shared static serialization.

storage agent
A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)
A dedicated storage network tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy
A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also storage pool.

storage pool
A named set of storage volumes that is the destination that is used to store client

data. See also active-data pool, copy storage pool, primary storage pool, storage hierarchy.

storage pool volume
A volume that has been assigned to a storage pool. See also active-data pool, copy storage pool, primary storage pool, server storage, volume.

storage privilege class
A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also privilege class.

stub A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file
A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from server storage. It also contains additional information that can be used to eliminate the need to recall a migrated file. See also migrated file, resident file.

stub file size
The size of a file that replaces the original file on a local file system when the file is migrated to server storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription
In a storage environment, the process of identifying the subscribers to which the profiles are distributed. See also enterprise configuration, managed server.

system privilege class
A privilege class that gives an administrator the authority to issue all server commands. See also privilege class.

T

tape library
A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix
The high-level-qualifier of the file name or the data set name in the standard tape label.

target node
A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See trusted communications agent.

TCP/IP
See Transmission Control Protocol/Internet Protocol.

threshold migration
The process of moving files from a local file system to server storage based on the high and low thresholds that are defined for the file system. See also automatic migration, demand migration, migration job, selective migration.

throughput
In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout
A time interval that is allotted for an event to occur or complete before operation is interrupted.

IBM Spectrum Protect command script
A sequence of IBM Spectrum Protect administrative commands that are stored in the database of the IBM Spectrum Protect server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic. See also macro file, script.

tombstone object
A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)
An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types. See also communication method.

transparent recall
The process that is used to automatically recall a migrated file to a workstation or file server when the file is accessed. See also selective recall.

trusted communications agent (TCA)
A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See Universal Naming Convention.

Unicode
A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus many classical and historical texts.

Unicode-enabled file space
Unicode file space names provide support for multilingual workstations without regard for the current locale.

Universally Unique Identifier (UUID)
The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier. See also Globally Unique Identifier.

Universal Naming Convention (UNC)
The server name and network name combined. These names together identify the resource on the domain.

UTF-8 Unicode Transformation Format, 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208. See also UCS-2.

UUID See Universally Unique Identifier.

V

validate
To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version
A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space
A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual mount point
A directory branch of a file system that is defined as a virtual file system. The virtual file system is backed up to its own file space on the server. The server processes the virtual mount point as a separate file system, but the client operating system does not.

virtual volume
An archive file on a target server that represents a sequential media volume to a source server.

volume
A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also scratch volume, server storage, storage pool, storage pool volume.

volume history file
A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service (VSS)
A set of Microsoft application-programming interfaces (APIs) that are used to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See Volume Shadow Copy Service.

VSS Backup
A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on IBM Spectrum Protect server storage.

VSS Fast Restore
An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a file-level copy method.

VSS Instant Restore
An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a hardware assisted restore method (for example, a FlashCopy operation).

VSS offloaded backup
A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the IBM Spectrum Protect server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore
A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on IBM Spectrum Protect server storage to their original location.

W

wildcard character
A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workload partition (WPAR)
A partition within a single operating system instance.

workstation
A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name (WWN)
A 64-bit, unsigned name identifier that is unique.

WPAR See workload partition.

WWN See worldwide name.

Index

A

accessibility features 95
activity log
  viewing in the client GUI 62
Activity Report 58, 59
administration folders
  identifying
    overview 3
  managing clients 3
Advanced panel of client Settings Notebook 41
Application Settings dialog 32
Applications and Extensions box 32
Applications and Extensions pane 12
Applications box 31
Applications pane 12

B

back up all files
  force a backup of all protected files 53
  force a scheduled backup 53
  stopping a backup 54
  when to back up all files 34, 52
Back up to: drop down list 14, 36
Back up with new settings check box 34
backup copies
  format 67
  modify with native file system tools 68
  restore files 63
  specify the local storage area 49
  specify the remote storage area 50
  versions 67
backup features
  client 50

C

clients 41
  logs
    viewing in the client GUI 62
  overview 1
closeapps.txt 43, 47
Compress backups radio button 40
configuration
  fpa config-set command 3
Configuration 17
configuration of clients
  performance settings 41
Configuration wizard 8, 9, 17
Configuration Wizard
  Email Protection page 13
  Initial Backup page 17
  Remote Storage page 13
  Select Setup Type 9
  Summary page 18
  Welcome page 9
  What is Critical page 9
continuous protection
  definition 2
  force a backup of all files 53
  monitoring 58
  restore files 63
  specify files to protect 45
  specify files using wildcard characters 11, 30
  specify the local storage area 49
  specify the remote storage area 50
  specify which files are included and excluded 29
  when to force a backup of all files 34, 52
Critical Settings page 12

D

deploying the client 23
documentation
  product v
  search v
drives, protected 29
dsm.opt 70

E

e-mail protection
  monitoring 58
  restore files 63
Email Application Data Folder text field 13, 36
Email Application drop down list 13, 35
email protection
  specify which applications are protected 48
Email Protection page (Initial Configuration Wizard) 13
Email Protection panel of client Settings Notebook 35
Encrypt backups 39
encryption 39
exclude files from protection 29
Expiratione panel of client Settings Notebook 41
external device
  remote storage location 14, 36

F

file server
  remote storage location 14, 36
File Server 17
FilePathSrv.exe
  run as a service 55
  starting 54, 72
files
  specifying 11, 30
Files are not backed up 69, 70
Files to protect are incorrectly specified 69
Files to Protect panel of client Settings Notebook 28
Files to Restore panel 64
Folders and Files box 28
Folders and Files Settings dialog for scheduled backups 42
Folders and Files Settings page for continuous protection 10, 28
Folders and Files summary box 10
force a backup
  back up all protected files 53
  scheduled backup 53
  stopping a backup 54
  when to force a backup of all files 34, 52
fpa config-set command 3
FpForFileServers.js 55

G

General panel of client Settings Notebook 26
glossary 101

H

How many versions to keep: field 38
How often to protect your email drop down list 13, 36

I

IBM Knowledge Center v
IBM Spectrum Protect 17, 70
  client node lacks authority to delete backup copies 70
  delete backup copies 70
  dsm.opt 70
  node name does not match hostname 70
  user security rights 71
IBM Spectrum Protect remote storage location 14, 36
Identify Backup 17
include files for protection 29
Initial Backup page 17
Initial configuration 8
Initial Configuration Wizard 9
  Email Protection page 13
  Initial Backup page 17
  Remote Storage page 13
  Select Setup Type 9
  Summary page 18
  Welcome page 9
  What is Critical page 9
installation
  client
    advanced 19

installation *(continued)*
client *(continued)*
basic 7
command 20
local silent installation 19
pull upgrade 21
pull upgrade considerations 22
push to remote computers 23
uninstall 18
system requirements
client 7
upgrade considerations 2
interpreting file and folder patterns 11, 30

L

Local Backup Copy Versions are Greater than Configured 73
local storage area
specify the location 49
Local Storage icon 58
Location text field 14, 36
logs
client activity log, viewing
client GUI 62

M

Maximum space for backups: field 16, 39
messages
central administration console 79
client 83
FBW prefix 79
format 79
severity codes 79
monitoring
continuous protection 58
e-mail protection 58
local client 57
managed clients 58
scheduled protection 58

N

name patterns with wildcard characters 11, 30
new for version 8.1.0
client v
Number of Backup Copy Versions are Greater than Configured 73

P

patterns with wildcard characters 11, 30
performance settings
clients 41
pop-up messages 57
product overview
clients 1
protected drives 29
pull upgrade installation, client 21
push the client installation to remote computers 23

R

Recover an existing configuration 17
Remote Backup Copy Versions are Greater than Configured 73
Remote server 17
remote storage
WebDAV server 14, 36
remote storage area
specify the location 50
Remote Storage icon 58
remote storage location
external device 14, 36
file server 14, 36
IBM Spectrum Protect 14, 36
USB device 14, 36
Remote Storage page (Initial Configuration Wizard) 13
Remote Storage panel of client Settings Notebook 36
restore files 63
Restore Location panel 65
Restore Wizard 63
Files to Restore panel 64
Restore Location panel 65
Summary panel 66
Welcome panel 63

S

scheduled protection
close applications prior to scheduled backup 43, 47
definition 2
force a scheduled backup 53
monitoring 58
restore files 63
scheduled backup considerations 43, 47
specify files using wildcard characters 11, 30
specify the schedule period 49
specify the storage area 50
specify which files are included and excluded 29
specify which files are protected 46
when to force a backup of all files 34, 52
Select folders page 11, 30
Settings Notebook 25
Advanced panel 41
Email Protection panel 35
Expiration panel 41
Files to Protect panel 28
General panel 26
Remote Storage panel 36
silent installation
command 20
local silent installation
client 19
push the client to remote computers 23
Specify Backup Server 17
specifying files to protect 11, 30
Start Restore Wizard 17
starting
back up all files 53
starting *(continued)*
client
run as a service 55
client GUI 51
FilePathSrv.exe client process 54, 72
scheduled backup 53
Starting and stopping the client 51
Status panel 60
starting 51
stopping
backup or restore activity 54
storage area
specify the local storage area 49
specify the remote storage area 50
Storage for backup copies is not correctly specified 69
sub-file copy radio button 41
Summary page (Initial Configuration Wizard) 18
Summary panel (Restore Wizard) 66
system requirements
client 7

T

Target file system can only handle sequential I/Os. 70
Throttle Settings dialog for network rules 44

U

upgrade the client
considerations for pull upgrade 22
pull installation 21
USB device
exclude from protection 29
remote storage location 14, 36
Use sub-file copy radio button 41
user interface contains no file data 72
Using the configuration wizard 8

V

Vault box 32
vault duration 33
Vault Settings dialog 32
vaulted protection
definition 2
specify vault duration 33
specify which files are vaulted 48

W

Web Server 17
WebDAV server remote storage location 14, 36
Welcome page (Initial Configuration Wizard) 9
Welcome panel (Restore Wizard) 63
What is Critical page (Initial Configuration Wizard) 9
when to back up all files 34, 52
wildcard characters in file specifications 11, 30

Windows installation folder 23
Windows, Notebooks, and Dialogs
  Application Settings dialog 32
  Critical Settings page 12
  Folders and Files Settings dialog for scheduled backups 42
  Folders and Files Settings page for continuous protection 10, 28
  Initial Configuration wizard 9
  Initial Configuration Wizard
    Email Protection page 13
    Initial Backup page 17
    Remote Storage page 13
    Select Setup Type page 9
    Summary page 18
    Welcome page 9
    What is Critical page 9
  Restore Wizard 63
    Files to Restore panel 64
    Restore Location panel 65
    Summary panel 66
    Welcome panel 63
  Select folders page 11, 30
  Settings Notebook 25
    Advanced panel 41
    Email Protection panel 35
    Expiration panel 41
    Files to Protect panel 28
    General panel 26
    Remote Storage panel 36
  Status panel 60
  Throttle Settings dialog for network rules 44
  Vault Settings dialog 32

Product Number: 5725-X12

Printed in USA