Symantec Backup Exec™ System Recovery

Symantec Backup Exec System Recovery User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 8.0

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be "commercial computer software" and "commercial computer software documentation" as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you are using.

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Select your region or language under Global Support.

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to recreate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support.

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade insurance and maintenance contracts
- Information about the Symantec Value License Program

- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

Additional Enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

Symantec Early Warning Solutions

These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.

Managed Security Services

These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services

Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.

Educational Services

Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Introducing Symantec Backup Exec™ System Recovery

This chapter includes the following topics:

About Symantec Backup Exec System Recovery

Symantec Backup Exec System Recovery is the gold standard in Windows® system recovery allowing businesses and IT to recover from system loss or disasters in minutes, not hours or days. Helping IT administrators meet recovery time objectives, Backup Exec System Recovery provides fast, easy to use system restoration or full bare metal recovery to dissimilar hardware and even virtual environments for servers, desktops or laptops. It also provides the ability to recover systems in remote, unattended locations.

Backup Exec System Recovery captures a recovery point of the entire live Windows system, including OS, applications, system settings, configurations, files, etc. – without impacting productivity. This Recovery Point can be conveniently saved to various media or disk storage devices including SAN, NAS, Direct Attached Storage, RAID, CD/DVD, etc. When systems fail, you can quickly restore them without the need for manual, lengthy and error prone processes.

Backup Exec System Recovery also has the ability to be managed remotely using either another licensed copy of Backup Exec System Recovery, or using Backup Exec System Recovery Manager (sold separately), a centralized management application that provides IT administrators with an at-a-glance view of system recovery jobs across your entire organization. Using Backup Exec System Recovery Manager, you can centrally deploy, modify and maintain recovery activities, jobs, and policies for local and remote systems, monitor real-time status and quickly resolve any problems identified. You can also create reports to analyze trends over time.

Extending your recovery capabilities even further, Backup Exec System Recovery integrates with Google™ Desktop as well as Backup Exec Retrieve for simple, end-user file recovery that does not require IT intervention. Using Symantec Backup Exec System Recovery Granular Restore Option (sold separately), you can quickly restore individual Microsoft® Exchange emails, folders and mailboxes.

And for a lower priced, streamlined version of Backup Exec System Recovery, consider Backup Exec for Windows Servers System Recovery Option, built specifically for Backup Exec for Windows Servers customers. Backup Exec for Windows Servers System Recovery Option includes only the necessary components for backing up and recovering Windows computers, giving you the same recovery power of Backup Exec System Recovery without some of the other features available with the full version of Backup Exec System Recovery.

See “About *Symantec Backup Exec for Windows Servers - System Recovery Option* ” on page 24.

From small businesses to the enterprise, Backup Exec System Recovery is the gold standard in Windows system recovery.

What's new in Backup Exec System Recovery 8

Backup Exec System Recovery includes many enhancements and new features. Refer to the following table for information about the latest features and enhancements:

Note: Not all features listed are available in all versions of this product.

Feature	Description
Support for the new Windows Server 2008	Backup Exec System Recovery has been designed and tested to run on the new Windows Server 2008 operating system, and still supports previous versions of Windows, including Windows Server 2003. See “System requirements” on page 21.
Support for NTFS partitions	Backup Exec System Recovery now supports NTFS partitions up to 16TB (formatted with 4k clusters).
Offsite Copy	The new Offsite Copy feature adds an additional level of protection to your data by copying recovery points to a second hard disk drive. You can use an external USB or FireWire drive, or copy them over the network to a remote location through a local area connection, or using FTP. See “About Offsite Copy” on page 79.
Create and manage aliases for your external drives	To help you more easily identify external drives for use as backup destinations, Backup Exec System Recovery lets you assign an alias to each external drive. Doing so does not change the drive label, but is for use only when you are accessing those drives from within Backup Exec System Recovery. See “Using aliases for external drives” on page 45.
Symantec ThreatCon integration	Symantec ThreatCon is Symantec's early threat warning system. You can now configure Backup Exec System Recovery to detect a change in the threat level whenever your computer is connected to the Internet. When the threat level meets or exceeds the level you specify, Backup Exec System Recovery automatically starts a backup job. You can specify a different ThreatCon level for each backup. See “Enabling Symantec ThreatCon Response” on page 94.

Feature	Description
Granular Restore Option (previously called Symantec Backup Exec Exchange Retrieve)	In addition to recovering Exchange files, you can also use the Granular Restore Option (an add-on to Backup Exec System Recovery) to restore documents from Microsoft SharePoint, or search and restore a version of a lost file using the File/Folder view.
Send Feedback tool	We want to hear what you think. From the Home page, you can now share your opinion with us. We look at every comment we receive and consider how we can make our product better. Tell us what you think.
Help and Support center	To help you help yourself, a new Help and Support dialog provides direct links to available resources for helping you to get the most out of Backup Exec System Recovery.

New features and enhancements added in the previous release

If you are upgrading from an earlier release, you might be interested to know of the following enhancements added in previous releases of Backup Exec System Recovery.

Feature	Description
Enhanced ease-of-use	An improved user interface simplifies what you need to know and do to successfully back up or recover files, folders, or your entire computer. And for Backup Exec System Recovery experts, the Advanced page gives you a single view to most product features.
Windows Vista support	Backup Exec System Recovery has been designed and tested to run in the new Windows Vista operating system, and still supports previous versions of Windows. See “System requirements” on page 21.
Improved Easy Setup	Now setting up your first backup is even easier with the enhanced Easy Setup, which appears either during install (unless you choose to skip it), or automatically the first time you run Backup Exec System Recovery. Specify a few preferences, and Backup Exec System Recovery can start backing up your computer on a regular basis.
File and folder backup	Limit your backup to include a select set of files or folders. File and folder backups are especially useful if your backup storage space is limited and you make frequent changes to important documents that you want to back up.

Feature	Description
One Time backups	Need to back up your data quickly? The new One Time Backup feature lets you define and run a backup at any time without saving the backup job for later use.
Desktop search engine support	Search for and recover files stored in recovery points using Google Desktop™. Also supports Granular Restore Option, previously called Symantec Backup Exec Retrieve.
Convert a recovery point to virtual disk format	Convert recovery points to one of two virtual disk formats for use in a virtual environment.
Restore Anyware	Restore a recovery point of a Windows Vista, XP, 2003, or 2000 system drive to a computer with different hardware, and make the changes necessary for the computer to be able to boot.
LightsOut Restore	Restore a computer from a remote location, regardless of the state of the computer, provided that its file system is intact.
Simplified schedule editor	You can now easily edit your existing backup schedules without having to click through multiple dialogs or complete the entire backup wizard again.
Manage backup data	Because recovery points and file and folder backup data require storage space, Backup Exec System Recovery gives you the freedom of where and how to handle the amount of disk space used for storing backup data. Backup Exec System Recovery offers simple tools for managing your backup data, and can even manage it for you automatically.
Improved backup and recovery status	The home page offers the backup protection status in a single view. But you can also use the new Backups Calendar to view past and upcoming scheduled backups to see how protected your data really is.
Automatic backup destination detection	Backup Exec System Recovery automatically detects when a new storage device is connected to your computer, and can prompt you to change your default backup destination to the new drive.
Browse lost or damaged files and folders	Enhanced browsing of files and folders inside recovery points makes recovery quick and easy; the new file and folder backup feature also lets you quickly search for and recover files or folders.
Event-triggered backups	In addition to scheduled and manual backups, Backup Exec System Recovery can detect certain events and run a backup automatically whenever they occur, providing an added level of protection for your computer.
Performance throttling	Manually adjust the effect of a running backup on the performance of your computer to better match your needs at the moment. This feature is especially useful if you are working on your computer and don't want the backup process to slow you down. And if you know the demographics of your network traffic, you can now set network throttling to prevent network overload.

Feature	Description
Maxtor OneTouch™ integration	If you have a Maxtor OneTouch™ external hard drive, you can back up your computer with the push of a button. No need to start Backup Exec System Recovery.
Modifiable Symantec Recovery Disk	When you cannot start Windows, the newly enhanced Symantec Recovery Disk (SRD) makes recovery easier than ever. If the Symantec Recovery Disk is missing specific drivers, use the Create Recovery Disk feature to create a modified Symantec Recovery Disk that includes the exact drivers needed to successfully boot your computer into the recovery enironment. **Note:** If you purchased Backup Exec System Recovery pre-installed on a new computer, some features in the recovery environment may or may not be included, depending on how the computer manufacturer chose to install it. The recovery environment has likely been pre-installed on a special partition on your computer.

About the Advanced page

The Advanced page offers experienced Backup Exec System Recovery users a single view of the most common product features. If you have a good understanding of Backup Exec System Recovery, you might prefer to perform most tasks from the Advanced view.

Note: When refering to the documentation while using the Advanced page, the first one or two steps do not apply because they indicate where to access each feature from the other pages of the product interface. From that point on, follow the remaining steps of each procedure.

The Advanced page can be hidden from view if you do not plan to use it.

To hide the Advanced page

1 Start Backup Exec System Recovery.

2 On the View menu, click **Show Advanced Page**.

To show the Advanced page

1 Start Backup Exec System Recovery.

2 On the View menu, click **Show Advanced Page**.

Where to find more information

To learn more about Symantec Backup Exec System Recovery, visit the new Help and Support page. Depending on which version and language of the product you have installed, the Help and Support page includes one-click access to more information, including the product help system, the product User's Guide, and access to the Symantec Knowledge Base where you can find troubleshooting information.

To access Help and Support

1. Start Backup Exec System Recovery.
2. On the Home page, click **Help > Help and Support**.

Chapter 2

Installing Backup Exec System Recovery

This chapter includes the following topics:

Preparing for installation

Before you install Backup Exec System Recovery, make sure that your computer meets the system requirements.

System requirements

Table 2-1 lists the system requirements for Backup Exec System Recovery.

Table 2-1 Minimum system requirements

Component	Minimum Requirements
Operating system	The following Windows 32- or 64-bit operating systems are supported: ■ Windows Vista Home Basic ■ Windows Vista Home Premium ■ Windows Vista Ultimate ■ Windows Vista Business ■ Windows Vista Enterprise ■ Windows XP Professional/Home (SP2 or later) ■ Windows XP Media Center ■ Windows 2000 Professional (SP4 or later) ■ Windows 2000 Server (SP4 or later) ■ Windows 2000 Advanced Server (SP4 or later) ■ Windows Small Business Server 2000 ■ Windows Server 2003 ■ Windows Small Business Server 2003 ■ Windows Server 2008
RAM	The following memory requirements are grouped by key components: ■ Backup Exec System Recovery Agent: 256 MB ■ Backup Exec System Recovery user interface and Recovery Point Browser: 256 MB ■ Symantec Recovery Disk: 512 MB minimum **Note:** If you are installing a multilingual or double-byte version of the product, you must have a minimum of 768 MB of RAM to run the Symantec Recovery Disk. ■ Backup Exec System Recovery LightsOut Restore feature: 1 GB
Available hard disk space	■ When installing the entire product: Approximately 250 to 300 MB, depending on the language of the product you are installing ■ Microsoft .NET Framework 2.0: 280 MB of hard disk space is required for 32-bit computers, and 610 MB is required for 64-bit computers ■ Recovery points: Sufficient hard disk space on a local hard disk or network server for storing recovery points. The size of recovery points depends on the amount of data you have backed up and the type of recovery point being stored. See “Best practices for backing up ” on page 52. ■ Backup Exec System Recovery LightsOut Restore feature: 2 GB

Table 2-1 Minimum system requirements *(continued)*

Component	Minimum Requirements
CD-ROM or DVD-ROM drive	The drive can be any speed, but it must be capable of using as the startup drive from the BIOS. Backup Exec System Recovery uses Gear Software technology. To verify that your CD writer or DVD writer is compatible, visit http://www.gearsoftware.com/support/recorders/index.cfm. You can look up information about your writer if you know the name of the manufacturer and model number of your writer.
Software	The Microsoft .NET Framework 2.0 is required to run Backup Exec System Recovery. If the .NET Framework is not already installed, then you will be prompted to install it after Backup Exec System Recovery is installed and your computer is rebooted.
Virtual platforms (for converted recovery points)	The following virtual platforms are supported: ■ VMware GSX Server 3.1 and 3.2 ■ VMware Server 1.0 (replacement/rename for GSX Server) ■ VMware ESX Server 2.5 and 3.0 ■ VMware Infrastructure 3 (replacement/rename for ESX Server) ■ Microsoft Virtual Server 2005 R2

Supported file systems and removable media

Backup Exec System Recovery supports the following file systems and removable media:

Supported file systems	Backup Exec System Recovery supports FAT16, FAT16X, FAT32, FAT32X, NTFS, GUID Partition Table (GPT), dynamic disks, Linux Ext2, Linux Ext3, and Linux swap partitions. **Note:** You must decrypt encrypted NTFS drives before you attempt to restore them. You cannot view the files that are in a recovery point for an encrypted NTFS drive.
Removable media	You can save recovery points locally (that is, on the same computer where Backup Exec System Recovery is installed) or to most CD-R, CD-RW, DVD-R(W), and DVD+RW recorders. You can find an updated list of supported drives on the Symantec Web site. Backup Exec System Recovery also lets you save recovery points to most USB devices, 1394 FireWire devices, REV, Jaz, Zip drives, and magneto-optical devices.

Unavailable features

Symantec Backup Exec System Recovery is packaged to meet various markets. Some features might not be available, depending on the product you have purchased. However, all features are documented. You should be aware of which features are included with the version of the product you have purchased. If a feature is not accessible in the product user interface, it is likely not included with your version of the product.

Refer to the Symantec Web site for information about features included with your version of Symantec Backup Exec System Recovery.

About *Symantec Backup Exec for Windows Servers - System Recovery Option*

If you are using Symantec Backup Exec for Windows Servers - System Recovery Option, the following features are not available without upgrading to the full version of Backup Exec System Recovery:

Table 2-2 Disabled features

Feature	What it does
CD/DVD support	Back up your computer directly to CD or DVD, or copy recovery points to CD or DVD.
Centralized manageability	Allows Backup Exec System Recovery Manager to remotely monitor and manage installations of Backup Exec System Recovery found in a network, including backing up and recovering data.
Copy My Hard Drive Wizard	Copy all contents of one hard drive to a second hard drive.
Event Triggers	Run a backup automatically whenever specified events occur, such as any time a new application is installed.
File and folder backup	Limit your backup to include a select set of files or folders.
LightsOut Restore	Restore a computer from a remote location, regardless of the state of the computer, provided that its file system is intact.
Recovery point sets	After an initial, full backup of a drive, additional back ups only capture changes made to data on the drive since the full backup was performed. Without this feature, you can only create independent recovery points (full backups) of a drive.
Search engine support	Search for and recover files stored in recovery points using Google Desktop™.

You can enable these features by purchasing an upgrade license for the full version of Backup Exec System Recovery.

For more information, or to purchase an upgrade license, refer to your local reseller. You can also visit http://www.symantec.com/backupexec/ to learn more.

When you delay licensing

If you choose to delay installation of the product license (for a maximum of 30 days from the date of installation), the following features are unavailable until you install a valid license:

- Copy Drive
- Create Recovery Disk
- LightsOut Restore
- Restore Anyware
- Convert to Virtual Disk

All other features are enabled during the 30 day grace period.

If you are using an Evaluation copy of the product, it also expires after 30 days. However, all features are enabled until the end of the evaluation period, at which time you must purchase the product or uninstall it. You can purchase a license at any time (even after the evaluation period expires) without reinstalling the software.

Note: If this product came pre-installed from a computer manufacturer, your trial period could be as long as 90 days. The product licensing or activation page during install will indicate the duration of your trial period.

See “Activating Backup Exec System Recovery later” on page 28.

Installing Symantec Backup Exec System Recovery

Before you begin, you should review the requirements and scenarios for installing Backup Exec System Recovery.

See “System requirements” on page 21.

Note: During the installation process, you might be required to restart the computer. To ensure proper functionality after the computer restarts, log on again using the same user credentials that you used to log on when you installed Backup Exec System Recovery.

The installation program scans your hardware for the required drivers. If the program does not find the required drivers, you receive a driver validation message. If you receive this message, you should test the Symantec Recovery Disk (SRD). Testing the SRD verifies whether the drivers are required or if the devices on your system have compatible drivers that are available on the SRD. The driver validation process should not interfere with your ability to install the product.

See “About ensuring the recovery of your computer” on page 31..

Warning: The SRD provides the tools that you need to recover your computer. It is included with your product either on a separate CD, or on your product CD, depending on the version of the product that you purchased. You should store the CD in a safe place.

To install Symantec Backup Exec System Recovery

1. Log on to your computer using either the Administrator account or an account that has administrator privileges.
2. Insert the Symantec Backup Exec System Recovery product CD into the media drive of the computer.

   The installation program should start automatically.
3. If the installation program does not run, type the following command at a command prompt:.

   ```
   <drive>:\autorun.exe
   ```

   where <drive> is the drive letter of your media drive.
4. In the CD browser panel, click **Install Backup Exec System Recovery**.
5. Read the license agreement, and then click **I accept the terms in the license agreement**.
6. Do one of the following:
   - Click **Install Now** to begin the installation.
   - If you want to customize your settings, click **Custom Install**, select or deselect the options you want installed, and then click **Install Now**. Installation options include:

User Interface	Installs the product user interface that is required for interacting with the Backup Exec System Recovery Service.
Backup and Recovery Service	The primary service that is required to back up or recover your computer.
CD/DVD Support	Required for backing up directly to CD/DVD, and for creating a customized Symantec Recovery Disk CD. A CD/DVD burner is required to use this feature.

Recovery Point Browser	Enables you to browse, mount, copy, verify, and restore files and folders using recovery points.
LiveUpdate	Keeps your Symantec software up-to-date with the latest product updates.
Change	Click this button if you want to install Backup Exec System Recoveryto an alternate location.

7. If a driver that is used on your computer is not available on the Symantec Recovery Disk, you receive a notification message that includes the name of the driver. Write down the name of the driver file, and then click **OK** to dismiss the message.

   Drivers are critical in the event that you need to use the Symantec Recovery Disk CD to recover your system drive (the drive where your operating system is installed).

   See “About ensuring the recovery of your computer” on page 31.

8. Click **Finish** to complete the installation.

9. Remove the product CD from the media drive, and then click **Yes** to exit the installation wizard and restart the computer.

   If you click **No** because you plan to restart your computer yourself at a later time, note that you cannot run Backup Exec System Recovery until after you restart your computer.

Completing the installation

After you install the product, you are prompted to license or activate your product. You can then run LiveUpdate to check for product updates, and then configure your first backup.

Note: If this product came pre-installed from a computer manufacturer, your trial period could be as long as 90 days. Refer to the Install license later label.

To complete the installation

1. In the Welcome panel, click **Next**.

   If the product was installed by your computer manufacturer, the Welcome page might appear the first time that you run Backup Exec System Recovery.

2. Do one of the following:

   - Click **I've already purchased the product and have a product key**.

Note: You can find the product key on the back of your product CD jacket. Do not lose the product key. You must use it when you install Backup Exec System Recovery.

- Click **Activate later** to delay the activation of your license. After the trial period ends, the product will no longer work.
- If this product is a trial version of Backup Exec System Recovery and you want to purchase a product key, click **Symantec Global Store** to connect to the Symantec Web site.
- Click **Install license later** to delay the activation of your license for 30 days. After 30 days, the product will no longer work.
  See "When you delay licensing " on page 25.
- If you have a Volume Incentive Program (VIP) Activation key, enter it in the appropriate spaces as it appears on your certificate.

3 Click **Next**.

4 Click **Run LiveUpdate** to check for any product updates since the product shipped.

5 Click **Launch Easy Setup** to open the Easy Setup box when you complete the install process.

6 Click **Enable Google Desktop File and Folder Recovery** if you want use Google Desktop to search your recovery points for the files and folders that you want to recover.

If you select this option, Backup Exec System Recovery automatically catalogs each file as it creates a recovery point. Google Desktop can then use this catalog to search for files by name. It does not index the content of the files.

Note: This option is available only if Google Desktop already is installed on your computer. If you plan to install Google Desktop, you can enable search engine support later.

7 Click **Finish**.

Activating Backup Exec System Recovery later

If you do not activate Backup Exec System Recovery before the trial period ends, the software stops working. However, you can activate the product at any time after the trial period expires.

To activate Backup Exec System Recovery at any time after installation

1. On the Help menu, click **Unlock Trial Product**.
2. Refer to step 2 in the *To complete the installation* procedure.

Setting up your first backup

Unless you unchecked the Run Easy Setup check box during the setup wizard, the Easy Setup window appears. If you don't run Easy Setup during the setup wizard, it appears the first time you open the Run or Manage Backups window.

Note: The Easy Setup window is unavailable in server versions of Backup Exec System Recovery.

When the Easy Setup window opens, you can either accept the default drive and file and folder backup settings, or you can click on any of the settings to modify them.

If you want the new backup to run immediately, be sure to select Run backup now, and then click OK.

Updating Backup Exec System Recovery

You can receive software updates that are associated with your version of the product over your Internet connection. LiveUpdate connects to the Symantec LiveUpdate server and automatically downloads and installs updates for each Symantec product that you own.

You run LiveUpdate as soon as you install the product. You should continue to run LiveUpdate periodically to obtain program updates.

To update Backup Exec System Recovery

1. On the Help menu, click **LiveUpdate**.
2. In the LiveUpdate window, click **Start** to select the updates.

   Follow the on-screen instructions.
3. When the installation is complete, click **Close**.

   Some program updates might require that you restart your computer before the changes take effect.

Uninstalling the product

When you upgrade Backup Exec System Recovery from a previous version of the product, the install program automatically uninstalls the previous versions. If needed, you can manually uninstall the product.

Follow your operating system's instructions on how to uninstall software.

Chapter 3

Ensuring the recovery of your computer

This chapter includes the following topics:

About ensuring the recovery of your computer

If Windows fails to start or it does not run normally, you can recover your computer by using the Symantec Recovery Disk (SRD). The drivers that are included on the recovery disk must match the drivers required to run your computer's network cards and hard disks.

To help ensure that you have the drivers that you need to recover your computer, the installation process runs a driver validation test. The driver validation tool compares hardware drivers that are contained on the recovery disk with the drivers that are required to run your computer's network cards and hard disks.

The installation process automatically runs the driver validation test. You can also run a validation test at anytime by running the Symantec Recovery Disk Wizard.

You should run the driver validation test any time you make changes to the NIC cards or storage controllers on a computer.

See "If driver validation fails" on page 32.

Note: Wireless network adapter drivers are not supported by the driver validation tool or by the SRD.

Testing Symantec Recovery Disk

You should test the SRD to ensure that the recovery environment runs properly on your computer.

Note: Depending on which version of the product you have purchased, the SRD is either included on your product CD, or as a separate CD. You should place the CD containing the SRD in a safe place. Should you lose the CD, you can create a new one if you have have a CD burner.

Testing the SRD allows you to identify and solve the following types of problems:

- You cannot boot into the recovery environment.
  See "To configure your computer to boot from a CD" on page 162.
- You do not have the necessary storage drivers to access recovery points on the computer.
- You need information about your system to help you run the recovery environment.

To test the SRD

1. Run the driver validation tool to test whether the SRD works with the network cards and storage devices on the computer.
2. Boot your computer using the SRD.

   See "Starting a computer by using the recovery environment " on page 160.
3. When you have booted into the recovery environment, do one of the following:
   - If you want to store recovery points on a network, run a mock restore of a recovery point that is stored on a network to test the network connection.
   - If you want to store recovery points on the computer, run a mock restore of a recovery point that is stored locally to test the local hard-drive connection.

If driver validation fails

The driver validation test verifies whether the drivers for all storage devices and network cards in use by the computer are available in the recovery environment.

If the drivers are available on the recovery disk, you receive a validation message. If any drivers are missing from the recovery disk, the Driver Validation Results dialog appears.

Without access to the correct drivers, a device cannot be used while running the SRD. Therefore, if the recovery points required for recovering your computer are stored on a network or a local hard drive, you might not have access to them.

You can find the drivers and copy them to a CD or a floppy disk, or you can create a custom Symantec Recovery Disk CD.

See "Creating a custom Symantec Recovery Disk CD" on page 33.

Creating a custom Symantec Recovery Disk CD

Even if driver validation succeeds and your Symantec Recovery Disk CD appears to work, you should create a custom Symantec Recovery Disk CD. A custom CD will contain your computer's current network and storage device drivers, helping to ensure that in an emergency you can get to the recovery points required to restore your computer.

Note: You must have a writeable DVD/CD-RW drive to create a custom Symantec Recovery Disk.

To create a custom Symantec Recovery Disk CD

1. Start Backup Exec System Recovery.
2. Attach and turn on all storage devices and network devices that you want to make available.
3. Insert the Symantec Recovery Disk CD into your CD-ROM drive.
4. From the main Backup Exec System Recovery window, click **Tasks > Create Recovery Disk**, and then click **Next**.
5. If prompted, click **Browse**, select the drive that contains the Symantec Recovery Disk CD, click **OK**, and then click **Next**.
6. Do one of the following:
   - Click **Automatic (Recommended)**, and then click **Next**.
   - Click **Custom**, and then click **Next**.

Select this option only if you know which drivers to select.

7 Follow the on-screen instructions to complete the wizard.

Warning: Be certain to test your new, customized Symantec Recovery Disk CD to make sure that it can start your computer and that you can access the drive containing your recovery points.

See "Testing Symantec Recovery Disk" on page 32.

Chapter 4

Getting Started

This chapter includes the following topics:

- Key product components
- How you use Backup Exec System Recovery
- Starting Symantec Backup Exec System Recovery
- Configuring Backup Exec System Recovery default options

Key product components

Backup Exec System Recovery includes two key components: the program itself, and the Symantec Recovery Disk.

Table 4-1 Key product components

Key Component	Description
Backup Exec System Recovery program (user interface)	The Backup Exec System Recovery program lets you define, schedule, and run backups of your computer. When you run a backup, recovery points of your computer are created, which you can then use to recover your entire computer, or individual drives, files, and folders. You can also manage recovery point storage (backup destination), and monitor the backup status of your computer to make sure your valuable data is backed up on a regular basis.

Table 4-1 Key product components *(continued)*

Key Component	Description
Symantec Recovery Disk	The Symantec Recovery Disk (SRD) is used to boot your computer into the recovery environment. If your computer's operating system fails, use the SRD to recover your *system drive* (the drive where your operating system is installed). **Note:** Depending on which version of the product you have purchased, the SRD is either included on your product CD, or as a separate CD. You should place the CD containing the SRD in a safe place. Should you lose the CD, you can create a new one if you have have a CD burner. See "About recovering a computer " on page 159.

How you use Backup Exec System Recovery

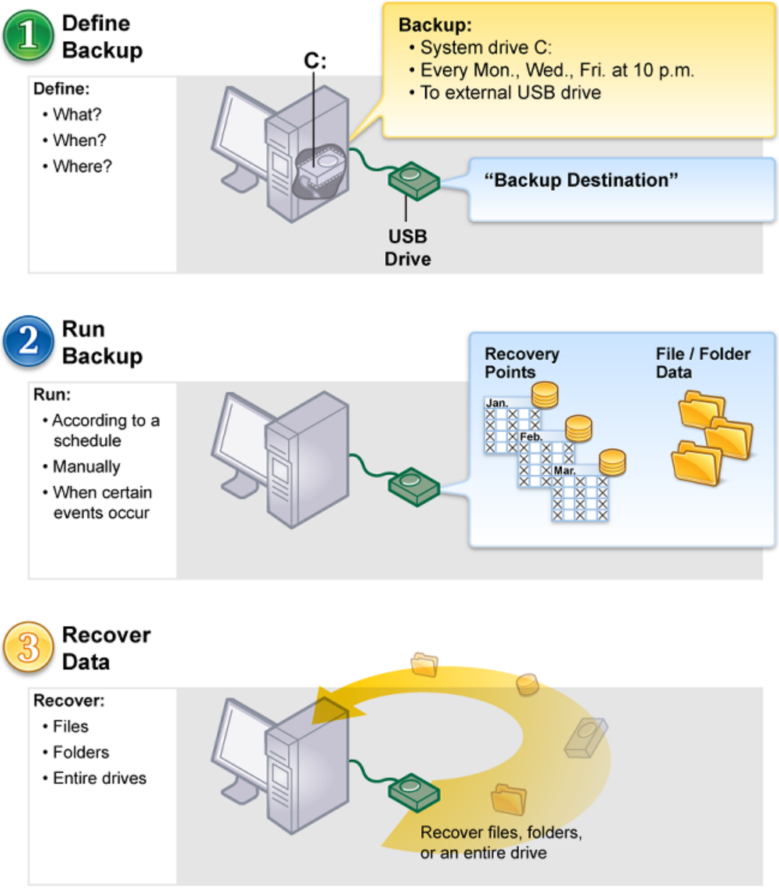
While Backup Exec System Recovery does the work of backing up your files, folders, or entire drives, you need to tell Backup Exec System Recovery what to backup, when to back it up, and where to put the backed up data.

Using Backup Exec System Recovery includes the following key tasks:

- Defining a backup
- Running a backup
- Recovering files, folders, or entire drives

Refer to the following figure to understand the relationship of these tasks.

Figure 4-1 Using Backup Exec System Recovery



Starting Symantec Backup Exec System Recovery

Backup Exec System Recovery is installed in the Windows Program Files folder by default. During installation, a program icon is installed in the Windows system tray from which you can open Backup Exec System Recovery. You can also open Backup Exec System Recovery from the Windows Start menu.

Note: To use the full version of Backup Exec System Recovery, you must activate the software.

See "Activating Backup Exec System Recovery later" on page 28.

To start Symantec Backup Exec System Recovery

- Do one of the following:
  - On the classic Windows taskbar, click **Start > Programs > Backup Exec System Recovery**.
  - On the Windows 2003 taskbar, click **Start > All Programs > Symantec > Backup Exec System Recovery**.
  - On the Windows XP or Windows Vista taskbar, click **Start > All Programs > Backup Exec System Recovery**.
  - In the Windows system tray, double-click the Backup Exec System Recovery tray icon.
  - In the Windows system tray, right-click the Backup Exec System Recovery tray icon, and then click **Open Symantec Backup Exec System Recovery**.

Configuring Backup Exec System Recovery default options

The Options dialog box includes several views that let you configure the following default settings:

Options	Description
General	Specify a default location where a backup will create and store recovery points and file and folder backup data. If the location you choose is on a network, you can enter your user authentication information. See "Selecting a default backup destination " on page 40.

Options	Description
Performance	Lets you specify a default speed for backup or recovery processes. Moving the slider closer to Fast increases the speed at which the program backs up or recovers your computer. However, choosing a slower speed could improve the performance of your computer, especially if you are working on your computer during a backup or recovery. **Note:** During a backup or recovery, you have the option to override this default setting to fit your needs at the time. You can also configure network throttling to limit the effects of backups on network performance. See "Adjusting the effects of a backup on computer performance" on page 41. See "Enabling network throttling " on page 42.
Tray Icon	You can turn the system tray icon on or off and specify whether to show only error messages when they occur, or to show both error messages and other information, such as the completion of a backup. See "Adjusting default tray icon settings " on page 43.
File Types	Lets you manage file types and file type categories, which are used as a method for selecting the types of files you want included in a file and folder backup. See "Managing file types " on page 44.
Google Desktop	If Google Desktop is installed on your computer when you install Backup Exec System Recovery, you have the option of enabling Google Desktop file and folder recovery. When you enable this feature, you can search for files (by file name) inside a recovery point that was created with search engine support enabled. If Google Desktop is not installed on your computer when you install Backup Exec System Recovery, you have the option of clicking a link to the Web site where you can download and install Google Desktop for free. See "About using a search engine to search recovery points" on page 187.
External Drives	Delete or rename the unique names you have given to external drives used as backup and Offsite Copy destinations. See "Using aliases for external drives" on page 45.

Options	Description
Configure FTP	Specify default FTP settings to be used with Offsite Copy. See "Configuring FTP settings for use with Offsite Copy" on page 46.
Log File	Lets you specify the types of product messages to log (errors, warnings, and information), where to store the log file, and set a maximum file size for the log file. See "Logging Backup Exec System Recovery messages" on page 47.
Event Log	Lets you specify the types of product messages to log (errors, warnings, and information) in the Windows event log. See "Logging Backup Exec System Recovery messages" on page 47.
SMTP E-mail	If you want a history of actions taken by Backup Exec System Recovery, or of error messages and warnings, you can choose to save them in a log file on your computer, or to have them emailed to an address you specify. See "Enabling email notifications for product (event) messages " on page 49.
SNMP Trap	If you have a Network Management System (NMS) application, you can enable SNMP Traps support to send notifications to you NMS application. See "Configuring Backup Exec System Recovery to send SNMP traps" on page 120.

To configure default options

1. Start Backup Exec System Recovery and click **Tasks > Options**.
2. Select an option you want to modify, make any necessary changes, and then click **OK**.

Selecting a default backup destination

You can specify the default destination for storing recovery points and file and folder backup data created when you run a backup. This default location is used if you do not specify a different location when you define a new backup.

To set a default backup destination

1. On the menu bar, click **Tasks > Options**.
2. Click **General**.
3. Check **Prepend computer name to backup data file names**.

   This is especially useful if you back up more than one computer to the same drive. For example, you might back up a laptop and a desktop computer to the same USB or network drive. By prepending the computer name to each backup data file name, you can more easily identify which backup data files belong to which computer.
4. Check **Save backup files to a unique subfolder** if you want Backup Exec System Recovery to create a new subfolder that will serve as your backup destination.

   Note: The new subfolder is given the same name as your computer. For example, if your computer name is "MyLaptop", the new subfolder would be named \MyLaptop.
5. Enter a path to a folder where you want to store recovery points and file and folder backup data, or click **Browse** to look for a location.

   You cannot use an encrypted folder as your backup destination. If you want to encrypt your backup data to prevent another user from accessing it, refer to the Advanced options when you define or edit a backup.
6. If you entered the path to a location on a network, enter the user name and password required to authenticate to the network.
7. Click **OK**.

Adjusting the effects of a backup on computer performance

If you are working on your computer when a backup is running—especially one that is creating an independent recovery point—your computer might slow down. This is because Backup Exec System Recovery is using your computer's hard disk and memory resources to perform the backup.

However, you can actually modify the speed of the backup as a way of minimizing the impact of Backup Exec System Recovery on your computer while you work.

To adjust the default effect of a backup on my computer's performance

1. On the main menu bar, click **Tasks > Options**.
2. Click **Performance**.

3. If you want to improve your computer's speed performance, move the slider bar closer to **Slow**.
4. If you want the backup to complete more quickly, move the slider bar closer to **Fast**.
5. Click **OK**.

Note: During a backup or recovery, you'll have the option of overriding this default setting to fit your needs at that moment.

See "Adjusting the speed of a backup " on page 91.

Enabling network throttling

Similar to computer performance adjustments, you can also limit the impact of a backup on network performance.

However, because network performance is affected by many variables, you should consider the following issues before enabling this feature:

- Network cards: Is your network wired or wireless? What are the speeds of your network cards?
- Network backbone: What is the size of your network pipeline? Does it support 10 MB transfer rates, or 1 GB transfer rates?
- Network server: How robust is your server hardware? How fast is its processor? How much RAM does it have? Is it fast or slow?
- Backing up: How many computers are scheduled to back up at the same time?
- Network traffic: Are backups scheduled to run when network traffic is heavy or light?

Consider using this feature only when you know what your network can handle. If you schedule your backups at staggered intervals, and if you schedule them when network traffic is low, you will likley not need to use this feature.

Gather the required information about your network's performance and then schedule backups accordingly. Then, if necessary, enable this feature and set the Maximum network throughput to a setting that matches the circumstances.

To enable network throttling

1. On the main menu bar, click **Tasks > Options**.
2. Click **Performance**.
3. Check **Enable network throttling**.

4 In the Maximum network throttling field, enter the maximum amount (in KB) of network throughput that Backup Exec System Recovery can send per second.

5 Click **OK**.

Adjusting default tray icon settings

You can turn the system tray icon on or off and specify whether to show only error messages when they occur, or to show both error messages and other information, such as the completion of a backup.

To adjust default tray icon settings

1 On the main menu bar, click **Tasks > Options**.

2 Click **Tray Icon** and select one of the following:

Show system tray icon	Displays the Backup Exec System Recovery icon in the system tray. You must select this option to enable or disable any of the remaining options.
Show missed backups	Notifies you when a backup was scheduled but did not run. This can happen when your computer was turned off at the time a backup was scheduled to run.
Show system tray questions	Offers helpful prompts in the form of questions that can help you keep your data backed up.
Show status messages	Displays messages about the status of backup operations, such as notifying that a backup has started, or that your backup destination is getting full.
Show error messages	Displays error messages when errors occur so that you can resolve any issues that might hinder data protection.

3 Click **OK**.

Managing file types

When you define a file and folder backup, file types are a quick way to include files you use the most. For example, if you keep music files on your computer, you can configure a file and folder backup to include all music files (for example, .mp3, .wav).

The most common file types and extensions are already defined for you. But you can define additional file type categories as needed, and then edit them at any time. For example, if you install a new program that requires the use of two new file extensions (.pft and .ptp, for example), you can define a new file type and define the two file extensions for that category. Then when you define a file and folder backup, you can select the new category. When the backup is run, all files ending with .pft and .ptp are backed up.

To create a new file type and extensions

1. On the main menu bar, click **Tasks > Options**.
2. Click **File Types**.
3. At the bottom of the File types list, click the **Add a file type** (+) button to add a file type category.
4. Type a descriptive name of the new file type category, and then press Enter.
5. At the bottom of the Extensions for list, click the **Add an extension** (+) button, and then type an asterisk (*) and a period, followed by the extension of the file type you want to define, and then press Enter.
6. Click **OK**.

To edit a file type and extensions

1. On the main menu bar, click **Tasks > Options**.
2. Click **File Types**.
3. Select a file type from the File types list, and then do one of the following:
   - Click the **Rename a file type** button (at the right of the - button) to edit the name of the selected file type.
   - Select an extension in the Extensions for column and click the **Rename an extension** button (at the right of the - button) to edit the name of the extension.
   - Click either the **Restore default file types list** or the **Restore default extension list** button to restore all default file types or extensions.

Caution: Any file types and extensions you have set up are removed. Once removed, you will have to add them again manually.

4 Click **OK**.

To delete a file type (and all of its extensions)

1 On the main menu bar, click **Tasks > Options**.

2 Select a file type in the File types column.

You cannot delete a default file type. You can delete all but one extension of a default file type, and you can add additional extensions to a default file type.

3 Click the **Remove a file type** (-) button , and then click **OK**.

Use this same procedure to remove file extensions from the Extensions for list.

Using aliases for external drives

When you choose an external drive for use with Backup Exec System Recovery as either a backup destination or an Offsite Copy destination, it can become confusing if you are using more than one drive, especially when the assigned drive letter changes each time you plug in the drive.

To help you manage these destinations, Backup Exec System Recovery lets you assign an alias to each external drive. Doing so does not change the drive label, but is for use only when you are accessing those drives from within Backup Exec System Recovery.

For example, you might be swapping out two different external drives used as Offsite Copy destinations during any given week. Depending on the drive labels assigned to each drive and whether or not the drive letter previously assigned has changed, it could become confusing as to which drive you are using at any given time.

However, by associating unique aliases to each drive, then as you use the drive with Backup Exec System Recovery, the aliases you assigned appear in various locations in Backup Exec System Recovery.

Note: It is also a good idea to place physical labels on each external drive to help you manage the task of swapping the drives.

For example, if you assigned the alias, "Drive A: Monday" to one drive, and "Drive B: Wednesday" to a second drive, their aliases appear in Backup Exec System Recovery whenever the drives are plugged in to your computer.

See "About Offsite Copy" on page 79.

To make it even easier, the Options dialog box lets you see all of your alias drive names in one view. From this view, you can remove or edit existing names.

To remove or edit external drive aliases

1. On the main menu bar, click **Tasks > Options**.
2. Under Destinations, click **External Drives**.
3. Select an external drive from the list and then do one of the following:
   - Click **Remove** to remove the alias associated with the external drive.
   - Click **Rename** to modify the alias.

Configuring FTP settings for use with Offsite Copy

File Transfer Protocol, or FTP, is the simplest and most secure way to copy files over the Internet. Backup Exec System Recovery serves as an FTP client to copy your recovery points to a remote FTP server as a secondary backup of your critical data.

The Options dialog box lets you configure basic FTP settings to help ensure that your recovery points are copied to your FTP server.

To configure default FTP settings

1. On the main menu bar, click **Tasks > Options**.
2. Under Destinations, click **Configure FTP**.
3. Refer to the following table when making changes:

Connection mode: Passive (Recommended)	Passive (sometimes written "PASV") mode helps avoid conflicts with security systems. This mode is necessary for some firewalls and routers because when using passive mode, the FTP client opens the connection to an IP Address and port that the FTP server supplies.
Connection mode: Active	Use active mode when connections or transfer attempts fail in passive mode, or when you receive data socket errors. When an FTP client connects using active mode, the server opens a connection to an IP Address and port that the FTP client supplies.
Limit connection attempts to	Specify the number of times Backup Exec System Recovery tries to connect to an FTP server before giving up. Backup Exec System Recovery can attempt a maximum of 100 times.
Stop trying to connect after	Specify the number of seconds Backup Exec System Recovery tries to connect to an FTP server before giving up. You can specify up to 600 seconds (10 minutes).
Default port	Specify the port of the FTP server that is listening for a connection. You should consult the FTP server administrator to be sure that the port you specify is configured to recieve incoming data.

Logging Backup Exec System Recovery messages

You can specify which product messages (errors, warnings, and information) are logged as they occur, and where the log file is stored. Product messages can provide useful information about the status of backups or related events, and can also provide helpful information when you are troubleshooting.

Two logging methods are available: Backup Exec System Recovery logging, and the Windows application log.

From the Options page, you can configure both methods.

To configure a Backup Exec System Recovery log file

1. On the main menu bar, click **Tasks > Options**.
2. Under Notifications, click **Log File**.
3. Click the **Select the priority and type of messages** drop-down list and select the priority level at which a message should be logged.

All messages	Send all messages, regardless of priority levels.
Medium and high priority messages	Send only medium and high priority messages.
High priority messages only	Send only high priority messages.
No messages	Do not send any messages, regardless of priority levels.

4. Select one or more of the following options:
   - Errors
   - Warnings
   - Information
5. In the Log file location field, enter a path to where the log file should be created and stored.

   If you don't know the path, click **Browse** and select a location.
6. In the Maximum file size field, specify a maximum size (in kilobytes) that the log file is allowed to grow.

   The file is kept within the limit you set by replacing the oldest logged items in the file with new items as they occur.
7. Click **OK**.

To configure which product events are written to a Windows event log

1. On the main menu bar, click **Tasks > Options**.
2. Under Notifications, click **Event Log**.

3. Click the **Select the priority and type of messages** drop-down list and select the priority level at which a message should be logged.

All messages	Send all messages, regardless of priority levels.
Medium and high priority messages	Send only medium and high priority messages.
High priority messages only	Send only high priority messages.
No messages	Do not send any messages, regardless of priority levels.

4. Select one or more of the following options:
   - Errors
   - Warnings
   - Information
5. Click **OK**.

Enabling email notifications for product (event) messages

Email notifications can be sent to a specified email address if there are any errors or warnings that occurred when a backup is run.

Note: If you do not have an SMTP server, this feature is unavailable to you.

Notifications can also be sent to the system event log and a custom log file located in the Agent folder of the product installation.

If notifications are not being delivered, check the setup of your SMTP server to ensure that it is functioning properly.

To enable email notifications

1. On the main menu bar, click **Tasks > Options**.
2. Under Notifications, click **SMTP E-mail**.

3. Click the **Select the priority and type of messages** drop-down list and select the priority level at which an email should be sent.

All messages	Send all messages, regardless of priority levels.
Medium and high priority messages	Send only medium and high priority messages.
High priority messages only	Send only high priority messages.
No messages	Do not send any messages, regardless of priority levels.

4. Select one or more of the following options:

    - Errors
    - Warnings
    - Information

5. In the To address text box, type the email address (for example, admin@domain.com) where notifications are to be sent.

6. If desired, type the email address of the sender in the From address text field.

    If you do not specify a From address, the name of the product will be used.

7. In the SMTP server text box, type the path to the SMTP server that will send the email notification (for example, smtpserver.domain.com).

8. From the SMTP Authentication drop-down box, select the method to use to authenticate to the SMTP server specified above.

9. Enter your SMTP username and password.

    If you are not sure what your username and password are, contact a system administrator.

10. Click **OK**.

Chapter 5

Best practices for backing up your data

This chapter includes the following topics:

About backing up your data

To back up your computer or your individual files and folders, you do the following steps:

- Define a backup
- Run the backup
  See "How you use Backup Exec System Recovery" on page 36.

When you define a backup, you make the following decisions:

- What to back up (files and folders, or an entire drive)
- Where to store the backup data (backup destination)
- Whether or not to use Offsite Copy to copy backup data to remote locations

- When to run the backup (automatically or manually)
- What compression levels to specify for recovery points, and whether to enable security settings (encryption and password protection).
- Which of the many other options you want to use. You can customize each backup according to your backup needs.

Choosing a backup type

There are two types of backups available:

- Drive-based backup: Backs up an entire hard drive
- File and folder backup: Backs up only the files and folders that you select

You can use the following guidelines to determine which type of backup to choose:

Drive-based backup	Use this backup type to do the following: ■ Back up and recover your computer's system drive (typically, the C drive, which includes your operating system). ■ Back up and recover a specific hard drive, such as a secondary drive (which is a drive other than the system drive on which your operating system is installed). ■ Recover lost or damaged files or folders from a specific point in time.
File and folder backup	Use this backup type to do the following: ■ Back up and recover specific files and folders, for example personal files that are stored in the My Documents folder. ■ Back up and recover files of a specific type, for example music (.mp3 or .wav) or photographs (.jpg or .bmp). ■ Recover a specific version of a file from a specific point in time.

See “Before you back up” on page 53.

Best practices for backing up

As you prepare to back up your computer, review this information:

- Before you back up
- During a backup

- When the backup is complete

About backups

When you back up your computer, you choose from two types of backups:

- *drive-based backup*: backs up an entire hard drive
- *file and folder backup*: backs up only the files and folders you select

Which backup type you choose depends on what you are trying to protect and how much storage space you have to store backup data (recovery points, and file and folder backup data).

The following table highlights the key uses of each backup type:

Backup type	Use to
Drive-based backup	■ Back up and recover your computer (system drive, typically drive C) ■ Back up and recover a specific hard drive (any secondary drive, drives other than your system drive) ■ Recover lost or damaged files or folders using recovery points
File and folder backup	■ Back up and recover specific files and folders, such as personal files stored in the My Documents folder ■ Back up and recover files of a specific type, such as music (.mp3, .wav) or photographs (.jpg, .bmp)

Before you back up

Consider these best practices before defining and running your first backup:

Schedule backups when you know your computer will be turned on.	Your computer must be turned on and Windows must be running at the time a backup occurs. If not, any scheduled backups are skipped until the computer is turned on again. You then are prompted to run the missed backup. See “Choosing a backup type” on page 52.
Use a secondary hard disk as your backup destination.	You should store recovery points on a hard disk other than your primary hard disk C. This practice helps ensure that you can recover your system in the event that your primary hard disk fails. See “About selecting a backup destination ” on page 58.

Consider using external drives as your backup destination.	Using an external drive makes your backup data more portable. Should you need to remove your critical data from a particular location, you can quickly grab an external drive on your way out the door. See “About Offsite Copy” on page 79.
Give nicknames to your external drives to help you easily identify them	You can assign a nickname to each external drive to help keep track of where your backup data is stored for each computer you back up. Because drive letters can change each time you unplug and plug an external drive into your computer, a nickname ensures that you can always know which drive you are using when you are running Backup Exec System Recovery. Using a nickname does not change the volume label of a drive. A nickname simply helps you identify the drive when using Backup Exec System Recovery. And the nickname sticks with the drive, so that if you plug the drive into a second computer running another copy of Backup Exec System Recovery, the nickname appears. **Note:** You might also consider placing a sticky label on each drive that matches the nickname you've assigned. See “Using aliases for external drives” on page 45.
Use Offsite Copy	Use Offsite Copy to copy your latest recovery points to either a portable storage device or a remote server. By copying recovery points to a portable hard disk, you can then take a copy of your data with you when you leave the office. See “About Offsite Copy” on page 79.
Run backups on a regular and frequent basis.	When you define your backups, schedule them to run frequently so that you have recovery points that span at least the last two months. See “Editing a backup schedule ” on page 95. See “Defining a drive-based backup ” on page 63.

Keep personal data on a separate drive than the drive on which Windows and your software programs are installed.	You should keep your operating system and software programs separate from your own data. This practice helps to speed the creation of recovery points and reduce the amount of information that needs to be restored. For example, use the C drive to run Windows and to install and run software programs. Use the D drive to create, edit, and store personal files and folders. For other drive management solutions, go to the Symantec Web site at the following URL: www.symantec.com/.
Verify the recovery point after you create it to ensure that it is stable.	When you define a backup, you should select the option to verify the recovery point to ensure that the recovery point can be used to recover lost data. See “Choosing a backup type” on page 52.

During a backup

While a backup is running, consider the following best practices:

Improve your computer's performance during a backup	If you are working at your computer and a backup starts to run, you might notice that the performance of your computer slows down. Backup Exec System Recovery requires significant system resources to run a backup. If slowing occurs, you can reduce the speed of the backup to improve computer performance until you are finished working. See “Adjusting the speed of a backup ” on page 91.

When the backup is complete

After a backup completes, consider the following best practices:

Review the contents of recovery points and file and folder backup data.	Periodically review the contents of your recovery points to ensure that you back up only your essential data. For file and folder backups, click Recover My Files from either the Home or Tasks pages. Then click Search to display the latest version of all the files that are included in your backup. For drive-based backups, see Opening files and folders stored in a recovery point.
Review the Status page to verify that backups have happened and to identify any potential problems.	Periodically review the Status page. You can also review the events log on the Advanced page. The event log records events when they occur, backups and any errors that might have occurred during or after a backup. If you do not see the Advanced page tab, click View > Show Advanced Page. **Note:** Backup status and other messages are also conveyed in the system tray. So you do not even need to start the product to identify the status of your backups. See “Verifying that a backup is successful ” on page 92.
Manage storage space by eliminating old backup data.	Delete outdated recovery points to make more hard disk space available. Also, reduce the number of file versions that are created by file and folder backups. See “Managing recovery points” on page 135. See “Managing file and folder backup data” on page 141.
Review the level of protection that is provided for each of your computer's drives.	Check the Status page on a regular basis to ensure that each drive has a defined backup.
Maintain backup copies of your recovery points.	Store backup copies of your recovery points in a safe place. For example you can store them elsewhere on a network, or you can store them on CDs, DVDs, or tapes for long-term, off-site storage. See “Making copies of recovery points ” on page 137.

Additional tips about backups

Consider the following tips when you run a defined backup:

- Backup Exec System Recovery does not need to be running for a scheduled backup to start. After you define a backup, you can close Backup Exec System Recovery.
- The computer that is being backed up must be turned on and Windows must be started.
- All defined backups are saved automatically so that you can edit them or run them later.
- Do not run a disk defragmentation program during a backup. Doing so will significantly increase the time that it takes to create the recovery point and might cause unexpected system resource issues.
- If you have two or more drives that are dependent on each other, you should include both drives in the same backup. This provides the safest protection.
- Include multiple drives in the same defined backup to reduce the total number of backups that must be run. Doing so minimizes interruptions while you work.
- Use the Progress and Performance feature to reduce the impact of a backup on your computer's performance. For example, if a scheduled backup starts while you are in the middle of a presentation, you can slow down the backup to give more processing resources back to your presentation program.
- The power management features on a computer can conflict with Backup Exec System Recovery during a backup.

  For example, your computer might be configured to go into hibernation mode after a period of inactivity. You should consider turning off the power management features during a scheduled backup.
- If a backup is interrupted, consider running it again.
- If you experience problems while creating a backup, you may need to reboot the computer.

After defining your backup job

All backup jobs you define are automatically saved so that you can edit or run them later.

After you define a backup and schedule it to run, you can close Backup Exec System Recovery. The program does not need to be running for a backup to start.

However, your computer must be turned on and Windows must be running at the time a backup occurs. If not, any scheduled backups are skipped until the computer is turned on again. You then are prompted to run the missed backup.

Viewing the properties of a backup job

You can review the settings and configuration of a defined backup without opening the backup job.

To view the properties of a backup job

1. On the Home page, click **Run or Manage Backups**.
2. In the Run or Manage Backups window, select a backup job and then click **Tasks > Properties**.

About selecting a backup destination

You should review the following information before deciding where to store recovery points and file and folder backup data.

Note: If you choose to use CDs or DVDs as your backup destination (not recommended), you cannot back up to a sub-folder on the disk. Backup data must be created at the root of CDs and DVDs.

Table 5-1 contains information that you need to consider when selecting a backup destination.

Table 5-1 Selecting a backup destination

Backup destination	Information to consider
Local hard drive, USB drive, or FireWire drive (recommended)	The benefits of this option are as follows: ■ Fast backup and recovery ■ Can schedule unattended backups ■ Inexpensive because drive space can be overwritten repeatedly ■ Off-site storage is possible ■ Reserves hard drive space for other uses Although you can save the recovery point to the same drive that you are backing up, it is not recommended for the following reasons: ■ As the number or size of recovery points grows, you will have less disk space available for regular use. ■ The recovery point is included in subsequent recovery points of the drive, which increases the size of those recovery points. ■ If the computer suffers a catastrophic failure, you may not be able to recover the recovery point you need, even if you save it to a different drive on the same hard disk.
Network folder	If your computer is connected to a network, you can save your recovery points and file and folder backup data to a network folder. Backing up to a network folder typically requires that you authenticate to the computer that is hosting the folder. If the computer is part of a network domain, you must provide the domain name, user name, and password. For example, domain\username. If you are connecting to a computer in a workgroup, you should provide the remote computer name and user name. For example: remote_computer_name\username.

Table 5-1 Selecting a backup destination *(continued)*

Backup destination	Information to consider
CD-RW/DVD-RW	When you save backup data to removable media, it is automatically split into the correct sizes if the backup spans more than one media. If more than one drive is being backed up, the recovery points for each drive are stored independently on the media, even if there is space to store recovery points from multiple drives on the same media. The scheduling of backups is not available when this option is used. **Note:** Using CD-RWs or DVD-RWs as your recovery point storage location is not the best option because you will be required to swap disks during the process.

Table 5-2 describes the advantages and disadvantages of different types of backup destinations.

Table 5-2 Advantages and disadvantages of backup destinations

Backup destination	Advantages	Disadvantages
Hard drive (recommended)	■ Fast backup and recovery ■ Can schedule unattended backups ■ Inexpensive because drive space can be overwritten repeatedly	■ Uses valuable drive space ■ Vulnerable to loss if the hard drive fails
Network drive (recommended)	■ Fast backup and recovery ■ Can schedule unattended backups ■ Inexpensive because drive space can be overwritten repeatedly ■ Protection from local hard drive failure ■ Off-site storage (through existing network backup strategies)	■ Must have supported NIC drivers to restore from the recovery environment ■ Must understand and assign the appropriate rights for users who will run backups and restore data

Table 5-2 Advantages and disadvantages of backup destinations *(continued)*

Backup destination	Advantages	Disadvantages
Removable media (local)	■ Protection from hard drive failure ■ Ideal for off-site storage ■ Reserves hard drive space for other uses	

About backing up dual-boot computers

You can back up dual-boot computers, even if you have drives (partitions) that are hidden in the operating system from which you run Backup Exec System Recovery.

When you run a drive backup, the entire contents of each drive is captured in a recovery point. When you restore a drive, the recovered drive is bootable.

Note: In order for your computer to boot the same from a restored system as it did from the original configuration, you must back up, and then restore, every drive that includes operating system boot information.

You should not create incremental backups of shared data drives if Backup Exec System Recovery is installed on both operating systems and they are both set to manage the shared drive.

You might encounter issues if you try to use the Backup Exec System Recovery LightsOut Restore feature on dual-boot systems. It is not supported.

The same is true of the Backup Exec System Recovery Restore Anyware™ feature.

Backing up entire drives

This chapter includes the following topics:

Defining a drive-based backup

A drive-based backup takes a snapshot of your entire hard drive, capturing every bit of information that is stored on it for later retrieval. All of your files, folders, desktop settings, programs, and your operating system are captured into a recovery point. You can then use that recovery point to restore individual files or folders or your entire computer.

For optimum protection, you should define a drive-based backup and run it on a regular basis.

By default, scheduled independent recovery points or recovery point set names are appended with 001.v2i, 002.v2i, and so forth. Recovery point set names are appended with _i001.iv2i, _i002.iv2i, and so forth. For example, if your base recovery point is called C_Drive001.v2i, the first incremental recovery point is called C_Drive001_i001.iv2i.

To define a drive-based backup

1. On the Home page, click **Run or Manage Backups**.
2. In the Run or Manage Backups window, click **Define New**.

   If you have not yet defined a backup, the Easy Setup dialog appears instead.

3. Click **Back up my computer**, and then click **Next**.

4. Select one or more drives to back up, and then click **Next**.

   Press and hold **Ctrl** to select multiple drives.

   If you do not see a drive that you expected to see, check **Show Hidden Drives**.

5. Do one of the following:

   - If you selected a drive that has already been included in a defined backup, click **Next**, and then skip to step 8.
   - Click **Add drives to an existing backup**, click the **Select the backup** drop-down list and select an existing backup, and then click **Next**.
   - Click **Define a new backup** to define a new backup, and then click **Next**.

6. Select the type of recovery point that you want the backup to create.

   Recovery point set (recommended)

   Schedule a base recovery point with additional recovery points that contain only incremental changes that were made to your computer since the previous recovery point.

   Incremental recovery points are created faster than the base recovery point. They also use less storage space than an independent recovery point.

   Note: You can only have one recovery point set defined for each drive. The Recovery Point Set option is not available if you have already assigned a selected drive to an existing backup and specified Recovery Point Set as the recovery point type. This option also is unavailable if you select an unmounted drive that cannot be part of a recovery point set.

   Independent recovery point

   Creates a complete, independent copy of the drives that you select. This backup type typically requires more storage space, especially if you run the backup multiple times.

7. Click **Next**.

8 On the Backup Destination page, select from the following options:

Folder field	Browse to the location in which you want to store the recovery points. If Backup Exec System Recovery detects that this location does not have enough available space, it alerts you. You should choose another location that has more space.
Network Credentials	If you want to save the recovery point on a network share, type the user name and password for network access. See "About network credentials" on page 72.
Customize recovery point file names	If you want to rename the recovery point, click **Rename**, and then type a new file name. Default file names include the name of the computer followed by the drive letter.
Add	Click this button to add up to two Offsite Copy destinations. Offsite Copy automatically copies your latest recovery points each time a backup completes to either a portable storage device, such as an external drive, or to a remote server either through a local area network connection or to a remote FTP server. See "About Offsite Copy" on page 79.

9 If you want to make copies of your recovery points to store at a remote location for added backup protection, do the following:

- Click **Add** and then check **Enable Offsite Copy**.
- Check the **Prompt me to start a copy when I attach an external Offsite Copy destination drive** option if you want recovery points automatically copied to external Offsite Copy destination drives whenever you plug one in to your computer.
- Click **Browse** to locate an Offsite Copy destination.
- Click **Add an additional Offsite Copy destination** if you want to add a second destination, and then specify the path (a local folder, network path, or FTP address) to that destination.
- Click **OK**.

See “About Offsite Copy” on page 79.

10 Click **Next**.

Note: You cannot use an encrypted folder as your backup destination. You can choose to encrypt your backup data to prevent another user from accessing it.

---

11 On the Options page, select from the following options:

Name	Type a name for your backup.
Compression	Select one of the following compression levels for the recovery point.: ■ None ■ Standard ■ Medium ■ High See “About setting a compression level for drive-based backups” on page 78. The results can vary depending on the types of files that are saved in the drive.
Verify recovery point after creation	Select this option to automatically test whether a recovery point or set of files is valid or corrupt.
Limit the number of recovery point sets saved for this backup	Select this option to limit the number of recovery point sets that can be saved for this backup. You can limit the number of recovery point sets to reduce the risk of filling up the hard drive with recovery points. Each new recovery point set replaces the oldest set on your backup destination drive.
Enable search engine support	Select this option to let a search engine, such as Google Desktop, index all of the file names that are contained in each recovery point. By indexing the file names, you can then use your search engine to locate files you want to restore. See “About using a search engine to search recovery points” on page 187.

Include system and temporary files	Check this option to include indexing support for operating system and temporary files when a recovery point is created on the client computer.
Description text box	Type a description for the recovery point. The description can be anything that helps you further identify the recovery point's contents.
Advanced	In the Advanced Options dialog box, select any of the following options, and then click OK. ■ Divide into smaller files to simplify archiving ■ Disable SmartSector Copying ■ Ignore bad sectors during copy ■ Use password ■ Use AES Encryption See “Setting advanced options for drive-based backups” on page 74.

12 Click **Next**.

13 If appropriate, in the drop-down lists, select the command file (.exe, .cmd, .bat) that you want to run during a particular stage in the recovery point creation process, and then specify the amount of time (in seconds) that you want the command to run before it is stopped.

If you added the command file to the CommandFiles folder, you may need to click **Back**, and then **Next** to see the files in each stage’s drop-down list.

See “Run command files during a backup ” on page 72.

14 Click **Next**.

15 Do one of the following:

- If you chose a recovery point set as your recovery point type in step 6, skip to the next step.
- If you chose an independent recovery point as your recovery point type, click the **Automatically create a recovery point** drop-down list, and then select one of the following options:

No Schedule	Runs the backup only when you run it yourself, manually.

Weekly	Runs the backup at the time and on the days of the week that you specify. When you select this option, the Select the days of the week to protect box appears.
Monthly	Runs the backup at the time and on the days of the week that you specify. When you select this option, the Select the days of the month to protect box appears.
Only run once	Runs the backup one time on the date and at the time you specify. When you select this option, the Create a single recovery point box appears.

16 Click **Schedule** if you want the backup to run automatically, according to a schedule.

If you only want to run the backup when you start it manually, uncheck **Schedule** and skip to the next step.

17 Enter a start time and select the days of the week when the backup should run.

18 Click the **Start a new recovery point set** drop-down list, and then select how frequently a new recovery point set should be started.

For example, if you select Monthly, a new base recover point is created the first time the backup runs during each new month.

19 For advanced scheduling options, such as setting up event triggers that start the backup in response to specific events, click **Advanced** and configure any of the following options:

Schedule (Backup Time)	Do one or more of the following: ■ Click **Schedule**, and then select the days and a start time for when the backup should run. ■ Check **Run more than once per day** if you frequently modify data that you want to protect. Also, specify the maximum time that should occur between backups and the number of times per day that the backup should run. ■ Click the **Automatically optimize** drop-down list, and then select how often optimization should occur to help manage the disk space that is used by your backup destination. ■ Click the **Start a new recovery point set** drop-down list and select how frequently a new recovery point set should be started. Click **Custom** to customize the option you select.
Event Triggers (General)	Select the type of events that should automatically start the backup. See “Enabling event-triggered backups ” on page 93.

20 Click **OK**, and then click **Next**.

21 If you want to run the new backup immediately, click **Run backup now**.

This option is not available if you configured an independent recovery point with the option to run it only once.

22 Click **Finish**.

Running a One Time Backup

The One Time Backup feature lets you quickly define and run a backup that creates an independent recovery point. You use the One Time Backup Wizard to define the backup. The backup runs when you complete the Wizard. The backup definition is not saved for future use. You can use the independent recovery point later.

This feature is useful when you need to back up your computer or a particular drive quickly before a significant event. For example, you can run a one-time backup before you install new software. Or, you can run it when you learn about a new computer security threat.

To run a one time backup

1 On the Tasks page, click **One Time Backup**.

2 Click **Next**.

3. Select one or more drives to back up and click **Next**.

Note: Press and hold **Ctrl** to select multiple drives.

4. Click **Next**.
5. In the Backup Destination dialog box, select from the following options:

Folder field

Browse to the location in which you want to store the recovery points.

If Backup Exec System Recovery detects that this location does not have enough available space, it alerts you. You should choose another location that has more space.

Rename button

If you want to rename the recovery point, click **Rename**, and then type a new file name.

Default file names include the name of the computer followed by the drive letter.

Network Credentials

If you want to save the recovery point on a network share, type the user name and password for network access.

See “About network credentials” on page 72.

6. Click **Next**.
7. On the Options page, select from the following options:

Compression

Select one of the following compression levels for the recovery point:

- None
- Standard
- Medium
- High

The results can vary depending on the types of files that are saved in the drive.

Verify recovery point after creation

Select this option to automatically test whether a recovery point or set of files is valid or corrupt.

Description text box	Type a description for the recovery point. The description can be anything that helps you further identify the recovery point's contents.
Advanced	In the Advanced Options dialog box, select any of the following options, and then click OK. ■ Use password ■ Use Encryption ■ Divide into smaller files to simplify archiving ■ Ignore bad sectors during copy ■ Disable SmartSector Copying See “Setting advanced options for drive-based backups” on page 74.

8 Click **Next**.

9 If appropriate, in the drop-down lists, select the command file (.exe, .cmd, .bat) that you want to run during a particular stage in the recovery point creation process, and then specify the amount of time (in seconds) that you want the command to run before it is stopped.

If you added the command file to the CommandFiles folder, you may need to click **Back**, and then **Next** to see the files in each stage’s drop-down list.

See “Run command files during a backup ” on page 72.

10 Click **Next**.

11 Click **Finish** to run the backup.

Files excluded from drive-based backups

The following files are intentionally excluded from drive-based backups:

- hiberfil.sys
- pagefile.sys

These files contain temporary data that can take up a large amount of disk space. They are not needed, and there is no negative impact to your computer system after a complete system recovery.

These files do appear in recovery points, but they are placeholders. They contain no data.

About network credentials

If you connect to a computer on a network, you must provide the user name and password for network access, even if you previously authenticated to the network. The Backup Exec System Recovery service runs on the local system account.

When you enter network credentials, the following rules apply:

- If the computer you want to connect to is on a domain, provide the domain name, user name, and password. For example:
  domain\username
- If you connect to a computer in a workgroup, provide the remote computer name and user name. For example:
  remote_computer_name\username
- If you have mapped a drive, you might be required to supply the user name and password again because the service runs in a different context and cannot recognize the mapped drive.

By going to the Tasks menu and selecting Options, you can set a default location, including network credentials. Then when you create future backup jobs, the dialog will default to the location you specified. Another option would be to create a specific "backup" user account. Then configure the Backup Exec System Recovery service to use this account.

Run command files during a backup

You can use command files (.exe, .cmd, .bat) during a backup. You can use command files to integrate Backup Exec System Recovery with other backup routines that you might be running on the computer. You can also use command files to integrate with other applications that use a drive on the computer.

Note: You cannot run command files that include a graphical user interface, such as notepad.exe. Running such command files will cause the backup job to fail.

You can run a command file during any of the following stages during the creation of a recovery point:

- Before data capture
- After data capture
- After recovery point creation

You can also specify the amount of time that a command file should be allowed to run.

You can specify the location of command files if you want them to be located in a place other than the default location. You can also specify a location on a per-job basis, as well as specify a location that can be shared among several computers. If you specify a network location, you must provide network credentials.

See “About network credentials” on page 72.

The most common use for running command files is to stop and restart non-VSS-aware databases that you want to back up.

To use a Visual Basic script file (.VBS) during a backup, you can create a batch file (.BAT) to run the script. For example, you can create a batch file called STOP.BAT that contains the following syntax:

```
Cscript script_filename.vbs
```

Make sure that `Cscript` precedes the file name of the Visual Basic script.

Warning: The command files cannot depend on any user interaction or have a visible user interface. You should test all command files independently of Backup Exec System Recovery before you use them during a backup.

When the backup begins, the command file is run during the specified stage. If an error occurs while a command file is running or the command file does not finish in the time you specified (regardless of the stage), the backup is stopped, the command file is terminated (if necessary), and the error information is logged and displayed.

Table 6-1 describes the stages of recovery point creation.

Table 6-1 Recovery point creation stages

Stage	Description
Before data capture	This stage occurs after a backup has started and before a recovery point is created. You can run a command during this stage to prepare for the recovery point creation process. For example, you can close any open applications that are using the drive. **Note:** If you use this option, be sure the command file has an error recovery mechanism built into it. If the computer has one or more services that must be stopped at this stage (such as stopping a non-VSS aware database or a resource intensive application), and the command file does not contain any form of error recovery, one or more of the stopped services may not be restarted. An error in the command file can cause the recovery point creation process to stop immediately. No other command files will run. See "How you use Backup Exec System Recovery" on page 36.
After data capture	This stage occurs after a snapshot is created. Running a command during this stage is typically a safe point for allowing services to resume normal activity on the drive while continuing the recovery point creation. Because the snapshot takes only a few seconds to create, the database is in the backup state momentarily. A minimal number of log files are created.
After recovery point creation	This stage occurs after the recovery point is created. You can run a command during this stage to act on the recovery point itself. For example, you can copy it to an offline location.

Setting advanced options for drive-based backups

When you define a drive-based backup, you can set the following advanced options:

Divide into smaller files to simplify archiving	You can split the recovery point into smaller files and specify the maximum size (in MB) for each file. For example, if you plan to copy a recovery point to ZIP disks from your backup destination, specify a file size of 100 MB or less, according to the size of each ZIP disk.
Disable SmartSector Copying	SmartSector technology speeds up the copying process by only copying the hard-disk sectors that contain data. However, in some cases, you might want to copy all sectors in their original layout, whether or not they contain data. This option lets you copy used and unused hard-disk sectors. This option increases processing time and usually results in a larger recovery point.
Ignore bad sectors during copy	This option lets you run a backup even if there are bad sectors on the hard disk. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard disk.
Use password	This option sets a password on the recovery point when it is created. Passwords can include standard characters, not extended characters or symbols. (Use characters with an ASCII value of 128 or lower.) A user must type this password before restoring a backup or viewing the contents of the recovery point.
Use AES encryption	You can encrypt your recovery point data to add another level of protection to your recovery points. You can choose from the following encryption levels: ■ Low (8+ character password) ■ Medium (16+ character password) ■ High (32+ character password).

Editing advanced backup options

After you define a backup, you can go back at any time and edit the advanced options you chose when you first defined the backup.

To edit advanced backup options

1. On the Home or Tasks page, click **Run or Manage Backups**.

   Select the backup you want to edit, and then click **Edit Settings**.

2. Click **Next** twice.
3. Click **Advanced**.

4 In the Advanced Options dialog box, make your changes, and then click **OK**.

5 Click **Next** three times, and then click **Finish**.

About recovery point encryption

You can enhance the security of your data by using the Advanced Encryption Standard (AES) to encrypt recovery points that you create or archive. You should use encryption if you store recovery points on a network and want to protect them from unauthorized access and use.

You can also encrypt recovery points that were created with earlier versions of Symantec LiveState Recovery or Backup Exec System Recovery. However, encrypting those files will make them readable with the current product only.

You can view the encryption strength of a recovery point at any time by viewing the properties of the file from the Recovery Point Browser.

Encryption strengths are available in 128-bit, 192-bit, or 256-bit. While higher bit strengths require longer passwords, the result is greater security for your data.

Table 6-2 explains the bit strength and required password length.

Table 6-2 Password length

Bit strength	Password length
128 (Standard)	8 characters or longer
192 (Medium)	16 characters or longer
256 (High)	32 characters or longer

You must provide the correct password before you can access or restore an encrypted recovery point.

Warning: Store the password in a secure place. Passwords are case-sensitive. When you access or restore a password encrypted recovery point, Backup Exec System Recovery prompts you for the case-sensitive password. If you do not type the correct password or you forget the password, you cannot open the recovery point.

Symantec Technical Support has no method for opening an encrypted recovery point.

Besides bit strength, the make-up of the password can improve the security of your data.

For better security, passwords should use the following general rules:

- Avoid using consecutive, repeating characters (for example, BBB or 88).
- Avoid using common words that you would find in a dictionary.
- Use at least one number.
- Use both uppercase and lowercase alpha characters.
- Use at least one special character such as ({}[],.<>;:’"?/|\`~!@#$%^&*()_-+=).
- Change the password after a set period of time.

Verifying a recovery point after creation

If you selected the Verify recovery point after creation option on the Options page of the Define Backup Wizard, the recovery point is checked to see that all of the files that make up the recovery point are available for you to open. Internal data structures in the recovery point are matched with the data that is available. Also, the recovery point can be uncompressed to create the expected amount of data (if you selected a compression level at the time of creation).

Note: The time required to create a recovery point is doubled when you use the Verify recover point after creation option.

To verify the integrity of a recovery point

1. On the Tools page, click **Run Recovery Point Browser**.
2. Select a recovery point, and then click **Open**.
3. In the tree panel of the Recovery Point Browser, select the recovery point.

   For example: C_Drive001.v2i.
4. On the File menu, click **Verify Recovery Point**.

   If the Verify Recovery Point option is unavailable, you must first dismount the recovery point. Right-click the recovery point and click **Dismount Recovery Point**.
5. When the validation is complete, click **OK**.

   If you prefer, you can have recovery points automatically verified for integrity at the time they are created.

   See “Setting advanced options for drive-based backups” on page 74.

Viewing the progress of a backup

You can view the progress of a backup while it runs to determine how much time remains until the backup completes.

To view the progress of a backup

- While a backup is running, on the View menu, click **Progress and Performance**.

About setting a compression level for drive-based backups

During the creation of a recovery point, compression results may vary, depending on the types of files saved to the drive you are backing up.

Table 6-3 describes the available compression levels.

Table 6-3 Compression levels

Compression level	Description
None	Use this option if storage space is not an issue. However, if the backup is being saved to a busy network drive, high compression may be faster than no compression because there is less data to write across the network.
Standard (recommended)	This option uses low compression for a 40 percent average data compression ratio on recovery points. This setting is the default.
Medium	This option uses medium compression for a 45 precent average data compression ratio on recovery points.
High	This option uses high compression for a 50 percent average data compression ratio on recovery points. This setting is usually the slowest method. When a high compression recovery point is created, CPU usage might be higher than normal. Other processes on the computer might also be slower. To compensate, you can adjust the operation speed of Backup Exec System Recovery. This might improve the performance of other resource-intensive applications that you are running at the same time.

About Offsite Copy

Backing up your data to a secondary hard disk is a critical first step to protect your information assets. But to make certain your data is safe, use Offsite Copy to copy your latest recovery points to either a portable storage device, remote server in your network, or to a remote FTP server.

Regardless of the method you use, storing copies of your recovery points at a remote location provides a crucial level of redundancy in the event that your office becomes innaccesible. Offsite Copy can double your data protection by ensuring that you have a remote copy.

How Offsite Copy works

You enable and configure Offsite Copy when you define a new drive-based backup job. Or you can edit an existing backup job to enable Offsite Copy.

When you enable Offsite Copy, you specify up to two Offsite Copy destinations. After the backup job finishes creating recovery points, Offsite Copy verifies that at least one of the Offsite Copy destinations are available. Offsite Copy then begins copying the new recovery points to the Offsite Copy destination.

Newest recovery points are copied first followed by the next oldest recovery points. If you have set up two Offsite Copy destinations, Offsite Copy copies recovery points to the destination that was added first. If an Offsite Copy destination is unavailable, Offsite Copy tries to copy recovery points to the second destination, if it is available. If neither destination is available, then Offsite Copy copies the recovery points the next time an Offsite Copy destination becomes available.

For example, suppose you have configured a backup job to run at 6 p.m. and configured an external drive as an Offsite Copy destination. However, when you leave the office at 5:30 p.m., you take the drive with you for safe keeping. When the backup job completes at 6:20 p.m., Backup Exec System Recovery detects that the Offsite Copy destination drive is not available and the copy process aborted. The following morning, you plug the drive back in to the computer. Backup Exec System Recovery detects the presence of the Offsite Copy destination drive and automatically begins copying your recovery points.

Offsite Copy is designed to use very little system resources so that the copying process is done in the background. This feature lets you continue to work at your computer with little or no impact on system resources.

If an Offsite Copy destination runs out of disk space, Offsite Copy identifies the oldest recovery points and removes them to make room for the most current recovery points. Offsite Copy then copies the current recovery points to the Offsite Copy destination.

See “To define a drive-based backup” on page 63.

See “Editing backup settings” on page 93.

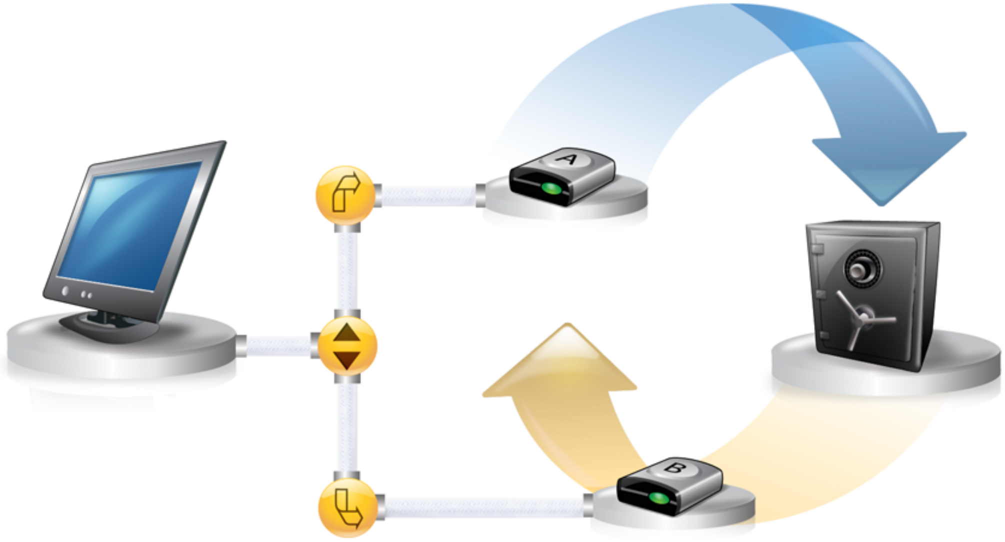
Using external drives as your Offsite Copy destination

Use an external drive as your Offsite Copy destination. This method lets you take a copy of your data with you when you leave the office. By using two external hard disks, you can be certain that you have a recent copy of your data both on and off site.

For example, suppose on a Monday morning you define a new backup job of your system drive. You choose a recovery point set as your backup job type. You set up an external drive (A) as the first Offsite Copy destination, and another external drive (B) as the second Offsite Copy destination. You schedule the backup job to run every midnight except on the weekends. You also enable recovery point encryption to protect the data that you take with you from unauthorized access.

See “About recovery point encryption ” on page 76.

Before you leave the office on Monday evening, you plug in drive A and take drive B home with you.



On Tuesday morning, you find that Monday's base recovery point has been successfully copied to drive A. At the end of the day, you unplug drive A and take it home for safe keeping.

On Wednesday morning, you bring drive B to the office. You plug in drive B and Backup Exec System Recovery detects that drive B is an Offsite Copy destination. Backup Exec System Recovery then automatically begins copying Monday night's base recovery point and Tuesday night's incremental recovery point. At the end of the day Wednesday, you take drive B home and place it in a safe place with drive A.

You now have multiple copies of recovery points stored at two separate, physical locations: your original recovery points stored on your backup destinations at the office, and copies of those same recovery points stored on your Offsite Copy destination drives. Your Offsite Copy destination drives are stored in a safe place at your home.

The next morning, Thursday, you take drive A to the office and plug it in. Tuesday and Wednesday night's recovery points are then automatically copied to drive A.

Note: Consider using the external drive naming feature that lets you provide a unique name, or alias, to each drive. Then place matching physical labels on each external drive to help you manage the task of swapping the drives.

See "Using aliases for external drives" on page 45.

Each time you plug in either drive A or B, the latest recovery points are added to the drive. This method gives you multiple points in time for recovering your computer in the event that the original backup destination drives fail or become unrecoverable.

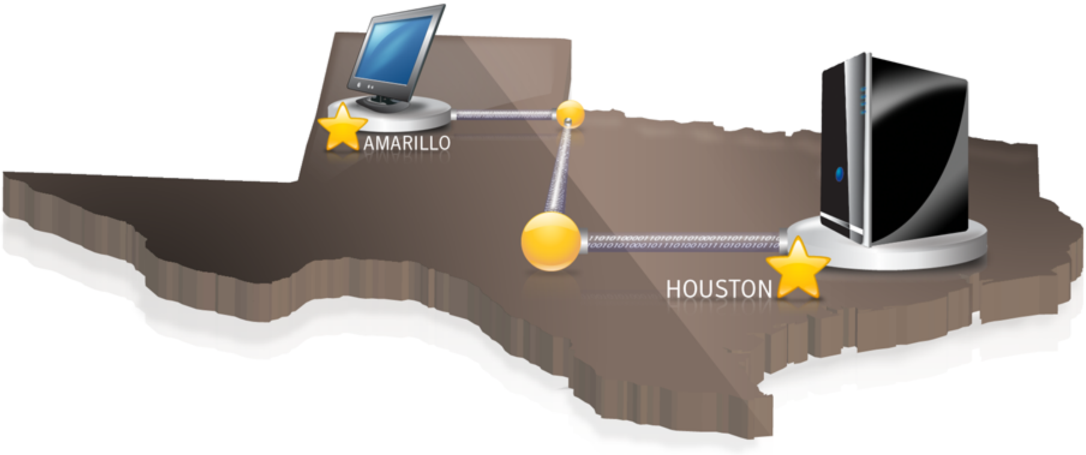
Using external drives as your Offsite Copy destination ensures that you have a copy of your backup data stored at two separate, physical locations.

Using a network server as your Offsite Copy destination

You can also specify a local area network server as an Offsite Copy destination. You must be able to access the server that you plan to use. You must either map a local drive to the server, or provide a valid UNC path.

For example, suppose that you set up a local external drive as your first Offsite Copy destination. Then you identify a server that is located at a second physical location from your own office. You add the remote server as a second Offsite Copy destination. As backups occur, recovery points are copied first to the external hard drive, and then to the remote server.

If the remote server becomes unavailable for a period of time, Offsite Copy copies all recovery points created since the last connection. If there is no room to hold all of the recovery points available, Offsite Copy removes the oldest recovery points from the FTP server, making room for the newest recovery points.



Using an FTP server as your Offsite Copy destination

Using an FTP server as your Offsite Copy destination is similar to using a server. You must provide a valid FTP path to the FTP server.

You must also provide the correct FTP connection information to Backup Exec System Recovery in order for this method to work correctly. When Offsite Copy is configured correctly, it copies recovery points to the directory that you specified on the FTP server. If the server becomes unavailable for a period of time, Offsite Copy copies all recovery points created since the last connection. If there is no room to hold all of the recovery points available, Offsite Copy removes the oldest recovery points from the FTP server, making room for the newest recovery points.

See “Configuring FTP settings for use with Offsite Copy” on page 46.

FTP

Chapter 7

Backing up files and folders

This chapter includes the following topics:

- Defining a file and folder backup
- Folders excluded by default from file and folder backups

Defining a file and folder backup

When you define and run a file and folder backup, copies are made of each of the files and folders that you have chosen to back up. They are converted into a compressed format, and then stored in a sub-folder at the location you specify, which by default is the same backup destination that is used for storing recovery points.

To define a file and folder backup

1. On the Home page, click **Run or Manage Backups**.
2. In the Run or Manage Backups window, click **Define New**.

   If you have not yet defined a backup, the Easy Setup dialog appears.
3. Select **Back up selected files and folders**, and then click **Next**.

4 Select the files and folders you want to include in your backup, and then click **Next**.

Selecting file types lets Backup Exec System Recovery find and include files that match the files you want backed up. If a file type is not included in the predefined list, click **Add File Type**. You can also manually select folders or individual files.

Note: On all versions of Windows, except for Windows Vista, the My Documents folder contains two subfolders by default: My Pictures and My Music. These folders contain only the shortcuts to folders at another location and not the actual files. This might lead you to think that by including My Documents and all subfolders in your backup, your picture and music files will get backed up.

If you intend to back up your pictures and music files, be sure to include the actual folders where your files are stored. On Windows Vista, these folders exist at the same level as Documents (formerly, My Documents).

---

5 In the Name box, type a name for your new backup.

6 In the Description (optional) box, type a description for the new backup.

7 Click **Browse** to locate a folder for storing your backup data or accept the default location.

Note: You cannot use an encrypted folder as your backup destination. If you want to encrypt your backup data to prevent another user from accessing it, refer to the next step.

---

8 To modify advanced options, click **Advanced**. Do any of the following:

- Click **Use password**, and then type a password.
  Use standard characters, not extended characters or symbols. You must type this password before you restore a backup or view its contents.
- For an additional level of security, click **Use encryption** to encrypt your file data.
- In the Exclude group box, uncheck any of the folders you want to include in your backup.
  The folders listed are typically not used for storing personal files or folders. These folders are backed up when you define and run a drive-based backup of your system drive (typically C).

9 Click **OK**, and then click **Next**.

10 Click **Schedule** if you want the backup to run automatically, according to a schedule.

If you want to run the backup only when you start it manually, uncheck **Schedule**.

11 Enter a start time and select the days of the week when the backup should run.

12 For advanced scheduling options, such as setting up event triggers that start the backup in response to specific events, click **Advanced** and configure any of the following options:

Schedule (Backup Time)	Do one or more of the following: ■ Click **Schedule**, and then select the days and a start time for when the backup should run. ■ Check **Run more than once per day** if you frequently modify data that you want to protect. Also, specify the maximum time that should occur between backups and the number of times per day that the backup should run.
Event Triggers (General)	Select the type of events that should automatically start the backup. See “Enabling event-triggered backups ” on page 93.

13 Click **Next** to review the backup options you have selected.

14 To review the total number and size of files to be included in the backup, click **Preview**.

Note: Depending on the amount of data you have identified for file and folder backup, the preview process could take several minutes.

15 If you want to run the new backup immediately, click **Run backup now**, and then click **Finish**.

Folders excluded by default from file and folder backups

The following folders and their contents are excluded automatically from file and folder backups:

- Windows folder
- Program Files folder
- Temporary folder
- Temporary Internet Files folder

These folders are typically not used for storing personal files or folders. However, they are backed up when you define and run a drive-based backup of your system drive (typically C).

See “Defining a file and folder backup ” on page 85.

You can include these folders when you define a file and folder backup.

Chapter 8

Running and managing backup jobs

This chapter includes the following topics:

Running an existing backup job immediately

This is particularly useful when you are about to install a new product and want to make sure you have a current recovery point in the event that something goes wrong with the installation. It can also help you to ensure that you have a backup of your work after you have modified a large number of files and you don't want to wait for a regularly scheduled backup.

You can run an existing backup at any time.

Note: If necessary, you can run a quick backup of a particular drive without using a defined backup.

See "Running a One Time Backup" on page 69..

Backup Exec System Recovery can be configured to run a backup automatically when an event occurs on your computer, such as installing a new software program.

See "Enabling event-triggered backups " on page 93.

When you run a backup, you should close any partitioning software that is running, such as Norton PartitionMagic. Also, you should not run any disk defragmenting software during a backup.

You can also schedule backups to run automatically, according to a schedule.

See "Editing a backup schedule " on page 95.

To run an existing backup immediately from the system tray

1. On the Windows desktop, right-click the Backup Exec System Recovery system tray icon.
2. Click **Run Backup Now**.
3. Click a backup job to start the backup.

   If the menus displays No Jobs, you must start Backup Exec System Recovery and define a backup.

To run an existing backup immediately from within Backup Exec System Recovery

1. On the Home page, click **Run or Manage Backups**.
2. Select a backup from the list, and then click **Run Now**.

Run a backup with options

If you want to quickly run an existing drive-based backup, but you want the backup to create an alternate type of recovery point, use the Run Backup With Options feature.

This is a unique option in that if you run an existing backup job, the recovery point created is dictated by the type of recovery point that was created the last time the backup job was run. Use this option to create an alternate recovery point type.

Note: Using this option does not change the settings of the defined backup. To do that, you must open the backup and modify its settings manually.

See "Editing a backup schedule " on page 95.

See "Editing backup settings" on page 93.

To run a backup with options

1. On the Home page, click **Run or Manage Backups**.
2. In the Run or Manage Backups window, select the drive-based backup job that you want to run.
3. Click **Tasks** > **Run Backup With Options**.
4. Select one of the following options:

Note: Depending on the current state of the backup, one or more options might be disabled. For example, if you have not yet run the backup, you cannot select the first option, Incremental recovery point of recent changes, because the base recovery point has not yet been created.

Incremental recovery point of recent changes	Select this option if the backup already has a base recovery point created and you want to simply capture changes made to the drive since the last backup.
New recovery point set	Select this option if you want to start a completely new recovery point set. When you select this option, a base recovery point is created.
Independent recovery point	Select this option to create an independent recovery point, which is a complete snap shot of your entire drive. To specify an alternate backup location, click **Browse**.

5. Click **OK** to run the backup job and create the recovery point type you selected.

Adjusting the speed of a backup

Depending on the speed of your computer, how much RAM you have installed, and the number of programs you are running during a backup, your computer could become sluggish.

You can manually adjust the effect of a backup on the performance of your computer to match your needs at the moment. This feature is useful if you are working on your computer and don't want the backup process to slow you down.

To adjust the performance of a backup

1. While a backup is running, on the View menu, click **Progress and Performance**.
2. Do one of the following:
   - If you want to increase the speed of your computer by reducing the speed of the backup, drag the slider toward **Slow**.
   - If you want the backup to complete as quickly as possible and you are not doing extensive work on your computer, drag the slider toward **Fast**.
3. When you are finished, click **Hide** to dismiss the Progress and Performance dialog box.

Stopping a backup or recovery task

You can stop a backup or a recovery task that has already started.

To stop a backup or recovery task

◆ Do one of the following:

- On the View menu, click **Progress and Performance**, and then click **Cancel Operation**.
- On the Windows system tray, right-click the Backup Exec System Recovery tray icon, and then click **Cancel Current Operation**.

Verifying that a backup is successful

After a backup completes, you can validate the success of the backup from the Status page to ensure you have a way to recover lost or damaged data.

The Status page contains a scrolling calendar that is aligned with each drive on your computer. The calendar lets you quickly identify when a backup ran, and what type of backup it was. It also identifies upcoming, scheduled backups.

See “Monitoring backup protection from the Status page ” on page 117.

Note: When you define a drive-based backup, you should select the option to verify the recovery point after it is created.

Depending on the amount of data being backed up, this can significantly increase the time it takes to complete the backup. However, it can ensure that you have a valid recovery point when the backup finishes.

See "Verifying a recovery point after creation " on page 77.

To verify the success of a backup

1. On the Status page, review the Backups calendar, and verify that the backup appears on the date that you ran it.
2. Move your mouse over a backup icon to review the status of the backup.

Editing backup settings

You can modify the settings of an existing backup. The Edit Settings feature gives you access to several of the key pages of the Define Backup Wizard. You can modify every setting except the option to change the recovery point type.

To edit backup settings

1. On the Home or Tasks pages, click **Run or Manage Backups**.
2. Select a backup to edit.
3. Click **Edit Settings**.
4. Make changes to the backup.

   See "Defining a drive-based backup " on page 63.

   See "Defining a file and folder backup " on page 85.

Enabling event-triggered backups

Backup Exec System Recovery can detect certain events and run a backup when they occur.

For example, to protect your computer when you install new software, Backup Exec System Recovery can run a backup when it detects that new software is being installed. If a problem occurs that harms your computer, you can use this recovery point to restore your computer to its previous state.

You can configure Backup Exec System Recovery to automatically run a backup when the following events occur:

- Any application is installed

- A specified application is started
- Any user logs on to Windows
- Any user logs off of Windows
- The data added to a drive exceeds a specified number of megabytes
  This option is unavailable for file and folder backups.
- The Maxtor OneTouch™ external hard drive button is pushed

Note: This feature only appears if you have a Maxtor OneTouch drive installed, and you are running a Windows XP 32-bit platform.

To enable event-triggered backups

1. On the Home or Tasks page, click **Run or Manage Backups**.
2. Select the backup you want to edit, and then click **Change Schedule**.
3. Click **General** under Event Triggers.
4. Select the events you want detected, and then click **OK**.

Enabling Symantec ThreatCon Response

ThreatCon is Symantec's early warning security threat system. When Symantec identifies various threats, the ThreatCon team adjusts the threat level to give people and systems adequate warning in order to protect data and systems against attack.

When you enable the Symantec ThreatCon Response trigger for a particular backup job, Backup Exec System Recovery detects changes in the threat level, assuming your computer is online at the time. When Backup Exec System Recovery detects that the ThreatCon level you chose is either reached or exceeded, the backup job in which you enabled Symantec ThreatCon Response is started automatically. You then have a recovery point to use to recover your data should your computer become affected by the latest threat.

Note: If your computer is not online, then it is not susceptible to online threats. But if you connect your computer to the Internet at any time, it becomes vulnerable. You do not have to enable or disable Symantec ThreatCon Response when you go on or off line. It simply works if you are online, but does nothing if you are off line.

Table 8-1 Backup Exec System Recovery ThreatCon levels

Threat Level	Description
Level 1	No discernable security threats exist.
Level 2	Security threats could occur, although no specific threats have been known to occur.
Level 3	An isolated security threat is in progress.
Level 4	Extreme global security threats are in progress.

For more information about Symantec ThreatCon, visit http://www.symantec.com.

To configure Symantec ThreatCon Response

1 On the Home or Tasks page, click **Run or Manage Backups**.

2 Select the backup you want to edit, and then click **Change Schedule**.

3 Click **ThreatCon Response** under Event Triggers.

4 From the drop-down list, select the threat level that when met or exceeded should start your backup job, and then click **OK**.

Note: Level 1 of Symantec ThreatCon indicates that there are no threats. Because level 1 suggests no threats, it is not an option in the drop-down list. However, you can disable Symantec ThreatCon Reponse by choosing the first option.

See "To disable Symantec ThreatCon Response" on page 95.

To disable Symantec ThreatCon Response

1 On the Home or Tasks page, click **Run or Manage Backups**.

2 Select the backup you want to edit, and then click **Change Schedule**.

3 Click **ThreatCon Response** under Event Triggers.

4 From the drop-down list, select **Do Not Monitor - Disable**, and then click **OK**.

Editing a backup schedule

You can edit any of the schedule properties for a defined backup to adjust the date and time.

To edit a backup schedule

1. On the Home page, click **Run or Manage Backups**.
2. Select a backup to edit.
3. Click **Change Schedule**.
4. Make changes to the schedule, and then click **OK**.

Turning off a backup job

You can turn off a backup and re-enable it later. When you turn off a backup, it will not run according to its defined schedule, if it has one. When a backup is turned off, triggered events will not run it, nor can you run it manually.

You can also delete a defined backup (not recovery points).

See “Deleting backup jobs ” on page 96.

To turn off a backup job

1. On the Home page, click **Run or Manage Backups**.
2. Select the backup that you want to turn off.
3. Click **Tasks > Disable Backup**.

   Repeat this procedure to re-enable the backup. The Disable Backup menu item changes to Enable Backup when you disable the selected backup.

Deleting backup jobs

You can delete backup jobs when they are no longer needed.

Deleting a backup job does not delete the recovery points or file and folder backup data from the storage location. Only the backup job is deleted.

If you want to delete backup data (recovery points and file and folder backup data), refer to the following topics:

See “Managing recovery points” on page 135.

To delete backup jobs

1. On the Home page, click **Run or Manage Backups**.
2. Select one or more backups, and then click **Remove**.
3. Click **Yes**.

Adding users who can back up your computer

You can use the Security Configuration Tool to control which users on your computer can access and configure key features of Backup Exec System Recovery.

For example, all users with Limited Windows accounts can run existing backup jobs, but they cannot create new jobs or modify existing jobs. However, using the Security Configuration Tool, you can grant administrative privileges to a Limited user account. When you do, that user has full access to Backup Exec System Recovery and can create, modify, delete, and run backup jobs.

Note: By default, all users can run existing backup jobs. But only users with administrative accounts can create, edit, or delete backup jobs.

To add users who can back up a computer

1 On the Windows taskbar, click **Start > Programs > Symantec > Backup Exec System Recovery > Security Configuration Tool**.

On Windows Vista, click **Start > All Programs > Symantec > Security Configuration Tool**.

2 Click **Add**.

3 In the Enter the object names to select box, type the names of the users or groups you want to add.

4 Click **OK**.

5 To delete users or groups, select a user or group, and then click **Remove**.

6 Click **OK** to apply your changes and close the Security Configuration Tool.

To configure access rights for users or groups

1 On the Windows taskbar, click **Start > Programs > Symantec > Backup Exec System Recovery > Security Configuration Tool**

On Windows Vista, click **Start > All Programs > Symantec > Security Configuration Tool**.

2 Select a user or group from the Group or user names box.

3 Choose from the following options:

Permissions	Allow	Deny
Full Control	Select to give the user or group full access to all of the features of Backup Exec System Recovery. Full control gives users the right to create, edit, and delete backup jobs, including existing jobs.	Select to deny the user or group administrative access to the features of Backup Exec System Recovery. They can run existing backup jobs, but they cannot create, edit, or delete them.
Status Only	Select to deny the user or group administrative access to the features of Backup Exec System Recovery. They can run existing backup jobs, but they cannot create, edit, or delete them.	When you deny Status Only, the user or group cannot access any of the features of Backup Exec System Recovery.

4 Click **OK** to apply your changes and close the Security Configuration Tool.

Chapter 9

Backing up remote computers from your computer

This chapter includes the following topics:

About backing up other computers from your computer

Backup Exec System Recovery lets you connect to, and back up a second computer on your home or office network. You can manage as many computers as needed, but you can only manage one computer at a time.

Note: You must purchase a separate license for each computer you want to manage. You can deploy the agent without a license for a 30-day evaluation. After that time, you must purchase and install the license to continue managing the remote computer. You can purchase additional licenses at the Symantec Global Store. Visit:

http://shop.symantecstore.com

First, you add a computer's name or IP address to the Computer List. Then, you deploy the Backup Exec System Recovery Agent to the remote computer. Once the agent is installed, the computer automatically restarts. After the computer restarts, you can then connect to the computer. When you do, the Backup Exec System Recovery product interface changes to reflect the status of the remote computer. At any time, you can switch back to manage your own, local computer.

Adding computers to the Computer List

Before you can back up drives on a remote computer, you must first add the computer to the Computer List. You can then quickly switch between your local computer and any other computer on the list.

To add computers to the Computer List

1. On the Backup Exec System Recovery menu bar, click **Computers** > **Add**.
2. Do one of the following:
   - Type the name of the computer
   - Type the IP address of the computer
     If you are in a workgroup environment instead of a domain you must manually specify the computer name for the computer you want to manage by browsing to it by using the Browse button.
3. If you don't know the name of the computer, or its IP address, click **Browse** and search for the computer you want to add, and then click **OK**.
4. Click **OK** to add the computer to the Computer List.

To add a local computer

1. On the Backup Exec System Recovery menu bar, click **Computers** > **Add Local Computer**.
2. Click **OK**.

To remove a computer from the Computer List

1. On the Backup Exec System Recovery menu bar, click **Computers** > **Edit List**.
2. Select the remote computer that you want to remove, click the minus sign (-), and then click **OK**.

Note: Removing a computer from the Computer List does not uninstall the agent from the computer. You must run your operating system's uninstall program.

Deploying the agent

You can deploy the Symantec Backup Exec System Recovery Agent to the computers that are on the Computer List by using the Agent Deployment feature. After you install the agent, you can create backup jobs directly from Backup Exec System Recovery.

Note: Because of increased security with Windows Vista, you cannot deploy the Symantec Backup Exec System Recovery Agent to Windows Vista without making security configuration changes. The same issue occurs when you attempt to deploy the agent from Windows Vista to another computer. You can manually install the agent on the target computer using the product CD.

Note: If you deselected the Agent Deployment option during installation, this feature is not available. You can run the installation again, and select the Modify option to add this feature back in.

You can install the agent to a computer that has less than 256 MB of RAM. However, Symantec Recovery Disk requires at least 512 MB of RAM for restoring the computer. Your computer must meet the minimum memory requirement to run the Recover My Computer wizard or the Recovery Point Browser from the recovery environment.

Note: If you are installing a multilingual version of the product, you must have a minimum of 768 MB of RAM to run the Symantec Recovery Disk.

If your computers are set up in a workgroup environment, you should prepare your local computer before you deploy an agent.

To prepare a computer in a workgroup environment to deploy the agent

1. On the Windows taskbar, right-click **Start**, and then click **Explore** .
2. On the Tools menu, click **Folder Options > View**.
3. On the View tab, scroll to the end of the list and verify that the Use simple file sharing check box is unchecked, and then click **OK**.
4. On the Windows taskbar, click **Start** > **Settings** > **Control Panel** > **Windows Firewall**.
5. On the Exceptions tab, check **File and Printer Sharing**, and then click **OK**.

Note: You should close any open applications before you continue with the agent installation. If the Reboot check box is selected, the computer will automatically restart at the end of the installation wizard.

To deploy the Backup Exec System Recovery Agent

1. On the Backup Exec System Recovery menu bar, click **Computers** > select a computer from the menu.

   You must have administrator rights on the computer to which you are installing the agent.
2. Click **Deploy Agent**.
3. In the Deploy Symantec Backup Exec System Recovery Agent dialog box, specify the administrator user name (or a user name that has administrator rights) and the password.

   In a workgroup environment, you must specify the remote computer name. You cannot use an IP address, even if you have successfully connected to the computer by using an IP address.

   For example, type *RemoteComputerName**UserName*
4. If you want to restart the computer when the agent installation is finished, click **Reboot when finished**.

   Note: The computer cannot be backed up until the computer is restarted. However, be sure to warn the user of the impending reboot so that they can save their work.

   ---
5. Click **OK**.

To manually install the agent

1. Insert the Symantec Backup Exec System Recovery product CD into the media drive of the computer.

   The installation program should start automatically.

2. If the installation program does not start, on the Windows taskbar, click **Start > Run**, type the following command, then click **OK**.

   ```
   <drive>:\autorun.exe
   ```

   where <drive> is the drive letter of your media drive.

   For Windows Vista, if the Run option is not visible, do the following:

   - Right-click the Start button, and click **Properties**.
   - On the Start Menu tab, click **Customize**.
   - Scroll down and check **Run command**.
   - Click **OK**.

3. In the CD browser panel, click **Install Backup Exec System Recovery**.
4. In the Welcome panel, click **Next**.
5. Read the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.
6. If you want to change the default location for the program files, click **Change**, locate the folder in which you want to install the agent, and then click **OK**.
7. Click **Next**.
8. Click **Custom**, and then click **Next**.
9. Click Backup Exec System RecoveryService, and then click **This feature will be installed on local hard drive**.

   This feature is the agent.

10. Set all other features to **This feature will not be installed**.
11. Click **Next**, and then click **Install**.

Granting rights to domain users on Windows 2003 SP1 servers

To remotely manage a Windows 2003 SP1 server that is in a domain with a user in the domain, the server administrator must grant rights to all of the domain users who will be using Symantec Backup Exec System Recovery to remotely manage the server.

To grant rights to all domain users on Windows 2003 SP1 servers

1. Run the dcomcnfg.exe tool.
2. Navigate to **Component Services** > **Computers** > **My Computer**.
3. Right-click **My Computer**, and then select **Properties**.
4. On the the COM Security tab, under Launch and Activation Permissions, click **Edit Limits**.
5. Add the domain users to the Group or user names list, and then allocate the appropriate permissions.
6. Click **OK**.
7. Close Component Services, and then restart the Symantec Backup Exec System Recovery service.

Using the Symantec Backup Exec System Recovery Agent

The Symantec Backup Exec System Recovery Agent is the unseen “engine” that does the actual backing up and restoring of data on a remote computer. Because the Symantec Backup Exec System Recovery Agent functions as a service, it does not have a graphical interface.

See “Managing the agent through Windows Services” on page 105.

See “Controlling access to Backup Exec System Recovery ” on page 110.

The Symantec Backup Exec System Recovery Agent does, however, have a tray icon available from the Windows system tray to provide feedback of current conditions and to perform common tasks. For example, you can view backup jobs created for the computer, reconnect the Symantec Backup Exec System Recovery Agent, or cancel a task that is currently running.

You can install the agent manually by visiting each computer you want to protect and install the agent from the product CD. A more efficient method, however, is to use the Symantec Backup Exec System Recovery Deploy Agent feature to remotely install the agent on a computer in the domain whose data you want to protect.

To use the Symantec Backup Exec System Recovery Agent

◆ On the Windows system tray, do one of the following:

- Right-click the Symantec Backup Exec System Recovery tray icon, and then click **Reconnect** to restart the service automatically.
  You cannot run a backup until the service is running.

- If Backup Exec System Recovery is installed on the computer, double-click the Backup Exec System Recovery tray icon to start the program.

  If only the agent is installed, double-clicking the tray icon only displays an About dialog box.
- If the computer has Backup Exec System Recovery installed, right-click the Symantec Backup Exec System Recovery tray icon to display a menu of common Symantec Backup Exec System Recovery Agent tasks.

Managing the agent through Windows Services

The Symantec Backup Exec System Recovery Agent is a Windows service that runs in the background.

It provides the following:

- locally running scheduled backup jobs, even when there are no users, or an unprivileged user, logged on to the computer
- Allows administrators to remotely back up computers throughout an enterprise from Symantec Backup Exec System Recovery running on another computer.

See "Using the Symantec Backup Exec System Recovery Agent " on page 104.

To use the features of Symantec Backup Exec System Recovery, the Symantec Backup Exec System Recovery Agent must be started and properly configured. You can use the Windows Services tool to manage and troubleshoot the agent.

Note: To manage the Symantec Backup Exec System Recovery Agent, you must be logged on as a local administrator.

You can manage the Symantec Backup Exec System Recovery Agent in the following ways:

- Start, stop, or disable the Symantec Backup Exec System Recovery Agent on local and remote computers.

  See "Starting or stopping the agent service" on page 107.
- Configure the user name and password that is used by the Symantec Backup Exec System Recovery Agent.

  See "Controlling access to Backup Exec System Recovery " on page 110.
- Set up recovery actions to take place if the Symantec Backup Exec System Recovery Agent fails to start.

  For example, you can restart the Symantec Backup Exec System Recovery Agent automatically or restart the computer.

  See "Setting up recovery actions when the agent does not start" on page 108.

Best practices for using services

Table 9-1 describes some best practices for using services.

Table 9-1 Best practices for using services

Best practice	Description
Check the Events tab first before using Services.	The Events tab in the Advanced view can help you to track down the source of a problem, particularly when it is associated with the Symantec Backup Exec System Recovery Agent. You should view the most recent log entries in the Events tab for more information about the potential causes of the problem.
Verify that the Symantec Backup Exec System Recovery Agent starts without user intervention.	The Symantec Backup Exec System Recovery Agent is configured to start automatically when Backup Exec System Recovery starts. You can view the status information to verify that the Symantec Backup Exec System Recovery Agent has started. The Status area in the Task pane displays a Ready status message when the agent starts. You can also test that the Symantec Backup Exec System Recovery Agent is starting automatically by looking in Services. You can check the status and restart the service if necessary. If the Startup type is set to automatic, you should restart the agent. See "Starting or stopping the agent service" on page 107.
Use caution when changing default settings for the Symantec Backup Exec System Recovery Agent.	Changing the default Symantec Backup Exec System Recovery Agent properties can prevent Symantec Backup Exec System Recovery from running correctly. You should use caution when changing the default Startup type and Log On settings of the Backup Exec System Recovery Agent. It is configured to start and log on automatically when you start Symantec Backup Exec System Recovery .

Opening Services

There are several methods you can use to open Services to manage the Symantec Backup Exec System Recovery Agent.

To open Services

1. Do one of the following:
   - On the Windows Vista taskbar, click **Start > Control Panel > Classic View > Administrative Tools**, and then double-click **Services**.
   - On the Windows taskbar, click **Start > Settings > Control Panel > Administrative Tools > Services**.
   - On the Windows XP taskbar, click **Start > Control Panel > Performance and Maintenance > Administrative Tools**, and then double-click **Services**.
   - On the Windows taskbar, click **Start > Run**.
     In the Open text field, type **services.msc**, and then click **OK**.
2. Under the Name column, scroll through the list of services until you see Backup Exec System Recovery (the name of the agent).

   Its status should be Started.

   See "Starting or stopping the agent service" on page 107.

Starting or stopping the agent service

To start, stop, or restart the Symantec Backup Exec System Recovery Agent service, you must be logged on as an administrator. (If your computer is connected to a network, network policy settings might prevent you from completing these tasks.)

You might need to start, stop, or restart the Symantec Backup Exec System Recovery Agent service for the following reasons:

Start or Restart	You should start or restart the agent if Symantec Backup Exec System Recovery is unable to connect to the Symantec Backup Exec System Recovery Agent on a computer, or you cannot reconnect from Backup Exec System Recovery.
Restart	You should restart the agent after you change the user name or password that you use to log on to the Symantec Backup Exec System Recovery Agent service, or you used the Security Configuration Tool to give additional users the ability to back up computers. See "Controlling access to Backup Exec System Recovery " on page 110.

Stop	You can stop the agent if you believe it is causing a problem on the computer, or you want to temporarily free memory resources. If you stop the agent, you also prevent all of your drive-based backups and file and folder backups from running.

If you stop the Symantec Backup Exec System Recovery Agent service and then start Backup Exec System Recovery, the agent restarts automatically. The Status changes to Ready.

If you stop the Symantec Backup Exec System Recovery Agent service while Backup Exec System Recovery is running, you receive an error message, and Backup Exec System Recovery is disconnected from the agent. In most cases, you can click Reconnect from the Task pane or from the Tray icon to restart the Symantec Backup Exec System Recovery Agent.

To start or stop the Symantec Backup Exec System Recovery Agent service

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run window, type **services.msc**
3. Click **OK**.
4. In the Services window, in the Name column, click **Backup Exec System Recovery**.
5. On the Action menu, select one of the following:
   - Start
   - Stop
   - Restart

Setting up recovery actions when the agent does not start

You can specify the computer’s response if the Symantec Backup Exec System Recovery Agent fails to start.

To set up recovery actions when the agent fails to start

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run window, type **services.msc**
3. Click **OK**.
4. In the Services window, on the Action menu, click **Properties**.

5 On the Recovery tab, in the First failure, Second failure, and Subsequent failures lists, select the action that you want:

Restart the Service	Specify the number of minutes before an attempt to restart the service is made.
Run a Program	Specify a program to run. You should not specify any programs or scripts that require user input.
Restart the Computer	Click Restart Computer Options, and then specify how long to wait before restarting the computer. You can also create a message that you want to display to remote users before the computer restarts.

6 In the Reset fail count after box, specify the number of days that the Symantec Backup Exec System Recovery Agent must run successfully before the fail count is reset to zero.

When the fail count is reset to zero, the next failure triggers the action set for the first recovery attempt.

7 Click **OK**.

Viewing Symantec Backup Exec System Recovery Agent dependencies

The Symantec Backup Exec System Recovery Agent depends on other required services to run properly. If a system component is stopped or is not running properly, the dependent services can be affected.

If the Symantec Backup Exec System Recovery Agent fails to start, check the dependencies to ensure that they are installed and that their Startup type is not set to Disabled.

Note: To view the Startup type setting for each of the interdependent services, you must select one service at a time and then click Action > Properties > General.

The top list box on the Dependencies tab displays services that are required by the Symantec Backup Exec System Recovery Agent to run properly. The bottom list box does not have any services that need the Symantec Backup Exec System Recovery Agent to run properly.

Table 9-2 lists the services that are required by the Symantec Backup Exec System Recovery Agent to run properly, along with their default startup setting.

Table 9-2 Required services

Service	Startup type
Event Log	Automatic
Plug and Play	Automatic
Remote Procedure Call (RPC)	Automatic

To view Symantec Backup Exec System Recovery Agent dependencies

1 In the Services window, under Name, click **Backup Exec System Recovery**.

See "Opening Services " on page 107.

2 On the Action menu, click **Properties**.

3 Click the **Dependencies** tab.

Controlling access to Backup Exec System Recovery

You can use the Security Configuration Tool to allow or deny users and groups the necessary permissions to access the Symantec Backup Exec System Recovery Agent , or to the full Backup Exec System Recovery user interface.

When you use the Security Configuration Tool, any permission that you grant to the Users group applies to the members within that group.

Note: The agent service can only be run as LocalSystem or by a user who belongs to the Adminstrator's group.

Table 9-3 describes the permissions that can be allowed or denied for user and groups who use the Symantec Backup Exec System Recovery Agent.

Table 9-3 Permission options

Option	Description
Full Control	Gives users or groups complete access to all Symantec Backup Exec System Recovery functionality as if they are the administrator. If you do not want users to define, change, or delete backups, or to manage recovery point storage, do not give them Full Control.

Table 9-3 Permission options *(continued)*

Option	Description
Status Only	Users or groups can get status information, and can run a backup job. But they cannot define, change, or delete any backup jobs, or use any other function of the product.
Deny	Users cannot perform any function, or see any information. They are blocked from any access to Backup Exec System Recovery.

A deny setting takes precedence over an inherited allow setting. For example, a user who is a member of two groups is denied permissions if the settings for one of the groups denies permissions. User-denied permissions override group-allow permissions.

To add users and groups

1. On the Windows taskbar, click **Start > Programs > Symantec > Backup Exec System Recovery > Security Configuration Tool**.
2. Click **Add**.
3. In the Select Users or Groups dialog box, click **Advanced**.
4. If necessary, click **Object Types** to select the types of objects that you want.
5. If necessary, click **Locations** to select the location that you want to search.
6. Click **Find Now**, select users and groups you want, and then click **OK**.
7. Click **OK** when you are finished.

To change permissions for a user or a group

1. On the Windows taskbar, click **Start > Programs > Symantec > Backup Exec System Recovery > Security Configuration Tool**.
2. In the Permissions for Symantec Backup Exec System Recovery dialog box, select the user or group whose permissions you want to change, and then do one of the following:
   - To set Full Control permissions, click **Allow** or **Deny** for the selected user or group.
   - To set Status Only permissions, click **Allow** or **Deny** for the selected user or group.
3. Click **OK** when you are finished.

To remove a user or group

1. On the Windows Start menu, click **Programs > Symantec > Backup Exec System Recovery > Security Configuration Tool**.
2. Select the user or group that you want to remove, and then click **Remove**.
3. Click **OK** when you are finished.

Running Backup Exec System Recovery using different user rights

If the permissions for a user are insufficient for running Backup Exec System Recovery, you can use the Run As feature in Windows to run the product using an account that has sufficient rights, even if you are not currently logged in with the account.

To perform Run As from Windows XP/2003

1. On the Windows taskbar, click **Start > Program Files > Symantec > Backup Exec System Recovery**.
2. Right-click **Backup Exec System Recovery**, and then click .
3. Click **The following user** to log onto with another account.
4. In the User Name and Password boxes, type the account name and password that you want to use.
5. Click **OK**.

To perform Run As from Windows 2000 Professional

1. On the Windows taskbar, click **Start > Program Files > Symantec > Backup Exec System Recovery**.
2. Press **Shift** and right-click .
3. Click **Run As**.
4. Click **Run the program as the following user** to log on with another account.
5. Do one of the following:
   - In the User name, Password, and Domain boxes, type the account name, password, and the domain that you want to use.
   - If you want to use the Administrator account on the computer, in the Domain box, type the name of the computer.
     If you want to run Backup Exec System Recovery as a domain administrator, in the Domain box, type the name of the domain.
6. Click **OK**.

To perform Run As from Windows Vista

1. On the Windows taskbar, click **Start > All Programs > Backup Exec System Recovery > Backup Exec System Recovery**.
2. Click **Yes** when prompted to add the required privileges.
3. Enter the password for an administrator account, and then click **OK**.

Chapter 10

Monitoring the status of your backups

This chapter includes the following topics:

About monitoring backups

You should monitor your backups to ensure that you can effectively recover lost data when you need it.

The Home page provides a general status of your backup protection. The Status page provides details about which drives are protected, as well as a calendar view of past and future backups.

Note: In addition to ensuring that you back up each drive, carefully review and follow best practices for backing up your computer.

Rescanning a computer's hard disk

Use Refresh to update the drive information that is displayed in various views of the product. This feature is useful when hard disk configurations have changed but the changes do not immediately appear in Backup Exec System Recovery. For example, adding hard disk space or creating a partition.

When you use Refresh, Backup Exec System Recovery scans all attached hard disks for any configuration changes. It also updates information on removable media, CD-ROM or DVD-ROM drives, basic drives, file systems, and hard drive letters.

To rescan a computer's hard disks

- On the View menu, click **Refresh**.

  The Status Bar at the bottom of the product's window indicates when the scanning is taking place.

Monitoring backup protection from the Home page

On the Home page, the Backup Status pane provides a summary of the backup protection status of your computer. For example, if one or more drives are not included in a defined backup, the background color and status icon changes to reflect the level of backup protection. The Status Details pane provides recommendations on which actions you should take.

Table 10-1 describes each of the levels of backup protection that the Home page displays.

Table 10-1 Backup protection levels

✓	Backed up	At least one drive-based backup is defined. It includes all fixed drives and runs on a regular basis. This status indicates that all drives, files, and folders can be fully recovered, if necessary.
⚠	Partially backed up	A backup is defined, but it is not scheduled or run for a long time. This status can indicate that the existing recovery points are outdated. It can also indicate that one or more drives are not assigned to a defined backup. A partially protected drive can be recovered, but if the recovery points are outdated, it might not contain the latest versions of your data.

Table 10-1 Backup protection levels *(continued)*

❌	At risk	No defined backup exists and no recovery points are available from which to recover the drive. An unprotected drive cannot be recovered and is at risk.
❓	Status unknown	The status is being calculated, or you have not yet licensed your product. Either wait a few seconds for the status to display, or make sure that you have licensed your copy of the product.
🚫	No backup protection assigned	The drive that displays this icon is not being monitored for backup status; or it is being monitored for errors only, but there are no errors to report. Use the Customize status reporting feature on the Status page to change the status report setting.

Monitoring backup protection from the Status page

The Status page lets you monitor the status of your backups. The Status page lists each drive on your computer and includes a calendar that contains your backup histories. The calendar lets you quickly identify when a backup ran, and what type of backup it was. It identifies your upcoming, scheduled backups. It also lists the file and folder backup history if you have defined one or more file and folder backups.

Note: You can right-click on any of the calendar icons to access a context-sensitive menu. These menus offer quick access to related tasks.

Refer to the following table for the meaning of each icon displayed in the Backups calendar.

Table 10-2 Backups calendar icons

Icon	Description	Icon states
	Represents a drive-based backup that is configured to create a single, independent recovery point. When this icon appears in the Backup timeline, it indicates that a drive-based backup is scheduled to occur.	This icon can appear in the following states: ✓ Indicates that the backup ran and that an independent recovery point was created. Indicates that the backup is unavailable. ✗ Indicates that the backup did not run as scheduled. This problem could occur if an error prevents the backup from running or if you manually cancel a backup before it completes. Indicates a drive-based backup scheduled to run at a future time.
	Represents a drive-based backup that is configured to create incremental recovery points. It indicates that a drive-based backup is scheduled to occur on the day that it appears in the backup timeline.	This icon can appear in the following states: ✓ Indicates that the backup ran and that an incremental recovery point was created. Indicates that the backup is unavailable. ✗ Indicates that the backup did not run as scheduled. This problem could occur if an error prevents the backup from running or if you manually cancel a backup before it completes. Indicates that the backup is scheduled to run at a future time.

Table 10-2 Backups calendar icons *(continued)*

Icon	Description	Icon states
📁	Represents a file and folder backup. It indicates that a file and folder backup is scheduled to occur on the day that it appears in the backup timeline.	This icon can appear in the following states: 📁✓ Indicates that the backup ran and that file and folder backup data was created successfully. 📁 Indicates that the backup is not available. 📁✗ Indicates that the backup did not run as scheduled. This problem could occur if an error prevents the backup from running, or if you manually canceled a backup before it completed. 📁 Indicates that the backup is scheduled to run at a future time.
⧉	Represents two or more backups are scheduled to run on the day on which this icon appears.	This icon can appear in the following states: ⧉✓ Indicates that two or more backups have run and the last backup was created successfully. ⧉ Indicates that two or more backups are scheduled and that at least one is unavailable. ⧉✗ Indicates that two or more backups have and adn the last one did not succeed. This problem could occur if an error prevents a backup from running. ⧉ Indicates that the backup is scheduled to run at a future time.

To monitor backup protection from the Status page

1. On the Status page, review the Backups calendar and verify that the backup appears on the date that you ran it.
2. In the Drives column, select the drive that you want to view.

   The status information appears in the bottom half of the Status page.
3. Move your mouse over a backup icon in the calendar to review the status of the backup.
4. To move around in the calendar, use one of the following methods:
   - Click anywhere in the title bar to navigate quickly to a different point in time.
   - Use the scroll bar at the bottom of the calendar to scroll backward or forward in time.

Configuring Backup Exec System Recovery to send SNMP traps

If you use Network Management System (NMS) applications, you can configure Backup Exec System Recovery to send SNMP traps for different priority and notification types.

By default, Backup Exec System Recovery is not enabled to send SNMP traps. You must enable this functionality in Backup Exec System Recovery, and you must install and configure the Windows SNMP service on your computer if it is not already.

To configure Backup Exec System Recovery to send SNMP traps

1. On the Tasks menu, click **Options**.
2. Under Notifications, click **SNMP Trap**.

3 Click the **Select the priority and type of messages** drop-down list and select the priority level at which traps should be generated.

All messages	Send all messages, regardless of priority levels.
Medium and high priority messages	Send only medium and high priority messages.
High priority messages only	Send only high priority messages.
No messages	Do not send any messages, regardless of priority levels.

4 Select one or more of the following options:

- Errors
- Warnings
- Information

5 Select the version of SNMP traps to be sent (Version 1 or Version 2), and then click **OK**.

About the Backup Exec System Recovery management information base

The Backup Exec System Recovery management information base (MIB) is an enterprise MIB. It contains the Backup Exec System Recovery SNMP trap definitions. All Network Management System (NMS) applications have options to load a MIB. You can use any of these options to load the Backup Exec System Recovery MIB. If you do not load the MIB, the NMS application will still receive and display the traps, but the traps will not be displayed in informative text. The .MIB file, named BESR_MIB.MIB, is located in the Support folder on the Symantec Backup Exec System Recovery product CD.

Customize status reporting

You can configure how Backup Exec System Recovery reports the status of a particular drive (or all file and folder backups).

For example, if drive D contains unimportant data and you have chosen not to include it in a drive-based backup, the status on the Home page continues to report that your computer is at risk. You can configure Backup Exec System Recovery to ignore drive D so that it does not calculate the status of drive D in the Backup Status panel on the Home page.

Or, you can specify that only errors, such as missed or failed backups, are to be figured in to the status report.

Note: The backup status of each drive is reported throughout the product, wherever the drive is listed. When you customize status reporting for a drive, the status is reflected anywhere that the drive is listed in Backup Exec System Recovery.

You should first determine how important the data is on a particular drive (or the data you have included in a file and folder backup) before deciding on the level of status reporting to assign to it.

To customize the status reporting of a drive (or file and folder backups)

1 On the Status page, click a drive (or **File and folders**) to select it.

  You can also click **Customize status reporting** from the Home page.

2 Click **Customize status reporting**.

3 Select one of the following options:

Full status reporting	Shows the current status of the selected drive or file and folder backups on the Home and Status pages. Select this option if the data is critical.
Errors only status reporting	Shows the current status of the selected drive or file and folder backups only when errors occur. Select this option if the data is important, but you only want the status to report errors, whenever they occur.
No status reporting	Does not show any status for the selected drive or file and folder backups. Select this option if the data is unimportant and missed or failed backups do not need to be reported.

4 Click **OK**.

Viewing drive details

The Advanced page lets you view details about your hard drives.

You can view the following drive details:

Name	Displays the name that you assigned to the backup when you defined it.
Type	Identifies the type of recovery point the backup creates when it runs.
Destination	Identifies the storage location of the recovery point, or the location in which the drive should be backed up.
Last Run	Displays the day and time when the backup was last run.
Next Run	Displays the day and time of the next scheduled backup.

To view drive details

1. On the Advanced page, on the Content Bar, click the Drives tab.

   If the Advanced page is not visible on the Primary Navigation Bar, click **View > Show Advanced Page**.
2. In the Drive column, select a drive.
3. Review the Details section below the Drives table.

Improving the protection level of a drive

When the status of a drive-based backup indicates that it needs attention, you should take steps to improve the status.

You might need to add a drive to an existing backup, modify the schedule of a backup, edit the settings of a backup, or define a new backup.

See “Best practices for backing up ” on page 52.

To improve the protection level of a drive

1. On the Status page, select a drive that requires attention from the Drives column.
2. In the Status section at the bottom of the page, right-click the backup you want to modify, and then select one of the following menu items:

Run Backup Now	Runs the selected backup job immediately.
Change Schedule	Opens the Run When dialog so that you can edit the backup schedule.
Edit Settings	Opens the Define Backup Wizard, which lets you modify the backup definition. This option takes you to the second page of the wizard.
Define New Backup	Opens the Define Backup Wizard from the beginning, which lets you define a new backup. This option is useful if a drive in the Drives column is not yet assigned to a backup. By selecting a drive that is assigned to an existing backup, you have access to this short-cut method for starting the Define Backup Wizard from the Status page.
Remove Backup Job	Deletes the backup that you have selected. When you delete a backup, only the backup definition is deleted. The backup data is not deleted (for example, the recovery points or the file and folder backup data).
Disable (Enable) Backup	Turns on or turns off the backup that you have selected.

See “Editing backup settings” on page 93.

Using event log information to troubleshoot problems

When Backup Exec System Recovery performs an action, it records the event (for example, when a backup job runs). It also records program error messages.

You can use the event log to track down the source of problems or to verify the successful completion of a backup job.

See “Logging Backup Exec System Recovery messages” on page 47.

Log entries provide information about the success or failure of numerous actions that were taken by Backup Exec System Recovery or by a user. It offers a single view of all of the information and program error messages.

The following information is included in the event log:

Type
Indicates if the event is an error message or other information, such as the successful completion of a backup job.

Source
Identifies if the message was generated by Backup Exec System Recovery or another program.

Date
Displays the exact date and time that a selected event occurred.

Description
Offers additional details about an event that can help you troubleshoot problems that might have occurred.

Exploring the contents of a recovery point

This chapter includes the following topics:

About exploring recovery points

You can use Backup Exec System Recovery to explore files in a recovery point by assigning it a drive letter that is visible from Windows Explorer.

You can perform the following tasks on the assigned drive:

- Run ScanDisk (or CHKDSK)
- Perform a virus check
- Copy folders or files to an alternate location
- View disk information about the drive such as used space and free space
- You can also run simple, executable programs that exist within the mounted recovery point.

> You can only run programs from within a mapped recovery point that do not rely on registry values, COM interfaces, dynamic link libraries (DLLs), or other similar dependencies.

You can set up a mounted drive as a shared drive. Users on a network can connect to the shared drive and restore files and folders from the recovery point.

You can mount one or more recovery points at a time. The drives remain mounted until you unmount them, or you restart the computer. Mounted drives do not take up extra hard-disk space.

All security on the NTFS volumes remains intact when they are mounted.

You do not need to mount a drive to restore the files or folders within a recovery point.

Note: Any data that is written to a mounted recovery point is lost when the recovery point is unmounted. This data includes any data that is being created, edited, or deleted at the time.

Exploring a recovery point through Windows Explorer

Unmounting a recovery point drive

Viewing the drive properties of a recovery point

Exploring a recovery point through Windows Explorer

When you explore a recovery point, Backup Exec System Recovery mounts the recovery point as a drive letter and opens it in Windows Explorer.

For each drive that is included in the recovery point, a new mounted drive letter is created. For example, if your recovery point contains backups of drives C and D, two newly mounted drives appear (for example, E and F). The mounted drives include the original drive labels of the drives that were backed up.

To explore a recovery point through Windows Explorer

1. On the Tools page, click **Manage Backup Destination**.
2. Select the recovery point or recovery point set that you want to explore, and then click **Explore**.
3. If you select a recovery point set that contains more than one recovery point, in the Range list, select a recovery point, and then click **OK**.

Mounting a recovery point from Windows Explorer

You can also manually mount a recovery point as a drive by opening your backup destination folder in Windows Explorer.

You can use Windows Explorer to search the contents of the recovery point. For example, if you cannot remember where a particular file was originally stored, you can use the Explorer search feature to locate the file, just as you would locate a file on your hard drive.

To mount a recovery point from Windows Explorer

1. In Windows Explorer, navigate to a recovery point.

   The recovery point is located in the storage location that you selected when you defined your backup.
2. Right-click the recovery point, and then click **Mount**.
3. In the Mount Recovery Point window, under the Drive Label column,select the drive that you want to mount.
4. In the Drive letter drop-down list, select the letter that you want to associate with the drive.
5. Click **OK**.
6. To mount additional drives, repeat steps 1-5.

Opening files within a recovery point

Using the Recovery Point Browser, you can open files within a recovery point. The file opens in the program that is associated with that file type. You can also restore files either by saving them using the application associated with them, or by using the Recover Files button in the Recovery Point Browser.

If the file type is not associated with a program, the Microsoft Open With dialog box is displayed. You can then select the correct program for opening the file.

Note: You cannot view encrypting file system (EFS) NTFS volumes.

To browse and open files inside of a recovery point

1. On the Tools page, click **Run Recovery Point Browser**.
2. Navigate to your backup destination folder, select the recovery point file that you want to browse, and then click **Open**.
3. In the Recovery Point Browser, in the tree panel on the left, select a drive.

4 In the right content panel, double-click the folder that contains the file that you want to view.

5 Right-click the file that you want to view, and then click **View File**.

The View option is unavailable if you select a program file that has a .exe, .dll, or .com file extension.

To restore one or more files

1 On the Tools page, click **Run Recovery Point Browser**.

2 Navigate to your backup destination folder, select the recovery point file you want to browse, and then click **Open**.

3 In the Recovery Point Browser, select a drive in the tree panel (on the left).

4 In the content panel (on the right), double-click a folder that contains the file you want to view.

5 Do one of the following:

- Right-click the file you want to view and click **View File**.
  The View option is dimmed (unavailable) if you selected a program file that has a .exe, .dll, or .com file extension.
- Select one or more files, click **Recover Files**, and then click **Recover** to restore them to their original location.
  If prompted, click **Yes** or **Yes to All** to overwrite the existing (original) files.

Using a search engine

If you have a desktop search engine, such as Google Desktop, you can configure your backups to create recovery points that are searchable.

Note: If your organization uses Symantec Backup Exec Web Retrieve, it is likely that your network administrator has already enabled this feature.

You can configure your backups to support one of these search engines. Be sure to check the Enable search engine support at the time you define the backup.

See “To define a drive-based backup” on page 63.

See “About using a search engine to search recovery points” on page 187.

Unmounting a recovery point drive

All of your mounted recovery point drives are unmounted when you restart the computer. You can also unmount the drives without restarting the computer.

To dismount a recovery point in Windows Explorer

1. In Windows Explorer, navigate to the mounted recovery point.
2. Right-click the drive, and then click **Dismount Recovery Point**.

To dismount a recovery point in Recovery Point Browser

1. In the Recovery Point Browser, in the tree view, locate the mounted recovery point.
2. Right-click the mounted recovery point, and then click **Dismount Recovery Point**.

Viewing the drive properties of a recovery point

You can view the following drive properties of a recovery point:

Description	A user-assigned comment that is associated with the recovery point.
Original drive letter	The original drive letter that was assigned to the drive.
Cluster size	The cluster size (in bytes) of the FAT, FAT32, or NTFS drive.
File system	The file system type used within the drive. For example, FAT, FAT32, or NTFS.
Primary/Logical	The selected drive's status as either a primary partition or a logical partition.
Size	The total size (in megabytes) of the drive. This total includes used space and unused space.
Used space	The amount of used space (in megabytes) within the drive.
Unused space	The amount of unused space (in megabytes) within the drive.
Contains bad sectors	Indicates if there are any bad sectors on the drive.

To view the drive properties of a recovery point

1. In the Recovery Point Browser, in the tree panel, click the recovery point that contains the drive that you want to view.
2. Select a drive.
3. Do one of the following:
   - On the File menu, click **Properties**.
   - Right-click the recovery point, and then click **Properties**.

Chapter 12

Managing backup destinations

This chapter includes the following topics:

About backup destinations

A *backup destination* is the location in which your backup data is stored.

Backup Exec System Recovery includes features for managing the size of your backup destinations so that you can use your computer's valuable disk space for other purposes.

How backup data works

Backup Exec System Recovery offers two backup methods:

Drive-based backup	Use this option to back up an entire drive (for example, your system drive, which is typically C). You can then restore any file, folder, or your entire drive.
File and folder backup	Use this option to back up only the files and folders that you select. You can then restore any file or all of them at any time. This option typically requires less disk space than drive-based backups.

About drive-based backups

When you run a drive-based backup, a snapshot is taken of everything that is stored on your computer's hard disk. Each snapshot is stored on your computer as a recovery point. A recovery point is a point in time that is used to restore your computer back to the way it was when the recovery point was created.

The types of recovery points are as follows:

Independent recovery point (.v2i)	Creates a complete, independent copy of the drives that you select. This backup type typically requires more storage space.
Recovery point set (.iv2i)	Includes a base recovery point. A base recovery point is a complete copy of your entire drive, and is similar to an independent recovery point. The recovery point set also includes recovery points that capture only the changes that are made to your computer since the creation of the base recovery point.

Although you can recover files and folders from a drive-based backup, you cannot select a specific set of files or folders to back up. Your entire hard drive is backed up.

About file and folder backups

If you want to modify or create a select set of personal documents and folders and you don't want to use hard disk resources to back up your entire computer, you can define a file and folder backup. Or, you might want to define a file and folder backup to capture one or more folders that contain the files that you modify on a regular basis.

File and folder backups let you select individual files or folders to back up. You can also specify a file type to back up and let Backup Exec System Recovery locate and back up all files of the type you specified. For example, if you have Microsoft Word documents stored at several locations on your computer, Backup Exec System Recovery locates all Word documents (files ending with .doc) and includes them in your backup. You can even modify the list of file types to include types unique to the software you are using.

Backup Exec System Recovery also keeps multiple versions of the same files for you, so that you can restore the version of a file containing the changes you need to restore. You can even set a limit to the number of versions kept so that you can control the use of disk space.

Managing recovery points

Backup Exec System Recovery includes several features that help you manage your backup data. The key is to prevent backup data from taking up too much hard disk space on your computer while providing adequate backup protection in the event that you need to recover your computer, files, or folders.

To manage recovery point storage manually

1 On the Tools page, click **Manage Backup Destination**.

2 From the Manage Backup Destination window, you can do any of the following tasks:

Clean Up	See "Cleaning up old recovery points" on page 135.
Delete	See "Deleting a recovery point set" on page 136. See "Deleting recovery points within a set" on page 136.
Explore	See "About exploring recovery points " on page 127.
Copy	See "Making copies of recovery points " on page 137.
Move	See "Moving your backup destination" on page 144.
Settings	See "Automating management of backup data" on page 143.

Cleaning up old recovery points

Over time, you might end up with recovery points that you no longer need. For example, you might have several recovery points created months ago that you no longer need because you have more current ones containing your latest work.

See "Automating management of backup data" on page 143.

The Clean Up feature deletes all but the most current recovery point set, to help make more space available on your hard disk.

Note: After a recovery point is deleted, you no longer have access to the files or system recovery from that point in time. You should explore the contents of the recovery point before you delete it.

See “Opening files within a recovery point” on page 129.

See “About exploring recovery points ” on page 127.

To clean up old recovery points

1. On the Tools page, click **Manage Backup Destination**.
2. Click **Clean Up**.

   The recovery point sets that can be safely removed without eliminating your latest recovery point are selected automatically. You can check or uncheck the recovery point sets to specify which ones to remove.
3. Click **Delete**.
4. Click **Yes** to confirm the deletion.
5. Click **OK**.

Deleting a recovery point set

If you know that you no longer want a particular recovery point set, you can delete it at any time.

Note: Once you delete a recovery point, you no longer have access to file or system recovery for that point in time.

To delete a recovery point set

1. On the Tools page, click **Manage Backup Destination**.
2. Select the recovery point set that you want to delete, and then click **Delete**.
3. Click **Yes** to confirm the deletion.
4. Click **OK**.

Deleting recovery points within a set

A recovery point set can contain multiple recovery points created over time that you can delete to reclaim storage space.

The Delete Points option lets you delete all of the recovery points created between the first recovery point and last recovery point in the set.

Warning: Be careful about which recovery points you choose to delete. You could inadvertently lose data. For example, you create a new document, which is captured in the third recovery point in a recovery point set. You then accidentally delete the file, which is captured by the fourth recovery point. If you delete the third recovery point, you permanently lose the version of the file that was backed up. If you are unsure, you should explore the contents of a recovery point before you delete it.

See “Opening files within a recovery point” on page 129.

You can manually select which recovery points to remove, if you know which recovery points that you want to keep within a set.

To delete recovery points within a set

1. On the Tools page, click **Manage Backup Destination**.
2. Select the recovery point set that you want to delete, and then click **Delete**.
3. Do one of the following:
   - To automatically delete all but the first and last recovery point in the set, click **Automatic**.
   - To manually select which recovery points in the set to delete, click **Manual**, and then select the recovery points you want to delete.
   - To delete all the recovery points in the set you selected, click **Delete all recovery points in the set**.
4. Click **OK**.

Making copies of recovery points

You can copy recovery points to another location for added security. For example, you can copy them to another hard disk, another computer on a network, or on removable media such as DVDs or CDs. You can then store these copies in a protected location.

You can also create archive copies of your recovery points to free up disk space. For example, you can copy recovery points to a CD or DVD, and then manually delete the original recovery points. You should verify the copies of the recovery points to ensure that they are on the disk and are valid.

To make copies of recovery points

1. On the Tools page, click **Manage Backup Destination**.
2. Select a recovery point set or an independent recovery point, and then click **Copy**.

3 Select which recovery point to copy, and then click **OK**.

4 On the Welcome page of the Copy Recovery Point Wizard, click **Next**.

5 Select the recovery point that you want to copy.

Recovery point sets appear as single recovery points. Check **View all recovery points** to display all incremental recovery points that are included within the recovery point sets.

6 Click **Next**.

7 Do one of the following:

- In the **Folder** box, type the path to which you want to copy the recovery point.
- Click **Browse** to locate the folder to which you want to copy the recovery point, and then click **OK**.

8 Select a level of compression for the copies of the recovery points.

See "About setting a compression level for drive-based backups" on page 78.

9 If you want to verify whether a recovery point is valid once the copy is complete, check **Verify recovery point after creation**.

10 Click **Advanced**, and then select from the following options:

- Divide into smaller files to simplify archiving
- Use password

See "Setting advanced options for drive-based backups" on page 74.

11 Click **OK**.

12 Click **Next**, review the options that you selected, and then click **Finish**.

Once the recovery points are safely copied, you can delete them from your computer.

See "Deleting a recovery point set" on page 136.

Converting a recovery point to a virtual disk format

You can use Symantec Backup Exec System Recovery to convert recovery points of a physical computer to a VMWare Virtual Disk (.vmdk) or a Microsoft Virtual Disk (.vhd).

Virtual disks created from recovery points are supported by the following platforms:

- VMware GSX Server 3.1 and 3.2

- VMware Server 1.0
- VMware ESX Server 2.5 and 3.0
- VMware Infrastructure 3
- Microsoft Virtual Server 2005 R2

To convert a recovery point to virtual disk format

1. On the Tools page, click **Convert to Virtual Disk**, and then click **Next**.
2. Select the recovery point that you want to convert, and then click **Next**.
3. If you don't see the recovery point that you want to use, do one of the following:
   - Click **View all recovery points**, and then select a recovery point.
   - Click **View by**, and then select one of the following alternatives:

     Filename

     Lets you browse to another location, for example, an external (USB) drive or removable media to select a recovery point (.v2i) file.

     Select this option, and then do the following:
     - Click **Browse**, locate and select a recovery point (.v2i file), and then click **Open**.
     - If you select a network location, type your network credentials.
       See “About network credentials” on page 72.
     - Click **Next**.

     System

     Displays a list of all of the drives on your computer and shows any associated recovery points. You can also select a system index file (.sv2i).

     Select this option, and then do the following:
     - Click **Browse**, locate and select a recovery point (.sv2i), and then click **Open**.
     - If you select a network location, type your network credentials.
       See “About network credentials” on page 72.
     - Click **Next**.

4. Click **Virtual disk format**, and then select a format.
5. Do one of the following:
   - In the folder in which you want to place the virtual disk image, type the path.

- Click **Browse** to locate the folder in which you want to place the virtual disk image.

6 If you select a network location, type your network credentials.

See "About network credentials" on page 72.

7 Click **Next**.

8 If you select Microsoft Virtual Disk (.vhd) as your virtual disk format, skip the next step.

9 If you select VMware Virtual Disk (.vmdk), do one of the following options:

- Check **Split into 2GB files** if you want to divide the virtual disk file into smaller files.
  For example, you can use this option if you need to copy the virtual disk to a FAT 32 drive, or if you want to copy the virtual disk files to a DVD but the size is larger than the DVD allows.
- Check **Store on ESX Server** if you want to store the virtual disk file on a VMware ESX Server, and then provide the following information:

Server name or address	Type the name of the server or the server's IP address.
User name	Type a valid administrator name that has sufficient rights. **Note:** The virtual disk files are transferred to an ESX Server through a secure shell (SSH) and secure file transfer protocol (SFTP). You might need to change the settings on the ESX Server. For more information, see your ESX server documentation.
Password	Type a valid password.
Upload location	Type the path to the folder to which the virtual disk files should be written.

Import location	Type the path to the folder to which you want to import the virtual disk files. **Note:** The folder that you select must be different than the upload location folder.
Remove intermediate files	Check this option if you want the temporary files to be removed once the virtual disk is created.

10 Click Next, and then review the summary of the choices you made.

If you need to make any changes, click **Back**.

11 Click **Finish**.

Managing file and folder backup data

Because drive-based backups capture your entire hard drive, the size of a recovery point is typically much larger than the data that is captured during the file and folder backups. However, file and folder backup data can take up significant disk space if it is not managed. For example, audio files, video files, and photographs are typically large files.

You must decide how many versions of backup files that you want to keep. This decision can depend on how frequently you change the content of your files and how frequently you run the backups.

Viewing how much file and folder backup data is being stored

Start by viewing the total amount of file and folder backup data you are currently storing.

To view how much file and folder backup data is being stored

1 On the Tools page, click **Manage Backup Destination**.

2 To select an alternate backup destination, in the Drives drop-down list, select another drive to use as a backup destination.

3 Near the bottom of the Manage Backup Destination window, view the Space used for file and folder storage box to see how much storage space is currently used.

Limiting the number of file versions to keep

You can manage your file and folder backup data by limiting the number of versions of backup files that you keep. This can significantly reduce the amount of disk space required, especially if the files are large, as is often the case with audio and video files.

To limit the number of file versions to keep

1. On the Tools page, click **Manage Backup Destination**.
2. Click **Settings**.
3. Check **Limit file versions for file and folder backups**, and then type a number between 1 and 99.
4. You can also check **Monitor disk space usage for backup storage**, and then specify a limit to the total amount of disk space that can be used for both recovery points and file and folder backup data.

   See "Automating management of backup data" on page 143.
5. Click **OK**.

Manually deleting files from your file and folder backup

You can manually delete files that are stored in your backup destination.

To manually delete files from your file and folder backup

1. On the Home or Tasks page, click **Recover My Files**.
2. Do one of the following:
   - In the Find files to recover box, type the file name of the file that you want to delete, and then click **Search**.
   - If you don't know the name of the file, click **Search** to return a list of all of the files that have been backed up, and then browse for the file.
3. Click **View All Versions** to display all versions of each file that exist in the file and folder backup data.
4. Select one or more files that you want to delete.
5. Right-click, and then click **Delete**.

Finding versions of a file or folder

You can use Windows Explorer to view information about the available versions that are included in a file and folder backup.

You can specify a limit to the number of versions of each file or folder stored in file and folder backup data.

See “Limiting the number of file versions to keep” on page 142.

To find versions of a file or folder

1 Open Windows Explorer.

2 Navigate to a file that you know is included in a file and folder backup.

3 Right-click the file, and then click **Show Versions**.

Automating management of backup data

Backup Exec System Recovery can monitor your backup storage space and notify you when it is getting full. It can also automatically delete old recovery points and older versions of files from file and folder backups that exceed the threshold. If you do not specify a threshold, Backup Exec System Recovery notifies you when the disk reaches 90percent of its total capacity.

To automate management of backup data

1 On the Tools page, click **Manage Backup Destination**.

2 Check **Limit file versions for file and folder backups**, and then type a number between 1 and 99.

3 Check **Monitor disk space usage for backup storage**, and then drag the slider to limit the total amount of disk space that can be used for your recovery points and your file and folder backup data.

4 Do one of the following:

   - Check **Warn me when backup storage exceeds threshold** if you only want to be notified when the storage size is exceeded, but you do not want any action to be taken.
   - Check **Automatically optimize storage** if you want Backup Exec System Recovery to manage the backup data automatically, without prompting you.
     If you select this option, Backup Exec System Recovery automatically deletes the old recovery points and limits file versions to remain within the threshold that you set.

5 Check **Delay changes until next backup** if you do not want your changes applied until the next backup runs.

6 Click **OK**.

Moving your backup destination

You can change the backup destination for your recovery points and move your existing recovery points to a new location. For example, suppose you install a new external hard drive for storing your backup data. You could then change the backup destination for one or more backups to the new drive.

When you select a new location, you can also choose to move the existing recovery points to the new destination. All future recovery points for the backups that you select are created at the new location.

Note: If you want to move your backup destination to a new internal or external hard drive, make sure the drive is properly installed or connected before you proceed.

To move your backup destination

1. On the Tools page, click **Manage Backup Destination**.
2. In the Manage Backup Destination window, in the Drives drop-down list, select the drive that contains the backup destination that you want to move.
3. Click **Move**.
4. In the Move Backup Destination dialog box, do one of the following:
   - In the New backup destination box, type the path to the new backup destination.
   - Click **Browse** to locate and select a new backup destination, and then click **OK**.
5. Select the defined backups that should use the new backup destination.

   Deselect the defined backups that you do not want to move.
6. Check **Save as default backup destination** if you want to use this destination as the default backup destination for any new backups that you define in the future.
7. Click **OK**.
8. To move existing recovery points to the new backup destination, check **Move recovery points**, and then do one of the following:
   - Check **Move the latest recovery points for each backup and delete the rest**.
   - Check **Move all recovery points to the new destination**.

9 If you have file and folder backup data that you want to move to the new backup destination, click **Move file backup data**.

The Move File Backup Data option is not available no file and folder backup data is found at the original backup destination.

10 Click **OK**.

Recovering files, folders, or entire drives

This chapter includes the following topics:

About recovering lost data

Backup Exec System Recovery can restore lost files, folders, or entire drives by using recovery points or file and folder backup data.

You must have either a recovery point or file and folder backup data to recover lost files and folders. You must have a recovery point to recover an entire drive. To recover recent changes that were made to a lost file or folder, your backup data must be at least as current as the changes that were made to the lost file or folder.

Recovering files and folders by using file and folder backup data

If you defined a file and folder backup and need to recover files, you can recover them from a recent file and folder backup.

Backup Exec System Recovery includes a search tool to help you locate the files that you want to recover.

To recover files and folders by using file and folder backup data

1. On the Home or Tasks page, click **Recover My Files**.
2. In the left pane of the Recover My Files window, select **File and Folder** as the search method.
3. Do one of the following:
   - In the Find files to recover search box, type the whole name or partial name of a file or folder that you want to restore, and then click **Search**.
     For example, type **recipe** to return any file or folder that includes the word recipe in its name, for example My Recipes.doc, Recipes.xls, Recipes for Success.mp3, and so forth.
   - Click **Advanced Search**, type your search criteria, and then click **Search**.
     To return to the standard search text box, click **Basic search**.
4. In the search results list box, select the files that you want to restore by using one of the following methods:

To select a single file	Click the file once.
To select all files	Press **Ctrl+A**.
To select a group of files that are next to each other	Click the top file, press and hold **Shift**, and then click the last file in the group.
To select a group of files that are not next to each other	Press and hold **Ctrl** while you select the files that you want.

5. Click **Recover Files**.
6. In the Recover My Files dialog box, do one of the following:
   - Click **Original folders** to restore your files to the same folder where they existed when they were backed up.
     If you want to replace the original files, check **Overwrite existing files**. If you do not check this option, a number is added to the file name The original file is untouched.

     Caution: The Overwrite existing files option replaces your original files (or the files of the same names that are currently stored at that location) with the files that you are restoring.

- Click **Recovered Files folder on the desktop** to restore your files to a Recovered Files folder on your Windows desktop.
  Backup Exec System Recovery creates this folder during the restore.
- Click **Alternate folder** and type the path to the location in which you want to restore your files.

7. Click **Recover**.
8. If you are prompted to replace the existing file, click **Yes** if you are certain that the file that you are recovering is the file that you want.
9. Click **OK**.

Recovering files and folders by using a recovery point

You can also restore files or folders using recovery points, provided you have defined and run a drive-based backup.

To restore files and folders using a recovery point

1. On the Home or Tasks page, click **Recover My Files**
2. In the left pane of the Recover My Files window, select **Recovery Point** as the search method.
3. If you want to use a different recovery point than the one selected for you in the Recovery Point box, click **Change**.

   Note: If Backup Exec System Recovery cannot locate any recovery points, the Select Recovery Point dialog box opens automatically.

   In the Select Recovery Point dialog box, click **View by** and select one of the following options:

Date	Displays all of the discovered recovery points in the order in which they were created. If no recovery points were discovered, the table will appear empty. You should then choose one of the remaining View by options.

Filename

Lets you browse to another location, for example, an external (USB) drive or removable media to select a recovery point (.v2i) file.

Select this option, and then do the following:

- Click **Browse**, locate and select a recovery point (.v2i file), and then click **Open**.
- If you select a network location, type your network credentials.

  See “About network credentials” on page 72.
- Click **Finish**.

System

Displays a list of all of the drives on your computer and shows any associated recovery points. You can also select a system index file (.sv2i).

Select this option, and then do the following:

- Click **Browse**, locate and select a recovery point (.sv2i), and then click **Open**.
- If you select a network location, type your network credentials.

  See “About network credentials” on page 72.
- Check each recovery point that you want to recover.

  If necessary, add, change, or remove recovery points from the list.
- Click **Finish**.

4. In the Find files to recover box, type the whole name or partial name of a file or folder that you want to restore, and then click **Search**.

   For example, type **recipe** to return any file or folder that includes the word recipe in its name, such as My Recipes.doc, Recipes.xls, Recipes for Success.mp3, and so forth.

5. In the Files to restore list, select the files that you want to restore by using one of the following methods:

To select a single file	Click the file once.
To select all files	Press **Ctrl+A**.
To select a group of files that are next to each other	Click the top file, press and hold **Shift**, and then click the last file in the group.
To select a group of files that are not next to each other	Press and hold **Ctrl** while you select the files that you want.

6 Click **Recover Files**.

7 In the Recover My Files dialog box, do one of the following:

- Click **Original folders** to have your files restored in the original folder where they existed when they were backed up.

  If you want to replace the original files, check **Overwrite existing files**. If you do not check this option, a number is added to the filename, leaving the original file untouched.

  Caution: Checking Overwrite existing files replaces your original files (or the files of the same names that are currently stored at that location) with the files you are restoring.

- Click **Recovered Files folder on the desktop** to have your files restored to a new folder that is created on your Windows desktop called Recovered Files.
- Click **Alternate folder** and specify the path to an alternate location where you want your files restored.

8 Click **Recover**.

9 If you are prompted to replace the existing file, click **Yes** if you are certain that the file that you are recovering is the file that you want.

10 Click **OK**.

Opening files and folders stored in a recovery point

If you are not sure which files you want to restore, you can locate, open and view their contents using the Recovery Point Browser. From there, you can also restore files and folders using the Recovery Point Browser.

See “Opening files within a recovery point” on page 129.

If you cannot find the files or folders you want

If you cannot find the files or folders that you want to restore by browsing through a recovery point, you can use the Backup Exec System Recovery Explore feature. This feature assigns a drive letter to a recovery point (mounts the recovery point) as if it were a working drive. You can then use the Windows Explorer search feature to search for the files. You can drag and drop files to restore them.

See “About exploring recovery points ” on page 127.

Recovering a secondary drive

If you lose data on a secondary drive, you can use an existing recovery point for that drive to restore the data. A secondary drive is a drive other than the drive on which your operating system is installed.

Note: You can recover your system drive (typically, drive C).

For example, if your computer has a D drive and the data has been lost, you can restore the D drive back to an earlier date and time.

See “About recovering a computer ” on page 159.

To recover a drive, you must have a recovery point that includes the drive that you want to recover. If you are not sure, review the Status page to determine what recovery points are available.

See “Monitoring backup protection from the Status page ” on page 117.

Note: Before you proceed, close any applications and files that are open on the drive that you want to restore.

Warning: When you recover a drive, all of the data on the drive to which you are restoring the recovery point is replaced by the data in the recovery point. Any changes that you made to the data on a drive after the date of the recovery point you use to recover it are lost. For example, if you created a new file on the drive after you created the recovery point, the new file is not recovered.

To recover a drive

1. On the Tasks page, click **Recover My Computer**.
2. Select a recovery point, and then click **Recover Now**.
3. Click **OK**.
4. Click **Yes**.

To customize the recovery of a drive

1. On the Tasks page, click **Recover My Computer**.
2. Select a recovery point, and then click **Recover Now**.
3. Click **Custom** to start the Recover Drive Wizard.
4. Click **Next**.

5. Do one of the following:
   - To use the recovery point that is selected, click **Next**.
   - Click **Browse** to select a different recovery point, and then click **Next**.
     If you need to access recovery points on a network that requires user authentication, enter your user name and password, and then click **Next**.
6. Select the drive that you want to restore, and then click **Next**.

   If the drive does not have enough space available to restore a recovery point, press **Shift** and then select multiple, contiguous destinations that exist on the same hard disk.
7. If the recovery point is password-protected, in the Password box, type the password and then click **OK**.
8. Select from the following restore options:

Verify recovery point before restore	Verifies whether a recovery point is valid or corrupt it is restored. This option can significantly increase the time required for the recovery to complete.
Check for file system errors	Checks the restored drive for errors after the recovery point is restored.
Resize restored drive	Automatically expands the drive to occupy the target drive's remaining unallocated space.
Set drive active (for booting OS)	Makes the restored drive the active partition (for example, the drive from which the computer starts). You should select this option if you are restoring the drive on which your operating system is installed.

Restore original disk signature	Restores the original, physical disk signature of the hard drive. Disk signatures are included in Windows Server 2003, Windows 2000 Advanced Server, and Windows NT Server 4.0 Enterprise Edition (SP3 and later). Disk signatures are required to use the hard drive. Select this option if either of the following situations are true: ■ Your computer's drive letters are atypical (for example, assigned letters other than C, D, E, and so forth). ■ You are restoring a recovery point to a blank hard drive.
Partition type	Sets the partition type as follows: ■ Primary partition: Because hard disks are limited to four primary partitions, select this type if the drive will have four or less partitions. ■ Logical partition: Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of your hard disk.
Drive letter	Lets you assign a drive letter to the partition.

The options that are available depend on the restore destination that you have selected.

9 Click **Next** to review your selections.

10 Click **Finish**.

11 Click **Yes**.

If the wizard cannot lock the drive to perform the recovery in Windows (typically, because the drive is in use by a program), make sure the drive is not in use by closing any files or applications that might be using it, and then click Retry.

If the Retry option fails, click Ignore to tell Windows to attempt to force a lock on the drive. If Ignore failes, you might be prompted to insert the Symantec Recovery Disk and manually start the recovery environment so that you can complete the recovery. When the recovery is finished, the computer restarts automatically.

About LightsOut Restore

Symantec Backup Exec System Recovery LightsOut Restore lets administrators restore a computer from a remote location. It works regardless of the state of the computer provided that its file system is intact.

For example, suppose you are on vacation in the Bahamas and a computer on your network in Los Angeles goes down. You can connect to the computer from your remote location by using your server's remote connection capabilities. You can remotely access the Symantec Recovery Disk to start the computer in the recovery environment. You can then use the recovery environment to restore files or an entire system partition.

LightsOut Restore installs a customized version of the Symantec recovery environment directly to the file system on the system partition. It then places a Symantec recovery environment boot option in the Windows boot menu. Whenever the Symantec recovery environment boot menu option is selected, the computer boots directly into the Symantec recovery environment by using the files that are installed on the system partition.

LightsOut Restore uses Symantec pcAnywhere technology, the Windows boot menu, and hardware devices such as RILO and DRAC to let an administrator remotely control a system during the boot process.

By default, when the recovery environment boots as part of LightsOut Restore, it automatically starts a pcAnywhere thin host. You can then use Symantec pcAnywhere from your remote location to connect to the thin host.

After you configure LightsOut Restore and add the boot menu option, you can use a hardware device to remotely connect to the system. After you connect, you can power on or reboot the system into the recovery environment.

Setting up and using LightsOut Restore

This section presents an overview of setting up and using LightsOut Restore.

Note: You must install a fully licensed version of Symantec Backup Exec System Recovery before you use the LightsOut feature to perform a restore operation. LightsOut Restore is not included in the evaluation version.

- Install a licensed version of Symantec pcAnywhere on a central computer that you use for management (for example, a helpdesk computer).
- Ensure that all of your servers can be managed remotely through a hardware device such as RILO or DRAC.

- Install Backup Exec System Recovery on the servers that you want to protect, and then define and run backups to create recovery points.
- Run the LightsOut Restore Wizard to install the Symantec recovery environment to the local file system.

  The wizard also creates an entry in the Windows boot menu that can be used to boot to the recovery environment.

  Note: LightsOut Restore works only on the primary operating system. It does not work on multiple-boot computers (for example, computer that boot multiple operating systems from the same partition). LightsOut Restore is accessible only from the boot menu. If the file system becomes corrupt and you cannot access the boot menu, you must boot the computer from the CD.

  Note: The LightsOut Restore feature requires at least 1 gigabyte of memory to run.

- When you need to recover and file or system from a remote location, use the RILO or DRAC device to connect to the remote server, and power on the system or restart it.
- As the remote server starts, open the boot menu, and then select the Symantec recovery environment.

  The remote server boots into the Symantec recovery environment and the connection through RILO or DRAC is lost. A pcAnywhere thin host automatically starts.
- Use Symantec pcAnywhere to connect to the pcAnywhere thin host that is waiting on the remote server.
- Through pcAnywhere, use the recovery environment to restore individual files, or entire drives.

Configuring LightsOut Restore

You must run the LightsOut Restore Wizard on the computer that you want to protect. The LightsOut Restore Wizard installs the Symantec recovery environment to the local file system. The wizard also creates an entry in the Windows boot menu that you use to boot into the recovery environment.

To configure LightsOut Restore

1. Start Backup Exec System Recovery, and then click **Tasks > Set Up LightsOut Restore**.

   If the product is not licensed, the LightsOut Setup menu item is not available. You must install a license file.

   See "Activating Backup Exec System Recovery later" on page 28.

2. Insert your Symantec Recovery Disk CD into your CD-ROM drive, and then click **Next**.

3. If necessary, specify the path to the CD-ROM drive in which you placed the Symantec Recovery CD, and then click **Next**.

4. Review the list of drivers to be included, and add additional drivers or remove the drivers you do not need, and then click **Next**.

5. On the Options page, do the following:

   - In the Time to display boot menu box, specify (in seconds) how long the boot menu should display.
     The default is 10 seconds.
   - If you do not want networking to start automatically when restoring the computer through LightsOut Restore, uncheck **Enable Networking**.
   - If you do not want the pcAnywhere thin host to start automatically when restoring the computer through LightsOut Restore, uncheck **Enable pcAnywhere**.
   - Select the type of IP address you want to use, and then click **Next**.

6. If you are shown a list of network and storage drivers that are not supported in the Symantec recovery environment, do the following:

   - Select the box next to the network driver that you would like to copy from your current Windows installation to the Symantec recovery environment.
   - Review the list of missing storage drivers, and then click **Next**.
   - Browse to the locations of your missing storage and network driver files.

     Note: The location that you specify should contain the fully extracted installation package for the driver. If you have more than one missing storage driver, you must rerun the LightsOut Restore Wizard for each missing driver. The drivers that you select should be compatible with Windows Vista.

The files are copied from the Symantec Recovery Disk. After the files are copied, you receive a message that indicates that LightsOut Restore successfully installed.

7 If you want to ensure that you can use the LightsOut feature when you need it, check the Test installed LightsOut Restore check box.

While doing so requires a reboot of your computer, it could be worth the extra effort in the event that you need to utilize LightOut Restore from a remote location.

8 Click **Finish**.

Editing or rerunning the LightsOut Restore setup

You can run the LightsOut Restore Wizard again if you need to edit the configuration settings, or if you need to rebuild an existing, modified Symantec Recovery Disk.

To edit or rerun the LightsOut Restore setup

1 Start Backup Exec System Recovery, and then click **File > LightsOut Setup**.

2 Step through the wizard panels to make your changes.

3 When you are finished, click **Finish**.

4 Do one of the following:

- Click **Yes** to recopy all of the files.
- Click **No**.

Chapter 14

Recovering a computer

This chapter includes the following topics:

- About recovering a computer
- Starting a computer by using the recovery environment
- Preparing to recover a computer
- Recovering a computer
- Restoring multiple drives by using a system index file
- Recovering to a computer that has different hardware
- Recovering files and folders from the recovery environment
- Using the networking tools in the recovery environment
- Viewing properties of recovery points and drives
- About the Support Utilities

About recovering a computer

If Windows fails to start or does not run normally, you can recover your computer using the Symantec Recovery Disk and an available recovery point.

Note: If you can start Windows and the drive that you want to restore is a secondary drive (which is any drive other than your system drive, or the drive where your operating system is installed), you can restore the drive within Windows.

The Symantec Recovery Disk lets you run a recovery environment that provides temporary access to Backup Exec System Recovery recovery features. For example, you can access the Recover My Computer Wizard to restart the computer into its previous, usable state.

Note: If you purchased Backup Exec System Recovery from your computer manufacturer, some features in the recovery environment might not be available. For example, if the manufacturer installed the recovery environment on your computer's hard disk. Your manufacturer might also assign a keyboard key for the purpose of starting the recovery environment.

When you restart your computer, watch for instructions on your computer monitor, or refer to your manufacturer's instructions.

Starting a computer by using the recovery environment

The Symantec Recovery Disk lets you start a computer that can no longer run the Windows operating system. The Symantec Recovery Disk is included with Backup Exec System Recovery. When you boot your computer using the SRD CD, a simplified version of Windows starts that runs a recovery environment. In the recovery environment, you can access the recovery features of Backup Exec System Recovery.

Note: Depending on which version of the product you have purchased, the SRD is either included on your product CD, or as a separate CD. You should place the CD containing the SRD in a safe place. Should you lose the CD, you can create a new one if you have a CD burner. See *If driver validation fails* in the *Symantec Backup Exec™ System Recovery User's Guide*.

Note: The recovery environment requires a minimum of 512 MB of RAM to run. If your computer's video card is configured to share your computer's RAM, you might need more than 512 MB of RAM.

Also, if you are installing a multilingual version of the product, you must have a minimum of 768 MB of RAM to run the Symantec Recovery Disk.

To start your computer by using the Symantec Recovery Disk

1 If you store your recovery points on a USB device, attach the device now (for example, and external hard drive).

Note: You should attach the device before you restart the computer. Otherwise, the recovery environment might not detect it.

2 Insert the Backup Exec System Recovery CD into the media drive of the computer.

If Backup Exec System Recovery was installed by your computer manufacturer, the recovery environment already could be installed on your computer's hard drive. Either watch your computer monitor after the computer restarts for on-screen instructions, or refer to your manufacturer's documentation.

3 Restart the computer.

If you cannot start the computer from the CD, you might need to change the startup settings on your computer.

See “Configuring your computer to boot from a CD” on page 161.

4 As soon as you see the prompt “Press any key to boot from CD”, press a key to start the recovery environment.

Note: You must watch for this prompt. It can come and go quickly. If you miss the prompt, you must restart your computer again.

5 Read the license agreement, and then click **Accept**.

If you decline, you cannot start the recovery environment, and your computer will restart.

Configuring your computer to boot from a CD

To run Symantec Recovery Disk, you must be able to start your computer using a CD.

To configure your computer to boot from a CD

1 Turn on your computer.

2 As the computer starts, watch the bottom of the screen for a prompt that tells you how to access the BIOS setup.

Generally, you need to press the Delete key or a function key to start your computer's BIOS setup program.

3 In the BIOS setup window, select Boot Sequence, and then press **Enter**.

4 Follow the on-screen instructions to make the CD or DVD device be the first bootable device in the list.

5 Put your SRD CD into the CD drive, and then restart your computer.

Note: Depending on which version of the product you have purchased, the SRD is either included on your product CD, or as a separate CD. You should place the CD containing the SRD in a safe place. Should you lose the CD, you can create a new one if you have have a CD burner.

6 Save the changes and exit the BIOS setup to restart the computer with the new settings.

7 Press any key to start the recovery environment (Symantec Recovery Disk).

When you start your computer with the SRD CD in the drive, you will see a prompt telling you to “Press any key to boot from CD”. If you do not press a key within five seconds, your computer will attempt to start from the next bootable device listed in the BIOS.

Note: Watch carefully as the computer starts. If you miss the prompt, the computer will need to be restarted again.

Preparing to recover a computer

You should also scan your computer for viruses. You can run this scan using some versions of the Symantec Recovery Disk.

See “Checking your hard disk for errors” on page 162.

Checking your hard disk for errors

If you suspect that your hard disk is damaged, you can examine it for errors.

To check your hard disk for errors

1 In the Analyze panel, click **Check Hard Disks for Errors**.

2 Select the drive that you want to check.

3 Select any of the following options.

Automatically fix file system errors	Fixes errors on the selected disk. When this option is not selected, errors are displayed but are not fixed.
Find and correct bad sectors	Locates bad sectors and recovers readable information.

4 Click **Start**.

Recovering a computer

You can restore your computer within the recovery environment. If you have a recovery point for the hard drives that you want to recover, you can fully recover your computer or other hard drive back to the state it was in when the recovery point was created.

Note: If you want to restore a recovery point to a computer that uses different hardware, you should use the Restore Anyware feature.

See "Recovering to a computer that has different hardware" on page 168.

To recover your computer

1 Start the computer by using the Symantec Recovery Disk.

See "Starting a computer by using the recovery environment " on page 160.

2 On the Home panel, click **Recover My Computer**.

Note: If your recovery points are stored on a CD or DVD and you only have one CD/DVD drive, you can eject the Symantec Recovery Disk CD now. Insert the CD or DVD that contains your recovery points.

3 On the Welcome page of the wizard, click **Next**.

If the Symantec Recovery Disk cannot locate any recovery points, you are prompted to locate one.

Click **View by**, and then select one of the following options:

Date

Displays all of the discovered recovery points in the order in which they were created.

If no recovery points were discovered, the table will appear empty. You should then choose one of the remaining View by options.

Filename

Lets you browse to another location, for example, an external (USB) drive or removable media to select a recovery point (.v2i) file.

Select this option, and then do the following:

- Click **Browse**, locate and select a recovery point (.v2i file), and then click **Open**.
- If you select a network location, type your network credentials.
- Click **Finish**.

System

Displays a list of all of the drives on your computer and shows any associated recovery points. You can also select a system index file (.sv2i).

Select this option, and then do the following:

- Click **Browse**, locate and select a recovery point (.sv2i), and then click **Open**.
- If you select a network location, type your network credentials.
- Check each recovery point that you want to recover.
  If necessary, add, change, or remove recovery points from the list.
- Click **Finish**.

4. Select the drive that you want to recover.

   If you are recovering your computer, select the drive on which Windows is installed. On most computer systems, this drive is the C drive. In the recovery environment, the drive letters and labels might not match what appears in Windows. You might need to identify the correct drive based on its label, the name assigned to it, or by browsing the files and folders in the recovery point.

   See “Recovering files and folders from the recovery environment ” on page 173.

5 If you need to delete a drive to make space available to restore your recovery point, click **Delete Drive**.

When you click Delete Drive, the drive is only marked for deletion. The actual deletion of the drive takes place after you click Finish in the wizard.

If you change your mind before you click Finish, go back to the Target Drive page of the wizard, and then click **Undo Delete**.

6 Click **Next**, and then select the options that you want to perform during the recovery process, as follows:

Verify recovery point before restore	Verifies whether a recovery point is valid or corrupt it is restored. This option can significantly increase the time required for the recovery to complete.
Check for file system errors after recovery	Checks the restored drive for errors after the recovery point is restored.
Resize restored drive	Automatically expands the drive to occupy the target drive's remaining unallocated space.
Partition type	Sets the partition type as follows: ■ Primary partition: Because hard disks are limited to four primary partitions, select this type if the drive will have four or less partitions. ■ Logical partition: Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of your hard disk.
Set drive active (for booting OS)	Makes the restored drive the active partition (for example, the drive from which the computer starts). You should select this option if you are restoring the drive on which your operating system is installed.

Restore original disk signature

Restores the original, physical disk signature of the hard drive.

Disk signatures are included in Windows Server 2003, Windows 2000 Advanced Server, and Windows NT Server 4.0 Enterprise Edition (SP3 and later). Disk signatures are required to use the hard drive.

Select this option if either of the following situations are true:

- Your computer's drive letters are atypical (for example, assigned letters other than C, D, E, and so forth).
- You are restoring a recovery point to a blank hard drive.

Restore Master Boot Record (MBR)

Restores the master boot record. The master boot record is contained in the first sector of a physical hard disk. The MBR consists of a master boot program and a partition table that describes the disk partitions. The master boot program looks at the partition table of the first physical hard disk to see which primary partition is active. It then starts the boot program from the boot sector of the active partition.

This option is recommended only for advanced users and is available only if you restore a whole drive in the recovery environment.

Select this option if any of the following situations are true:

- You are restoring a recovery point to a new, blank hard disk.
- You are restoring a recovery point to the original drive, but the drive's partitions were modified since the recovery point was created.
- You suspect that a virus or some other problem has corrupted your drive's master boot record.

Preserve domain trust token on destination

Preserves the token that is used to authenticate a user or a computer on a domain. This option helps ensure that a recovered computer is recognized by a network domain after it is recovered.

The options that are available depend on the restore destination that you selected.

7 Click **Next** to review the restore options that you selected.

Note: The Restore Anyware pane appears if your recovery point was configured for use with the Restore Anyware feature. You should cancel the current operation and follow the instructions for using Restore Anyware.

See "Recovering to a computer that has different hardware" on page 168.

8 Check **Reboot when finished** if you want the computer to restart automatically after the recovery process finishes.

9 Click **Finish**.

10 Click **Yes** to restore the drive.

Restoring multiple drives by using a system index file

You can run the Recover My Computer wizard from the *Symantec Recovery Disk* to restore a computer that has multiple drives. This type of restore operation uses a system index file (*.sv2i*) to reduce the amount of time that is needed to restore the drives. When a recovery point is created, a system index file is saved with it. The system index file contains a list of the most recent recovery points, which includes the original drive location of each recovery point.

If you have suffered a catastrophic hard drive failure, you can also use Symantec Recovery Disk to perform a *bare metal recovery* of a computer.

To restore multiple drives using a system index file

1 Start the computer by using the Symantec Recovery Disk.

See "Starting a computer by using the recovery environment " on page 160.

Drive letters in the recovery environment might not match those in the Windows environment.

2 On the Home panel, click **Recover My Computer**.

3 Click **Next**.

4 Click **View by**, and then select **System**.

5 Click **Browse**, locate and select a system file (.sv2i), and then click **Open**.

The system index file is in the same location as the recovery point location.

6 If you select a network location, type your network credentials.

7. Check each recovery point that you want to recover.

   If necessary, add, change, or remove recovery points from the list.

8. Click **Finish**.

Recovering to a computer that has different hardware

The Symantec Backup Exec System Recovery Restore Anyware™ feature lets administrators restore a system drive of a Windows 2000/2003/XP/Vista computer that has different hardware than was found in the orginal computer from which the recovery point was made.

Restore Anyware lets you make the necessary changes for the system to be able to boot. Depending on your configuration, you may need to make additional changes for the computer to run exactly as it did previously.

About using Restore Anyware

You must install a fully licensed version of Symantec Backup Exec System Recovery to use the Restore Anyware feature. This feature is not available in the evaluation version.

Restore Anyware lets you restore a recovery point onto new hardware. For example, you can use Restore Anyware in the following scenarios:

- The motherboard fails
- You want to upgrade to new hardware from an older computer

This feature is used to recover drives only; it cannot be used to recover at a file and folder level.

Note: For more information about domain controller support, visit http://entsupport.symantec.com/docs/1544.

Warning: If you have an OEM license from your hardware vendor or a single-user license, you might be prompted to reactivate your Windows software by using your Windows product license key. Be aware that OEM and single-user licenses might have a limited number of activations. Verify that using Restore Anyware does not violate your operating system or application license agreements.

Keep in mind the following when using Restore Anyware:

- Performing Restore Anyware to hardware that is significantly different might require you to:

  - Add mass storage device drivers.
  - Install hotfixes for the Windows operating system that you restore.
  - Reactivate your Windows operating system when the system restarts.
  - Provide your license key when the system restarts.
  - Provide a local user name and password for the recovery point when the system restarts.

- When you restore a recovery point by using Restore Anyware, you might be prompted for the local administrator name and password. You should have this information ready before you perform the restore. Technical Support cannot restore a lost password.
- You cannot use Restore Anyware to restore a single recovery point to multiple computers. The product does not generate a unique SID for every computer.
- If you use Restore Anyware with a computer that uses a static IP address, you must manually reconfigure the computer once the restore is complete.
- Backup Exec System Recovery supports one NIC on a system. If you have a dual NIC system, you might need to manually configure the additional NICs to perform a restore through Restore Anyware.

Restoring a computer through Restore Anyware

Before you restore a computer by using Restore Anyware, you must save the recovery point that you want to use for the restore to a location that you can access (for example, to a location that you can browse to). During the restore, you might also be prompted to supply disk drivers, service packs, hotfixes, and so forth. You should have your Windows media CD available.

For more information about getting Restore Anyware drivers, go to the Symantec Knowledge Base at the following URL.

See document ID 2006020809453660 in the Symantec Knowledge Base.

Warning: Before you restore a computer through Restore Anyware, test your access to the recovery points in the recovery environment. You should ensure that you have access to SAN volumes and that you can connect to the network.

To restore a computer through Restore Anyware

1. Start the computer by using the Symantec Recovery Disk.

   See “Starting a computer by using the recovery environment ” on page 160.

2. On the Home panel, click **Recover My Computer**.

3. On the Welcome page of the wizard, click **Next**.

   If the Symantec Recovery Disk cannot locate any recovery points, you are prompted to locate one.

   Click **View by**, and then select one of the following options:

   Date

   Displays all of the discovered recovery points in the order in which they were created.

   If no recovery points were discovered, the table will appear empty. You should then choose one of the remaining View by options.

   Filename

   Lets you browse to another location, for example, an external (USB) drive or removable media to select a recovery point (.v2i) file.

   Select this option, and then do the following:

   - Click **Browse**, locate and select a recovery point (.v2i file), and then click **Open**.
   - If you select a network location, type your network credentials.

     See "About network credentials" on page 72.
   - Click **Finish**.

   System

   Displays a list of all of the drives on your computer and shows any associated recovery points. You can also select a system index file (.sv2i).

   Select this option, and then do the following:

   - Click **Browse**, locate and select a recovery point (.sv2i), and then click **Open**.
   - If you select a network location, type your network credentials.
   - Check each recovery point that you want to recover.

     If necessary, add, change, or remove recovery points from the list.
   - Click **Finish**.

4. Select the drive that you want to recover.

   If you are recovering your computer, select the drive on which Windows is installed. On most computer systems, this drive is the C drive. In the recovery environment, the drive letters and labels might not match what appears in Windows. You might need to identify the correct drive based on its label, the name assigned to it, or by browsing the files and folders in the recovery point.

   See "Recovering files and folders from the recovery environment " on page 173.

5 If you need to delete a drive to make space available to restore your recovery point, click **Delete Drive**.

When you click Delete Drive, the drive is only marked for deletion. The actual deletion of the drive takes place after you click Finish in the wizard.

If you change your mind before you click Finish, go back to the Target Drive page of the wizard, and then click **Undo Delete**.

6 Click **Next**.

7 Check **Use Restore Anyware (for recovery to different hardware)**.

8 Click **Next**.

Select the options that you want to perform during the recovery process, as follows:

Verify recovery point before restore	Verifies whether a recovery point is valid or corrupt it is restored. This option can significantly increase the time required for the recovery to complete.
Check for file system errors after recovery	Checks the restored drive for errors after the recovery point is restored.
Resize restored drive	Automatically expands the drive to occupy the target drive's remaining unallocated space.
Partition type	Sets the partition type as follows: ■ Primary partition: Because hard disks are limited to four primary partitions, select this type if the drive will have four or less partitions. ■ Logical partition: Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of your hard disk.
Set drive active (for booting OS)	Makes the restored drive the active partition (for example, the drive from which the computer starts). You should select this option if you are restoring the drive on which your operating system is installed.

Restore original disk signature

Restores the original, physical disk signature of the hard drive.

Disk signatures are included in Windows Server 2003, Windows 2000 Advanced Server, and Windows NT Server 4.0 Enterprise Edition (SP3 and later). Disk signatures are required to use the hard drive.

Select this option if either of the following situations are true:

- Your computer's drive letters are atypical (for example, assigned letters other than C, D, E, and so forth).
- You are restoring a recovery point to a blank hard drive.

Restore Master Boot Record (MBR)

Restores the master boot record. The master boot record is contained in the first sector of a physical hard disk. The MBR consists of a master boot program and a partition table that describes the disk partitions. The master boot program looks at the partition table of the first physical hard disk to see which primary partition is active. It then starts the boot program from the boot sector of the active partition.

This option is recommended only for advanced users and is available only if you restore a whole drive in the recovery environment.

Select this option if any of the following situations are true:

- You are restoring a recovery point to a new, blank hard disk.
- You are restoring a recovery point to the original drive, but the drive's partitions were modified since the recovery point was created.
- You suspect that a virus or some other problem has corrupted your drive's master boot record.

Preserve domain trust token on destination

Preserves the token that is used to authenticate a user or a computer on a domain. This option helps ensure that a recovered computer is recognized by a network domain after it is recovered.

The options that are available depend on the restore destination that you selected.

9 Click **Next** to review the restore options you have selected.

Note: The Restore Anyware pane appears if your recovery point was configured for use with the Restore Anyware feature. You should cancel the current operation and follow the instructions for using Restore Anyware.

See "Recovering to a computer that has different hardware" on page 168.

---

10 Check **Reboot when finished** if you want the computer restarted for you automatically when the recovery process finishes.

11 Click **Finish**.

12 Click **Yes** to restore the drive.

Recovering files and folders from the recovery environment

You can use the Symantec Recovery Disk to start your computer and to restore files and folders from within a recovery point.

The recovery environment includes several support utilities that you can run to troubleshoot networking or hardware issues. For example, you can ping a computer, renew IP addresses, or get information about a hard-disk partition table.

To recover files and folders from the recovery environment

1 Start the computer by using the Symantec Recovery Disk.

See "Starting a computer by using the recovery environment " on page 160.

2 Click **Recover**, and then click **Recover My Files**.

3 Do one of the following:

- If the Symantec Recovery Disk cannot locate any recovery points, you are prompted to locate one. In the Open dialog box, navigate to a recovery point, select one, and then click **Open**.
- If the Symantec Recovery Disk finds recovery points, select a recovery point from the list, and then click **OK**.

Note: If you have trouble finding the recovery points in a network location, in the File name box, type the name of the computer and share that holds your recovery points. For example, \\computer_name\share_name.

If you are still having problems, try entering the computer's IP address.

Using the networking tools in the recovery environment .

4 In the tree view pane of the Recovery Point Browser, double-click the drive that contains the files or folders that you want to restore to expand it.

5 In the content pane of the Recovery Point Browser, do one of the following to select the files or folders that you want to restore.

To select all items	Press **Ctrl+A.**
To select a group of files that are next to each other	Select the top file, press **Shift**, and then select the last file in the list.
To select a group of files that are not next to each other	Press **Ctrl** as you select the files.

6 Click **Recover Files**.

Where possible, the Recover Items dialog box automatically completes the Restore to this folder box with the original path from which the files originated.

If the original location does not include a drive letter you must type the drive letter at the beginning of the path.

Note: While in the recovery environment, drive letters and labels might not match what appears in Windows. You might have to identify the correct drive based on its label, which is the name assigned to it.

7 If the original path is unknown or you want to restore the selected files to a different location, click **Browse** to locate the destination.

8 Click **Recover** to restore the files.

9 Click **OK** to finish.

Exploring your computer

You can explore the files and folders on your computer from the recovery environment by using the Explore My Computer feature.

This feature uses the Recovery Point Browser and functions similarly to Windows Explorer. You can browse the file structure of any drive that is attached to your computer from the recovery environment.

To explore your computer

◆ In the Analyze pane, click **Explore My Computer**.

Using the networking tools in the recovery environment

If you store your recovery points on a network, you need access to the network to restore your computer or your files and folders from the recovery environment.

Note: Additional computer memory might be required to recover your computer across a network.

Starting networking services

If you need to start networking services, you can do so manually.

To start networking services

◆ On the Network panel, click **Start My Networking Services**.

  To verify the connection to the network, you can map a network drive.

  See "Mapping a network drive in the recovery environment " on page 177.

Using the pcAnywhere thin host for a remote recovery

The Symantec Recovery Disk includes a pcAnywhere thin host, which lets you remotely access a computer in the recovery environment. The pcAnywhere thin host contains the minimum settings that are needed to support a single-use remote control session. The thin host requires an IP address for hosting a remote control session.

Note: You cannot deploy a thin host to the recovery environment. The thin host can only be started from Symantec Recovery Disk to host a remote control session in the recovery environment. The thin host in Symantec Recovery Disk does not support file transfers and cannot be used to add drivers for network or storage devices.

To start the pcAnywhere thin host

After you start the thin host from the Symantec Recovery Disk, it waits for a connection from a remote computer. You can connect to the thin host to remotely manage a recovery or to perform other tasks in the recovery environment. You must use Symantec pcAnywhere to connect to the thin host.

To start the pcAnywhere thin host

◆ On either the Home or Network panels in the recovery environment, click **Start the pcAnywhere Thin Host**.

  The networking services are started if necessary. The thin host waits for a connection.

Remotely connecting to the thin host

Symantec pcAnywhere lets you remotely connect to a computer that is running in the recovery environment. The computer must be running the pcAnywhere thin host that is included in the Symantec Recovery Disk, and it must be waiting for a connection. Once connected, the client computer can remotely manage a recovery or perform other tasks that are supported in the recovery environment.

Note: The client computer cannot transfer files or add additional drivers for network or storage devices on the computer that is running the thin host.

To remotely connect to the thin host

1. Ensure that the computer to be remotely managed (the host) has started in the recovery environment and that the pcAnywhere thin host is waiting for a connection.
2. Obtain the IP address of the thin host computer.
3. On the client computer, in Symantec pcAnywhere, configure a remote connection item.

   For more information, see the *Symantec pcAnywhere User's Guide*.

   Note: You do not need to choose to automatically login to the host on connection.

   ---

4. When you configure the connection in pcAnywhere, do the following:
   - Select TCP/IP as the connection type.
   - Specify the IP address of the host computer.

- Choose to automatically login to the host on connection.
  If you do not include the login information, you are prompted for it when you connect to the thin host.
- Type the following login name:
  symantec
- Type the following password:
  recover

The thin host shuts down when there is an attempt to connect by using any incorrect configuration settings.

To prevent unauthorized users from tampering with your settings or launching a session without your permission, set a password for your remote connection item.

This option is available in the Remote Properties window on the Protect Item tab. The thin host does not support encryption.

5 In pcAnywhere, start the remote control session.

If the connection attempt is unsuccessful, the thin host must be restarted on the host computer before you make another attempt to connect.

6 Remotely perform the necessary tasks on the host computer.

The remote control session ends when the thin host is closed, when the thin host computer is restarted, or when the remote control session is ended.

After the host computer starts Windows, the client computer can deploy and connect a thin host on the computer to verify the success of tasks that were performed in the recovery environment.

Mapping a network drive in the recovery environment

If you started the networking services after you started the recovery environment, you must map a network drive. This lets you browse to that drive and select the recovery point that you want to restore.

If there is no DHCP server or the DHCP server is unavailable, you must provide a static IP address and a subnet mask address for the computer on which you are running Symantec Recovery Disk.

See “Configuring network connection settings ” on page 178.

After you provide the static IP address and subnet mask address, you can enter the recovery environment. However, because there is no way to resolve computer names, when you run the Recover My Computer Wizard or the Recovery Point Browser, you can only browse the network by using the IP addresses to locate a recovery point. You can map a network drive so that you can locate the recovery points more effectively.

To map a network drive in the recovery environment

1 In the recovery environment main window, click **Network**, and then click **Map a network drive**.

2 Map a network drive by using the UNC path of the computer on which the recovery point is located.

For example: **\\computer_name\share_name** or **\\IP_address\share_name**

Configuring network connection settings

You can access the Network Configuration window to configure basic network settings while running in the recovery environment.

To configure network connection settings

1 In the recovery environment main window, click **Network**, and then click **Configure Network Connection Settings**.

2 If you are prompted to start networking services, click **Yes**.

Getting a static IP address

If you want to restore a recovery point that is located on a network drive or share, but you are unable to map a drive or browse to the drive/share on the network (usually caused by the lack of an available DHCP service), you can assign a unique static IP address to the computer that is running the recovery environment. You can then map to the network drive or share.

To get a static IP address

1 In the Network Adapter Configuration box, click **Use the following IP address**.

2 Specify a unique IP address and subnet mask for the computer that you want to restore.

Be sure that the subnet mask matches the subnet mask of the network segment.

3 Click **OK**.

4 Click **Close** to return to the recovery environment's main menu.

5 In the Network pane, click **Ping a Remote Computer**.

6 Type the address of the computer that you want to ping on the network segment.

7 Click **OK**.

If you specified a computer name or a computer name and domain as the address method, make note of the IP address that is returned from the computer that you pinged.

If communication to the storage computer is operating as expected, you can use the Map Network Drive utility to map a drive to the recovery point location.

Getting a static IP address if the ping is unsuccessful

If you ping an address and the address does not respond, you can use the ipconfig /all command to determine the correct IP address.

To get an IP address if the ping is unsuccessful

1 On the computer that contains the recovery point that you want to restore, at a DOS prompt, type the following command, and then press **Enter**.

ipconfig /all

2 Write down the IP address that is displayed.

3 Return to the computer that is running the recovery environment and run the utility Ping Remote Computer with this IP address.

Viewing properties of recovery points and drives

You can view the properties of recovery points and the drives that are contained in them.

- Viewing properties of a recovery point
- Viewing the properties of a drive within a recovery point

Viewing properties of a recovery point

You can view various properties of a recovery point by using the Recovery Point Browser. The following properties are available for viewing:

Description	A user-assigned comment associated with the recovery point
Size	The total size (in megabytes) of the recovery point
Created	The date and time that the recovery point file was created

Compression	The compression level that is used in the recovery point
Spanned	Whether the entire recovery point file is spanned over several files
Password protected	The password protection status of the selected drive
Encryption	The encryption strength that is used with the recovery point
Format	The format of the recovery point
Computer name	The name of the computer on which the recovery point was created
Restore Anyware	If Restore Anyware was enabled for the recovery point, this property is displayed.
Catalogued	If you enabled search engine support for the recovery point, this property is displayed.
Created by	Identifies the application (Backup Exec System Recovery) that was used to create the recovery point.

To view the properties of a recovery point

1. In the Recovery Point Browser, in the tree panel, select the recovery point that you want to view.
2. Do one of the following:
   - On the File menu, click **Properties**.
   - Right-click the recovery point, and then click **Properties**.

Viewing the properties of a drive within a recovery point

You can view the following properties of a drive within a recovery point:

Description	A user-assigned comment associated with the recovery point.
Original drive letter	The original drive letter that was assigned to the drive.
Cluster size	The cluster size (in bytes) that is used in a FAT, FAT32, or NTFS drive.
File system	The file system type that is used within the drive.
Primary/Logical	The selected drive's drive status as either the primary partition or the logical partition.

Size	The total size (in megabytes) of the drive. This total includes used and unused space.
Used space	The amount of used space (in megabytes) within the drive.
Unused space	The amount of unused space (in megabytes) within the drive.
Contains bad sectors	Indicates if there are any bad sectors on the drive.

To view the properties of a drive within a recovery point

1. In the Recovery Point Browser, in the tree panel, double-click the recovery point that contains the drive that you want to view.
2. Select a drive.
3. Do one of the following:
   - On the menu bar, click **File** > **Properties**.
   - Right-click the recovery point, and then click **Properties**.

About the Support Utilities

The recovery environment has several support utilities that Symantec Technical Support might ask you to use to troubleshoot any hardware issues that you encounter.

You might be required to supply the information that is generated by these utilities if you call Symantec Technical Support for help resolving problems.

Note: You should only use these tools as directed by Symantec Technical Support.

Chapter 15

Copying a drive

This chapter includes the following topics:

About copying a drive

You can use the Copy Drive feature to copy your operating system, applications, and data from one hard drive to another hard drive.

You can even copy a larger hard drive to a smaller hard drive if the data on the drive being copied is at least 1/16th smaller in size than the total size of the new drive.

If the hard drive that you want to copy contains more than one partition, you must copy the partitions one at a time to the new hard drive.

You can use the Copy Drive feature when you upgrade to a larger hard drive or when you add a second hard drive. You should not use the Copy Drive feature to set up a hard drive that will be used in another computer. The drivers that are used to run the hardware on one computer will likely not match the drivers on a second computer.

See “Recovering to a computer that has different hardware” on page 168..

Note: You must install a fully licensed version of Symantec Backup Exec System Recovery before you can use the Copy Drive feature. This feature is not available in the evaluation version.

Preparing to copy drives

Before you can copy drives, you must have the hardware configured correctly.

To prepare to copy drives

1 Do all of the following:

- Prepare the computer.
- Get the manufacturer's directions for installing the drive.
- Shut down the computer, and then disconnect the power cord.
- Discharge electricity by touching a grounded metal object.
- Remove the computer cover.

2 Change the jumper settings on the hard drive to make the new hard drive the slave drive, or connect it as the slave drive if you are using cable select instead of jumper settings to determine the master and slave drives.

3 Do the following to attach the new hard drive:

- Connect the cable so that the colored stripe on the edge lines up with the I/O pins on the motherboard.
  The motherboard is marked Pin1 or 1 where the colored stripe should go.
- Connect the other end of the cable to the back of the hard drive, and match the striped edge with the I/O pin position on the drive itself.
  The I/O pin is usually on the side closest to the power supply.

4 Attach the power connector to the new hard drive.

Make sure that the angled edge of the plastic connector lines up with the angled edge of the pin socket.

5 Anchor the drive in the bay area according to the manufacturer's instructions.

6 Do the following to change the BIOS settings to recognize the new hard drive:

- Open the BIOS setup. As the computer starts, watch the computer screen for instructions on how to open the BIOS setup.
- Select Auto Detect for both the master and slave drives.
- Save the BIOS changes, and then exit.
  Your computer will restart automatically.

Copying one hard drive to another hard drive

After you install a new hard drive, you can copy your old hard drive to the new one. The new hard drive does not need to be formatted.

If the hard drive that you want to copy contains more than one partition, you must copy each partition, one at a time, to the new hard drive.

If the power or the hardware fails while you copy the data, no data is lost from the source drive. However, you must restart the copying process.

Note: This feature is not available in the evaluation version of the product.

To copy one hard drive to another hard drive

1. On the Tools page, click **Copy My Hard Drive**.
2. Complete the steps in the wizard to copy the drive.

   The wizard steps you through the process of selecting the right drive to copy, selecting the destination drive, and selecting the options for copying the data from one drive to another.

Drive-to-drive copying options

When you copy a drive from one hard drive to another, you can use the drive-to-drive copying options.

Table 15-1 describes the options for copying from one hard drive to another.

Table 15-1 Drive-to-drive copying options

Option	Description
Check source for file system errors	Check the source drive for errors before you copy it. The source drive is the original drive.
Check destination for file system errors	Check the destination drive for errors after you copy the drive. The destination drive is the new drive.
Resize drive to fill unallocated space.	This option automatically expands the drive to occupy the destination drive's remaining unallocated space.

Table 15-1 Drive-to-drive copying options *(continued)*

Option	Description
Set drive active (for booting OS)	Make the destination drive the active partition (the drive from which the computer starts). Only one drive can be active at a time. To boot the computer, it must be on the first physical hard disk, and it must contain an operating system. When the computer boots, it reads the partition table of the first physical hard disk to find out which drive is active. It then boots from that location. If the drive is not bootable or you are not certain if it is, have a boot disk ready. You can use the Symantec Recovery Disk. The Set drive active option is valid for basic disks only (not dynamic disks).
Disable SmartSector copying	The SmartSector technology from Symantec speeds up the copying process by only copying the clusters and sectors that contain data. However, in a high-security environments, you might want to copy all clusters and sectors in their original layout, regardless of whether they contain data.
Ignore bad sectors during copy	This option copies the drive even if there are errors on the disk.
Copy MBR	This option copies the master boot record from the source drive to the destination drive. Select this option if you are copying the C:\ drive to a new, empty hard drive. You should not select this option if you want to copy a drive to another space on the same hard drive as a backup. You should also not select this option if you want to copy the drive to a hard drive that has existing partitions that you do not want to replace.
Destination partition type	Click Primary partition to make the destination (new) drive a primary partition. Click Logical partition to make the destination (new) drive a logical partition inside an extended partition.
Drive letter	Select the drive letter you want assigned to the partition from the Drive letter drop-down list

Appendix A

Using a search engine to search recovery points

This appendix includes the following topics:

- About using a search engine to search recovery points
- Enabling search engine support
- Recovering files using Google Desktop's Search Desktop feature

About using a search engine to search recovery points

Backup Exec System Recovery supports the use of Google Desktop for searching for file names that are contained in recovery points.

Note: Symantec Backup Exec Retrieve is also supported, but it must be installed by your company's IT department. When they install it, there is nothing you have to do to enable it. Ask your IT department for details.

When a backup runs, Backup Exec System Recovery generates a catalog of all of the files that are included in the recovery point. Google Desktop can then use the catalog to generate an index of the files that are contained in each recovery point.

When you enable search engine support, Backup Exec System Recovery creates a catalog of all of the files that are contained in a recovery point. Search engines like Google Desktop use the catalog file generate an index. You can then search for files by name. Google Desktop does not index the content of files. It only indexes the file names.

Enabling search engine support

To use this feature with a search engine, such as Google Desktop, you must do all of the following:

Install a search engine	Backup Exec Retrieve is installed by an organization's IT department. Ask your IT department if it is available. You can download and install Google Desktop for free from the Internet. Visit desktop.google.com. See "To install Google Desktop" on page 189.
Enable Google Desktop support	A Google plug-in for Backup Exec System Recovery is required before you can use Google Search to locate and recover files. The plug-in is installed for you automatically when you enable this feature. See "To enable Google Desktop support" on page 189.
Enable search engine support when defining or editing a backup job	When you define a backup job, or edit an existing backup job, enable search engine support. The next time the backup is run, it creates a list of all files contained in the resulting recovery point. A search engine, such as Google Desktop, can then use the list to generate its own index, enabling you to perform searches by file name. See "To enable search engine support for a backup job" on page 189.

Note: Recovery points that already exist when you enable this feature cannot be indexed. This restriction is because the generated list of files that are required by search engines for generating searchable indexes are appended to recovery points as they are created. After you enable this feature, run each of your backups in order to create a new recovery point that contains the required information for indexing.

Note: If your backup destination is on a network drive, be sure to add the location to the Google Desktop preferences.

To install Google Desktop

1. Start Backup Exec System Recovery.
2. Click **Tasks > Options > Google Desktop**.
3. Click **Download Google Desktop from the Web** and follow instructions for installation.
4. Once installed, click **OK** in the Backup Exec System Recovery Options window.

   For more information, visit desktop.google.com.

To enable Google Desktop support

1. Start Backup Exec System Recovery.
2. Click **Tasks > Options > Google Desktop**.
3. Check **Enable Google Desktop File and Folder Recovery**.
4. Click **OK**.

   This option is not available if you do not have Google Desktop installed. Install Google Desktop, and then repeat this procedure.
5. Click **OK** to install the Google Plugin.

To enable search engine support for a backup job

1. Start Backup Exec System Recovery.
2. Do one of the following:
   - Edit an existing backup job and check **Enable search engine support for Google Desktop and Backup Exec Retrieve** on the Options page of the wizard.
   - Define a new backup job and check **Enable search engine support for Google Desktop and Backup Exec Retrieve** on the Options page of the wizard.

Recovering files using Google Desktop's Search Desktop feature

If you have correctly set up and enabled support for Google Desktop, you can search recovery points to located and recover files using Google Desktop.

See “Enabling search engine support” on page 188.

To recover files using Google Desktop

1. Start Google Desktop.
2. Enter the name (or part of the name) of a file you want to recover, and then click **Search Desktop**.
3. Click the search result containing the file you want to recover.
4. When the file opens in the associated application, click **File > Save As** to save the recovered file.

   You can also right-click the search result and click Open to open the recovery point in the Recovery Point Browser.

   See "Opening files within a recovery point" on page 129.

If a file cannot be found using Google Desktop

If you are certain that your file is included in a recovery point that has search engine support enabled, but the file is not found, do the following:

- Right-click the Google Desktop icon in the system tray and click Indexing > Re-Index.
  Re-indexing can take a significant amount of time. Be sure to wait until it completes before attempting to search again.
- Right-click the Google Desktop icon in the system tray and click Preferences.
  Under Search Types, verify that Web history is checked. This option must be checked or Google Desktop cannot index the content of your recovery points.
- Verify that the drive containing your recovery points (backup destination) is available.
  For example, if your backup destination is on a USB drive, be sure that the drive is plugged in and that the power is turned on. Or, if your backup destination is on a network, be sure you are connected and logged in with the correct credentials.
- Adding **v2i** to the search string to narrow down the number of search results. For example, if you are searching for My Tune mp3, add v2i so that the search string is **My Tune mp3 v2i**.
  Recovery point files use .v2i as their file extension name. Adding it to the search string eliminates search results that are not found in a recovery point.
- If your backup destination is on a network drive, be sure to add the location to the Search These Locations setting in Google Desktop Preferences.

Backing up VSS-aware databases

This appendix includes the following topics:

About backing up VSS-aware databases

Symantec Backup Exec System Recovery integrates with Microsoft Volume Shadow Copy Service (VSS) to automate the process of backing up VSS-aware databases like production Exchange 2003, transaction logs on Exchange 2003, and Windows 2003 Domain Controller.

VSS-aware databases are auto-enabled and cannot be turned off. VSS lets administrators create a shadow copy backup of volumes on a server. The shadow copy includes all files and includes open files.

When it creates a recovery point, Backup Exec System Recovery alerts the Volume Shadow Copy Service. VSS then puts the VSS-aware databases into a temporary sleep state. While in this quiesced state, the database continues to write to transaction logs while it is being backed up. Once the databases are quiesced, Backup Exec System Recovery takes the snapshot. VSS is then notified that the snapshot is completed. The databases are awakened, and the transaction logs continue to be committed to the database. Meanwhile, the recovery point is created. The databases are only quiesced for the snapshot, and are active for the rest of the recovery point creation.

Backup Exec System Recovery supports VSS Exchange Server 2003, which implements Microsoft's Volume Shadow Copy Service (VSS) technology. There are known issues that if the database load is heavy, the VSS request might be ignored.

Create recovery points at the lightest load time. There are known VSS issues that are resolved in 2003 Service Pack 1, and also the Exchange 2003 Service Pack 1.

Backup Exec System Recovery performs traditional Exchange server maintenance as follows:

1. VSS makes a call to quiesce the database.

2. The API calls are made to perform Exchange database maintenance.

3. The snapshot is used to capture the recovery point.

4. The database and other procedures on the system continue in parallel.

Note: Database operations are not interrupted.

Recommended use of Backup Exec System Recovery with Exchange Databases

Additional backup applications are not needed to run with Backup Exec System Recovery.

Note: NTbackup incrementals might not function properly.

About backing up non-VSS-aware databases

With Backup Exec System Recovery, you can create manual or automatic cold recovery points or hot recovery points of non-VSS-aware databases.

Creating a cold recovery point manually

A manual cold (or offline) recovery point ensures that all database transactions are committed to the hard disk. You can then use Backup Exec System Recovery to create the recovery point, and then restart the database.

To create a cold recovery point manually

1. Stop the database manually.
2. Use Backup Exec System Recovery to run a backup immediately using the Run Backup or One-time Backup feature.

   See “Running a One Time Backup” on page 69.

   Backup Exec System Recovery instantaneously snaps a “virtual volume recovery point” of the database.
3. Manually restart the database anytime after the recovery point progress bar appears in the Monitor page of the console.

   While the database is restarted, the actual recovery point is already being created from the virtual volume recovery point.

Creating a cold recovery point automatically

When you automate the creation of a cold recovery point of a non-VSS-aware database, you run a command file in the backup job, before data capture, to stop (quiesce) the database momentarily and commit all transaction logs to the hard disk. Backup Exec System Recovery will then instantaneously snap a “virtual volume recovery point.” A second command file is run in the backup to automatically restart the database while the recovery point is created from the virtual volume recovery point.

Because the virtual volume snapshot takes only a few seconds to create, the database is in the recovery point state momentarily, resulting in a minimal number of created log files.

Note: In cases where the domain controller is running on a Windows 2000 server without VSS support, the Active Directory database must first be backed up using NTbackup prior to using Backup Exec System Recovery to protect the full system. This process can be automated by running command files in the backup.

See “Run command files during a backup ” on page 72.

To create a cold recovery point automatically

1. Define a backup that includes command files that you have created for the following stages of the recovery point:

Before data capture	A command file that stops the database.
After data capture	A command file that restarts the database.

2. Use Backup Exec System Recovery to run the backup job that includes the command files.

Creating a hot recovery point

If a cold recovery point is not possible in your organization, the next available option for backing up non-VSS-aware databases is a hot (or online) recovery point.

Backup Exec System Recovery takes a “crash consistent” recovery point. Such a recovery point is equivalent to the state of a system that was running when the power failed. A database that can recover from this type of failure can be recovered from a “crash consistent” recovery point.

To create a hot recovery point

◆ Use Backup Exec System Recovery to create a recovery point without stopping or restarting the database.

  Backup Exec System Recovery instantaneously snaps a “virtual volume recovery point” from which the recovery point is created.

About Active Directory

This appendix includes the following topics:

- The role of Active Directory

The role of Active Directory

When protecting a domain controller with Symantec Backup Exec System Recovery, be aware of the following:

- If your domain controller is Windows Server 2003, it supports VSS. Backup Exec System Recovery will automatically call VSS to prepare the Active Directory database for backup. Windows 2000 Domain Controllers do not support VSS. In cases where the domain controller is running on a Windows 2000 server, the Active Directory database must be backed up using NTbackup prior to using Backup Exec System Recovery to protect the full system. This process can be automated using an external command that is called by Backup Exec System Recovery. When configuring a job, you have the option to enter external commands. This provides a simple process for protecting domain controllers that do not support VSS.

  See "Run command files during a backup " on page 72.

- In order to participate on a domain, every domain computer must negotiate a trust token with a domain controller. This token is refreshed every 30 days by default. This time frame can be changed, and is referred to as a secure channel trust. But a trust token contained in a recovery point cannot be updated by the domain controller automatically. Therefore, when a computer is recovered using a recovery point that contains an out dated token, the recovered computer cannot participate in the domain until it has been added to the domain by someone who has the required credentials.

  In Backup Exec System Recovery, this trust token can be re-established automatically if the computer is currently participating in the domain at the time the recovery process is started.

- In most cases, domain controllers should be restored non-authoritatively. This will prevent outdated objects in the Active Directory from being restored. Outdated objects are referred to as tombstones. Active Directory will not restore data older than the limits it sets. Restoring a valid recovery point of a domain controller is the equivalent of a non-authoritative restore. To determine which type of restore you want to perform, please refer to the Microsoft documentation. A non-authoritative restore will prevent tombstone conflicts.

For additional details about protecting non-VSS aware domain controllers, see the white paper titled "Protecting Active Directory," located on the Web.

http://sea.symantec.com/protectingdc

You can also refer to the Symantec Knowledge Base

http://entsupport.symantec.com/docs/1544

Index