Symantec™ System Recovery 2011 User's Guide

Windows Edition

✔Symantec™

Symantec System Recovery 2011 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: 9.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

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 features and functionality. The Technical Support group also creates 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
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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 replicate 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/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

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 assurance and maintenance contracts

- Information about the Symantec Buying Programs

- 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	customercare_apac@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 is 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

Introducing Symantec™ System Recovery 2011

This chapter includes the following topics:

- About Symantec System Recovery
- About the components of Symantec System Recovery
- What is new in Symantec System Recovery 2011
- Accessing Help & Support for Symantec System Recovery
- Sending your feedback regarding Symantec System Recovery 2011

About Symantec System Recovery

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

Symantec System Recovery captures a recovery point of the entire live Windows system. The backup includes the operating system, applications, system settings, files, and other items. The recovery point can be conveniently saved to various media or disk storage devices including SAN, NAS, Direct Attached Storage, RAID, Blu-ray/DVD/CD, and so forth. When systems fail, you can quickly restore them without the need for manual, lengthy, and error-prone processes.

You can manage Symantec System Recovery remotely using one of the following:

■ Another licensed copy of Symantec System Recovery

■ Symantec System Recovery Management Solution (sold separately)

Symantec System Recovery Management Solution is a centralized management application. It provides IT administrators an at-a-glance view of system recovery jobs across your entire organization. You can centrally deploy, modify, and maintain recovery activities, jobs, and policies for local and remote systems. You can also monitor real-time status and quickly resolve any problems that are identified.

Symantec System Recovery integrates with Google™ Desktop and Backup Exec Retrieve to enable recovery of your files without IT intervention.

Using the integrated **Granular Restore Option**, you can quickly restore individual Microsoft® Exchange emails, folders, and mailboxes.

See "About the components of Symantec System Recovery" on page 18.

See "What is new in Symantec System Recovery 2011 " on page 19.

About the components of Symantec System Recovery

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

Table 1-1   Key product components

Key component	Description
Symantec System Recovery program (user interface)	The Symantec 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. You can then use the recovery points to recover your entire computer, or individual drives, files, and folders.
	The Symantec System Recovery also lets you do the following:
	■ Manage the size of the recovery point storage (backup destination) so that you can use your computer's valuable disk space for other purposes.
	■ Monitor the backup status of your computer to make sure that your valuable data is backed up on a regular basis.

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

Key component	Description
Symantec System Recovery Disk	The Symantec System Recovery Disk is used to start your computer in the recovery environment. If your computer's operating system fails, use Symantec System Recovery Disk to recover your *system drive* (the drive where your operating system is installed).
	Note: Depending on which version of the product you have purchased, Symantec System Recovery Disk is either included on your product CD, or as a separate CD. You should place the CD that contains Symantec System Recovery Disk in a safe place.
	See "About recovering a computer" on page 227.

See "About Symantec System Recovery" on page 17.

See "What is new in Symantec System Recovery 2011 " on page 19.

What is new in Symantec System Recovery 2011

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

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

Table 1-2   What is new in Symantec System Recovery 2011

Feature	Description
Improved support for virtual formats	Symantec System Recovery now includes support for the following virtual platforms: ■ VMware ESX 4.1i ■ VMware ESX 4.1 ■ Citrix XenServer 5.5 and 5.6
Improved platform support	Symantec System Recovery now includes support for the following platforms: ■ Microsoft Exchange Server 2010 SP1 ■ Microsoft SharePoint 2010 ■ Microsoft SQL Server 2008 R2

Table 1-2   What is new in Symantec System Recovery 2011 *(continued)*

Feature	Description
Create custom Symantec System Recovery Disk on a USB device.	Symantec System Recovery now enables you to create a custom Symantec System Recovery Disk on a USB device.
Use ISO image file for creating custom Symantec System Recovery Disk.	Symantec System Recovery now lets you use an Symantec System Recovery Disk ISO image file directly for creating a custom Symantec System Recovery Disk. Until now you were required to extract the ISO image file for creating a custom Symantec System Recovery Disk.
Add 64-bit drivers to the custom Symantec System Recovery Disk.	You can now add 64-bit drivers to the custom Symantec System Recovery Disk. The 64-bit drivers are used only for restoring a recovery point of a 64-bit operating system on a computer with different hardware. **Note:** Symantec System Recovery Disk does not use 64-bit drivers for starting a computer. To start a computer having a 64-bit operating system using Symantec System Recovery Disk the equivalent 32-bit drivers are required.

See "About Symantec System Recovery" on page 17.

See "About the components of Symantec System Recovery" on page 18.

Accessing Help & Support for Symantec System Recovery

To learn more about Symantec System Recovery, visit the **Help and Support** page. The **Help and Support** page provides access to the product's Help system and the User's Guide. It also includes access to the Symantec Knowledge Base where you can find troubleshooting information.

To access Help & Support

1   Start Symantec System Recovery.

2   On the **Help** menu, click **Help and Support**.

See "About Symantec System Recovery" on page 17.

Sending your feedback regarding Symantec System Recovery 2011

Please take a moment to share your feedback and ideas with Symantec regarding Symantec System Recovery 2011.

To send feedback

◆ Do one of the following:

■ Click **Share Your Ideas** in the upper-right corner of the Symantec System Recovery 2011 window.

■ On the **Help** menu, click **Share Your Ideas**.

See "About Symantec System Recovery" on page 17.

Installing Symantec System Recovery

This chapter includes the following topics:

- Before you install Symantec System Recovery

- Installing Symantec System Recovery

- Updating Symantec System Recovery with LiveUpdate

- About uninstalling Symantec System Recovery

Before you install Symantec System Recovery

Installation procedures might vary, depending on your work environment and which installation options you choose. This chapter focuses on installing the full version of Symantec System Recovery from the installation CD.

Before you install Symantec System Recovery, ensure that your computer meets the system requirements. Review the Readme file on the installation CD for any known issues.

See "System requirements for Symantec System Recovery" on page 23.

System requirements for Symantec System Recovery

The following table lists the system requirements for Symantec System Recovery to function properly.

Table 2-1   Minimum system requirements

Component	Minimum requirements
Operating system	The following Windows 32-bit or 64-bit operating systems are supported: ■ Windows 7 (all editions) ■ 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 (SP2 or later) ■ Windows Server 2003 ■ Windows Small Business Server 2003 ■ Windows Server 2008, including SP1 ■ Windows Server 2008 R2 ■ Windows Essential Business Server 2008 ■ Windows Small Business Server 2008
RAM	The following list indicates the memory requirements for each component of Symantec System Recovery: ■ Symantec System Recovery Agent: 512 MB ■ Symantec System Recovery user interface and Recovery Point Browser: 512 MB ■ Symantec System Recovery Disk: 1 GB (dedicated) ■ LightsOut Restore: 1 GB
Available hard disk space	The following list indicates the hard disk space requirements for Symantec System Recovery and other items: ■ When you install the entire product: Up to 430 MB is required for a full install, depending on the language of the product you select. ■ 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 that is stored. ■ LightsOut Restore: 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 being used as the startup drive from the BIOS.
	Symantec System Recovery uses Gear Software technology. To verify that your CD writer or DVD writer is compatible, visit the Gear Software Web site.
	http://www.gearsoftware.com
	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 or later is required to run Symantec System Recovery.
	If .NET Framework is not already installed, you are prompted to install it after Symantec System Recovery is installed and your computer is restarted.
	If you want to be able to restore email using the **Granular Restore Option**, you must have Microsoft Outlook 2003, 2007, or 2010 installed.
Virtual platforms (for converted recovery points)	The following virtual platforms are supported:
	■ VMware Workstation 4, 5, 6, and 6.5
	■ VMware ESX 3.0, 3.5, 4.0, and 4.1
	■ VMware ESX 3.5i , 4.0i, and 4.1i
	■ VMware Server 1
	■ VMware GSX Server 3.x (replaced by VMware Server)
	■ Microsoft Virtual Server 2005 R2 and later
	■ Microsoft Hyper-V 1.0 and 2.0
	■ Citrix XenServer 5.5

Note: Windows 2000 Server/Advanced Server, and Windows Small Business Server 2000 are not supported in Symantec System Recovery 2011. You can still use Backup Exec System Recovery 8.5 on these versions of Windows 2000. You can also perform backup and restore functions remotely on Windows 2000 computers using Symantec System Recovery 2011 or Symantec System Recovery 2011 Management Solution.

About supported file systems and removable media

Symantec System Recovery supports the following file systems and removable media:

Supported file systems	Symantec System Recovery supports the following file systems: ■ FAT16, FAT16X ■ FAT32, FAT32X ■ NTFS ■ GUID partition table (GPT) ■ Dynamic disks ■ Linux Ext2, Linux Ext3 ■ 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 Symantec System Recovery is installed). Or, you can save recovery points to most Blu-ray, DVD-R(W), DVD+RW, CD-R, and CD-RW recorders. You can find an updated list of supported drives on the Gear Software Web site. http://www.gearsoftware.com Symantec System Recovery also lets you save recovery points to most USB devices, 1394 FireWire devices, REV, Jaz, Zip drives, and magneto-optical devices.

See "System requirements for Symantec System Recovery" on page 23.

About the availability of features in Symantec System Recovery

Symantec 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 the features that are included with your version of Symantec System Recovery.

See "About Symantec System Recovery Basic Edition" on page 27.

About Symantec System Recovery Basic Edition

The following features are not available in Symantec System Recovery Basic Edition. If you want to use these features, upgrade to the full version of Symantec System Recovery.

Table 2-2   Disabled features

Disabled feature	Description
Centralized manageability	Allows Symantec System Recovery Management Solution to remotely monitor and manage installations of Symantec System Recovery that are found on a network. It also includes the ability to remotely back up and recover data.
Recovery point sets	Captures an initial, full backup of a drive. Additional backups only capture the changes that were made to data on the drive since the full backup was performed. Without this feature, you can create only independent recovery points (full backups) of a drive.
Copy My Hard Drive Wizard	Copies all contents of one hard drive to a second hard drive.
Blu-ray/DVD/CD support	Backs up your computer directly to Blu-ray, DVD, or CD media. Or, copy recovery points to Blu-ray, DVD, or CD media.
LightsOut Restore	Restores a computer from a remote location, regardless of the state of the computer, provided that its file system is intact.
Recovery point indexing	Lets a search engine 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 the files to restore.
Google Desktop™ support	Searches for and recovers the files that are stored in recovery points by using Google Desktop.
Backup Exec Retrieve support	Searches for and recovers the files that are stored in recovery points by using Backup Exec Retrieve.
File and folder backup	Limits your backup to include a selected set of files or folders.
Offsite Copy	Copies your recovery points and stores them at one or two locations.

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

Symantec System Recovery Basic Edition may not be available in all regions. For more information, or to purchase an upgrade license, contact your local reseller.

http://www.symantec.com/backupexec/

See "About the availability of features in Symantec System Recovery" on page 26.

See "About the trial version of Symantec System Recovery " on page 28.

About the trial version of Symantec System Recovery

If you choose to delay installation of the license key, all features in Symantec System Recovery remain enabled during the 60-day trial period.

However, you cannot use Symantec System Recovery Disk, a component of Symantec System Recovery, during the trial period.

You need a valid license key to use the following key features of Symantec System Recovery Disk:

- **Back Up My Computer** wizard
  See "About running a one-time backup from Symantec System Recovery Disk" on page 94.

- **Recover My Computer** wizard, which lets you use Restore Anyware to restore a virtual disk (.vmdk or .vhd) back to a physical computer that has different hardware.
  See "About recovering to a computer with different hardware" on page 243.

The trial period of Symantec System Recovery begins when you do any one of the following in the software:

- Define a drive-based or file and folder backup.

- Recover a computer.

- Copy a drive.

- Consolidate incremental recovery points.

- Run a drive-based backup or file and folder backup.

- Define a scheduled convert to virtual disk job.

- Run a scheduled convert to virtual disk job.

- Define a one time convert to virtual disk job.

- Define a drive-based or file and folder backup.

- Recover a computer.

- Consolidate incremental recovery points.

■ Run a drive-based or file and folder backup.

If you use the product in trial mode, it expires after 60 days. However, all features are enabled until the end of the trial period, at which time you must purchase the product or uninstall it. You can purchase a license at any time (even after the trial period expires) without reinstalling the software.

Note: If this product came already installed from a computer manufacturer, your trial period could be as long as 90 days. The product licensing or activation page in the installation wizard indicates the duration of your trial period.

See "Activating Symantec System Recovery after the trial period" on page 33.

Installing Symantec System Recovery

Before you begin, you should review the system requirements for installing Symantec System Recovery.

See "System requirements for Symantec System Recovery" on page 23.

Note: During the installation process, you might be required to restart the computer. You should ensure proper functionality of the computer after it restarts. To do so, log on again using the same user credentials that you used to log on when you installed Symantec System Recovery.

Warning: The Symantec System Recovery Disk provides the tools that you need to recover your computer. The Symantec System Recovery Disk may be included on your product CD or on a separate CD, depending on your version of the product. Store the CD in a safe place.

To install Symantec System Recovery

1   Log on to your computer using either the Administrator account or an account with administrator privileges.

2   Insert the Symantec 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>:\browser.exe
```

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

4 In the **CD browser** panel, click **Install Symantec System Recovery**.

5 In the **License Agreement** panel, read the license agreement, and then click **I accept the terms in the license agreement**.

6 Do one of the following:

■ In the **License Agreement** panel, click **Install Now** to begin the installation.

■ In the **License Agreement** panel, click **Custom Install**, select the options you want installed, and then click **Install Now**.

> **Note:** Deselect any of the options you do not want to install at this time. You can install them later by modifying the Symantec System Recovery program using the Windows Add or Remove Programs tool.

See "Custom Install options" on page 30.

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

8 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**, you cannot run Symantec System Recovery until after you restart your computer.

See "Completing the installation of Symantec System Recovery" on page 31.

Custom Install options

The following table describes the options that are available on the **Custom Setup** panel.

Table 2-3 Custom Install options

Options	Description
Backup and Recovery Service	Installs the primary service that is required to back up or recover your computer.
Recovery Point Browser	Enables you to browse, mount, copy, verify, and restore files and folders using recovery points.

Table 2-3   Custom Install options *(continued)*

Options	Description
User Interface	Installs the product user interface that is required for interacting with the Symantec System Recovery Service.
Agent Deployment	This option appears when you expand the **User Interface** option. Allows the computer on which you have installed Symantec System Recovery to deploy the Symantec System Recovery Agent to other computers. The Symantec System Recovery Agent is required for remote recovery management.
Granular Restore Option	This option appears when you expand the **User Interface** option. Lets you open recovery points and restore Microsoft Exchange mailboxes, folders, and individual messages. You can also restore Microsoft SharePoint documents and unstructured files and folders.
CD/DVD Support	Lets you back up directly to a CD or a DVD and create a custom Symantec System Recovery Disk. A CD or a DVD writer is required to use this feature.
LiveUpdate	Keeps your Symantec software up to date with the latest product updates.

Completing the installation of Symantec System Recovery

After you complete Symantec System Recovery installation and restart your computer, the Symantec System Recovery setup wizard starts automatically. Using the setup wizard you can 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 already installed from a computer manufacturer, your trial period could be as long as 90 days. Refer to the **Activate later** label on the **Product Activation** panel in the setup wizard.

To complete the installation of Symantec System Recovery

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

If your computer manufacturer installed the product, the **Welcome** page might appear the first time that you run Symantec System Recovery.

2   Do one of the following:

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

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

■   Click **Activate later** to delay the activation of your license. After the trial period ends, the product will no longer work.
See "About the trial version of Symantec System Recovery " on page 28.

■   If Symantec System Recovery is a trial version and you want to purchase a license key, click **Symantec Global Store**.

■   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   Do any of the following:

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

■   Click **Launch Easy Setup** to open the **Easy Setup** window when you complete the install process. (This option is not available in the server versions of Symantec System Recovery.)

■   Click **Enable Google Desktop File and Folder Recovery** if you want Google Desktop to search your recovery points for the files and folders that you want to recover.
If you select this option, Symantec 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 contents of the files.

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

See "Enabling search engine support" on page 277.

5 Click **Finish**.

See "Activating Symantec System Recovery after the trial period" on page 33.

Activating Symantec System Recovery after the trial period

If you do not activate Symantec 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 Symantec System Recovery after the trial period

1 On the **Help** menu, click **Enter License Key**.

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

> **Note:** You can find the license key on the back of your product CD jacket.

3 Enter the license key in the appropriate spaces.

4 Click **Next**, and then click **Finish**.

See "About the trial version of Symantec System Recovery " on page 28.

Updating Symantec System Recovery with LiveUpdate

You can receive software updates for your version of the product over an 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 Symantec System Recovery with LiveUpdate

1 On the **Help** menu, click **Run LiveUpdate**.

2 In the **LiveUpdate** window, click **Start** to install the updates.

3 When the installation is complete, click **Close**.

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

See "Installing Symantec System Recovery" on page 29.

About uninstalling Symantec System Recovery

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

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

See "Activating Symantec System Recovery after the trial period" on page 33.

Ensuring the recovery of your computer

This chapter includes the following topics:

- About ensuring the recovery of your computer
- About testing Symantec System Recovery Disk
- Creating a custom Symantec System Recovery Disk

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 System Recovery Disk. The drivers that are included on the recovery disk must match the drivers that are required to run your computer's network cards and hard disks.

To ensure that you have the drivers required to recover your computer, you can use the **Run Driver Validation** tool. The driver validation tool is available on the Symantec System Recovery Disk. It compares hardware drivers on the Symantec System Recovery Disk with the drivers required to run your computer's network cards and hard disks.

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

Note: The driver validation tool on Symantec System Recovery Disk does not support wireless network adapter drivers.

See "About testing Symantec System Recovery Disk" on page 36.

See "Testing Symantec System Recovery Disk" on page 36.

About testing Symantec System Recovery Disk

You should test the Symantec System Recovery Disk to ensure that the recovery environment runs properly on your computer.

Note: Depending on the product version you have purchased, Symantec System Recovery Disk is either included on your product CD, or as a separate CD. You should place the CD containing Symantec System Recovery Disk in a safe place.

Testing the Symantec System Recovery Disk lets you identify and solve the following types of problems:

■ You cannot start Symantec System Recovery Disk.

See "Configuring a computer to start from a CD/DVD or a USB device" on page 229.

■ 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 Symantec System Recovery Disk.

See "Testing Symantec System Recovery Disk" on page 36.

Testing Symantec System Recovery Disk

The following table summarizes the steps for testing Symantec System Recovery Disk.

Table 3-1   Testing Symantec System Recovery Disk.

Step	Action	Description
Step 1	Run driver validation tool	Run the driver validation tool to test whether Symantec System Recovery Disk works with the network cards and storage devices on the computer. If any drivers are not included on the recovery disk, the **Driver Validation Results** dialog box appears.
		Without access to the correct drivers, a device cannot be used while you run Symantec System Recovery Disk. Therefore, if the recovery points 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. You can also create a custom Symantec System Recovery Disk.
		See "Creating a custom Symantec System Recovery Disk" on page 37.
Step 2	Boot your computer using Symantec System Recovery Disk	Boot your computer using the Symantec System Recovery Disk.
		See "Booting a computer by using the Symantec System Recovery Disk" on page 228.
Step 3	Test the connection	Run a mock restore of a recovery point that is stored either on a network or locally on a computer. Running a mock restore helps you to test if you can connect to the network or the local hard drive.

See "About testing Symantec System Recovery Disk" on page 36.

Creating a custom Symantec System Recovery Disk

Symantec recommends that you create a custom Symantec System Recovery Disk, even if driver validation succeeds, and your Symantec System Recovery Disk appears to work. You can create a custom Symantec System Recovery Disk on a CD/DVD or on a USB device. A custom Symantec System Recovery Disk contains your computer's current network and storage device drivers. It helps to ensure that in an emergency you can get to the recovery points that are required to restore your computer.

After creating a custom Symantec System Recovery Disk, you can use it as a source for creating another custom Symantec System Recovery Disk.

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

To create a custom Symantec System Recovery Disk

1   Attach and turn on all storage devices and network devices that you want to make available.

2   Start Symantec System Recovery.

3   Insert the Symantec System Recovery Disk CD into your media drive.

4   On the **Tasks** menu, click **Create Custom Recovery Disk**.

5   Click **Next**.

6   Do one of the following:

If you know the path to the source Symantec System Recovery Disk	Type the path in the **Symantec System Recovery Disk media location** field.
If you do not know the path to the source Symantec System Recovery Disk	Do the following in the order listed: ■ Click **Browse**. ■ Click **Symantec System Recovery Disk ISO File** to locate the path for the ISO image file, or click **Symantec System Recovery Disk Folder** to locate the path for the disk on other media. ■ On the **Open** dialog box, navigate to the location of the appropriate ISO image file, media drive, or folder. ■ Click **Open**.

7   Click **Next**.

8   In the **Symantec System Recovery Disk Creation** panel, select the settings for creating the Symantec System Recovery Disk.

   See "Symantec System Recovery Disk creation settings" on page 40.

9   Click **Next**.

10 Review the list of storage and network drivers to be included, and add additional drivers or remove the drivers you do not need.

You can add 64-bit drivers to the custom Symantec System Recovery Disk. The 64-bit drivers are used only for restoring a recovery point of a 64-bit operating system on a computer with different hardware.

Note: Symantec System Recovery Disk does not use 64-bit drivers for starting a computer. To start a computer that has a 64-bit operating system using Symantec System Recovery Disk, the equivalent 32-bit drivers are required.

11 Click **Next**.

12 In the **Startup Options** panel, select the default keyboard layout, display language, and time zone from the respective lists.

13 Click **Next**.

14 In the **Options** panel, select the optional settings for the custom Symantec System Recovery Disk.

See "Optional settings for Symantec System Recovery Disk" on page 41.

15 Click **Next**.

16 In the **License Setup** panel, specify how you want to enable licensed features in the customized Symantec System Recovery Disk. For example, the cold imaging feature called **Back Up My Computer**.

17 Click **Next**.

18 Review the summary of the options you have selected for creating the custom Symantec System Recovery Disk.

19 Click **Finish**.

Warning: Be certain to test your new custom Symantec System Recovery Disk. It ensures that you can use the Symantec System Recovery Disk to start your computer and can access the drive that contains your recovery points.

See "Testing Symantec System Recovery Disk" on page 36.

See "Creating a custom Symantec System Recovery Disk" on page 37.

See "About testing Symantec System Recovery Disk" on page 36.

See "About updating Symantec System Recovery Disk on USB" on page 40.

About updating Symantec System Recovery Disk on USB

Whenever new drivers or driver versions are added to your computers, you must add them to the Symantec System Recovery Disk. If your Symantec System Recovery Disk is on a CD/DVD, you need to create a new custom recovery disk to include the new drivers. However, if your Symantec System Recovery Disk is on a USB device, you can update it rather than creating a new one.

To update an existing Symantec System Recovery Disk on a USB device, run the **Create Custom Symantec Recovery Disk** wizard. Ensure that you use the existing Symantec System Recovery Disk on the USB device as the source as well as the destination. During Symantec System Recovery Disk creation, the existing drivers are retained and only the new drivers are added to the recovery disk.

Note: You can add drivers from multiple computers to a single Symantec System Recovery Disk on a USB device.

See "Creating a custom Symantec System Recovery Disk" on page 37.

Symantec System Recovery Disk creation settings

The following table describes the options on the **Symantec System Recovery Disk Creation** panel in the **Create Custom Symantec System Recovery Disk** wizard.

Table 3-2   Symantec System Recovery Disk creation settings

Option	Description
Disk label	Lets you specify the name that you want to use for the Symantec System Recovery Disk label.
Create Symantec System Recovery Disk on CD/DVD or USB device	Lets you save your customized Symantec System Recovery Disk to a CD/DVD or a USB device. Select this option and then select the media drive in which you have placed the CD/DVD or plugged in the USB device. **Note:** The existing data on the USB device is not formatted during Symantec System Recovery Disk creation.
Save a copy of the custom Symantec System Recovery Disk (ISO file)	Lets you save your customized Symantec System Recovery Disk as a CD/DVD image (.iso) file. To save the Symantec System Recovery Disk as an .iso file, select this option. Then specify the path where you want to save the resulting file.

Table 3-2   Symantec System Recovery Disk creation settings *(continued)*

Option	Description
Skip Symantec System Recovery Disk Customization	Lets you skip the remaining panels of the **Create Custom Symantec System Recovery Disk** wizard. If you do not want to change any of the default Symantec System Recovery Disk options, select this option.

See "Creating a custom Symantec System Recovery Disk" on page 37.

Optional settings for Symantec System Recovery Disk

The following table describes the options on the **Options** panel in the **Create Custom Symantec System Recovery Disk** wizard.

Table 3-3   Optional settings for Symantec System Recovery Disk

Option	Description
Automatically start network services	Starts networking automatically when you recover the computer through LightsOut Restore.
Dynamic IP	Connects to a network without the need for additional network configuration. You can click this option if you know there is a DHCP server available on the network at the time you restore.
Static IP	Connects to a network with a particular network adapter and specific address settings. You should click this option if you know there is no DHCP server (or the DHCP server is unavailable) when you recover.
Automatically start Symantec pcAnywhere	Starts the Symantec pcAnywhere thin host automatically when you start Symantec System Recovery Disk.
Configure	Lets you configure log on credentials and other optional parameters for pcAnywhere. See "Options for configuring pcAnywhere" on page 42.
Use Windows firewall settings	Saves the current Windows firewall settings to the Symantec System Recovery Disk.

See "Creating a custom Symantec System Recovery Disk" on page 37.

Options for configuring pcAnywhere

The following table describes the options on the **Configure Symantec pcAnywhere** panel. This panel is available from the **Options** panel in the **Create Custom Symantec System Recovery Disk** wizard.

Table 3-4   Options for configuring pcAnywhere

Option	Description
User name	Lets you type the user name for authenticating to pcAnywhere.
Password	Lets you type the password for authenticating to pcAnywhere.
Confirm password	Lets you retype the password for authenticating to pcAnywhere.
Host name	Lets you type the name that you want to use for the host. You can leave this box blank to configure the host name to be the same as the computer name.
Encryption level	Lets you encrypt the data stream between the host and remote computer.
Encryption level-None	Lets you specify that no encryption of the data stream occurs between the host and the remote computer.
Encrytion level-pcAnywhere	Lets you scramble the data using a mathematical algorithm so that a third party cannot easily interpret it. This option is available on any operating system that pcAnywhere supports.
Encryption level-Symmetric	Lets you encode and decode data using a cryptographic key. This option is available on any Windows operating system that supports the Microsoft CryptoAPI.

See “Optional settings for Symantec System Recovery Disk” on page 41.

See “Creating a custom Symantec System Recovery Disk” on page 37.

Getting Started

This chapter includes the following topics:

- How to use Symantec System Recovery

- Starting Symantec System Recovery

- Configuring Symantec System Recovery default options

- Setting up your first backup using Easy Setup

- Hiding or showing the Advanced page

How to use Symantec System Recovery

Symantec System Recovery helps you in backing up your files, folders, or entire drives. To back up your data, you need to define a backup. A backup specifies what data to back up, when to back it up, and where to put the backed up data.

Using Symantec 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 Symantec System Recovery
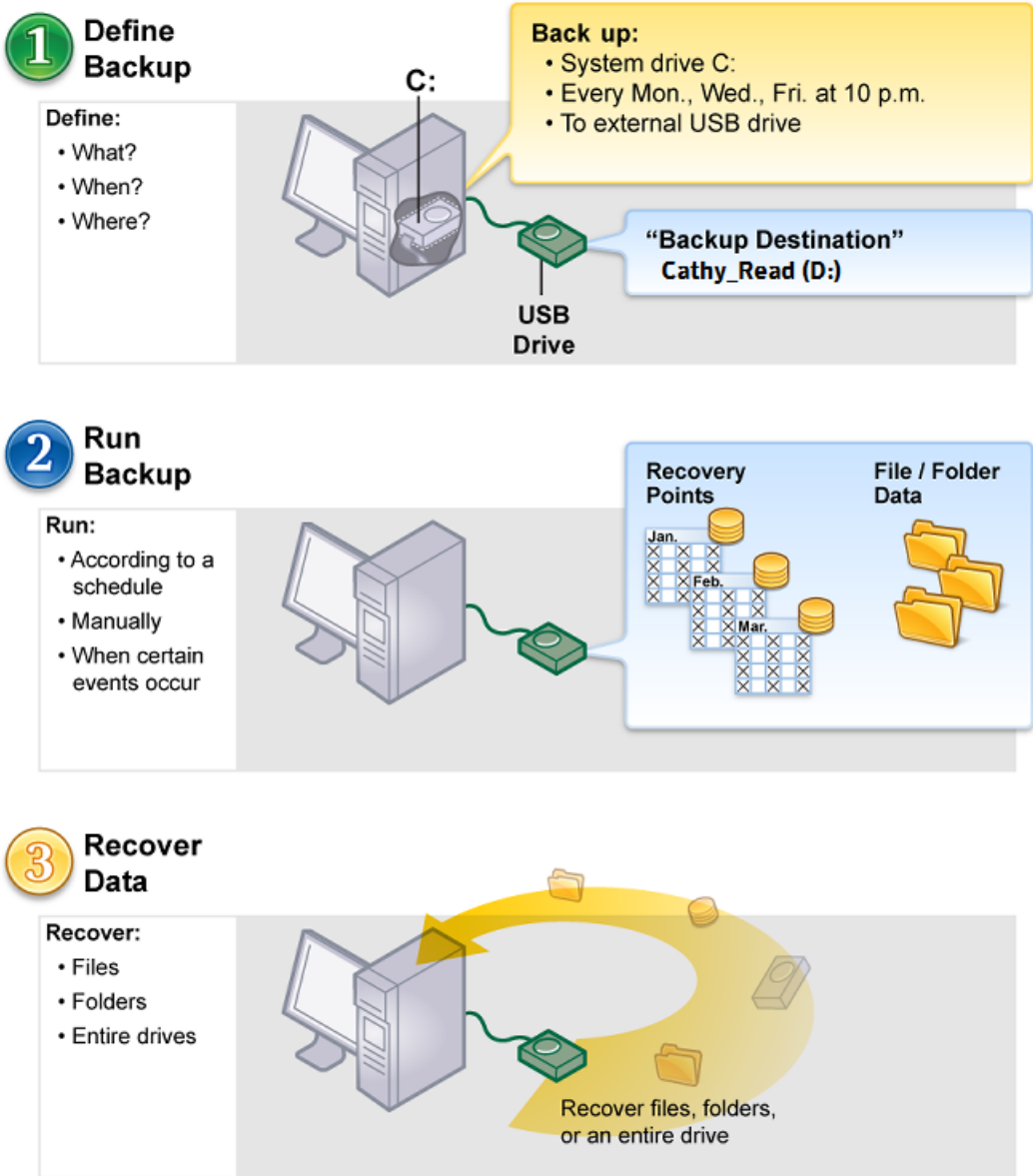
See "Starting Symantec System Recovery" on page 45.

See "Configuring Symantec System Recovery default options" on page 45.

Starting Symantec System Recovery

Symantec 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 Symantec System Recovery. You can also open Symantec System Recovery from the Windows Start menu.

To start Symantec System Recovery

◆ Depending on the Windows version you are running, use one of the following methods:

- On the classic Windows taskbar, click **Start > Programs > Symantec System Recovery**.

- On the Windows taskbar, click **Start > All Programs > Symantec System Recovery**.

- In the Windows system tray, double-click the **Symantec System Recovery** tray icon.

- In the Windows system tray, right-click the **Symantec System Recovery** tray icon, and then click **Open Symantec System Recovery**.

See "Configuring Symantec System Recovery default options" on page 45.

Configuring Symantec System Recovery default options

The **Options** dialog box includes several views that let you configure Symantec System Recovery default options.

To configure Symantec System Recovery default options

1 On the **Tasks** menu, click **Options**.

2 Select an option you want to edit, make any necessary changes, and then click **OK**.

See "Setting up general backup options" on page 46.

See "Adjusting the effect of a backup on computer performance" on page 48.

See "Enabling network throttling" on page 49.

See "Adjusting default tray icon settings" on page 49.

See "Adding new file types and extensions" on page 51.

See "Renaming file types and extensions" on page 51.

See "Restoring default file types and extensions" on page 52.

See "Deleting a file type and all of its extensions" on page 53.

See "Enabling search engine support" on page 277.

See "Removing or changing the unique name for an external drive" on page 54.

See "Configuring default FTP settings for use with Offsite Copy" on page 54.

See "Logging Symantec System Recovery messages" on page 56.

See "Enabling email notifications for product (event) messages" on page 58.

See "Configuring Symantec System Recovery to send SNMP traps" on page 155.

Setting up general backup options

You can specify the default destination for storing recovery points and file and folder backup data that is 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.

You can also choose to prepend your computer's name to backup data file names and save each backup file to a new subfolder.

To set up general backup options

1   On the **Tasks** menu, click **Options**.

2   Click **General**.

3   Set the appropriate options for your backups.

    See "General options" on page 46.

4   Click **OK**.

See "Configuring Symantec System Recovery default options" on page 45.

General options

The following table describes the options on the **General** page. The options you configure here are used as default backup options.

Table 4-1   General options

Option	Description
Prepend computer name to backup data file names	Adds the computer name to the beginning of each backup data file name.
	This option is 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.
Save backup files to a unique subfolder	Creates a new subfolder that serves as your backup destination.
	Note: The new subfolder is given the same name as your computer. For example, if your computer name is "My_Laptop", the new subfolder is named \My_Laptop.
Default backup destination	Lets you specify a path to the folder where you want to store recovery points and file and folder backup data. If you do not know the path, you can browse to the location.
	If you entered the path to a location on a network, enter the user name and password that are required for authentication.
	Note: You cannot use an encrypted folder as your backup destination. However, you can encrypt your backup data to prevent other users from accessing it. To encrypt your backup data, refer to the **Advanced** options when you define or edit a backup.
	See "Defining a drive-based backup" on page 74.
	See "Editing advanced backup options" on page 88.

See "Configuring Symantec System Recovery default options" on page 45.

Adjusting the effect of a backup on computer performance

If a backup is running on your computer, your computer's performance might slow down. The slow down in the computer's performance might be more prominent if it is the one creating an independent recovery point. The performance slows down because Symantec System Recovery uses your computer's hard disk and memory resources to perform the backup.

You can change the speed of the backup to minimize the effect of Symantec System Recovery on your computer while you work.

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

To adjust the effect of a backup on computer performance

1   On the **Tasks** menu, click **Options**.

2   Click **Performance**.

3   Do one of the following:

   ■   To improve your computer's performance during backup jobs, move the slider bar closer to **Slow**.

   ■   To enable backup jobs to run more quickly, move the slider bar closer to **Fast**.

4   Click **OK**.

See "Adjusting the speed of a backup" on page 120.

See "Configuring Symantec System Recovery default options" on page 45.

About enabling network throttling

You can limit the effect of a backup on network performance by enabling network throttling.

Many variables affect the network performance. Consider the following points before you use 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?

See "Enabling network throttling" on page 49.

See "Configuring Symantec System Recovery default options" on page 45.

Enabling network throttling

Consider using this feature only when you know what your network can handle. If you schedule your backups at staggered intervals and when network traffic is low, you may not need to use this feature. Avoid backing up multiple computers at the same time and to the same network destination.

Gather the required information about your network's performance and then schedule backups accordingly. Enable this feature and set the **Maximum network throttling** to a setting that matches the circumstances.

To enable network throttling

1   On the **Tasks** menu, click **Options**.

2   Click **Performance**.

3   Select **Enable network throttling**.

4   In the **Maximum network throttling** field, enter the maximum amount (in KB) of network throughput.

5   Click **OK**.

See "About enabling network throttling" on page 48.

See "Configuring Symantec System Recovery default options" on page 45.

Adjusting default tray icon settings

You can turn on the system tray icon or turn it off as required. You can choose to show only error messages, 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 **Tasks** menu, click **Options**.

2   Click **Tray Icon**, and then select the options you want to use for the tray icon.

    See "Tray Icon options" on page 50.

3   Click **OK**.

See "Configuring Symantec System Recovery default options" on page 45.

Tray Icon options

The following table describes the options that you can select to adjust the default tray icon settings.

Table 4-2   Tray Icon options

Options	Description
Show system tray icon	Displays the Symantec 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.
	For example, it notifies you when your computer was turned off at the time a backup was scheduled to run.
Show system tray questions	Offers you helpful prompts in the form of questions that can help you keep your data backed up.
Show status messages	Displays the messages about the status of backup operations. For example, a backup has started, or your backup destination is about to get full.
Show error messages	Displays the error messages when errors occur so that you can resolve any issues that might hinder data protection.

See "Adjusting default tray icon settings" on page 49.

See "Configuring Symantec System Recovery default options" on page 45.

About managing file types and file extensions

When you define file and folder backups, file types are a quick way to include the files that you use the most. For example, if you keep music files on your computer, you can configure a 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 (for example, .pft and .ptp,). You can define a new file type and define the two file extensions for that category. Then when you define a backup, you can select the new category. When the backup runs, all files that end with .pft and .ptp are backed up.

See "Adding new file types and extensions" on page 51.

See "Renaming file types and extensions" on page 51.

See "Restoring default file types and extensions" on page 52.

See "Deleting a file type and all of its extensions" on page 53.

Adding new file types and extensions

The most common file types and extensions are already defined for you. However, you can add additional file type categories as needed.

To add a new file type and extensions

1 On the **Tasks** menu, click **Options**.

2 Click **File Types**.

3 At the bottom of the **File types** list, click **Add a file type** (+).

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 **Add an extension** (+).

6 Type an asterisk (*) and a period, followed by the extension of the file type you want to define, and then press **Enter**.

7 Click **OK**.

See "Renaming file types and extensions" on page 51.

See "Restoring default file types and extensions" on page 52.

See "Deleting a file type and all of its extensions" on page 53.

See "About managing file types and file extensions" on page 50.

See "Configuring Symantec System Recovery default options" on page 45.

Renaming file types and extensions

You can rename existing file types and extensions as needed.

To rename a file type and extensions

1   On the **Tasks** menu, click **Options**.

2   Click **File Types**.

3   Select a file type from the **File types** list, and then do one of the following:

■   Click **Rename a file type** to edit the name of the selected file type.

■   Select an extension from the **Extensions for** list and click **Rename an extension** to edit the name of the extension.

4   Click **OK**.

See "Adding new file types and extensions" on page 51.

See "Restoring default file types and extensions" on page 52.

See "Deleting a file type and all of its extensions" on page 53.

See "About managing file types and file extensions" on page 50.

See "Configuring Symantec System Recovery default options" on page 45.

Restoring default file types and extensions

You can restore default file types and extensions as needed.

To restore default file types and extensions

1   On the **Tasks** menu, click **Options**.

2   Click **File Types**.

3   Select a file type from the **File types** list.

4   Click either **Restore default file types list** or **Restore default extensions list** to restore all default file types or extensions.

Caution: Any file types and extensions you have set up are removed. You must add them again manually.

---

5   Click **OK**.

See "Adding new file types and extensions" on page 51.

See "Renaming file types and extensions" on page 51.

See "Deleting a file type and all of its extensions" on page 53.

See "About managing file types and file extensions" on page 50.

See "Configuring Symantec System Recovery default options" on page 45.

Deleting a file type and all of its extensions

You can delete a file type and all its extensions as needed.

To delete a file type and all of its extensions

1   On the **Tasks** menu, click **Options**.

2   Click **File Types**.

3   Select a file type from the **File types** list, and then do one of the following:

- Click the **Remove a file type** to delete a file type and all its extensions.

- Select an extension from the **Extensions for** list and click **Remove an extension** to edit the name of the extension.

Note: 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.

---

4   Click **OK**.

See "Adding new file types and extensions" on page 51.

See "Renaming file types and extensions" on page 51.

See "Restoring default file types and extensions" on page 52.

See "About managing file types and file extensions" on page 50.

See "Configuring Symantec System Recovery default options" on page 45.

About using unique names for external drives

Symantec System Recovery lets you assign unique names to external drives when you use them as a backup destination or an Offsite Copy destination. Assigning unique names helps you to manage these destinations and avoid confusion if you use more than one drive. It is especially helpful when the assigned drive letter changes each time you plug in the drive.

Note: Using a unique name does not change the drive label. The unique name is used only when you access a drive from within Symantec System Recovery.

For example, you might swap out two different external drives that are used as Offsite Copy destinations during any given week. It would be difficult to identify which drive your use at any given time based on the drive labels. It becomes more confusing if the previously assigned drive letter has changed.

However, you can associate unique names with each drive when you use them with Symantec System Recovery. The unique name that is associated with a drive is displayed in various locations in Symantec System Recovery.

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

For example, if you assigned the unique name, "Cathy Read" to one drive, and "Thomas Read" to a second drive. Their unique names appear in Symantec System Recovery whenever the drives are plugged in to your computer.

See "About Offsite Copy" on page 100.

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

See "Removing or changing the unique name for an external drive" on page 54.

Removing or changing the unique name for an external drive

You can remove or change the unique name for the drive as needed.

Note: Symantec System Recovery lets you assign a unique name when you plug in an external drive in to your computer for the first time.

To remove or change unique name for an external drive

1 On the **Tasks** menu, click **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 delete the unique name that is associated with the external drive.

   ■ Click **Rename** to edit the unique name.

4 Click **OK**.

See "About using unique names for external drives" on page 53.

Configuring default 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. Symantec System Recovery serves as an FTP client to copy your recovery points to a remote FTP server. You can copy your recovery points to an FTP server as a secondary backup of your critical data.

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

To configure default FTP settings for use with Offsite Copy

1   On the **Tasks** menu, click **Options**.

2   Under **Destinations**, click **Configure FTP**.

3   Select the appropriate options.

    See "FTP configuration options" on page 55.

4   Click **OK**.

See "Configuring Symantec System Recovery default options" on page 45.

FTP configuration options

The following table describes the options that you can select to configure the default FTP settings for use with Offsite Copy.

Table 4-3   FTP configuration options

Option	Description
Connection mode: Passive (Recommended)	Helps prevent conflicts with security systems. This mode is necessary for some firewalls and routers. When you use passive mode, the FTP client opens the connection to an IP address and port that the FTP server supplies.
Connection mode: Active	Enables a server to open a connection to an IP address and port that the FTP client supplies. Use active mode when connections or transfer attempts fail in passive mode, or when you receive data socket errors.
Limit connection attempts to	Indicates the number of times Symantec System Recovery tries to connect to an FTP server before it gives up. Symantec System Recovery can attempt a maximum of 100 times.
Stop trying to connect after	Indicates the number of seconds Symantec System Recovery tries to connect to an FTP server before it gives up. You can specify up to 600 seconds (10 minutes).
Default port	Indicates the port of the FTP server that listens for a connection. You should consult the FTP server administrator to be sure that the port you specify is configured to receive incoming data.

Logging Symantec 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. They can also provide helpful information when you need to troubleshoot.

Two logging methods are available: Symantec System Recovery logging and the Windows application log.

To log Symantec System Recovery messages

1   On the **Tasks** menu, click **Options**.

2   Under **Notifications**, click **Log File**.

3   Select the appropriate log file options.

4   Click **OK**.

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

1   On the **Tasks** menu, click **Options**.

2   Under **Notifications**, click **Event Log**.

3   Select the appropriate event log options.

4   Click **OK**.

Log File options

The following table describes the options to log Symantec System Recovery messages.

Table 4-4   Log File options

Option	Description
Select the priority and type of messages	Lets you select the priority level at which messages should be logged. You can choose to log all or no messages regardless of priority levels.
	Select one of the following options:
	■ **All messages**
	■ **Medium and high priority messages**
	■ **High priority messages**
	■ **No messages**
Errors	Logs the error messages as they occur.
Warnings	Logs the warning messages as they occur.
Information	Logs the information messages as they occur.
Log file location	Lets you specify a path where you want to create and store the log file.
	If you do not know the path, you can browse to the location.
Maximum file size	Lets you specify the 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.

See

Event log options

The following table describes the options to configure which product events are written to a Windows event log.

Table 4-5   Event log options

Option	Description
Select the priority and type of messages	Lets you select the priority level at which messages should be logged. You can choose to log all or no messages regardless of priority levels. Select one of the following options: - **All messages** - **Medium and high priority messages** - **High priority messages** - **No messages**
Errors	Logs the error messages as they occur.
Warning	Logs the warning messages as they occur.
Information	Logs the information messages as they occur.

See "Logging Symantec System Recovery messages" on page 56.

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. The custom log file is located in the Agent folder of the product installation.

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

To enable email notifications for product (event) messages

1   On the **Tasks** menu, click **Options**.

2   Under **Notifications**, click **SMTP Email**.

3   Select the appropriate options.

    See "SMTP Email options" on page 59.

4   Click **OK**.

See "Configuring Symantec System Recovery default options" on page 45.

SMTP Email options

The following table describes the options to enable email notifications for product (event) messages.

Table 4-6 SMTP Email options

Option	Description
Select the priority and type of messages	Lets you select the priority level at which messages should be logged. You can choose to log all or no messages regardless of priority levels.
	Select one of the following options:
	■ **All messages**
	■ **Medium and high priority messages**
	■ **High priority messages**
	■ **No messages**
Errors	Logs the error messages as they occur.
Warnings	Logs the warning messages as they occur.
Information	Logs the information messages as they occur.
To address (admin@domain.com)	Lets you specify the email address (for example, admin@domain.com) where notifications are to be sent.
From address	Lets you specify the email address of the sender.
	The From address is not mandatory. If you do not specify a From address, the name of the product is used.
SMTP server (smtp.domain.com)	Lets you specify the path to the SMTP server that sends the email notification (for example, smtpserver.domain.com).
SMTP Authentication	Lets you specify the method to authenticate to the specified SMTP server.
User name	Lets you specify the SMTP user name.
Password	Lets you specify the SMTP password.

Note: If you are not sure what your SMTP user name and password are, contact a system administrator.

See "Enabling email notifications for product (event) messages" on page 58.

Setting up your first backup using Easy Setup

If you had selected the **Launch Easy Setup** check box during the setup wizard, the **Easy Setup** window appears the first time you open the **Run or Manage Backups** window.

Note: The **Easy Setup** window is not available in server versions of Symantec System Recovery.

To set up your first backup using Easy Setup

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

2 In the **Easy Setup** window, either accept the default drive and file and folder backup settings, or click any of the settings to edit them.

3 Click **OK**.

4 In the **First Backup** window, do one of the following:

- Select **Run first backup according to schedule** to run the backup as per the schedule that you specified.

- Select **Run backup now** to run the backup immediately.

5 Click **OK**.

See "Configuring Symantec System Recovery default options" on page 45.

Hiding or showing the Advanced page

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

Note: When you refer to the documentation while you use the **Advanced** page, the first one or two steps do not apply. The first one or two steps merely indicate where to access each feature from the other pages of the user 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 or show the Advanced page

1   Start Symantec System Recovery.

2   On the **View** menu, click **Advanced** to hide or show the **Advanced** page.

See "Configuring Symantec System Recovery default options" on page 45.

Best practices for backing up your data

This chapter includes the following topics:

- About backing up your data
- About choosing a backup type
- What to do before you back up
- What to do during a backup
- What to do when a backup is finished
- Tips for running defined backups
- Viewing the properties of a backup job
- About selecting a backup destination
- About backing up dual-boot computers

About backing up your data

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

- Define a backup.
- Run the backup.
  See "How to use Symantec System Recovery" on page 43.

When you define a backup, you decide on the following:

- 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.

See "About choosing a backup type" on page 64.

See "About selecting a backup destination" on page 69.

See "About backing up dual-boot computers" on page 71.

About choosing a backup type

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, it is the C drive, which includes your operating system).
	■ Back up and recover a specific hard drive. For example, a secondary drive other than the system drive that includes your operating system.
	■ 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, your 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 "About selecting a backup destination" on page 69.

See "About backing up your data" on page 63.

What to do before you back up

Consider these best practices before you define and run your first backup:

Schedule backups at a time when you know your computer is 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 "About choosing a backup type" on page 64.
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). It helps ensure that you can recover your system in the event that your primary hard disk fails. See "Setting up general backup options" on page 46.
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 100.
Give unique names to your external drives to help you easily identify them.	You can assign a unique name to each external drive. A unique name helps you to keep a track of where your backup data is stored for each computer you back up. It is more useful in situations when the drive letters change each time you unplug and plug an external drive into your computer. A unique name ensures that you always know which drive is used when you are running Symantec System Recovery. Using a unique name does not change the volume label of a drive. A unique name helps you to identify the drive when you use Symantec System Recovery. Once a unique name is assigned, it stays with the drive. If you plug the drive into a second computer running another copy of Symantec System Recovery, the unique name appears. **Note:** You might also consider placing a sticky label on each drive that matches the unique name that you have assigned. See "About using unique names for external drives" on page 53.

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 100. |
| Run backups frequently on a regular 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 126.

See "Defining a drive-based backup" on page 74. |
| 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. It speeds the creation of recovery points and reduces 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. | While defining a backup, select the option to verify that the recovery point is stable and can be used to recover lost data.

See "About choosing a backup type" on page 64. |

See "What to do during a backup" on page 66.

See "What to do when a backup is finished " on page 67.

What to do during a backup

When a backup starts to run on your computer, you might notice that the performance of your computer slows down. Symantec 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 120.

See "What to do before you back up" on page 64.

What to do when a backup is finished

After a backup finishes, 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. See "About opening files and folders stored in a recovery point" on page 213. See "To open files within a recovery point" on page 165.
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. **Note:** Backup status and other messages are also conveyed in the system tray. So you do not need to start the product to identify the status of your backups. See "Verifying that a backup is successful" on page 121. See "To hide or show the Advanced page" on page 61.
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 when you back up your files and folders. See "About managing file and folder backup data" on page 202.
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 177.

Tips for running defined backups

Consider the following tips when you run a defined backup:

- Symantec System Recovery does not need to be running for a scheduled backup to start. After you define a backup, you can close Symantec System Recovery.

- The computer that is 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 significantly increases 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. Including both the drives in the same backup 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 effect of a backup on your computer's performance. For example, say 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 Symantec 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 restart the computer.

See "What to do before you back up" on page 64.

See "What to do during a backup" on page 66.

See "What to do when a backup is finished " on page 67.

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**.

See "Running an existing backup job immediately" on page 117.

See "Running a backup with options" on page 118.

See "Editing backup settings" on page 122.

About selecting a backup destination

You should review the following information before you decide 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 subfolder on the disk. Backup data must be created at the root of CDs and DVDs.

The following table contains the 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: ■ Provides for fast backup and recovery. ■ Lets you schedule unattended backups. ■ Reduces cost because drive space can be overwritten repeatedly. ■ Allows for off-site storage. ■ Reserves hard drive space for other uses. Although you can save the recovery point to the same drive that is backed up, it is not recommended for the following reasons: ■ As the number or size of recovery points grows it consumes more disk space. As a result you have less disk space 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 may not be able to recover the recovery point 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 hosts 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 connect 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, the data is automatically split into the correct sizes if the backup spans more than one media.
	If more than one drive is backed up, the recovery points for each drive are stored independently on the media. The recovery points are stored independently on the media even if there is space to store them on same media.
	The scheduling of backups is not available when this option is used.
	Note: Using CD-RW or DVD-RW as your recovery point storage location is not the best option. You might be required to swap disks during the process.

About backing up dual-boot computers

You can back up dual-boot computers, even if you have hidden drives (partitions) in the operating system from which you run Symantec 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 can be used to start up your computer.

Consider the following points when backing up dual-boot computers:

- To boot your computer from a restored system, you must back up, and then restore every drive that includes operating system boot information.

- Do not create incremental backups of shared data drives if both the following conditions are true:

  - Symantec System Recovery is installed on both operating systems.

  - Both the operating systems are set to manage the shared drive.

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

The same is true for the Symantec System Recovery Restore Anyware feature.

See "Defining a drive-based backup" on page 74.

See "About backing up your data" on page 63.

Backing up entire drives

This chapter includes the following topics:

About 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 point file names and recovery point set file names are appended with 001.v2i, 002.v2i, and so forth. Incremental recovery point file names within a set are appended with _i001.iv2i, _i002.iv2i, and so forth. For example, if your base recovery point is called CathyReadF001.v2i, the first incremental recovery point is called CathyReadF001_i001.iv2i.

See "Defining a drive-based backup" on page 74.

See "About backing up files and folders" on page 107.

Defining a drive-based backup

Define a drive-based backup to take a snapshot of your entire hard drive.

See "About defining a drive-based backup" on page 73.

See "About backing up files and folders" on page 107.

To define a drive-based backup

1   On the **Tasks** menu, 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 box appears instead.

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

4   In the **Drives** panel, select one or more drives to back up, and then click **Next**.

   See "Drives options" on page 75.

5   If the **Related Drives** panel appears, set the appropriate option, and then click **Next**. Otherwise, skip to the next step.

   See "Related drives options" on page 75.

6   On the **Recovery point type** panel, select the recovery point type that you want the backup to create, and then click **Next**.

   See "Recovery point type options" on page 76.

7   On the **Backup Destination** panel, select the appropriate options.

   See "Backup destination options" on page 77.

   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.

8   (Optional) If you want to make copies of your recovery points to store at a remote location for added backup protection, click **Add**, select the appropriate options, and then click **OK**.

   See "Offsite Copy Settings options" on page 78.

9   Click **Next**.

10   On the **Options** panel, set the recovery point options you want, and then click **Next**.

See "Recovery point options" on page 79.

See "Advanced options for drive-based backups" on page 86.

See "Command files options" on page 84.

11   On the **Backup Time** panel, select the appropriate options to specify the time and frequency of the backup, and then click **Next**.

Note: Ensure that the time for running a base backup and an incremental backup is not the same.

See "Backup time options" on page 91.

12   (Optional) 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.

13   Review the options you have selected, then click **Finish**.

See "About backing up files and folders" on page 107.

Drives options

The following table describes the options on the **Drives** panel. This panel is available in the **Define Backup** wizard.

Table 6-1   Drives options

Option	Description
Show Hidden Drives	Lets you see any hidden drives on your hard disk. The drives are displayed in the drive selection table.
Drive selection table	Lets you select one or more drives to include in the backup.

See "Defining a drive-based backup" on page 74.

Related drives options

The following table describes the options on the **Related Drives** panel.

Table 6-2   Related drives options

Option	Description
Add all related drives (recommended)	Lets you select and include all related drives in the backup definition.
Edit the list of selected drives	Lets you select or deselect related drives that you want or do not want to include in the backup definition.
Do not add related drives	Lets you deselect (not include) all related drives in the backup definition.

The **Related Drives** wizard panel appears only if you initially selected a drive with applications configured to use one or more of the drives that are listed in this panel.

Such applications include the following:

■ Windows Server 2008 R2 with Hyper-V

■ Domain controllers

■ Boot configuration databases (as found in Windows Vista and Windows 7) that are on a separate drive from where the operating system is installed.

If you want to back up an attached Microsoft Virtual Hard Disk (VHD), you must create a separate backup job for the host drive and for the attached VHD. For example, if the VHD host is on the C: drive and the attached VHD is the D: drive, you must create a backup job for C: and a backup job for D:. Also, you cannot back up an attached VHD that is nested within another attached VHD.

See "About backing up Microsoft virtual hard disks" on page 291.

If you use Microsoft's BitLocker Drive Encryption to encrypt the data on a data drive (any drive that does not have the operating system installed on it), be aware that Symantec System Recovery does not work with locked data drives. Instead, you must unlock the bitlocked drive before you can back it up.

Generally, you should accept the preselected option **Add all related drives (recommended)**. If you deselect certain related drives, you may experience an incomplete recovery or an unsuccessful recovery.

See "Defining a drive-based backup" on page 74.

Recovery point type options

The following table describes the options on the **Recovery Point Type** panel.

Table 6-3   Recovery point type options

Option	Description
Recovery point set (recommended)	Schedules 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.

See "Defining a drive-based backup" on page 74.

Backup destination options

The following table describes the options on the **Backup Destination** panel.

Table 6-4   Backup destination options

Option	Description
Folder	Indicates the location where you want to store the recovery points.
	If Symantec System Recovery detects that this location does not have enough available space, it alerts you. You should choose another location that has more space.

Table 6-4   Backup destination options *(continued)*

Option	Description
Browse	Lets you browse to locate a backup destination that you want to use.
Destination Details	Displays the type of destination path. If you add a network path it also displays the user name.
Edit	Lets you enter the user name and password for access to the network that is specified in the **Folder** field. This option is available only if you selected a backup destination that is on a network. This also applies if you want to save the recovery point on a network share. See "About network credentials" on page 83.
Customize recovery point file names	Lets you rename the recovery point. Default file names include the name of the computer followed by the drive letter. You can also save recovery points to a unique subfolder.
Add	Lets you 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 100.

See "Defining a drive-based backup" on page 74.

Offsite Copy Settings options

The following table describes the options on the **Offsite Copy Settings** panel.

Table 6-5   Offsite Copy Settings options

Options	Description
Enable Offsite Copy	Turns on the Offsite Copy feature.
Prompt me to start a copy when I attach an external Offsite Copy destination drive	Indicates that you want to have recovery points automatically copied to external Offsite Copy destination drives whenever you plug one in to your computer.
Folder, Network Path, or FTP address	Lets you specify the destination path of the offsite copy.
Browse	Lets you browse to locate an offsite copy destination that you want to use.
Destination Details	Displays the type of destination path. If you add a network path or an ftp path, it also displays the user name.
Edit	Lets you edit the user name or password of a specified network path or an ftp path.
Add an additional Offsite Copy destination	Lets you add a second destination, and then specify the path to that destination.

See "Defining a drive-based backup" on page 74.

Recovery point options

The following table describes the recovery point options on the **Options** panel.

Table 6-6   Recovery point options

Options	Description
Name	Indicates a name for your backup.
	Note: This option does not appear if you create a recovery point using the **Back Up My Computer** feature in Symantec System Recovery Disk.

Table 6-6   Recovery point options *(continued)*

Options	Description
Compression	Lets you set one of the following compression levels for the recovery point: ■ None ■ Standard ■ Medium ■ High See "Compression levels for recovery points" on page 92. The results can vary depending on the types of files that are saved in the drive.
Verify recovery point after creation	Tests whether a recovery point or set of files is valid or corrupt.
Limit the number of recovery point sets saved for this backup	Limits 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. This option appears only if you are creating a recovery point set. **Note:** This option does not appear if you create a recovery point using the **Back Up My Computer** feature in Symantec System Recovery Disk.

Table 6-6   Recovery point options *(continued)*

Options	Description
Enable search engine support	Lets 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. This option is for NTFS file systems only. See "About using a search engine to search recovery points" on page 277. **Note:** This option does not appear if you create a recovery point using the **Back Up My Computer** feature in Symantec System Recovery Disk.
Include system and temporary files	Includes indexing support for operating system and temporary files when a recovery point is created on the client computer. **Note:** This option does not appear if you create a recovery point using the **Back Up My Computer** feature in Symantec System Recovery Disk.
Advanced	Lets you add, among other things, security options to the recovery point. See "Advanced options for drive-based backups" on page 86.
Command Files	Lets you use command files (.exe, .cmd, .bat) during a backup. See "About running command files during a backup" on page 83.
Description	Indicates a description for the recovery point. The description can be anything that helps you further identify the recovery point's contents.

See "Defining a drive-based backup" on page 74.

Advanced Scheduling options

The following table describes the properties of the **Advanced Scheduling** panel.

Table 6-7   Advanced Scheduling options

Option	Description
Schedule	Lets you select the days and a start time for when the backup should run.
Run more than once per day	Indicates that you can run the backup more than once a day to protect data that you edit or change frequently.
Time between backups	Specifies the maximum time that should occur between backups.
Number of times	Specifies the number of times per day that the backup should run.
Automatically optimize	Lets you select how often optimization should occur to help manage the disk space that is used by your backup destination.
Start a new recovery point set	Indicates how frequently a new recovery point set should be started.
Custom	Lets you customize the start time, and the days of the week or month to run the backup.
Event Triggers - General	Lets you select the type of events that automatically starts a backup. See "Enabling event-triggered backups" on page 122.
Event Triggers - ThreatCon Response	Lets you set the ThreatCon Response level that automatically starts a backup. See "ThreatCon Response options" on page 125.

See "Defining a drive-based backup" on page 74.

About files that are 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 file names do appear in recovery points, but they are placeholders. They contain no data.

See "Defining a drive-based backup" on page 74.

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 Symantec 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. If the default location is a computer on a network, you can also click the **Edit** option and specify the necessary 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 Symantec System Recovery service to use this account.

See "Defining a drive-based backup" on page 74.

See "About files that are excluded from drive-based backups" on page 82.

About running command files during a backup

You can use command files (.exe, .cmd, .bat) during a backup. You can use command files to integrate Symantec 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 causes the backup job to fail.

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

- Run before snapshot creation
- Run after snapshot creation
- Run after recovery point creation

See "Command files options" on page 84.

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 Symantec System Recovery before you use them during a backup.

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

See "Defining a drive-based backup" on page 74.

See "Running a one-time backup from Symantec System Recovery" on page 93.

Command files options

The following table describes the options that are available in the **Command file** panel.

Table 6-8   Command files options

Option	Description
Command files folder	Specifies 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 are prompted for network credentials.
Browse	Lets you browse to locate a folder for any command files that you want to use.
User name	Specifies the user name to a command file folder that is located in a network path.
Password	Specifies the password to a command file folder that is located in a network path.
Run before snapshot creation	Indicates that you can run a command file 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 to use Symantec System Recovery" on page 43.

Table 6-8   Command files options *(continued)*

Option	Description
Run after snapshot creation	Indicates that you can run a command file 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.
Run after recovery point creation	Indicates that you can run a command file after the recovery point file 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.
Timeout (applies to each stage)	Lets you specify the amount of time (in seconds) that a command file is allowed to run.

See "About running command files during a backup" on page 83.

See "Defining a drive-based backup" on page 74.

See "Running a one-time backup from Symantec System Recovery" on page 93.

Advanced options for drive-based backups

The following table describes the Advanced options that are available when you create a drive-based backup.

Table 6-9   Advanced options for drive-based backups

Option	Description
Divide into smaller files to simplify archiving	Splits the recovery point into smaller files and specifies the maximum size (in MB) for each file.

Table 6-9   Advanced options for drive-based backups *(continued)*

Option	Description
Disable SmartSector™ Copying	Copies used and unused hard-disk sectors. This option increases process time and usually results in a larger recovery point. SmartSector technology speeds up the copying process by copying only 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.
Ignore bad sectors during copy	Runs 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.
Perform full VSS backup	Lets you perform a full backup on the VSS storage and send a request for VSS to review its own transaction log. This option is used for VSS applications, such as Microsoft Exchange Server 2003 or Microsoft SQL. VSS determines what transactions are already committed to the database and then truncates those transactions. Among other things, truncated transaction logs help keep the file size manageable and limits the amount of hard drive space that the file uses. If you do not select this option, backups still occur on the VSS storage. However, VSS does not automatically truncate the transaction logs following a backup. **Note:** This option does not appear if you create a recovery point using the **Back Up My Computer** wizard feature in Symantec System Recovery Disk.

Table 6-9   Advanced options for drive-based backups *(continued)*

Option	Description
Use password	Sets a password on the recovery point when it is created. Passwords can include standard characters. Passwords cannot include 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	Encrypts recovery point data to add another level of protection to your recovery points.
	Choose from the following encryption levels:
	■ **Standard 128-bit (8+ character password)**
	■ **Medium 192-bit (16+ character password)**
	■ **High 256-bit (32+ character password)**

See "Defining a drive-based backup" on page 74.

See "About files that are excluded from drive-based backups" on page 82.

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 **Tasks** menu, click **Run or Manage Backups**.

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

3   Click **Next** twice.

4   Click **Advanced**.

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

     See "Advanced options for drive-based backups" on page 86.

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

See "Defining a drive-based backup" on page 74.

See "About files that are excluded from drive-based backups" on page 82.

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 Symantec System Recovery. However, encrypting those files makes 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.

The following table explains the bit strength and required password length.

Table 6-10   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 recovery point that is password encrypted, Symantec 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 cannot open an encrypted recovery point.

Besides bit strength, the format of the password can improve the security of your data.

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

■ Do not use consecutive repeating characters (for example, BBB or 88).

■ Do not use common words 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.

See "Defining a drive-based backup" on page 74.

See "Backing up files and folders" on page 107.

See "Verifying the integrity of a recovery point" on page 90.

Verifying the integrity of a recovery point

If you selected the **Verify recovery point after creation** option on the **Options** panel of the **Define Backup** wizard, the following occurs:

- Symantec System Recovery verifies 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 that is required to create a recovery point is doubled when you use the **Verify recovey point after creation** option.

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

See "Advanced options for drive-based backups" on page 86.

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 **OK**.

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**.

See "About recovery point encryption" on page 89.

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**.

See "Defining a drive-based backup" on page 74.

See "Backing up files and folders" on page 107.

Backup time options

The following tables describe the options on the **Backup Time** panel. The options vary depending on the backup type you create.

Table 6-11   Backup time options for a recovery point set

Option	Description
Schedule	Runs the backup automatically according to a specified start time and the selected days of the week.
Default	Lets you use the default backup time schedule.
Advanced	Sets advanced scheduling options, such as setting up event triggers that start the backup in response to specific events. See "Advanced Scheduling options" on page 81.
Run more than once per day	Sets the time between backups and the number of times to back up.
Start a new recovery point set (base)	Starts a new recovery point set (base) weekly, monthly, quarterly, or yearly.
Custom	(Optional) Indicates how frequently a new recovery point set should be started. For example, if you select **Monthly**, a new base recovery point is created the first time the backup runs during each new month.
Select event triggers	Lets you select events that will automatically create a recovery point.
Details	Shows you information about the backup time option you have selected or specified.

Table 6-12 Backup Time options for an independent recovery point

Option	Description
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** dialog box appears.
Monthly	Runs the backup at the time and on the days of the month that you specify. When you select this option, the **Select the days of the month to protect** dialog 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** dialog box appears.
Details	Indicates information about the backup time option you have selected or specified.

See "Defining a drive-based backup" on page 74.

See "Editing a backup schedule" on page 126.

Compression levels for recovery points

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

The following table describes the available compression levels.

Table 6-13 Compression level options

Option	Description
None	Indicates that no compression is applied to the recover point. 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)	Uses low compression for a 40 percent average data compression ratio on recovery points. This setting is the default.

Table 6-13   Compression level options *(continued)*

Option	Description
Medium	Uses medium compression for a 45 percent average data compression ratio on recovery points.
High	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 Symantec System Recovery. This might improve the performance of other resource-intensive applications that you are running at the same time.

See "Defining a drive-based backup" on page 74.

See "Making copies of recovery points" on page 177.

Running a one-time backup from Symantec System Recovery

You can use **One Time Backup** to 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.

You can also use Symantec System Recovery Disk to create one-time cold backups.

See "About running a one-time backup from Symantec System Recovery Disk" on page 94.

To run a one-time backup from Symantec System Recovery

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

2   Click **Next**.

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

4   If the **Related Drives** dialog box is displayed, set the appropriate option, and
    then click **Next**. Otherwise, skip to the next step.

    See "Related drives options" on page 75.

5   In the **Backup Destinations** panel, select the appropriate options.

    See "Backup destination options" on page 77.

6   Click **Next**.

7   On the **Options** panel, select the appropriate options.

    See "Recovery point options" on page 79.

8   Click **Next**.

9   If appropriate, in the lists, select the command files that you want to run
    during a particular stage in the recovery point creation process. 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 **Command Files folder**, you may need
    to click **Back**, and then **Next** to see the files in each stage's list.

    See "Command files options" on page 84.

10 Click **Next**.

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

About running a one-time backup from Symantec System Recovery Disk

Using a valid license key, you can create independent recovery points using the
Back Up My Computer feature in Symantec System Recovery Disk. You can create
recovery points of a partition without the need to install Symantec System
Recovery or its agent. This feature is sometimes known as a cold backup or offline
backup.

With a cold backup, all files are closed when the backup occurs. You do not copy
any data that may be in the middle of being updated or accessed on the desktop
or server. Cold backups are particularly useful for databases. They ensure that
no files are written to or accessed at any time during the backup so you have a
complete recovery point.

You can also use the Symantec System Recovery Disk to create recovery points
if you experience any of the following:

■   A level of corruption prevents you from starting Windows on the computer.

- Symantec System Recovery does not function properly while it runs on a Windows operating system.

- You want to back up the condition of a damaged system before you recover. For example, if a computer is severely damaged, you can use the Symantec System Recovery Disk. You can back up what remains of the system. Then, you can recover what you can later, after you restore an independent recovery point.

Note: Recovery points that you create using Symantec System Recovery Disk are restored to dissimilar hardware using Restore Anyware.

When you want to create a backup fromSymantec System Recovery Disk , you are prompted for a valid license key only for the following scenarios:

- You use the original, shipping version of the Symantec System Recovery Disk CD to create a backup of a computer. The computer does not have Symantec System Recovery installed.

- The computer that you intend to back up using the original, shipping version of the Symantec System Recovery Disk CD has an unlicensed installation of the software.

- You create a custom Symantec System Recovery Disk on a computer that has an unlicensed installation (60-day trial) of Symantec System Recovery. You then use the custom Symantec System Recovery Disk to create a backup of a computer. The computer does not have an installation of Symantec System Recovery.
  See "Creating a custom Symantec System Recovery Disk" on page 37.

- You choose not to add a license key at the time you create the customized Symantec System Recovery Disk.

Running a one-time backup from Symantec System Recovery Disk

Using a valid license key, you can create independent recovery points using the **Back Up My Computer** feature in Symantec System Recovery Disk. You can create recovery points of a partition without the need to install Symantec System Recovery or its agent. This feature is sometimes known as a cold backup or offline backup.

To run a one-time backup from Symantec System Recovery Disk

1   If you intend to store the resulting recovery point on a USB device (for example, an external hard drive), attach the device now.

2   Start the Symantec System Recovery Disk on the computer you want to back up.

    See "Booting a computer by using the Symantec System Recovery Disk" on page 228.

3   On the **Home** panel, click **Back Up My Computer**, and then click **Next**.

4   On the **Welcome** panel, click **Next**.

5   If you are prompted, on the **Specify License Key** panel, enter a valid license key, and then click **Next**.

6   On the **Drives** panel, select one or more drives that you want to back up, and then click **Next**.

7   On the **Backup Destination** panel, set the options you want, then click **Next**.

    See "Backup Destination options" on page 96.

8   On the **Options** panel, set the desired backup options and advanced options for the recovery point.

    See "Back Up My Computer options" on page 97.

9   On the **Options** panel, click **Advanced**.

10   On the **Advanced options** panel, set the advanced backup options you want for the recovery point, and then click **OK**.

    See "Advanced options" on page 98.

11   On the **Options** panel, click **Next**.

12   On the **Completing the Back Up My Computer Wizard** panel, click **Finish** to run the backup.

13   When the backup is finished, click **Close** to return to the main Symantec System Recovery Disk window.

See "About running a one-time backup from Symantec System Recovery Disk" on page 94.

Backup Destination options

The following table describes the options on the **Backup Destination** panel. This panel is available from the **Back Up My Computer** wizard in Symantec System Recovery Disk.

Table 6-14   Backup Destination options

Option	Description
Folder	Lets you browse to and specify the location where you want to store the independent recovery point.
Map a network drive	Maps a network drive by using the UNC path of the computer on which you want to store the recovery point. For example, \\computer_name\share_name or \\IP_address\share_name.
Browse	Lets you browse to locate a backup destination that you want to use.
Destination Details	Displays the type of destination path. If you add a network path it also displays the user name.
Recovery point file name	Lets you edit the recovery point file name.
Rename	Lets you rename the recovery point file name. Default file names include the name of the computer and then followed by the drive letter.

See

Back Up My Computer options

The following table describes the options on the **Options** panel. This panel is available from the **Back Up My Computer** wizard in Symantec System Recovery Disk.

Table 6-15   Back Up My Computer options

Options	Description
Compression	Lets you set one of the following compression levels for the recovery point: ■ None ■ Standard ■ Medium ■ High See "Compression levels for recovery points" on page 92. The results can vary depending on the types of files that are saved in the drive.
Verify recovery point after creation	Tests whether a recovery point or set of files is valid or corrupt.
Description	Indicates a description for the recovery point. The description can help you further identify the recovery point's contents.
Advanced	Lets you further add security options to the recovery point. See "Advanced options" on page 98.

See "Running a one-time backup from Symantec System Recovery Disk" on page 95.

Advanced options

The following table describes the options on the **Advanced options** panel. This panel is available from the **Back Up My Computer** wizard in Symantec System Recovery Disk.

Table 6-16   Advanced options for drive-based backups

Option	Description
Divide into smaller files to simplify archiving	Lets you split the recovery point into smaller files and specify the maximum size (in MB) for each file.

Table 6-16   Advanced options for drive-based backups *(continued)*

Option	Description
Disable SmartSector™ Copying	Lets you copy used and unused hard-disk sectors. This option increases process time and usually results in a larger recovery point. SmartSector technology speeds up the copying process by copying only 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.
Ignore bad sectors during copy	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	Sets a password on the recovery point when it is created. Passwords can include standard characters. Passwords cannot include extended characters, or symbols. (Use characters with an ASCII value of 128 or lower.) A user must type this password before they can restore a backup or view the contents of the recovery point.
Use AES encryption	Encrypts recovery point data to add another level of protection to your recovery points. Choose from the following encryption levels: ■ **Standard 128-bit (8+ character password)** ■ **Medium 192-bit (16+ character password)** ■ **High 256-bit (32+ character password)**

See "Back Up My Computer options" on page 97.

See "Running a one-time backup from Symantec System Recovery Disk" on page 95.

About Offsite Copy

Backing up your data to a secondary hard disk is a critical first step to protecting your information assets. But to make certain your data is safe, use **Offsite Copy**.

This feature can copy your latest complete recovery points to the following:

■ A portable storage device.

■ A remote server in your network.

■ 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 inaccessible. Offsite Copy can double your data protection by ensuring that you have a remote copy.

See "How Offsite Copy works" on page 100.

See "About using external drives as your offsite copy destination" on page 101.

See "About using a network server as your offsite copy destination" on page 103.

See "About using an FTP server as your offsite copy destination" on page 104.

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 is available. **Offsite Copy** then begins copying the new recovery points to the offsite copy destination.

The most recent recovery points are copied first, followed by the next newest 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 6:00 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 safekeeping. When the backup job completes at 6:20 p.m., Symantec System Recovery detects that the offsite copy destination drive is not available and the copy process is aborted.

The following morning, you plug the drive back in to the computer. Symantec 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 few 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 "About using external drives as your offsite copy destination" on page 101.

See "About using a network server as your offsite copy destination" on page 103.

See "About using an FTP server as your offsite copy destination" on page 104.

See "Defining a drive-based backup" on page 74.

See "Editing backup settings" on page 122.

About using external drives as your offsite copy destination

You can 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 site 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 from unauthorized access.

See "About recovery point encryption" on page 89.

Before you leave the office on Monday evening, you plug in drive A and take drive B home with you.
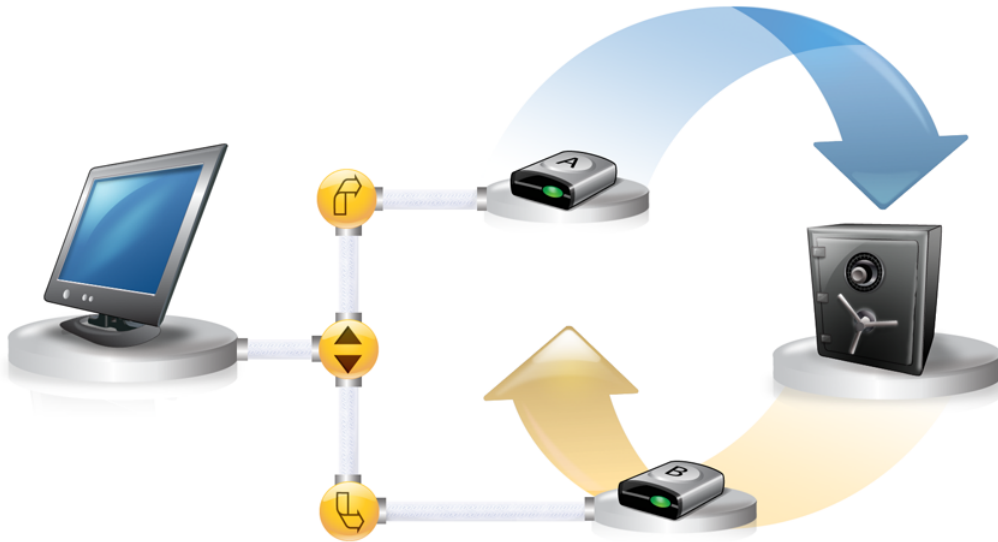
On Tuesday morning, you find that Monday's base recovery point has been successfully copied to drive A. At the end of the day, you unplug drive A and take it home for safekeeping.

On Wednesday morning, you bring drive B to the office. You plug in drive B and Symantec System Recovery detects that drive B is an offsite copy destination. Symantec 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 to each drive. Then place matching physical labels on each external drive to help you manage the task of swapping the drives.

See "About using unique names for external drives" on page 53.

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.

See "How Offsite Copy works" on page 100.

About using a network server as your offsite copy destination

You can 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 that were created since the last connection. If there is no room to hold all of the recovery points that are available, **Offsite Copy** removes the oldest recovery points from the network server. In turn, it makes room for the newest recovery points.
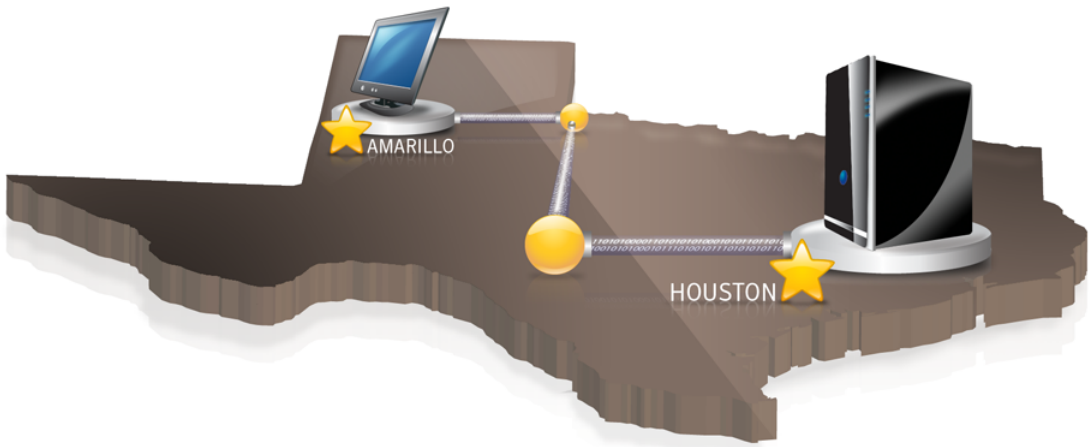
See "How Offsite Copy works" on page 100.

About using an FTP server as your offsite copy destination

Using an FTP server as your offsite copy destination is similar to using a network path. You must provide a valid FTP path to the FTP server.

You must also provide the correct FTP connection information to Symantec System Recovery 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 that were created since the last connection. If there is no room to hold all of the recovery points that are available, **Offsite Copy** removes the oldest recovery points or recovery point sets from the FTP server. In turn, it makes room for the newest recovery points.

See "Configuring default FTP settings for use with Offsite Copy" on page 54.

See

Backing up files and folders

This chapter includes the following topics:

■ About backing up files and folders

About backing up files and folders

You can back up specific files and folders you want to protect. When you run this type of backup, copies are made of the files and folders you chose to back up. The files are converted into a compressed format. They are then stored in a subfolder at the location you specify. By default this location is the same backup destination that is used for storing recovery points.

The following folders and their contents are excluded by default 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).

If you want, you can choose to include these folders when you define the backup.

Backing up files and folders

You can select specific files and folder to back up.

To back up files and folders

1   On the **Tasks** menu, 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 box appears.

3   Select **Back up selected files and folders**, and then click **Next**.

4   On the **Select Files and Folders to Back Up** panel, select the files and folders
    that you want to include in your backup.

    See "Select Files and Folders to Back Up options" on page 109.

    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.

    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   Click **Next**.

6   In the **Name and Destination** panel, enter a backup name and destination.

    See "Name and Destination options" on page 111.

7   Click **Next**

8   In the **Backup Time** panel, select the scheduling options you want.

    Note: Ensure that the time for running a base backup and an incremental
    backup is not the same.

    See "Backup Time options for a file and folder backup" on page 113.

9   Click **Next**.

10 In the **Completing the Define Backup Wizard** panel, review the backup options
    you have selected.

11 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 can take several minutes.

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

See "About backing up files and folders" on page 107.

Select Files and Folders to Back Up options

The following table describes the options on the **Select Files and Folders to Back Up** panel.

Table 7-1 Select Files and Folders to Back Up options

Option	Description
Select All	Selects all check boxes in the **Types and Folders** column. Selected data types and folders are backed up.
Select None	Deselects all check boxes in the **Types and Folders** column. Deselected data types and folders are not backed up.
Add Folder	Lets you specify additional folders to back up. See "Add Folder options" on page 110.
Add File	Lets you specify additional files to back up.
Add File Type	Lets you specify additional data file types to back up. See "Add File Type options" on page 110.
Edit	Lets you edit the options, settings, or properties for a selected data type name or folder name in the table list.

Table 7-1   Select Files and Folders to Back Up options *(continued)*

Option	Description
Remove	Lets you remove from the table list a selected data type name or folder name that you have added.
	Default data types and folders are not removable from the table list.

See "Backing up files and folders" on page 107.

Add Folder options

The following table describes the options on the **Add Folder** panel. This panel is available from the **Select Files and Folder to Back Up** panel in the **Define Backup** wizard for files and folders.

Table 7-2   Add Folder options

Option	Description
Folder to back up	Lets you specify the path to a folder that you want to back up.
Browse	Lets you browse to a path that contains a folder that you want to back up.
Subfolders	Indicates that you want to back up all subfolders under the parent folder.
All files	Indicates that you want to back up all files in all subfolders.
Only files of type	Lets you specify the data file types that you want to back up.

See "Select Files and Folders to Back Up options" on page 109.

See "Backing up files and folders" on page 107.

Add File Type options

The following table describes the options on the **Add File Type** panel. This panel is available from the **Select Files and Folder to Back Up** panel in the **Define Backup** wizard for files and folders.

Table 7-3   Add File Type options

Option	Description
Name	Specifies the name of a data file type and folder. The name is added to the table list in the **Select Files and Folder to Back Up** panel.
Add an extension	Adds a specific data type file extension that you want to back up.
Remove an extension	Deletes a specific data type file extension from the list.
Rename an extension	Renames a specific data type file extension that you added to the list.
Restore default extension list	Restores the default file extensions that were added to the predefined list of types and folders in the **Select Files and Folder to Back Up** panel.

See "Select Files and Folders to Back Up options" on page 109.

See "Backing up files and folders" on page 107.

Name and Destination options

The following table describes the options on the **Name and Destination** panel. This panel is available in the **Define Backup** wizard for files and folders.

Table 7-4   Name and Destination options

Option	Description
Name	Indicates the name for the new backup.
Description (optional)	Lets you type a description for the new backup.
Advanced	Adds security options to the recovery point. See "Advanced Options for a file and folder backup" on page 112.
Backup destination	Indicates the default backup location. Or, you can specify your own local or network path for the recovery point files.

Table 7-4   Name and Destination options *(continued)*

Option	Description
Browse	Lets you browse to locate a folder for storing your backup data.

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, you can use the **Advanced** option. |
| **User name** | Specifies the user name if you back up to a folder that is located in a network path. |
| **Password** | Specifies the password to a network path. |

Advanced Options for a file and folder backup

The following table describes the options on the **Advanced Options** panel. This panel is available from the **Name and Destination** panel in the **Define Backup** wizard for files and folders.

Table 7-5   Advanced Options for a file and folder backup

Option	Description
Use password	Indicates whether password protection is enabled for the backup.
Password	Lets you specify a password for the backup.

Use standard characters, not extended characters, or symbols. You must type this password before you restore a backup or view its contents. |
| **Confirm password** | Lets you retype the password for confirmation. |

Table 7-5 Advanced Options for a file and folder backup *(continued)*

Option	Description
Use AES encryption	Indicates whether or not AES encryption is enabled for the backup for additional security.
	You can select from the following levels of encryption:
	■ **Standard 128-bit (8+ character password)** ■ **Medium 192-bit (16+ character password)** ■ **High 256-bit (32+ character password)**
	See "About recovery point encryption" on page 89.
Exclude	Lets you deselect any of the following folders that you do not want to include in the backup:
	■ **Windows folder** ■ **Program Files folder** ■ **Temporary folder** ■ **Temporary Internet Files folder** ■ **Save backup files to a unique subfolder**
	The folders that are listed are typically not used for storing personal files or folders. Therefore, they are all selected for backup exclusion by default. These folders are backed up when you define and run a drive-based backup of your system drive (typically C).
	See "Defining a drive-based backup" on page 74.

See "Name and Destination options" on page 111.

See "Backing up files and folders" on page 107.

Backup Time options for a file and folder backup

The following table describes the options on the **Backup Time** panel. This panel is available in the **Define Backup** wizard for files and folders.

Table 7-6   Backup Time options

Option	Description
Schedule	Indicates whether a schedule is enabled for the backup .
Default	Lets you use the default backup schedule.
Start time	Specifies the start time of the backup.
Sun Mon Tue Wed Thu Fri Sat	Lets you select the days of the week that you want the backup to run.
Advanced	Runs the backup more than once per day at a set number of times. You can also specify the amount of time that should lapse between backups. See "Change Schedule - File Backup options" on page 114.
Select event triggers	Lets you select the types of events that automatically start a backup. See "Change Schedule - File Backup options" on page 114.

See "Backing up files and folders" on page 107.

Change Schedule - File Backup options

The following table describes the options on the **Change Schedule - File Backup** panel. This panel is available from the **Backup Time** panel in the **Define Backup** wizard for files and folders.

Table 7-7   Change Schedule - File Backup scheduling options

Schedule options	Description
Schedule	Lets you select the days and a start time for when you want to back up files and folders.
Run more than once per day	Runs the backup more than once a day to protect the data that you edit or change frequently.
Time between backups	Specifies the maximum time that should occur between file and folder backups.

Table 7-7   Change Schedule - File Backup scheduling options *(continued)*

Schedule options	Description
Number of times	Specifies the number of times per day file and folder backups should run.

Table 7-8   Change Schedule - File Backup event trigger options

Event trigger options	Description
General	Lets you select the types of events that automatically start a backup, such as when you log off from the computer. See "Enabling event-triggered backups" on page 122.
ThreatCon Response	Sets the ThreatCon Response level that automatically starts a backup. See "ThreatCon Response options" on page 125.

See "Backing up files and folders" on page 107.

See "Backup Time options for a file and folder backup" on page 113.

Running and managing backup jobs

This chapter includes the following topics:

- Running an existing backup job immediately
- Adjusting the speed of a backup
- Stopping a backup or a recovery task
- Verifying that a backup is successful
- Editing backup settings
- Enabling event-triggered backups
- Editing a backup schedule
- Turning off a backup job
- Deleting backup jobs
- Adding users who can back up your computer
- Configuring access rights for users or groups

Running an existing backup job immediately

If you have a backup job already defined, you can use **Run Backup Now** to make a recovery point immediately. This feature is sometimes useful if you are about to install a software program. Or, maybe you have modified a large number of files and you do not want to wait for a regularly scheduled backup.

You can run an existing backup job at any time.

To run an existing backup immediately from the system tray

1   On the Windows desktop, right-click the Symantec 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 Symantec System Recovery and define a backup.

To run an existing backup immediately from within Symantec System Recovery

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

2   Select a backup from the list, and then click **Run Now**.

See "Running a one-time backup from Symantec System Recovery" on page 93.

See "Enabling event-triggered backups" on page 122.

See "Editing a backup schedule" on page 126.

Running a backup with options

You can use **Run Backup With Options** to run an existing drive-based backup but create an alternate type of recovery point.

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

To run a backup with options

1   On the **Tasks** menu, 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   On the **Tasks** menu, click **Run Backup With Options**.

4 On the **Run Backup With Options** panel, select the appropriate 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 **Incremental recovery point of recent changes** because the base recovery point is not yet created.

See "Run Backup With Options properties" on page 119.

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

See "Editing a backup schedule" on page 126.

See "Editing backup settings" on page 122.

Run Backup With Options properties

The following table describes the options that are available in the **Run Backup With Options** dialog box.

Table 8-1 Run Backup With Options properties

Options	Description
Incremental recovery point of recent changes	Creates a backup that includes the changes that were made to the drive since the last backup. This option is available only if a base recovery point exists.
New recovery point set	Starts a completely new recovery point set and creates a base recovery point.
Independent recovery point	Creates an independent recovery point, which is a complete snapshot of your entire drive. After you select this option, you must enter a backup location.
Folder	Indicates the location where you want to store the recovery point.
Browse	Lets you browse to locate a backup destination that you want to use.
Description Details	Displays the type of destination path. If you add a network path it also displays the user name.

Table 8-1   Run Backup With Options properties *(continued)*

Options	Description
Edit	Lets you enter the user name and password for access to the network that is specified in the **Folder** field. This option is available only if you selected a backup destination that is on a network. Or, if you want to save the recovery point on a network share. See "About network credentials" on page 83.

See "Running a backup with options" on page 118.

Adjusting the speed of a backup

Depending on your computer's speed, amount of installed RAM, and the number of programs you run during a backup, your computer can 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 while you work on your computer and do not want the backup process to slow you down.

To adjust the speed 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 quickly, and you have minimal work to do on your computer, drag the slider toward **Fast**.

3   When you are finished, click **Hide** to dismiss the **Progress and Performance** dialog box.

See "Defining a drive-based backup" on page 74.

See "Editing backup settings" on page 122.

Stopping a backup or a recovery task

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

To stop a backup or a recovery task

◆ Do one of the following:

■ If the Progress and Performance dialog box is displayed, click **Cancel Operation**.

■ If the Progress and Performance dialog box is hidden, on the **View** menu, click **Progress and Performance**, and then click **Cancel Operation**.

■ If the **Progress and Performance** dialog box is hidden, on the Windows system tray, right-click the Symantec System Recovery tray icon. Click **Cancel Current Operation**.

See "Defining a drive-based backup" on page 74.

See "Editing backup settings" on page 122.

Verifying that a backup is successful

After a backup completes, you can validate the success of the backup to ensure that 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 "About the icons on the Status page" on page 150.

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 verification 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 the integrity of a recovery point" on page 90.

To verify that a backup is successful

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.

See "Defining a drive-based backup" on page 74.

See "Editing backup settings" on page 122.

Editing backup settings

You can edit 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 edit every setting except the option to change the recovery point type.

To edit backup settings

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

2   Select a backup to edit.

3   On the **Run or Manage Backups** toolbar, click **Edit Settings**.

4   Make changes to the backup.

See "Defining a drive-based backup" on page 74.

See "Enabling event-triggered backups" on page 122.

Enabling event-triggered backups

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

For example, when you install new software, a backup can run when it detects that new software is about to be 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 Symantec System Recovery to automatically run a backup when the following events occur:

■   Any application is installed or uninstalled.

■   A specified application is started.

■   Any user logs on or off of the computer.

■   The data that was added to a drive exceeds a specified number of megabytes. This option is unavailable for backing up files and folders.

To enable event-triggered backups

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

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

3   Under **Event Triggers**, click **General**.

4 Select the events you want to be detected.

See "General Event Trigger options" on page 123.

See "ThreatCon Response options" on page 125.

5 Click **OK**.

See "Defining a drive-based backup" on page 74.

See "Editing backup settings" on page 122.

General Event Trigger options

The following table describes the options on the **Event Triggers** panel.

Table 8-2 Event Triggers - General options

Option	Description
Any application is installed or uninstall	Creates a backup at the time you initiate an install or uninstall of a software application.
Specific applications are launched	Creates a backup when you start a software application.
Application	Lets you specify the software applications that can trigger a backup when you start them. See "Trigger Application options" on page 123.
Any user logs on to the computer	Creates a backup when a user logs on to the computer.
Any user logs off to the computer	Creates a backup when a user logs off from the computer.
Data added to the drive exceeds	Creates a backup when the amount of data that is added to the hard disk exceeds a specified number of megabytes.

See "Enabling event-triggered backups" on page 122.

See "About ThreatCon Response" on page 124.

Trigger Application options

The following table describes the options on the **Trigger Application** panel.

Table 8-3   Trigger Application options

Option	Description
Application	Identifies the name of the software application's executable file (.exe, .com).
Browse	Lets you browse to a software application.
Applications that trigger a backup	Lists the software applications that can trigger a backup when you start them.
Add	Adds the software application to the list box.
Remove	Removes the software application from the list box.

See "General Event Trigger options" on page 123.

See "Enabling event-triggered backups" on page 122.

About ThreatCon Response

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

When you enable the ThreatCon Response trigger for a selected backup job, Symantec System Recovery detects changes in the threat level. Your computer must be connected to the Internet at the time. If the ThreatCon level is either reached or exceeded, the backup job in which you enabled ThreatCon Response is started automatically. You then have a recovery point to use to recover your data if your computer becomes 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 ThreatCon Response when you go online or offline. It works if you are online, but does nothing if you are offline.

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

Configuring ThreatCon Response for a backup job

You can set the ThreatCon Response level for backups.

To configure ThreatCon Response for a backup job

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

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

3   Select the desired threat option that when met or exceeded runs the selected backup job.

    See "ThreatCon Response options" on page 125.

4   Click **OK**.

    On the **Home** page, in the **Current ThreatCon Level** box, you can also click **Change ThreatCon event** to change the ThreatCon response level for a selected backup job.

See "About ThreatCon Response" on page 124.

ThreatCon Response options

The following table describes the four ThreatCon Response options.

Table 8-4   ThreatCon Response options

Option	Description
Do Not Monitor - Disable	Turns off monitoring of ThreatCon levels for the selected backup job. **Note:** Level 1 of Symantec ThreatCon indicates that there are no discernable security threats. Because level 1 suggests no threats, it is not an option.
Level 2	Indicates that security threats can occur, although no specific threats have been known to occur.
Level 3	Indicates that an isolated security threat is in progress.
Level 4	Indicates that extreme global security threats are in progress.

See "Configuring ThreatCon Response for a backup job" on page 124.

See "Enabling event-triggered backups" on page 122.

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 **Tasks** menu, click **Run or Manage Backups**.

2   Select a backup to edit.

3   On the toolbar, click **Change Schedule**.

4   Make changes to the schedule.

    See "Backup time options" on page 91.

5   Click **OK**.

See "Enabling event-triggered backups" on page 122.

Turning off a backup job

You can turn off a backup and turn it on later. When you turn off a backup, it does not run according to its defined schedule, if it has one. When a backup is turned off, triggered events do not run the backup, nor can you manually run the backup.

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

To turn off a backup job

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

2   Select the backup that you want to turn off.

3   On the **Run or Manager Backups** dialog box, on the **Tasks** menu, click **Disable Backup**.

    Repeat this procedure to turn on the backup. The **Disable Backup** menu item changes to **Enable Backup** when you disable the selected backup.

See "Deleting backup jobs" on page 126.

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 backed up file and folder data from the storage location. Only the backup job is deleted.

To delete backup jobs

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

2   Select one or more backup names.

3   On the toolbar, click **Remove**.

4   Click **Yes**.

See "About backup destinations" on page 172.

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 Symantec System Recovery.

For example, all users with Limited Windows accounts can run existing backup jobs, but they cannot create new jobs or edit existing jobs. Using the **Security Configuration Tool**, you can grant administrative privileges to a Limited user account. When you do, that user has full access to Symantec System Recovery and can create, edit, 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 or users who can back up a computer

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

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

2   Click **Add**.

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

4   Click **OK**.

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

See "Configuring access rights for users or groups" on page 127.

Configuring access rights for users or groups

You can use the **Security Configuration Tool** to give users or groups certain access rights to the features of Symantec System Recovery.

To configure access rights for users or groups

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

    On Windows Vista and Windows 7, click **Start > All Programs > Symantec System Recovery > Security Configuration Tool**.

2   In **Group or user names**, select a user or group.

3   Choose from the following options:

Permissions	Allow	Deny
Full Control	Gives a user or a group access to all of the features of Symantec System Recovery. Allows a user and group to create, edit, and delete backup jobs, including existing jobs.	Lets the selected user or group run existing backup jobs. Prevents the selected user or group from creating, editing, or deleting backup jobs.
Status Only	Lets the selected user or group run existing backup jobs. Prevents the selected user or group from creating, editing, or deleting backup jobs.	Prevents the selected user or group from accessing any of the features of Symantec System Recovery.

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

See "Adding users who can back up your computer" on page 127.

Backing up remote computers from your computer

This chapter includes the following topics:

- About backing up other computers from your computer
- About deploying the Symantec System Recovery Agent
- About the Symantec System Recovery Agent
- Best practices for using services
- About viewing Symantec System Recovery Agent dependencies
- About controlling access to Symantec System Recovery

About backing up other computers from your computer

Symantec System Recovery lets you connect to a second computer and back it up on your home or your 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 60-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 the following Web site:
>
> http://shop.symantecstore.com

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

See "Adding remote computers to the Computer List" on page 130.

See "Adding local computers to the Computer List" on page 131.

See "Removing a computer from the Computer List" on page 131.

Adding remote 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 remote computers to the Computer List

1   On the **Computers** menu, click **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. You can do so by browsing to it using the **Browse** option.

   ■ Click **Browse** to search for the name or IP address of the computer

3   Click **OK** to add the computer to the **Computer List**.

See "About backing up other computers from your computer" on page 129.

See "Adding local computers to the Computer List" on page 131.

See "Removing a computer from the Computer List" on page 131.

Adding local computers to the Computer List

Before you can back up drives on a local 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 a local computer to the Computer List

1   On the **Computers** menu, click **Add Local Computer**.

2   Click **OK**.

See "About backing up other computers from your computer" on page 129.

See "Adding remote computers to the Computer List" on page 130.

See "Removing a computer from the Computer List" on page 131.

Removing a computer from the Computer List

You can remove local or remote computers from the **Computer List**.

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

To remove a computer from the Computer List

1   On the **Computers** menu, click **Edit List**.

2   Select the remote or the local computer that you want to remove, and then click the minus sign (–).

3   Click **OK**

See "About backing up other computers from your computer" on page 129.

See "Adding remote computers to the Computer List" on page 130.

See "Adding local computers to the Computer List" on page 131.

See "Removing a computer from the Computer List" on page 131.

About deploying the Symantec System Recovery Agent

You can deploy the Symantec 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 Symantec System Recovery.

See "About backing up other computers from your computer" on page 129.

Note: Because of increased security with Windows Vista, you cannot deploy the Symantec 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 by using the product CD.

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.

Your computer must meet the minimum memory requirement to run the **Recover My Computer** wizard or the **Recovery Point Browser** in Symantec System Recovery Disk.

If you install a multilingual version of the product, you must have a minimum of 1 GB of RAM to run Symantec System Recovery Disk.

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

See "Preparing a computer in a workgroup environment to deploy the agent" on page 132.

See "Deploying the Symantec System Recovery Agent" on page 133.

See "Manually installing the Symantec System Recovery Agent" on page 134.

See "Granting rights to domain users on Windows 2003 SP1 servers" on page 135.

Preparing a computer in a workgroup environment to deploy the agent

You must complete certain steps in Windows to prepare a computer in a workgroup environment to deploy the Symantec System Recovery 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 not selected, and then click **OK**.

4   On the Windows Control Panel, click **Windows Firewall**.

    You may need to also click **Change Settings** if you are running Windows Server 2008.

5   On the **Exceptions** tab, select **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 automatically restarts at the end of the installation wizard.

See "About deploying the Symantec System Recovery Agent" on page 131.

See "Deploying the Symantec System Recovery Agent" on page 133.

See "Manually installing the Symantec System Recovery Agent" on page 134.

Deploying the Symantec System Recovery Agent

You can deploy the Symantec System Recovery Agent to local or to remote computers.

To deploy the Symantec System Recovery Agent

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

    You must have administrator rights on the computer to which you install the agent.

2   Click **Deploy Agent**.

3   In the **Deploy Symantec 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**.

See "About deploying the Symantec System Recovery Agent" on page 131.

See "Preparing a computer in a workgroup environment to deploy the agent" on page 132.

See "Manually installing the Symantec System Recovery Agent" on page 134.

Manually installing the Symantec System Recovery Agent

You can manually install the Symantec System Recovery Agent to local or to remote computers.

To manually install the Symantec System Recovery Agent

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

    The installation program should start automatically.

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

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

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

2   In the **CD browser** panel, click **Install Symantec System Recovery**.

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

4   Read the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.

5   If you want to change the default location for the program files, click **Change**. Then locate the folder in which you want to install the agent, and then click **OK**.

6   Click **Next**.

7   Click **Custom**, and then click **Next**.

8   Click **Symantec System Recovery Service**, and then click **This feature will be installed on local hard drive**.

    This feature is the agent.

9   Set all other features to **This feature will not be installed**.

10 Click **Next**, and then click **Install**.

See "About deploying the Symantec System Recovery Agent" on page 131.

See "Deploying the Symantec System Recovery Agent" on page 133.

See "Preparing a computer in a workgroup environment to deploy the agent" on page 132.

See "Manually installing the Symantec System Recovery Agent" on page 134.

Granting rights to domain users on Windows 2003 SP1 servers

You can 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 use Symantec System Recovery to remotely manage the server.

To grant rights to domain users on Windows 2003 SP1 servers

1   On the Windows taskbar, click **Start > Run**.

2   In the **Open** field of the **Run** dialog box, type **dcomcnfg** and then click **OK**

3   Navigate to **Component Services** > **Computers** > **My Computer**.

4   Right-click **My Computer**, and then select **Properties**.

5   On the **COM Security** tab, under **Launch and Activation Permissions**, click **Edit Limits**.

6   Add the domain users to the **Group or user names** list, and then allocate the appropriate permissions.

7   Click **OK**.

8   Close **Component Services**, and then restart the Symantec System Recovery service.

See "About deploying the Symantec System Recovery Agent" on page 131.

See "Deploying the Symantec System Recovery Agent" on page 133.

See "Preparing a computer in a workgroup environment to deploy the agent" on page 132.

See "Manually installing the Symantec System Recovery Agent" on page 134.

About the Symantec System Recovery Agent

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

See "Using the Symantec System Recovery Agent" on page 136.

The Symantec System Recovery Agent does, however, have a tray icon.available from the Windows system tray. The icon provides feedback of current conditions and lets you perform common tasks. For example, you can view backup jobs, reconnect the Symantec 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 installing the agent from the product CD. A more efficient method, however, is to use the Symantec System Recovery Deploy Agent feature. You can remotely install the agent on a computer in the domain whose data you want to protect.

See "About managing the Symantec System Recovery Agent through Windows Services" on page 136.

See "About controlling access to Symantec System Recovery " on page 142.

Using the Symantec System Recovery Agent

You can use the Symantec System Recovery tray icon in the Windows system tray to quickly access a variety of useful tasks.

To use the Symantec System Recovery Agent

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

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

- If Symantec System Recovery is installed on the computer, double-click the Symantec 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 the software installed, right-click the Symantec System Recovery tray icon to display a menu of common agent tasks.

See "About the Symantec System Recovery Agent " on page 135.

See "About managing the Symantec System Recovery Agent through Windows Services" on page 136.

About managing the Symantec System Recovery Agent through Windows Services

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

It provides the following:

- The ability to locally run scheduled backup jobs, even when there are no or unauthorized users that are logged on to the computer.

- The ability to allow administrators to remotely back up computers throughout an enterprise from Symantec System Recovery running on another computer.

See "Using the Symantec System Recovery Agent" on page 136.

To use the features of Symantec System Recovery, the Symantec 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 System Recovery Agent, you must be logged on as a local administrator.

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

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

  See "Starting or stopping the Symantec System Recovery Agent service" on page 140.

- Configure the user name and password that the Symantec System Recovery Agent uses.

  See "About controlling access to Symantec System Recovery " on page 142.

- Set up recovery actions to take place if the Symantec System Recovery Agent fails to start.

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

  See "Setting up recovery actions when the Symantec System Recovery Agent does not start" on page 140.

Best practices for using services

The following table 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 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.

Table 9-1   Best practices for using services *(continued)*

Best practice	Description
Verify that the Symantec System Recovery Agent starts without user intervention.	The Symantec System Recovery Agent is configured to start automatically when Symantec System Recovery starts. You can view the status information to verify that the Symantec 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 System Recovery Agent starts 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 Symantec System Recovery Agent service" on page 140.
Use caution when changing default settings for the Symantec System Recovery Agent.	Changing the default Symantec System Recovery Agent properties can prevent Symantec System Recovery from running correctly. You should use caution when changing the default **Startup type** and **Log On** settings of the Symantec System Recovery Agent. It is configured to start and log on automatically when you start Symantec System Recovery .

See "Opening Windows services " on page 138.

Opening Windows services

You can use several methods to open Windows services to manage the Symantec System Recovery Agent.

To open Windows services

1   Do one of the following:

   ■ On the Windows **Control Panel**, click **Administrative Tools > 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
Symantec System Recovery (the name of the agent).

Its status should be **Started**.

See "About starting or stopping the Symantec System Recovery Agent service"
on page 139.

See "Starting or stopping the Symantec System Recovery Agent service"
on page 140.

About starting or stopping the Symantec System Recovery Agent service

To start, stop, or restart the Symantec 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 System Recovery Agent
service for the following reasons:

Start or Restart	You should start or restart the agent if Symantec System Recovery is unable to connect to it on a computer. Or, you cannot reconnect from Symantec System Recovery.
Restart	You should restart the agent. This restart is necessary if you changed the user name or password that you use to log on to the agent service. You should also restart the agent after you have used the Security Configuration Tool to give additional users the ability to back up computers. See "About controlling access to Symantec System Recovery " on page 142.
Stop	You can stop the agent if you believe that it causes a problem on the computer, or if 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 System Recovery Agent service and then start Symantec
System Recovery, the agent restarts automatically. The Status changes to Ready.

If you stop the Symantec System Recovery Agent service while the software runs,
you receive an error message. Symantec 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 System Recovery Agent.

See "Starting or stopping the Symantec System Recovery Agent service" on page 140.

See "Setting up recovery actions when the Symantec System Recovery Agent does not start" on page 140.

Starting or stopping the Symantec System Recovery Agent service

You can start or stop the Symantec System Recovery Agent service.

To start or stop the Symantec 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 **Symantec System Recovery**.

5   On the **Action** menu, select one of the following:

   ■   **Start**

   ■   **Stop**

   ■   **Restart**

See "About starting or stopping the Symantec System Recovery Agent service" on page 139.

Setting up recovery actions when the Symantec System Recovery Agent does not start

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

To set up recovery actions when the Symantec System Recovery Agent does not 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 agent
    must run successfully before the fail count is reset.

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

7   Click **OK**.

See "About starting or stopping the Symantec System Recovery Agent service"
on page 139.

About viewing Symantec System Recovery Agent dependencies

The Symantec 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 System Recovery Agent fails to start, check the dependencies.
Check 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. Then click **Action > Properties > General**.

The top list box on the **Dependencies** tab displays services the Symantec System
Recovery Agent requires to run properly. The bottom list box does not have any
services that need the Symantec System Recovery Agent to run properly.

The following table lists the services the Symantec System Recovery Agent requires 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

See "Viewing Symantec System Recovery Agent dependencies" on page 142.

Viewing Symantec System Recovery Agent dependencies

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

To view Symantec System Recovery Agent dependencies

1　　On the Windows taskbar, click **Start > Run**.

2　　In the **Run** window, type **services.msc**

3　　Click **OK**.

4　　In the **Services** window, under **Name**, click **Symantec System Recovery**.

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

6　　Click the **Dependencies** tab.

See "About viewing Symantec System Recovery Agent dependencies " on page 141.

About controlling access to Symantec System Recovery

You can use the **Security Configuration Tool** to grant the necessary permissions to access the agent, or the full Symantec 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 Administrator's group.

The following table describes the permissions that can be allowed or denied for user and groups who use the Symantec System Recovery Agent.

Table 9-3   Permission options

Option	Description
Full Control	Gives the user or the group complete access to all Symantec 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.
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 Symantec 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.

See "Adding users and groups" on page 143.

See "Changing permissions for a user or a group" on page 144.

See "Removing a user or a group" on page 144.

See "Running Symantec System Recovery using different user rights" on page 145.

Adding users and groups

You can use the **Security Configuration Tool** to add a user or a group so they can access Symantec System Recovery.

To add users and groups

1   On the Windows taskbar, click **Start > Programs > Symantec 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.

See "About controlling access to Symantec System Recovery " on page 142.

See "Changing permissions for a user or a group" on page 144.

See "Removing a user or a group" on page 144.

See "Running Symantec System Recovery using different user rights" on page 145.

Changing permissions for a user or a group

You can use the **Security Configuration Tool** to change the Symantec System Recovery access permissions of a user or a group.

To change permissions for a user or a group

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

2 In the **Permissions for Symantec System Recovery** dialog box, select the user or group whose permissions you want to change. 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.

See "About controlling access to Symantec System Recovery " on page 142.

See "Adding users and groups" on page 143.

See "Removing a user or a group" on page 144.

See "Running Symantec System Recovery using different user rights" on page 145.

Removing a user or a group

You can use the **Security Configuration Tool** to remove a user or a group so they cannot access Symantec System Recovery.

To remove a user or a group

1   On the **Windows Start** menu, click **Programs > Symantec 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.

See "About controlling access to Symantec System Recovery " on page 142.

See "Adding users and groups" on page 143.

See "Changing permissions for a user or a group" on page 144.

See "Running Symantec System Recovery using different user rights" on page 145.

Running Symantec System Recovery using different user rights

If the permissions for a user are insufficient for running Symantec System Recovery, you can use the **Run As** feature in Windows. The **Run As** feature lets you run the software using an account that has sufficient rights. This situation is true even if you are not currently logged on with the account.

To perform Run As from Windows

1   On the Windows taskbar, click **Start > All Programs > Symantec System Recovery**.

2   Right-click **Symantec System Recovery**, and then click **Run As**.

3   In the **Run As** dialog box, click **The following user** to log onto with another account.

4   In the **User name** and **Password** fields, enter the account name and password that you want to use, and then click **OK**.

See "About controlling access to Symantec System Recovery " on page 142.

See "Adding users and groups" on page 143.

See "Changing permissions for a user or a group" on page 144.

See "Removing a user or a group" on page 144.

Monitoring the status of your backups

This chapter includes the following topics:

- About monitoring backups
- About the icons on the Home page
- About the icons on the Status page
- Configuring Symantec System Recovery to send SNMP traps
- About customizing the status reporting of a drive (or file and folder backups)
- Viewing drive details
- Improving the protection level of a drive
- About using event log information to troubleshoot problems

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 Symantec System Recovery. For example, adding hard disk space or creating a partition.

When you use Refresh, Symantec System Recovery scans all attached hard disks for any configuration changes. It also updates information on removable media, media drives, hard 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 takes place.

About the icons on the Home page

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

The following table describes each of the levels of backup protection that the **Home** page displays.

Table 10-1   Backup protection levels

Icon	Title	Description
	Backed up	At least one drive-based backup is defined and it runs on a regular basis. This status indicates that all drives, files, and folders can be fully recovered, if necessary.

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

Icon	Title	Description
	Partially backed up	A backup is defined, but it is not scheduled or has not 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.
	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 forthcoming, 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 monitored for backup status; or, it is monitored for errors only. However, there are no errors to report.
		Use the **Customize Status Report** feature on the **Status** page to change the status report setting.

See "About monitoring backups" on page 147.

About the icons on 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 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 that is displayed in the Backups calendar.

Table 10-2   Backups calendar icons

Icon	Description	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 a backup has run and 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 that is scheduled to run at a future time.

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

Icon	Description	States
	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 a backup has run and 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	States
	Represents backing up files and folders. It indicates that a backup of files and folders occurs on the day that it appears in the backup timeline.	This icon can appear in the following states: Indicates that a backup has run and that backup data for files and folders 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.

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

Icon	Description	States
	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 run and the last backup was unsuccessful. 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, you can do the following:

- On the **Status** page, review the **Backups calendar** and verify that the backup appears on the date that you ran it.

- In the **Drives** column, select the drive that you want to view.
  The status information appears in the bottom half of the **Status** page.

- Move your mouse over a backup icon in the calendar to review the status of the backup.

- 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.

See "About monitoring backups" on page 147.

See "About the icons on the Home page" on page 148.

Configuring Symantec System Recovery to send SNMP traps

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

By default, Symantec System Recovery is not enabled to send SNMP traps to NMS managers. You can configure Symantec System Recovery to send SNMP traps for different priority and notification types.

To configure Symantec 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** 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**.

See "About the Symantec System Recovery Management Information Base" on page 156.

About the Symantec System Recovery Management Information Base

The Symantec System Recovery Management Information Base (MIB) is an enterprise MIB. It contains the Symantec System Recovery SNMP trap definitions. All Network Management System (NMS) applications have options to load an MIB. You can use any of these options to load the Symantec System Recovery MIB. If you do not load the MIB, the NMS application can still receive, and display the traps. However, the traps are not displayed in informative text. The MIB file, named ssr_mib.mib, is located in the **Support** folder on the Symantec System Recovery product CD.

See "Configuring Symantec System Recovery to send SNMP traps" on page 155.

About customizing the status reporting of a drive (or file and folder backups)

You can configure how Symantec System Recovery reports the status of a particular drive (or all backups of files and folders).

For example, suppose that 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 Symantec System Recovery to ignore drive D. By ignoring it, you ensure 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 included in 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 Symantec System Recovery.

You should first determine the importance of the data that is on a particular drive. Or, the importance of data you have included in a backup of files and folders. Then you can decide on the level of status reporting to assign to it.

See "Customizing the status reporting of a drive (or file and folder backups)" on page 157.

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

You can customize the status reporting of a selected drive, or files and folders.

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 a status reporting option.

     See "Customize Status Reporting options" on page 157.

4   Click **OK**.

See "About customizing the status reporting of a drive (or file and folder backups)"
on page 156.

Customize Status Reporting options

The following table describes the options available on the **Customize Status
Reporting** dialog box.

Table 10-3   Customize Status Reporting options

Option	Description
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.

See "Customizing the status reporting of a drive (or file and folder backups)"
on page 157.

See "About customizing the status reporting of a drive (or file and folder backups)" on page 156.

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 that 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 **View** menu, click **Advanced**.

2 On the **Drives** tab, in the **Drive** column of the table, select a drive.

3 Review the **Details** section.

See "Improving the protection level of a drive" on page 158.

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, edit the schedule of a backup, or edit the settings of a backup. Or, you may need to define a new backup.

See "About backing up your data" on page 63.

To improve the protection level of a drive

1   On the **View** menu, click **Status**.

2   In the **Drives** column, select a drive that requires attention.

3   In the **Status** panel, right-click on the name of a backup job you want to edit, and then select one of the following menu items:

Run Backup Now	Runs the selected backup job immediately.
Run Backup With Options	Opens the **Run Backup With Options** dialog box, which lets you select the desired recovery point type. Recovery point option types include Incremental recovery point, Recovery point set, and Independent recovery point.
Change Schedule	Opens the **Run When** dialog box so that you can edit the backup schedule.
Edit Settings	Opens the **Define Backup Wizard**, which lets you edit the backup definition. This option takes you to the second page of the wizard.
Edit Offsite	Opens the **Offsite Copy Settings** dialog box, where you can edit or change settings for the **Offsite Copy** feature.
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 backup data of files and folders).
Disable (Enable) Backup	Turns on or turns off the backup that you have selected.
Define New Backup	Opens the **Define Backup Wizard**, where you can select between backing up your computer or backing up selected files and folders. This option is useful if a drive in the **Drives** column is not yet assigned to a backup. You can select a drive that is assigned to a backup job. Then you have access to the shortcut method for starting the **Define Backup Wizard** from the **Status** page.
Manage Backup Destination	Opens the **Manage Backup Destination** dialog box, where you can specify destination drives as well as delete, copy, or explore existing recovery points on destination drives.
Customize Status Reporting	Opens the **Customize Status Reporting** dialog box, where you can specify if you want status reporting, and the type of status reporting.

About using event log information to troubleshoot problems

When Symantec 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.

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

The following information is included in the event log:

Table 10-4   Event log information

Option	Description
Type	Indicates if the event is an error message or other information, such as the successful completion of a backup job.
Source	Identifies if Symantec System Recovery generates the message or another program.
Date	Displays the exact date and time that a selected event occurred.
Description	Lets you review information about an event that can help you troubleshoot errors.

Chapter **11**

Exploring the contents of a recovery point

This chapter includes the following topics:

- About exploring recovery points
- Exploring a recovery point through Windows Explorer
- Opening and restoring files within a recovery point
- About configuring a backup to create searchable recovery points
- Dismounting a recovery point drive
- Viewing the drive properties of a recovery point

About exploring recovery points

You can use Symantec System Recovery to explore files in a recovery point. You mount the recovery point and assign it a drive letter so 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.
- Run programs existing within a mounted recovery point.

Within a mounted recovery point, programs that you run cannot rely on any registry values. The programs also cannot rely on 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 from 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 created, edited, or deleted at the time.

See "Exploring a recovery point through Windows Explorer" on page 164.

See "Dismounting a recovery point drive" on page 167.

See "Viewing the drive properties of a recovery point" on page 167.

Exploring a recovery point through Windows Explorer

When you explore a recovery point, Symantec System Recovery mounts the recovery point as a drive letter and it opens 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 **Tasks** menu, 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** column, select a recovery point, and click **OK**.

See "About exploring recovery points" on page 163.

Mounting a recovery point from Windows Explorer

You can 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 Windows Explorer search feature. You can locate the file, as you normally 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** list, select the letter that you want to associate with the drive.

5   Click **OK**.

6   To mount additional drives, repeat steps 1-5.

See "About exploring recovery points" on page 163.

Opening and restoring 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 by saving them using the application that is associated with them. Or, you can restore files by using the **Recover Files** option 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 encrypted file system (EFS) NTFS volumes.

To open files within 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 dimmed (unavailable) if you select program files with any of the following file extensions.

.exe

.dll

.com

To restore files within 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 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 you want to view and click **View File**.

The **View** option is dimmed (unavailable) if you select program files with any of the following file extensions.

.exe

.dll

.com

6 In the **Recovery Point Browser**, in the list panel on the right, select one or more files.

7 Click **Recover Files**, and then click **Recover** to restore them to their original location.

If you are prompted, click **Yes**, or **Yes to All** to overwrite the existing (original) files.

See "About exploring recovery points" on page 163.

See "About configuring a backup to create searchable recovery points" on page 167.

About configuring a backup to create searchable recovery points

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 Retrieve, it is likely that your network administrator has already enabled this feature.

Be sure to select the **Enable search engine support** option at the time you define the backup.

See "To define a drive-based backup" on page 74.

See "About using a search engine to search recovery points" on page 277.

Dismounting 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 drive

1   Do one of the following:

- ■ To dismount a recovery point drive in **Windows Explorer**, navigate to the mounted recovery point.

- ■ To dismount a recovery point drive in **Recovery Point Browser**, in the tree view, locate the mounted recovery point.

2   Right-click the mounted recovery point that is displayed as a drive, and then click **Dismount Recovery Point**.

See "About exploring recovery points" on page 163.

See "Viewing the drive properties of a recovery point" on page 167.

Viewing the drive properties of a recovery point

You can use **Properties** to view various drive properties of a recovery point.

To view the drive properties of a recovery point

1   In the **Recovery Point Browser**, in the tree panel on the left, 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**.

See "About exploring recovery points" on page 163.

See "Recovery point drive properties" on page 168.

Recovery point drive properties

The following table describes the drive properties on the **Recovery Point Properties** dialog box.

Table 11-1   Recovery point drive properties

Property	Description
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 that is 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 MB) of the drive. This total includes used space and unused space.
Used space	The amount of used space (in MB) within the drive.
Unused space	The amount of unused space (in MB) within the drive.
Contains bad sectors	Indicates if any bad sectors exist on the drive.

Table 11-1   Recovery point drive properties *(continued)*

Property	Description
Cleanly quiesced	Indicates whether the database application quiesced properly when a recovery point was created.

See "Viewing the drive properties of a recovery point" on page 167.

See "About exploring recovery points" on page 163.

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.

Symantec 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.

See "Cleaning up old recovery points" on page 174.

See "Deleting a recovery point set" on page 175.

See "Deleting recovery points within a set" on page 175.

See "Making copies of recovery points" on page 177.

About backup methods

Symantec 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 or folder, or your entire drive.
	See "About drive-based backups" on page 172.
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.
	See "About file and folder backups" on page 173.

See "About defining a drive-based backup" on page 73.

See "About backing up files and folders" on page 107.

About drive-based backups

When you run a drive-based backup, a snapshot of everything is taken and 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. You can use the recovery point to restore your computer back to the way it was when the snapshot 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 than a recovery point set.
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. These recovery points capture only the changes that were 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.

See "About backup methods" on page 172.

See "About backing up files and folders" on page 107.

About file and folder backups

You can edit or create a select set of personal documents and folders, and then define a backup for those files and folders. For example, you might want to define a backup to capture one or more folders. Within those folders contain the files that you change on a regular basis. This kind of backup is useful because you do not need to use additional hard disk resources to back up your entire computer.

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

Symantec System Recovery also keeps multiple versions of the same files for you. This redundancy means you can restore the version of a file that contains the changes you need to restore. You can even set a limit to the number of versions that are kept so that you can control the use of disk space.

See "About backup methods" on page 172.

See "About defining a drive-based backup" on page 73.

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 the management of backup data" on page 204.

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 you delete a recovery point, 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.

To clean up old recovery points

1   On the **View** menu, click **Tools**.

2   Click **Manage Backup Destination**.

3   Do one of the following:

   ■   In the **Clean Up Recovery Points** dialog box, select the recovery points that you want to delete.

   ■   In the **Manage Backup Destination** window, on the toolbar, click **Clean Up**. Select the recovery points that you want to delete.

   The recovery point sets that can be safely removed without eliminating your latest recovery point are selected automatically. You can also select or deselect the recovery point sets to specify which ones to remove.

4   Click **Delete**.

5   Click **Yes** to confirm the deletion.

6   Click **OK**.

See "Opening and restoring files within a recovery point" on page 165.

See "About exploring recovery points" on page 163.

See "Deleting a recovery point set" on page 175.

See "Deleting recovery points within a set" on page 175.

See "Making copies of recovery points" on page 177.

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: After 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 **View** menu, click **Tools**.

2   Click **Manage Backup Destination**.

3   In the **Recovery Point Sets** table, select a recovery point set that you want to delete.

    The recovery point set you select should have just one set associated with it and appear as "1 Recovery Point" in the table.

4   In the **Manage Backup Destination** window, on the **Tasks** menu, click **Delete**.

5   In the **Delete Recovery Point Set** dialog box, click **Yes** to confirm the deletion.

6   Click **OK**.

See "Cleaning up old recovery points" on page 174.

See "Deleting recovery points within a set" on page 175.

See "Making copies of recovery points" on page 177.

See "About exploring recovery points" on page 163.

Deleting recovery points within a set

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

The **Delete Recovery Points** option lets you delete all of the recovery points that were 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 and restoring files within a recovery point" on page 165.

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

See "Cleaning up old recovery points" on page 174.

To delete recovery points within a set

1   On the **View** menu, click **Tools**.

2   Click **Manage Backup Destination**.

3   In the **Recovery Point Sets** table, select the recovery point set that contains recovery points that you want to delete.

    The recovery point set you select should have more than one set associated with it. For example, a recovery point set that contains more than one recovery point may appear as "4 Recovery Points" in the table.

4   In the **Manage Backup Destination** window, on the **Tasks** menu, click **Delete**.

5   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**.

6   Click **OK**.

See "Deleting a recovery point set" on page 175.

See "Making copies of recovery points" on page 177.

See "About exploring recovery points" on page 163.

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 **View** menu, click **Tools**.

2   Click **Manage Backup Destination**.

3   In the **Recovery Point Sets** table, select a recovery point set.

4   In the **Manage Backup Destination** window, on the **Tasks** menu, click **Copy**.

5   If the **Copy Recovery Point** dialog box is displayed, select a recovery point within the set that you want to copy. Otherwise, skip to the next step.

6   On the **Welcome** panel of the **Copy Recovery Point Wizard**, click **Next**.

7   Do one of the following:

   ■ If you selected a recovery point in step 5, the recovery point that you want to copy is already highlighted (selected) for you in the **Date** table of the **Source** panel. Click **Next**.

   ■ On the **Source** panel, select the recovery point that you want to copy. See "Source options" on page 178.
   Recovery point sets appear as single recovery points. Select **View all recovery points** to display all incremental recovery points that are included within the recovery point sets.

8   Click **Next**.

9   In the **Destination Location** panel, specify the folder path where you want to copy the recovery point, and then click **Next**.

   See "Destination Location options" on page 180.

10 On the **Options** panel, set the options you want.for the copied recovery point, and then click **Next**.

   See "Copy recovery point options" on page 181.

11 Review the options that you selected, and then click **Finish**.

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

See "Deleting a recovery point set" on page 175.

See "Cleaning up old recovery points" on page 174.

See "Deleting recovery points within a set" on page 175.

See "About exploring recovery points" on page 163.

Source options

The following table describes the options on the **Source** panel. This panel is available in the **Copy Recovery Point Wizard** wizard from the **Manage Backup Destination** window.

Table 12-1   Source options when you copy recovery points by Date

Option	Description
View by - Date	Displays all of the discovered recovery points in the order in which they were created.
Date	Lets you select an alternate date by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.
View all recovery points	Lets you view all recovery points that are available.

Table 12-2   Source options when you copy recovery points by File name

Option	Description
View by - File name	Lets you view recovery points by their file name.
File name	Specifies a path and a file name of a recovery point.

Table 12-2   Source options when you copy recovery points by File name
(continued)

Option	Description
Browse	Lets you browse to a path that contains a recovery point.
	For example, you can browse for a recovery point (.v2i) or incremental recovery point (.iv2i) file on an external (USB) drive. Or, you can browse to a network location, or removable media.
User name	Specifies the user name if you specify a recovery point file name that is located in a network path.
	See "About network credentials" on page 83.
Password	Specifies the password to a network path.

Table 12-3   Source options when you copy recovery points by System

Option	Description
View by - System	Lets you use the current system index file that is located in the recovery point storage location. The system index file displays a list of all of the drives on your computer and any associated recovery points from which you can select.
	The use of a system index file reduces the time it takes to convert multiple recovery points. 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.
Date	Lets you select an alternate date of a system index file date by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.

Table 12-3   Source options when you copy recovery points by System *(continued)*

Option	Description
Use latest recovery points for this computer	Restores the most recent recovery points that exist in the recovery point storage location on your computer. The list of drives, source files (.v2i and .iv2i files), and dates comes from the most current system index file (.sv2i).
Use alternate system index (.sv2i) file	Restores recovery points that exist on another computer.
Browse to and select the .sv2i file for the desired system	Specifies a path to a system index file (.sv2i) file that resides elsewhere, such as a network location. If you selected a system index file that is stored on a network, you are prompted for your network credentials. See "About network credentials" on page 83.
Browse	Lets you browse to a path that contains a system index file. For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.
Drives	Lets you select the drives with the recovery points that you want to restore based on the selected system index file.

See "Making copies of recovery points" on page 177.

Destination Location options

The following table describes the options on the **Destination Location** panel. This panel is available in the **Copy Recovery Point Wizard** wizard from the **Manage Backup Destination** window.

Table 12-4   Destination Location options

Option	Description
Folder	Lets you type the path to which you want to copy the recovery point.
Browse	Lets you browse to a folder path where you want to copy the recovery point.
Edit	Lets you edit the destination information.
File name	Lets you select a file name that you want to rename.
Rename	Lets you renames the file that you have selected in the File name table.

See "Making copies of recovery points" on page 177.

Copy recovery point options

The following table describes the options on the **Options** panel. This panel is available in the **Copy Recovery Point Wizard** wizard from the **Manage Backup Destination** window.

Table 12-5   Copy recovery point options

Option	Description
Compression	Lets you use one of the following compression levels for the recovery point: ■ None ■ Standard ■ Medium ■ High See "Compression levels for recovery points" on page 92. The results can vary depending on the types of files that are saved in the drive.
Verify recovery point after creation	Verifies whether the recovery point is valid after it is created.

Table 12-5   Copy recovery point options *(continued)*

Option	Description
Enable search engine support	Lets 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. This option is for NTFS file systems only. See "About using a search engine to search recovery points" on page 277.
Include system and temporary files	Includes indexing support for operating system and temporary files when a recovery point is created or copied on the client computer.
Advanced	Lets you add, among other things, security options to the recovery point. See "Advanced Options" on page 182.
Description	Indicates a description for the recovery point. The description can be anything that helps you further identify the recovery point's contents.

See "Making copies of recovery points" on page 177.

Advanced Options

The following table describes the options on the **Advanced Options** panel. This panel is available in the **Copy Recovery Point Wizard** wizard from the **Manage Backup Destination** window.

See "Copy recovery point options" on page 181.

Table 12-6   Advanced options for drive-based backups

Option	Description
Divide into smaller files to simplify archiving	Lets you split the recovery point into smaller files and specifies 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 maximum file size of 100 MB, according to the size of each ZIP disk.
Use password	Sets a password on the recovery point when it is created. Passwords can include standard characters. Passwords cannot include extended characters, or symbols. (Use characters with an ASCII value of 128 or lower.)
	A user must type this password before he or she can restore a backup or view the contents of the recovery point.
Use AES encryption	Encrypts recovery point data to add another level of protection to your recovery points.
	Choose from the following encryption levels:
	■ **Standard 128-bit (8+ character password)**
	■ **Medium 192-bit (16+ character password)**
	■ **High 256-bit (32+ character password)**

See "Making copies of recovery points" on page 177.

Defining a virtual conversion job

You can create a schedule to convert recovery points and incremental recovery points to a VMware virtual disk or a Microsoft virtual disk . You can also convert recovery points directly to VMware ESX Server. Virtual disks are excellent for testing and evaluation purposes.

The following platforms support virtual disks created from recovery points:

■ VMware Workstation 4, 5, 6, and 6.5

■ VMware ESX 3.0, 3.5, 4.0, and 4.1

- VMware ESXi 3.5, 4.0, and 4.1

- VMware Server 1 and 2

- VMware GSX Server 3.x (replaced by VMware Server)

- Microsoft Virtual Server 2005 R2 and later

- Microsoft Hyper-V 1.0 and 2.0

Scheduled conversions use the system index file (.sv2i) to convert recovery points to virtual disks. The .sv2i file reduces the time it takes to convert multiple recovery points. When a recovery point is created, a .sv2i file is saved with it. The .sv2i file contains a list of the most recent recovery points, which includes the original drive location of each recovery point.

You can also create a one-time virtual conversion.

See "Running a one-time conversion of a physical recovery point to a virtual disk" on page 194.

To define a virtual conversion job

1   On the **Tasks** menu, click **Run or Manage Virtual Conversions**.

2   On the toolbar, click **Define New**.

3   Select the virtual disk type (and version, if applicable) that you want to create, and then click **Next**.

4   In the **Source** panel, select the recovery points you want to convert, and then click **Next**..

See "Source options" on page 195.

5   In the **Virtual Disks Destination** panel, set the options you want based on the virtual disk format and version (if applicable) that you selected earlier. Then click **Next**.

See "Virtual Disks Destination options" on page 198.

6   In the **General Options** panel set the conversion options you want, and then click **Next**.

See "General Options properties" on page 200.

7   In the **Conversion Time** panel, set the conversion job schedule that you want, and then click **Next**:

See "Conversion Time options" on page 190.

8 If you want to run the new conversion job immediately, click **Run conversion now**.

This option is not available if you selected the **Only run once** option in the **Conversion Time** panel.

9 Click **Finish**.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

Source options

The following table describes the options on the **Source** panel. This panel is available from the **Define Virtual Conversion Wizard**.

Table 12-7 Source options when you view recovery points by System

Option	Description
Perform conversion using latest recovery points for this computer	Converts the most recent recovery points that exist in the recovery point storage location on your computer.
	The list of drives, source files (.v2i and .iv2i files), and dates comes from the most current system index file (.sv2i).
Perform conversion using recovery points for another computer	Converts recovery points that exist on another computer.
Browse to and select the .sv2i file for the desired system	Specifies a path to a system index file (.sv2i) that resides elsewhere, such as a network location.
	If you selected a system index file that is stored on a network, you are prompted for your network credentials.
	See "About network credentials" on page 83.

Table 12-7   Source options when you view recovery points by System *(continued)*

Option	Description
Browse	Lets you browse to a path that contains a system index file. For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.
Drives	Lets you select the drives with the recovery points that you want to convert based on the selected system index file.

See "Defining a virtual conversion job" on page 183.

Virtual Disks Destination options

The following table describes the options on the **Virtual Disks Destination** panel. This panel is available from the **Define Virtual Conversion Wizard**.

Table 12-8   Virtual Disks Destination options for converting to VMware virtual disk or Microsoft virtual disk

Option	Description
Folder for virtual disks	Lets you type the path to the folder where you want to place the virtual disk files.
Browse	Lets you browse to locate the folder in which you want to place the virtual disk files.
User name	Lets you type the user name if you specified a virtual disk folder location on a network See "About network credentials" on page 83.
Password	Specifies the password to a network path.

Table 12-8   Virtual Disks Destination options for converting to VMware virtual disk or Microsoft virtual disk *(continued)*

Option	Description
Create one virtual disk per volume	Creates one virtual disk file per volume.
	If you do not select this option, each drive is matched to its respective hard drive letter assignment during the conversion. Therefore, it results in multiple drives within one virtual disk file.
	Note: This option is not available if the volumes are on separate disks.
Rename	Lets you edit the file name of the resulting virtual disk file.

Table 12-9   Virtual Disks Destination options for converting to VMware ESX Server

Option	Description
ESX server name or IP address	Lets you type the name of the server or the server's IP address.
User name	Lets you type a valid administrator user name that has sufficient rights to an ESX server.
Password	Lets you type a valid password to the ESX server.
Destination for the virtual disks	Lets you type the path to the folder where you want to place the virtual disk files.
Browse	Lets you browse to a destination location for the virtual disks.
Rename	Lets you edit the name of the resulting virtual disk file.
Next	Specifies additional options for VMware ESX Server virtual disks.
Temporary location for conversion	Lets you type the name of the server or the server's IP address that you can use as a temporary location for files.

Table 12-9 Virtual Disks Destination options for converting to VMware ESX Server *(continued)*

Option	Description
Temporary Location Credentials	Lets you type a valid administrator user name and password that has sufficient rights.

General Options properties

The following table describes the properties on the **General Options** panel. This panel is available from the **Define Virtual Conversion Wizard**.

Table 12-10 General Options properties

Option	Description
Conversion job name	Lets you type a name for the virtual conversion job or you can leave the default name.

Table 12-10 General Options properties *(continued)*

Option	Description
Run Windows Mini-Setup	Runs Windows Mini-Setup when you restart the computer after recovery.
	During recovery a text-based answer file is generated that scripts the answers for a series of dialog boxes. When the Mini-Setup Wizard starts, it looks for this answer to automate the wizard. For example, the answer file can automatically apply network card settings and other hardware and software settings on the computer.
	Unlike Windows Welcome which can take up to 60 minutes or more to set up Windows, Mini-Setup takes about six minutes. Specific information such as accepting the End–User license agreement, and entering the product key get applied automatically by Mini-Setup which uses the answer file.
	Deselect this option if you want any of the following to occur at the time of recovery instead:
	■ Run Windows Welcome instead Mini-Setup ■ You do not want to change any of the configurable options for which the Mini-Setup Wizard changes for you at the time of recovery. This state ensures that the computer is recovered to its original state before recovery.
	For more detailed information about Mini-Setup. you can perform a search for "Mini-Setup" on the Microsoft Help & Support Web site.

Table 12-10   General Options properties *(continued)*

Option	Description
Split virtual disk into 2 GB (.vmdk) files	Lets you split the virtual disk into multiple 2 GB .vmdk files.
	For example, use this option if your virtual disk is stored on a FAT32 drive. Or, any file system that does not support files larger than 2 GB. Or, if you want to copy the virtual disk files to a DVD but the size is larger than the DVD allows.
	Note: This option is specific to VMware; it is not available if you selected **Microsoft Virtual Disk** as the conversion format.

Conversion Time options

The following table describes the options on the **Conversion Time** panel. This panel is available from the **Define Virtual Conversion Wizard**.

Table 12-11   Conversion Time options for a Weekly schedule

Option	Description
Automatically convert latest recovery points - Weekly	Converts the latest recovery points to virtual disks using a weekly schedule.
Default	Uses the default conversion schedule.
Start time	Lets you select the time you want the conversion to start.
Days	Lets you select the day of the week that you want the conversion to take place.
Run more than once per day	Converts recovery points multiple times throughout a day.
Time between conversions	Lets you select the amount of time to elapse before the next conversion.
Number of times	Specifies the number of times that you want the conversion to occur, beginning from the selected start time.

Table 12-11   Conversion Time options for a Weekly schedule *(continued)*

Option	Description
Details	Displays the conversion time information you have selected.

Table 12-12   Conversion Time options for a Monthly schedule

Option	Description
Automatically convert latest recovery points - Monthly	Converts the latest recovery points to virtual disks using a monthly schedule.
Default	Lets you use the default conversion schedule.
Start time	Lets you select the time you want the conversion to start.
Days of the month	Lets you select the day of the month that you want the conversion to take place.
Details	Displays the conversion time information you have selected.

Table 12-13   Conversion Time options for an Only Run Once schedule

Option	Description
Automatically convert latest recovery points - Only run once	Runs the conversion one time on the date and at the time that you specify.
Date	Lets you select the day, month, and year that you want the conversion to run.
Time	Lets you select the time that you want the conversion to start.
Details	Displays the conversion time information you have selected.

See "Defining a virtual conversion job" on page 183.

Running an existing virtual conversion job immediately

After you create a conversion job, you can use **Run Now** to create an on-demand recovery point conversion to virtual disk format. A manual conversion starts immediately.

To run an existing virtual conversion job immediately

1 On the **Tasks** menu, click **Run or Manage Virtual Conversions**.

2 Select the name of a conversion job that you want to run immediately.

3 On the toolbar, click **Run Now**.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Deleting a virtual conversion job" on page 193.

Viewing the properties of a virtual conversion job

You can use **Properties** for a selected virtual conversion job to review a summary of the settings, options, and assigned schedule.

To view the properties of a virtual conversion job

1 On the **Tasks** menu, click **Run or Manage Virtual Conversions**.

2 Select the name of a conversion job whose properties you want to view.

3 On the **Tasks** menu, click **Properties**.

4 Click **OK**.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

Viewing the progress of a virtual conversion job

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

To view the progress of a virtual conversion job

◆ Do one of the following:

■ On the **View** menu, click **Progress and Performance**.

■ On the **Tasks** menu, click **Run or Manage Virtual Conversions**, and then on the **View** menu, click **Progress and Performance**.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

Editing a virtual conversion job

You can edit the schedule portion of an existing conversion job or you can edit all aspects of the job.

To edit a virtual conversion job

1   On the **Tasks** menu, click **Run or Manage Virtual Conversions**.

2   Select the name of a conversion job that you want to edit.

3   Do one of the following:

To change the schedule	On the toolbar, click **Change Schedule**.
	Make changes to the conversion schedule, and then click **OK**.
To change the job settings	On the toolbar, click **Edit Settings**.
	Make the changes you want in each wizard pane, and then click **Finish**.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

Deleting a virtual conversion job

You can delete virtual conversion jobs you no longer need or use.

When you delete a virtual conversion job, no recovery points or virtual disks are deleted from the storage location. Only the conversion job itself is deleted.

To delete a virtual conversion job

1   On the **Tasks** menu, click **Run or Manage Virtual Conversions**.

2   Select the names of one or more conversion jobs that you want to delete.

3   On the toolbar, click **Remove**.

4   Click **Yes** to confirm the deletion.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

Running a one-time conversion of a physical recovery point to a virtual disk

You can use Symantec System Recovery to convert recovery points of a physical computer to VMware virtual disk. You can also convert recovery points to Microsoft virtual disk, or a VMware ESX Server. Virtual disks are excellent for testing and evaluation purposes.

The following platforms support virtual disks created from recovery points:

■ VMware Workstation 4, 5, 6, and 6.5

■ VMware ESX Server 3.0, 3.5, 3.5i, 4.0, 4.0i, 4.1, and 4.1i

■ VMware Server 1

■ Microsoft Virtual Server 2005 R2 and later

■ Microsoft Hyper-V 1.0 and 2.0

You can also create scheduled recovery point conversions to virtual disks.

See "Defining a virtual conversion job" on page 183.

To run a one-time recovery point conversion to virtual disk

1   On the **Tasks** menu, click **One Time Virtual Conversion**.

2   Click the virtual disk type (and version, if applicable) that you want to create, and then click **Next**.

3   Do one of the following:

- ■ Click **View all recovery points** near the bottom of the pane, and then select a recovery point in the list based on its creation date.

- ■ In the **View by** list, select a recovery point source.
  See "Source options" on page 195.

4   Click **Next**.

5   Set the virtual disk destination options based on the virtual disk format and version (if applicable) that you selected, and then click **Next**.

     See "Virtual Disks Destination options" on page 198.

6   Set the general conversion options you want, and then click **Next**.

     See "General Options properties" on page 200.

7   Review the summary of the choices you made.

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

8   Click **Finish**.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

Source options

The following table describes the options on the **Source** panel. This panel is available from the **One Time Virtual Conversion Wizard**.

See "Running a one-time conversion of a physical recovery point to a virtual disk" on page 194.

Table 12-14   Source options when you view recovery points by Date

Option	Description
View by - Date	Displays all of the discovered recovery points in the order in which they were created.
Date	Lets you select an alternate date by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.

Table 12-14   Source options when you view recovery points by Date *(continued)*

Option	Description
View all recovery points	Lets you view all recovery points that are available.

Table 12-15   Source options when you view recovery points by File name

Option	Description
View by - File name	Lets you view recovery points by their file name.
File name	Specifies a path and a file name of a recovery point.
Browse	Lets you browse to a path that contains a recovery point. For example, you can browse for a recovery point (.v2i) or incremental recovery point (.iv2i) file on an external (USB) drive. Or, you can browse to a network location, or removable media.
User name	Specifies the user name if you specify a recovery point file name that is located in a network path. See "About network credentials" on page 83.
Password	Specifies the password to a network path.

Table 12-16   Source options when you view recovery points by System

Option	Description
View by - System	Lets you use the current system index file that is located in the recovery point storage location. The system index file displays a list of all of the drives on your computer and any associated recovery points from which you can select.
	The use of a system index file reduces the time it takes to convert multiple recovery points. 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.
Date	Lets you select an alternate date of a system index file by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.
Perform conversion using latest recovery points for this computer	Converts the most recent recovery points that exist in the recovery point storage location on your computer.
	The list of drives, source files (.v2i and .iv2i files), and dates comes from the most current system index file (.sv2i).
Perform conversion using recovery points for another computer	Converts recovery points that exist on another computer.
Browse to and select the .sv2i file for the desired system	Specifies a path to a system index file (.sv2i) that resides elsewhere, such as a network location.
	If you selected a system index file that is stored on a network, you are prompted for your network credentials.
	See "About network credentials" on page 83.

Table 12-16   Source options when you view recovery points by System *(continued)*

Option	Description
Browse	Lets you browse to a path that contains a system index file.
	For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.
Drives	Lets you select the drives with the recovery points that you want to convert based on the selected system index file.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

Virtual Disks Destination options

The following table describes the options on the **Virtual Disks Destination** panel. This panel is available from the **One Time Virtual Conversion Wizard**.

See "Running a one-time conversion of a physical recovery point to a virtual disk" on page 194.

Table 12-17   Virtual Disks Destination options for converting to VMware virtual disk or Microsoft virtual disk

Option	Description
Folder for virtual disks	Lets you type the path to the folder where you want to place the virtual disk files.
Browse	Lets you browse to locate the folder in which you want to place the virtual disk files.
User name	Lets you type the user name if you specified a virtual disk folder location on a network
	See "About network credentials" on page 83.
Password	Specifies the password to a network path.

Table 12-17   Virtual Disks Destination options for converting to VMware virtual
disk or Microsoft virtual disk *(continued)*

Option	Description
Create one virtual disk per volume	Lets you create one virtual disk file per volume.
	If you do not select this option, each drive is matched to its respective hard drive letter assignment during the conversion. Therefore, it results in multiple drives within one virtual disk file.
	Note: This option is not available if the volumes are on separate disks.
Rename	Lets you edit the file name of the resulting virtual disk file.

Table 12-18   Virtual Disks Destination options for converting to VMware ESX
Server

Option	Description
ESX server name or IP address	Indicates the name of the server or the server's IP address.
User name	Indicates a valid administrator user name that has sufficient rights to an ESX server.
Password	Indicates a valid password to the ESX server.
Destination for the virtual disks	Indicates the path to the folder where you want to place the virtual disk files.
Browse	Lets you browse to a destination location for the virtual disks.
Rename	Lets you edit the name of the resulting virtual disk file.
Next	Specifies temporary location options for VMware ESX Server virtual disks.
Temporary location for conversion	Lets you type the name of the server or the server's IP address that you can use as a temporary location for files.

Table 12-18   Virtual Disks Destination options for converting to VMware ESX
Server *(continued)*

Option	Description
Temporary Location Credentials	Lets you type a valid administrator user name and password that has sufficient rights.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

General Options properties

The following table describes the properties on the **General Options** panel. This panel is available from the **One Time Virtual Conversion Wizard**.

See "Running a one-time conversion of a physical recovery point to a virtual disk" on page 194.

Table 12-19   General Options properties

Option	Description
Run Windows Mini-Setup	Runs Windows Mini-Setup when you restart the computer after recovery.
	During recovery a text-based answer file is generated that scripts the answers for a series of dialog boxes. When the Mini-Setup Wizard starts, it looks for this answer to automate the wizard. For example, the answer file can automatically apply network card settings and other hardware and software settings on the computer.
	Unlike Windows Welcome which can take up to 60 minutes or more to set up Windows, Mini-Setup takes about six minutes. Specific information such as accepting the End–User license agreement, and entering the product key get applied automatically by Mini-Setup which uses the answer file.
	Deselect this option if you want any of the following to occur at the time of recovery instead:
	■ Run Windows Welcome instead Mini-Setup ■ You do not want to change any of the configurable options for which the Mini-Setup Wizard changes for you at the time of recovery. This state ensures that the computer is recovered to its original state before recovery.
	For more detailed information about Mini-Setup. you can perform a search for "Mini-Setup" on the Microsoft Help & Support Web site.

Table 12-19 General Options properties *(continued)*

Option	Description
Split virtual disk into 2 GB (.vmdk) files	Splits the virtual disk into multiple 2 GB .vmdk files.
	For example, use this option if your virtual disk is stored on a FAT32 drive. Or, any file system that does not support files larger than 2 GB. Or, if you want to copy the virtual disk files to a DVD but the size is larger than the DVD allows.
	Note: This option is specific to VMware; it is not available if you selected **Microsoft Virtual Disk** as the conversion format.

See "Viewing the properties of a virtual conversion job" on page 192.

See "Viewing the progress of a virtual conversion job" on page 192.

See "Editing a virtual conversion job" on page 193.

See "Running an existing virtual conversion job immediately" on page 192.

See "Deleting a virtual conversion job" on page 193.

About managing file and folder backup data

Drive-based backups capture your entire hard drive. As such, the size of a recovery point is typically much larger than the data that is captured during the backup of files and folders. 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.

See "Viewing how much file and folder backup data is stored" on page 203.

See "Limiting the number of file versions to keep" on page 203.

See "Manually deleting files from your backups of files and folders" on page 203.

See "Finding versions of a file or folder" on page 204.

Viewing how much file and folder backup data is stored

Start by viewing the total amount of file and folder backup data that you currently store.

To view how much file and folder backup data is stored

1   On the **Tasks** menu, click **Manage Backup Destination**.

2   To select an alternate backup destination, in the **Drives** 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.

See "About managing file and folder backup data" on page 202.

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 kind of maintenance can significantly reduce the amount of disk space that is required, especially if the file size is large.

To limit the number of file versions to keep

1   On the **Tasks** menu, click **Manage Backup Destination**.

2   Click **Settings**.

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

4   You can also select **Monitor disk space usage for backup storage**. Then you can specify a limit to the total amount of disk space that can be used.

See "Automating the management of backup data" on page 204.

5   Click **OK**.

See "About managing file and folder backup data" on page 202.

Manually deleting files from your backups of files and folders

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

To manually delete files from your backups of files and folders

1   On the **Tasks** menu, 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 do not know the name of the file, click **Search**, and then browse for the file.

3 Click **View All Versions** to display all versions of each file that exist in the backup of files and folders data.

4 Select one or more files that you want to delete.

5 Right-click, and then click **Delete**.

See "About managing file and folder backup data" on page 202.

Finding versions of a file or folder

You can use **Windows Explorer** to view information about the available versions that are included in a backup of files and folders.

You can limit the number of versions of each file and folder that you want to store.

See "Limiting the number of file versions to keep" on page 203.

To find versions of a file or folder

1 Open **Windows Explorer**.

2 Navigate to a file that you know is included in a backup of files and folders.

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

See "About managing file and folder backup data" on page 202.

Automating the management of backup data

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

To automate the management of backup data

1 On the **Tasks** menu, click **Manage Backup Destination**.

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

3 Select **Monitor disk space usage for backup storage**. Drag the slider to limit the total amount of disk space that can be used for your backup data.

4   Do one of the following:

  ■ Select **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.

  ■ Select **Automatically optimize storage** if you want Symantec System
    Recovery to manage the backup data automatically, without prompting
    you.
    Symantec System Recovery automatically deletes the old recovery points,
    and limits file versions to remain within the threshold that you set.

5   Select **Delay changes until next backup** if you do not want to apply your
    changes until the next backup runs.

6   Click **OK**.

See "About managing file and folder backup data" on page 202.

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 an
external hard drive for storing your backup data. You can 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: You can move your backup destination to a new internal or external hard
drive. Make sure that the drive is properly installed or connected before you
proceed.

To move your backup destination

1   On the **Tasks** menu, click **Manage Backup Destination**.

2   In the **Manage Backup Destination** window, in the **Drives** 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 Select **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, select **Move recovery points**, and then do one of the following:

■ Select **Move the latest recovery points for each backup and delete the rest**.

■ Select **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 if no backup data of files and folders is found at the original backup destination.

10 Click **OK**.

See "About managing file and folder backup data" on page 202.

Recovering files, folders, or entire drives

This chapter includes the following topics:

- About recovering lost data
- Recovering files and folders by using file and folder backup data
- Recovering files and folders by using a recovery point
- About opening files and folders stored in a recovery point
- About finding the files or folders you want
- Recovering a secondary drive
- Customizing the recovery of a drive
- About restoring a computer from a remote location by using LightsOut Restore

About recovering lost data

Symantec 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. You can recover recent changes to a lost file or folder. However, your backup data must be at least as current as the changes that were made to the lost file or folder.

See "Recovering files and folders by using file and folder backup data" on page 208.

See "Recovering files and folders by using a recovery point" on page 209.

Recovering files and folders by using file and folder backup data

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

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

See "About recovering lost data" on page 207.

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

1   On the **Tasks** menu, click **Recover My Files**.

2   In the left pane of the **Recover My Files** dialog box, 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. Click **Search**.
   For example, type **recipe**. Any file or folder that includes the word recipe in its name such as Chocolate Cheesecake Recipes.doc, Cathy Read Recipes.xls, Recipes for Success.mp3 are found.

   ■   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.

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 folders where they existed when they were backed up.
   If you want to replace the original files, select **Overwrite existing files**. If you do not select 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 with the files that you restore. Or, it replaces the files of the same names that are currently stored at that location.

   ■   Click **Recovered Files folder on the desktop** to restore your files to a **Recovered Files** folder on your Windows desktop.
   Symantec 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**. Be certain that the file that you what to recover is the file that you want.

9   Click **OK**.

See "Recovering files and folders by using a recovery point" on page 209.

Recovering files and folders by using a recovery point

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

See "About recovering lost data" on page 207.

To recover files and folders by using a recovery point

1   On the **Tasks** menu, click **Recover My Files**

2   In the left pane of the **Recover My Files** dialog box, 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** dialog box, click **Change**. Locate the recovery point you want to use, and then click **OK**.

See "Select Recovery Point options" on page 210.

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

---

4   In the **Find files to recover** field, 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**. Any file or folder that includes the word recipe in its name such as Chocolate Cheesecake Recipes.doc, Cathy Read Recipes.xls, Recipes for Success.mp3 are found.

5   In the **Name** table, select the files that you want to restore.

6   Click **Recover Files**.

7   In the **Recover My Files** dialog box, select the option you want.

See "Recover My Files options" on page 212.

8   Click **Recover**.

9 If you are prompted to replace the existing file, click **Yes**. Be certain that the file that you want to recover is the file that you want.

10 Click **OK**.

See "Recovering files and folders by using file and folder backup data" on page 208.

Select Recovery Point options

The following table describes the options on the **Select Recovery Point** dialog box. This dialog box is available from the **Recovery My Files** dialog box.

Table 13-1   Select Recovery Point options when you view recovery points by Date

Option	Description
View by - Date	Displays all of the discovered recovery points in the order in which they were created.
Date	Lets you select an alternate date by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.
View all recovery points	Lets you view all recovery points that are available.

Table 13-2   Select Recovery Point options when you view recovery points by File name

Option	Description
View by - File name	Lets you view recovery points by their file name.
File name	Specifies a path and a file name of a recovery point.
Browse	Lets you browse to a path that contains a recovery point. For example, you can browse for a recovery point (.v2i) or incremental recovery point (.iv2i) file on an external (USB) drive. Or, you can browse to a network location, or removable media.

Table 13-2   Select Recovery Point options when you view recovery points by File
name *(continued)*

Option	Description
User name	Specifies the user name if you specify a recovery point file name that is located in a network path. See "About network credentials" on page 83.
Password	Specifies the password to a network path.

Table 13-3   Select Recovery Point options when you view recovery points by
System

Option	Description
View by - System	Uses the current system index file that is located in the recovery point storage location. The system index file displays a list of all of the drives on your computer and any associated recovery points from which you can select. The use of a system index file reduces the time it takes to convert multiple recovery points. 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.
Date	Lets you select an alternate date of a system index file date by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.
Use latest recovery points for this computer	Restores the most recent recovery points that exist in the recovery point storage location on your computer. The list of drives, source files (.v2i and .iv2i files), and dates comes from the most current system index file (.sv2i).
Use alternate system index (.sv2i) file	Restores recovery points that exist on another computer.

Table 13-3 Select Recovery Point options when you view recovery points by System *(continued)*

Option	Description
Browse to and select the .sv2i file for the desired system	Specifies a path to a system index file (.sv2i) file that resides elsewhere, such as a network location. If you selected a system index file that is stored on a network, you are prompted for your network credentials. See "About network credentials" on page 83.
Browse	Lets you browse to a path that contains a system index file. For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.
Drives	Lets you select the drives with the recovery points that you want to restore based on the selected system index file.

See "Recovering files and folders by using a recovery point" on page 209.

Recover My Files options

The following table describes the options on the **Recover My Files** dialog box. This dialog box is available from the **Recover My Files** main dialog box.

Table 13-4 Recover My Files options

Option	Description
Original folders	Recovers files to the original folder where they existed when they were backed up.
New folder ("Recovered Files") on the desktop	Recovers files to a new folder that is created on your Windows desktop called Recovered Files.
Alternate folder	Specifies the path to an alternate location where you want your files to be restored.

See "Recovering files and folders by using a recovery point" on page 209.

About 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 by using the **Recovery Point Browser**. From there, you can also restore files and folders using the **Recovery Point Browser**.

See "Opening and restoring files within a recovery point" on page 165.

About finding 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 **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 163.

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, suppose your computer has a D drive and the data is lost. You can restore the D drive back to an earlier date and time.

See "About recovering a computer" on page 227.

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 "About the icons on the Status page" on page 150.

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, the data in the recovery point replaces all of the data on the drive. 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 secondary drive

1   On the **Tasks** menu, click **Recover My Computer**.

2   Select a recovery point.

    See " Recover My Computer options" on page 214.

3   Click **Recover Now**.

4   Click **OK**.

5   Click **Yes**.

See "Customizing the recovery of a drive" on page 216.

Recover My Computer options

The following table describes the options on the **Recover My Computer** dialog box.

Table 13-5   Recover My Computer options when you view recovery points by Date

Option	Description
View by - Date	Displays all of the discovered recovery points in the order in which they were created.
Date	Lets you select an alternate date by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.
View all recovery points	Lets you view all recovery points that are available.

Table 13-6   Recover My Computer options when you view recovery points by File name

Option	Description
View by - File name	Views recovery points by their file name.

Table 13-6   Recover My Computer options when you view recovery points by
File name *(continued)*

Option	Description
File name	Specifies a path and a file name of a recovery point.
Browse	Lets you browse to a path that contains a recovery point. For example, you can browse for a recovery point (.v2i) or incremental recovery point (.iv2i) file on an external (USB) drive. Or, you can browse to a network location, or removable media.
User name	Specifiesy the user name if you specify a recovery point file name that is located in a network path. See "About network credentials" on page 83.
Password	Specifies the password to a network path.

Table 13-7   Recover My Computer options when you view recovery points by
System

Option	Description
View by - System	Uses the current system index file that is located in the recovery point storage location. The system index file displays a list of all of the drives on your computer and any associated recovery points from which you can select. The use of a system index file reduces the time it takes to convert multiple recovery points. 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.
Date	Lets you select an alternate date of a system index file date by using the drop-down calendar. Use the calendar if no recovery points are discovered and displayed in the table.

Table 13-7   Recover My Computer options when you view recovery points by
                   System *(continued)*

Option	Description
Use latest recovery points for this computer	Restores the most recent recovery points that exist in the recovery point storage location on your computer.
	The list of drives, source files (.v2i and .iv2i files), and dates comes from the most current system index file (.sv2i).
Use alternate system index (.sv2i) file	Restores recovery points that exist on another computer.
Browse to and select the .sv2i file for the desired system	Specifies a path to a system index file (.sv2i) file that resides elsewhere, such as a network location.
	If you selected a system index file that is stored on a network, you are prompted for your network credentials.
	See "About network credentials" on page 83.
Browse	Lets you browse to a path that contains a system index file.
	For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.
Drives	Lets you select the drives with the recovery points that you want to restore based on the selected system index file.

See "Recovering a secondary drive" on page 213.

See "Customizing the recovery of a drive" on page 216.

Customizing the recovery of a drive

You can set various options to customize the recovery of a drive.

To customize the recovery of a drive

1   On the **Tasks** menu, click **Recover My Computer**.

2   Select a recovery point, and then click **Recover Now**.

3   In the **Recover My Computer** dialog box, click **Custom** to start the **Recover Drive Wizard**.

4   On the wizard's **Welcome** panel, click **Next**.

5   In the **Recovery Point to Restore** panel, set the options you want.

See "Recovery Point to Restore options" on page 217.

6   In the **Target Drive** panel, select one or more drives 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**. Select multiple, contiguous destinations that exist on the same hard disk.

7   If the recovery point is password-protected, in the **Password** dialog box, type the password, and then click **OK**.

8   In the **Recovery Options** panel, select the restore options you want.

See "Recovery options" on page 218.

The options that are available depend on the restore destination that you have selected.

9   Click **Next**, and then review your selections.

10   Click **Finish**, then click **Yes**.

Sometime the wizard cannot lock the drive to perform the recovery in Windows (typically, because the drive is in use by a program). In such cases, make sure that the drive is not in use. For example, close any files or applications that may be in use, and then click **Retry**.

If the **Retry** option fails, click **Ignore** to attempt a forced lock on the drive. If **Ignore** fails, you might be prompted to insert the Symantec System Recovery Disk. You must then manually start the recovery environment so that you can complete the recovery. When the recovery is finished, the computer restarts automatically.

See "Recovering a secondary drive" on page 213.

Recovery Point to Restore options

The following table describes the options on the **Recovery Point to Restore** panel. This panel is available from the **Recover Drive Wizard**.

Table 13-8   Recovery Point to Restore options

Option	Description
Recovery point file name	Specifies the recovery point you want to use to recover the drive. You can use the recovery point that is already added to this field, or you can browse to a different recovery point.
Browse	Lets you browse to a path that contains a recovery point. For example, you can browse for a recovery point (.v2i) or incremental recovery point (.iv2i) file on an external (USB) drive. Or, you can browse to a network location, or removable media.
User name	Specifies the user name if you specify a recovery point file name that is located in a network path. See "About network credentials" on page 83.
Password	Specifies the password to a network path.

See "Customizing the recovery of a drive" on page 216.

Recovery options

The following table describes the options on the **Recovery Options** panel. This panel is available from the **Recover Drive Wizard**.

Table 13-9   Recovery options

Option	Description
Verify recovery point before restore	Verifies whether a recovery point is valid or corrupt before it is restored. This option can significantly increase the time that is required for the recovery to complete.
Check for file system errors	Checks the restored drive for errors after the recovery point is restored.

Table 13-9   Recovery options *(continued)*

Option	Description
Resize restored drive	Expands the drive automatically 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). This option is appropriate if you restore 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 part of all Windows operating systems that Symantec System Recovery supports. 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 restore a recovery point to a new, empty hard disk.
Primary partition	Because hard disks are limited to four primary partitions, this option is appropriate if the drive has four or fewer partitions.
Logical partition	This option is appropriate 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.

See "Customizing the recovery of a drive" on page 216.

About restoring a computer from a remote location by using LightsOut Restore

Symantec 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 Vancouver goes down. You can connect to the computer from your remote location by using your server's remote connection capabilities. You can remotely access Symantec System Recovery Disk to start the computer in the recovery environment. You can then use Symantec System Recovery Disk to restore files or an entire system partition.

LightsOut Restore installs a custom version of Symantec System Recovery Disk directly to the file system on the system partition. It then places a Symantec System Recovery Disk boot option in the **Windows boot** menu. Whenever the boot menu option is selected, the computer boots directly into Symantec System Recovery Disk. It uses the files that are installed on the system partition.

LightsOut Restore uses Symantec pcAnywhere technology. It also uses the Windows boot menu, and hardware devices such as RILO and DRAC. These features combine to let an administrator remotely control a system during the boot process.

When the custom Symantec System Recovery Disk boots as part of LightsOut Restore, you can have it automatically start 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 turn on or reboot the system into Symantec System Recovery Disk.

Note: If you use Microsoft BitLocker to secure the data on a drive, be aware that LightsOut Restore does not work on BitLocked drives. Therefore, if you "BitLock" your system drive, you cannot recover the drive using LightsOut Restore.

See "About setting up and using LightsOut Restore" on page 220.

See "Configuring LightsOut Restore" on page 222.

About setting up and using LightsOut Restore

Before you set up LightsOut Restore, review the following information:

> **Note:** If you use Microsoft's BitLocker Drive Encryption to encrypt the data on a drive, be aware that LightsOut Restore does not work on encrypted drives. You must turn off BitLocker and then decrypt the drive before you can use LightsOut Restore on it.

- Install a licensed version of Symantec pcAnywhere on a central computer that you use for management (for example, a help desk computer).
- Ensure that all of your servers can be managed remotely through a hardware device such as RILO or DRAC.
- Install Symantec System Recovery on the servers that you want to protect, and then define and run backups to create recovery points.
- Run the **Set Up LightsOut Restore** wizard to install a custom Symantec System Recovery Disk directly to the computer's local file system.
  The wizard creates an entry in the **Windows boot** menu that can be used to boot into Symantec System Recovery Disk .

> **Note:** LightsOut Restore works only on the primary operating system. It does not work on multiple-boot computers (for example, a computer that starts 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 Symantec System Recovery Disk.

> **Note:** The LightsOut Restore feature requires at least 1 GB of memory to run.

- Use the RILO or the DRAC device to connect to the remote server so you can recover a file or system from a remote location. Then you can turn on the system or restart it.
- Open the boot menu as the remote server starts, and then select the name that you have given to Symantec System Recovery Disk.
  The remote server boots into Symantec System Recovery Disk and the connection through RILO or DRAC is lost. If you configured it during the **Set Up LightsOut Restore** wizard, a pcAnywhere thin host automatically starts.
- Use Symantec pcAnywhere to connect to the pcAnywhere thin host that waits on the remote server.
- Use Symantec System Recovery Disk to restore individual files, or entire drives by way of pcAnywhere.

See

Configuring LightsOut Restore

You must run the LightsOut Restore Wizard on the computer that you want to protect. The **Set Up LightsOut Restore Wizard** installs a customized version of Symantec System Recovery Disk to the computer's local file system. The wizard creates an entry in the **Windows boot** menu that you use to boot into LightsOut Restore.

You can run the **Setup LightsOut Restore Wizard** again if you need to edit the configuration settings. Or, run the wizard again if you need to rebuild an existing, customized Symantec System Recovery Disk.

To configure LightsOut Restore

1   Insert the Symantec System Recovery Disk into your media drive.

2   Start Symantec System Recovery.

3   On the **Tasks** menu, click **Set Up LightsOut Restore**, then click **Next**.

4   On the **Source Location** panel, specify the path or browse to the media drive in which you placed the Symantec System Recovery Disk, then click **Next**.

5   On the **Drivers to Include** panel, review the list of any storage or network drivers to be included, and then click **Next**.

    See "Drivers to Include options" on page 223.

6   On the **Startup Options** panel, specify Symantec System Recovery Disk startup options you want, and then click **Next**.

    See "Startup options" on page 223.

7   On the **Options** panel, select the options you want, and then click **Next**.

    See "LightsOut Restore options for Symantec System Recovery Disk" on page 224.

8   On the **Licensing** panel, specify how you want to enable licensed features (such as the cold imaging feature called **Back Up My Computer**) in the customized recovery environment.

    See "Licensing options" on page 226.

9   Click **Next**.

10 Click **Finish** to set up LightsOut Restore on your computer.

    At the conclusion of the setup , you should test LightsOut Restore.

11 To ensure that you can use the LightsOut Restore feature when you need it, click **Yes**.

12 Click **Yes** to restart the computer.

See "About setting up and using LightsOut Restore" on page 220.

Drivers to Include options

The following table describes the options on the **Drives to Include** panel in the LightsOut Restore Wizard.

Table 13-10   Drivers to Include options

Options	Description
Storage and network drivers	Lets you review the list of any storage or network drivers to be included.
Add	Lets you add additional drivers. The location that you specify should contain the fully extracted installation package for the driver you add. If you have more than one missing storage or network driver, you must rerun the **Set Up LightsOut Restore** wizard for each missing driver.
Remove	Deletes the drivers you do not need.
Reset	Resets the list to the original list of drivers.

See "Configuring LightsOut Restore" on page 222.

Startup options

The following table describes the options on the **Startup Options** panel in the LightsOut Restore Wizard.

Table 13-11   Startup options

Options	Description
Time zone	Sets the time zone to use inside LightsOut Restore.
Display language	Sets the default display language for LightsOut Restore.
Keyboard layout	Lets you select the default keyboard layout to use when you run LightsOut Restore.

Table 13-11   Startup options *(continued)*

Options	Description
Boot menu label	Indicates the title that you want to appear on the **Windows boot** menu for LightsOut Restore.
Time to display boot menu	Specifies (in seconds) how long you want the boot menu to display. The default is 10 seconds.

LightsOut Restore options for Symantec System Recovery Disk

The following table describes the options on the **Options** panel in the LightsOut Restore Wizard.

Table 13-12   LightsOut Restore options for Symantec System Recovery Disk

Option	Description
Automatically start network services	Starts networking automatically when you recover the computer through LightsOut Restore.
Dynamic IP	Connects to a network without the need for additional network configuration. This option is also appropriate if you know there is a DHCP server available on the network at the time you restore.
Static IP	Connects to a network with a particular network adapter and specific address settings. You should click this option if you know there is no DHCP server (or the DHCP server may be unavailable) when you recover.
Automatically start Symantec pcAnywhere	Starts the Symantec pcAnywhere thin host automatically when you start the Symantec Recovery Environment . This option is appropriate for troubleshooting a system recovery.

Table 13-12   LightsOut Restore options for Symantec System Recovery Disk
                       (continued)

Option	Description
Configure	Lets you configure Symantec pcAnywhere options. See "Configure Symantec pcAnywhere options" on page 225.

See "Configuring LightsOut Restore" on page 222.

Configure Symantec pcAnywhere options

The following table describes the options on the **Options** panel in the LightsOut Restore Wizard.

Table 13-13   Configure Symantec pcAnywhere options

Option	Description
User name	Indicates the user name for authenticating to pcAnywhere.
Password	Indicates the password for authenticating to pcAnywhere.
Confirm password	Lets you retype the password for authenticating to pcAnywhere.
Host name	Indicates the name that you want to use for the host. You can leave this box blank to configure the host name to be the same as the computer name.
Encryption level	Encrypts the data stream between the host and remote computer.
Encryption level–None	Specifies that no encryption of the data stream occurs between the host and the remote computer.

Table 13-13 Configure Symantec pcAnywhere options *(continued)*

Option	Description
Encryption level–pcAnywhere	Scrambles the data using a mathematical algorithm so that a third party cannot easily interpret it.
	This option is available on any operating system that pcAnywhere supports.
Encryption level–Symmetric	Encodes and decode data using a cryptographic key.
	This option is available on any Windows operating system that supports the Microsoft CryptoAPI.

See

Licensing options

The following table describes the options on the **Licensing** panel in the LightsOut Restore Wizard.

Table 13-14 Licensing options

Options	Description
Use the license key that is activated on this computer	Enables features in the customized Symantec System Recovery Disk by using the activated product license key. The key must already reside on the computer that you want to restore.
Use the following license key	Enables features in the customized Symantec System Recovery Disk by typing a product license key.
Prompt for a license key	Prompts you for a product license key at the time you want to enable features in the customized Symantec System Recovery Disk.

See

Recovering a computer

This chapter includes the following topics:

About recovering a computer

If Windows fails to start or does not run normally, you can still recover your computer. You can use the Symantec System Recovery Disk and an available recovery point or a virtual disk that you created from a recovery point.

Note: If you can start Windows and the drive that you want to restore is a non-operating system drive, you can restore the drive within Windows.

The Symantec System Recovery Disk lets you run a recovery environment that provides temporary access to Symantec System Recovery recovery features. For example, you can access the recovery features of Symantec System Recovery to restart the computer into its previous, usable state.

Note: If you purchased Symantec 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.

Booting a computer by using the Symantec System Recovery Disk

The Symantec System Recovery Disk lets you boot a computer that can no longer run the Windows operating system. Symantec System Recovery Disk is included with Symantec System Recovery. When you boot your computer using the Symantec System Recovery Disk, a simplified version of Windows starts that runs a recovery environment. In the recovery environment, you can access the recovery features of Symantec System Recovery.

Note: Depending on which product version you have purchased, Symantec System Recovery Disk is either included on your product CD, or as a separate CD. You should place the CD containing Symantec System Recovery Disk in a safe place.

Note: Symantec System Recovery Disk requires a minimum of 1 GB of RAM to run. If your computer's video card is configured to share your computer's RAM, you might need more than 1 GB of RAM.

To boot a computer by using the Symantec System Recovery Disk

1   If you store your recovery points on a USB device, attach the device now (for example, an external hard drive).

> **Note:** You should attach the device before you restart the computer. Otherwise, Symantec System Recovery Disk might not detect it.

2   Insert the CD containing the Symantec System Recovery Disk into the media drive of the computer. If your Symantec System Recovery Disk is on a USB device, plug in the USB device into the media drive of the computer.

    If a computer manufacturer installed Symantec System Recovery, 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/DVD or the USB device, you might need to change the startup settings on your computer.

    See "Configuring a computer to start from a CD/DVD or a USB device" on page 229.

4   As soon as you see the prompt **Press any key to boot from CD/DVD or USB device**, press a key to start Symantec System Recovery Disk.

> **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 Symantec System Recovery Disk, and your computer restarts.

See "Recovering a computer" on page 231.

Configuring a computer to start from a CD/DVD or a USB device

Your Symantec System Recovery Disk might be on a CD/DVD or a USB device. Accordingly, to run Symantec System Recovery Disk, you must be able to start your computer using a CD/ DVD or a USB device.

See "Booting a computer by using the Symantec System Recovery Disk" on page 228.

To configure a computer to start from a CD/DVD or a USB device

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 program.

3   In the **BIOS setup** window, select **Boot Sequence**, and then press **Enter**.

4   Follow the on-screen instructions to set the CD/DVD or the USB device to be the first startup device in the list.

5   Place your Symantec System Recovery Disk CD/DVD into the media drive. If your Symantec System Recovery Disk is on a USB device, plug in the USB device into the media drive.

    Note: Depending on which product version you have purchased, Symantec System Recovery Disk is either included on your product CD or as a separate CD. You should place the CD that contains Symantec System Recovery Disk in a safe place. If you lose the CD, you can create a new one if you 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 Symantec System Recovery Disk.

    When you start your computer with the Symantec System Recovery Disk CD/DVD or USB device in the drive, you see a prompt to **Press any key to boot from CD/DVD or USB device**. If you do not press a key within five seconds, your computer attempts to start from the next startup device.

    Note: Watch carefully as the computer starts. If you miss the prompt, you must restart the computer again.

See

Preparing to recover a computer by checking the hard disk for errors

If you suspect that your hard disk is damaged, you can examine it for errors.

To prepare to recover a computer by checking the hard disk for errors

1   Boot the computer by using the Symantec System Recovery Disk.

    See "Booting a computer by using the Symantec System Recovery Disk"
    on page 228.

2   In the **Analyze** panel of Symantec System Recovery Disk, click **Check Hard
    Disks for Errors**.

3   Select the drive that you want to check.

4   Select any of the following options.

    ■   **Automatically fix file system errors**
        Fixes the errors on the selected disk. If you do not select this option, errors
        are displayed but are not fixed.

    ■   **Find and correct bad sectors**
        Locates the bad sectors and recovers readable information.

5   Click **Start**.

See "Recovering a computer" on page 231.

Recovering a computer

You can restore your computer from within the recovery environment that is
known as Symantec System Recovery Disk. If you have a recovery point for the
hard drives that you want to recover, you can fully restore your computer. Or,
you can recover another hard drive back to the state it was in when the recovery
point was created.

Note: If you restore a recovery point to a computer that uses different hardware,
the Restore Anyware feature is automatically enabled for you.

See "Recovering a computer through Restore Anyware" on page 244.

To recover a computer

1   Boot the computer by using the Symantec System Recovery Disk.

    See "Booting a computer by using the Symantec System Recovery Disk"
    on page 228.

2   On the **Home** panel of Symantec System Recovery Disk, click **Recover My
    Computer**.

    If your recovery points are stored on media and you only have one media
    drive, you can eject the Symantec System Recovery Disk now. Insert the
    CD/DVD or the USB device that contains your recovery points.

3   On the **Welcome** page of the wizard, click **Next**.

4   On the **Select a Recovery Point to Restore** panel, select a recovery point to
    restore, and then click **Next**.

    See "Select a Recovery Point to Restore options" on page 233.

5   On the **Drives to Recover** panel, select each drive that you want to recover
    and set the options that you want, and then click **Next**.

    See "Drives to Recover options" on page 235.

    When you recover 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. Or,
    you can identify the drive by its name, or by browsing the files and folders
    in the recovery point.

6   Optionally, select a drive that you want to recover, and then click **Edit**.

    Select the options that you want to perform during the recovery process, and
    then click **OK** to return to the **Drives to Recover** panel.

    See "Edit target drive and options" on page 236.

7   Click **Next** to review the recovery options that you selected.

8   Select **Reboot when finished** if you want the computer to restart automatically
    after the recovery process finishes.

9   Click **Finish**.

10 Click **Yes** to begin the recovery process.

See "Recovering a computer from a virtual disk file" on page 238.

See "Recovering files and folders by using Symantec System Recovery Disk "
on page 246.

Select a Recovery Point to Restore options

The following table describes the options on the **Select a Recovery Point to Restore** panel. This panel is available from the **Recover My Computer** wizard in Symantec System Recovery Disk.

Table 14-1   Select a Recovery Point to Restore options when you view recovery points by Date

Option	Description
View by - Date	Displays all of the discovered recovery points in the order in which they were created.
	If no recovery points were discovered, the table is empty. In such cases, you can search all local drives on the computer or browse to find a recovery point.
Select source folder	Lets you view a list of all available recovery points that may exist on your computer's local drives or on a specific drive.
Map a network drive	Specifies a shared network folder path and assign it a drive letter. You can then browse the folder location for the recovery point file you want.
Browse	Locates a recovery point on a local drive or a network folder.
Select a recovery point	Lets you select the recovery point to restore.
Recovery point details	Gives you additional information about the recovery point you want to restore.

Table 14-2   Select a Recovery Point to Restore options when you view recovery points by File name

Option	Description
View by - File name	Lets you view recovery points by their file name.
Recovery point folder and file name	Specifies a path and a file name of a recovery point.

Table 14-2 Select a Recovery Point to Restore options when you view recovery points by File name *(continued)*

Option	Description
Map a network drive	Specifies a shared network folder path and assign it a drive letter. You can then browse the folder location for the recovery point file you want.
Browse	Locates a recovery point on a local drive or a network folder.
Recovery point details	Gives you additional information about the recovery point you want to restore.

Table 14-3 Select a Recovery Point to Restore options when you view recovery points by System

Option	Description
View by - System	Lets you use the current system index file that is located in the recovery point storage location. The system index file displays a list of all of the drives on your computer and any associated recovery points from which you can select.
	The use of a system index file reduces the time it takes to convert multiple recovery points. 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.
System index folder and filename	Specifies a path and a file name of a system index file that you want to use for recovery.
Map a network drive	Specifies a shared network folder path and assign it a drive letter. You can then browse the folder location for the system index file (.sv2i) you want.

Table 14-3   Select a Recovery Point to Restore options when you view recovery
points by System *(continued)*

Option	Description
Browse	Lets you browse to a path that contains a system index file.
	For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.

See "Recovering a computer" on page 231.

See "Recovering a computer through Restore Anyware" on page 244.

Drives to Recover options

The following table describes the options on the **Drives to Recover** panel. This
panel is available from the **Recover My Computer** wizard in Symantec System
Recovery Disk.

Table 14-4   Drives to Recover options

Option	Description
Select drives to recover	Lets you select the drives that you want to recover.
Add	Adds additional drives you want to recover.
Remove	Removes selected drives from the list of drives to recover.
Edit	Lets you edit the recovery options for a selected drive.
	See "Edit target drive and options" on page 236.
Verify recovery point before restore	Verifies whether a recovery point is valid or corrupt before it is restored. If the recovery point is invalid, the recovery is discontinued.
	This option can significantly increase the time that is required for the recovery to complete.

Table 14-4   Drives to Recover options *(continued)*

Option	Description
Use Restore Anyware to recover to different hardware	Selected automatically if any of the following are true: ■ You recover a non-operating system drive to new or to different computer hardware. Or, you can recover both an operating system drive and one or more data drives to new or to different computer hardware. ■ You upgrade to new or to different computer hardware from an older computer. ■ The motherboard on the computer has failed. If you recover a data drive only to new or to different computer hardware, this option is not selected for you.

Edit target drive and options

The following table describes the options on the **Edit Target Drive and Options** panel. This panel is available from the **Drives to Recover** panel in the **Recover My Computer** wizard of Symantec System Recovery Disk.

Table 14-5   Edit target drive and options

Options	Description
Delete Drive	Deletes a selected drive in the list to make space available to restore your recovery point. When you use this option, the drive is only marked for deletion. The actual deletion of the drive takes place after you click **Finish** in the wizard.
Undo Delete	Returns a deleted drive to the list of drives.

Table 14-5   Edit target drive and options *(continued)*

Options	Description
Resize drive after recover (unallocated space only)	Resizes a disk after the recovery point is restored. After you select this option, you can specify the new size in megabytes. The size must be greater than the identified size of the disk that you selected in the list.
Primary partition	Because hard disks are limited to four primary partitions, this option is appropriate if the drive has four or fewer partitions.
Logical partition	This option is appropriate 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.
Check for file system errors after recovery	Checks the restored drive for errors after the recovery point is restored.
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 restore 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 part of all Windows operating systems that Symantec System Recovery supports. 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 restore a recovery point to a new, empty hard disk.

Table 14-5 Edit target drive and options *(continued)*

Options	Description
Restore master boot record	Restores the master boot record. The master boot record is contained in the first sector of a physical hard disk. The master boot record consists of a master boot program and a partition table that describes the disk partitions. The master boot program analyzes the partition table of the first 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 restore a recovery point to a new, empty hard disk.
	■ You restore 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.

See "Drives to Recover options" on page 235.

See "Recovering a computer" on page 231.

See "Recovering a computer through Restore Anywhere" on page 244.

Recovering a computer from a virtual disk file

Using the recovery environment, you can recover your computer from within a virtual disk file (.vmdk or .vhd). If you have a virtual disk for the hard drives that you want to recover, you can fully recover your computer. Or, you can recovery another hard drive back to the state it was in when the original virtual disk was created.

See "Defining a virtual conversion job" on page 183.

See "Running a one-time conversion of a physical recovery point to a virtual disk" on page 194.

Note: If you restore a virtual disk to a computer that uses different hardware, the Restore Anywhere feature is automatically enabled for you.

To recover a computer from a virtual disk file

1   Boot the computer by using the Symantec System Recovery Disk.

    See "Booting a computer by using the Symantec System Recovery Disk" on page 228.

2   On the **Home** panel of Symantec System Recovery Disk, click **Recover My Computer**.

3   On the **Welcome** panel of the wizard, click **Next**.

4   On the **Select a Recovery Point to Restore** panel, in the **View recovery points by** list, select **Filename**.

5   On the **Select a Recovery Point to Restore** panel, click **Browse** to locate, select, and open a virtual disk file (.vmdk or .vhd).

    If necessary, click **Map a network drive**. Specify a shared network folder path and assign it a drive letter. You can then browse the folder location for the virtual disk file you want.

6   Click **Next**.

7   In the **Target Drive** panel, select the target drive where you want to restore the virtual disk.

8   Optionally, do any of the following:

    ■   Click **Delete Drive**.
        Delete a selected drive in the list to make space available to restore your virtual disk.
        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.

    ■   Click **Undo Delete**.
        If you delete a drive and then change your mind, click **Undo Delete** to return the drive to the list.

9   Click **Next**.

     Use Restore Anyware to recover to different hardware is already selected for you if you recover an operating system drive (the drive on which Windows is installed; usually the C drive).

     This option is not selected if the virtual disk already contains the necessary drivers for the target computer. Or, if you restore a virtual disk that contains a data drive.

10 If necessary, enter the product license key.

     A license key is required to use Restore Anyware when you recover a system from a virtual disk file.

     If you choose, you can add a license key directly to a custom Symantec System Recovery Disk by using the **Create Custom Recovery Disk** wizard. When you restore a virtual disk and Restore Anyware is enabled in Symantec System Recovery Disk, you are not prompted to enter the license key. It is already a part of the custom Symantec System Recovery Disk.

     See "Creating a custom Symantec System Recovery Disk" on page 37.

11 Click **Next**.

12 In the **Recovery Options** panel, select the options that you want to perform during the recovery process.

     See "Recovery Options" on page 240.

     The options that are available depend on the target drive that you selected earlier.

13 Click **Next** to review the recovery options that you selected.

14 Select **Reboot when finished** if you want the computer to restart automatically after the recovery process finishes.

15 Click **Finish**.

16 Click **Yes** to begin the recovery process.

See "Recovering a computer" on page 231.

See "Recovering a computer through Restore Anyware" on page 244.

Recovery Options

The following table describes the options on the **Recovery Options** panel. This panel is available when you use the **Recover My Computer** wizard of Symantec System Recovery Disk to recover a virtual disk.

Table 14-6   Recovery Options

Option	Description
Verify recovery point before recovery	Verifies whether a recovery point is valid or corrupt before it is restored. If the recovery point is invalid, the recovery is discontinued.
	This option can significantly increase the time that is 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 drive after recover (unallocated space only)	Specifies the new drive size in megabytes.
Primary partition	Because hard disks are limited to four primary partitions, this option is appropriate if the drive has four or fewer partitions.
Logical partition	This option is appropriate 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 restore the drive on which your operating system is installed.

Table 14-6   Recovery Options *(continued)*

Option	Description
Restore original disk signature	Restores the original, physical disk signature of the hard drive.
	Disk signatures are part of all Windows operating systems that Symantec System Recovery supports. 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 restore a recovery point to a new, empty hard disk.
Restore master boot record	Restores the master boot record. The master boot record is contained in the first sector of a physical hard disk. The master boot record consists of a master boot program and a partition table that describes the disk partitions. The master boot program analyzes the partition table of the first 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 restore a recovery point to a new, empty hard disk.
	■ You restore 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.

About recovering to a computer with different hardware

The Symantec System Recovery Restore Anyware feature lets administrators restore a system drive of a supported Windows platform computer. You can restore the system even if it has different hardware than was found in the original computer from which the recovery point was made.

Restore Anyware lets you make the necessary changes for the system to be able to start. Depending on your configuration, you may need to make additional changes for the computer to run exactly as it did previously.

If you restore to identical (or very similar) hardware on which the recovery point was originally made, the Restore Anyware feature is deselected for you.

How to use Restore Anyware

Restore Anyware lets you restore a recovery point onto new hardware. For example, Restore Anyware is automatically used for you in the following scenarios:

- Your computer's motherboard has failed and you replaced it with a new or a different motherboard.

- You want to upgrade to new hardware from an older computer.

- You want to restore a virtual disk file back to a physical computer.

This feature is used to recover drives only; it cannot be used to recover at a more granular level such as files and folders.

Note: You can obtain more information about domain controller support.

See http://entsupport.symantec.com/umi/V-269-16

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. You can reactivate by using your Windows 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 Restore Anyware is used:

- Performing a Restore Anyware to hardware that is significantly different might require you to do the following:

  - 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 when the system restarts.

- When you restore a recovery point with 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.

- Restore Anyware is not used to restore a single recovery point to multiple computers. The product does not generate a unique SID (security identifier) for every computer.

- When you use Restore Anyware with a computer that uses a static IP address, you must manually reconfigure the computer after the restore is complete.

- Symantec 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.

See "About recovering to a computer with different hardware" on page 243.

See "Recovering a computer through Restore Anyware" on page 244.

Recovering a computer through Restore Anyware

Before you restore a computer with Restore Anyware, you must save the recovery point or virtual disk file to an accessible location. During the recovery, 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:

http://entsupport.symantec.com/umi/V-269-15

Warning: Before you restore a computer through Restore Anyware, test your access to the recovery points or virtual disk in the recovery environment. You should ensure that you have access to SAN volumes and that you can connect to the network.

To recover a computer through Restore Anyware

1   Start the computer by using the Symantec System Recovery Disk.

    See "Booting a computer by using the Symantec System Recovery Disk"
    on page 228.

2   On the **Home** panel, click **Recover My Computer**.

    Your recovery points or virtual disks may be stored on media. In such cases,
    if you only have one CD/DVD or USB drive, you can eject the Symantec System
    Recovery Disk now. Insert the CD/DVD or the USB device that contains your
    recovery points or virtual disks.

3   On the **Welcome** panel of the wizard, click **Next**.

4   Do one of the following:

    ■ If Symantec System Recovery Disk located recovery points, proceed to
       step 7.

    ■ If Symantec System Recovery Disk did not locate any recovery points,
       proceed to the next step.

5   On the **Select a Recovery Point to Restore** panel, select a recovery point to
    restore.

    See "Select a Recovery Point to Restore options" on page 233.

6   Click **Next**.

7   On the **Drives to Recover** panel, select each drive that you want to recover
    and set the options that you want, and then click **Next**.

    See "Drives to Recover options" on page 235.

    When you recover 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. Or,
    you can identify the drive based on the name that is assigned to it. Or, you
    can browse the files and folders in the recovery point.

    See "Recovering files and folders by using Symantec System Recovery Disk
    " on page 246.

8   Optionally, select a drive that you want to recover, and then click **Edit**.

    Select the options that you want to perform during the recovery process, and
    then click **OK** to return to the **Drives to Recover** panel.

    See "Edit target drive and options" on page 236.

9   Click **Next** to review the recovery options you have selected.

10   Select **Reboot when finished** if you want the computer to restart automatically when the recovery process finishes.

11   Click **Finish**.

12   Click **Yes** to begin the recovery process.

See "Recovering a computer" on page 231.

See "Recovering a computer from a virtual disk file" on page 238.

Recovering files and folders by using Symantec System Recovery Disk

You can use the Symantec System Recovery Disk to start your computer and to restore files and folders from within a recovery point.

To recover files and folders by using Symantec System Recovery Disk

1   Start the computer by using the Symantec System Recovery Disk.

   See "Booting a computer by using the Symantec System Recovery Disk" on page 228.

2   Click **Recover**, and then click **Recover My Files**.

3   Do one of the following:

   ■ If Symantec System Recovery Disk cannot locate any recovery points, you are prompted to locate one. In the **Select Recovery Point** dialog box, navigate to a recovery point, select one, and then click **OK**.
     See "Select Recovery Point options" on page 247.

   ■ If Symantec System Recovery Disk finds recovery points, select a recovery point from the list, and then click **OK**.

   Note: If you cannot find the recovery points in a network location, type the name of the computer and the share that holds your recovery points. For example, \\computer_name\share_name.

   If you still have trouble, try entering the computer's IP address.

   See "About using the networking tools in Symantec System Recovery Disk" on page 249.

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.

5   In the content pane of the Recovery Point Browser, select the files or folders that you want to restore.

6   Click **Recover Files**.

In the **Recover Items** dialog box, the **Restore to this folder** field may already contain 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.

See "Recovering a computer" on page 231.

See "Recovering a computer from a virtual disk file" on page 238.

Select Recovery Point options

The following table describes the options on the **Select Recovery Options** panel. This panel is available when you use the **Recover My Files** wizard of Symantec System Recovery Disk.

Table 14-7   Select Recovery Point options when you view recovery points by date

Option	Description
View by - Date	Displays all of the discovered recovery points in the order in which they were created. If no recovery points were discovered, the table is empty. In such cases, you can search all local drives on the computer or browse to find a recovery point.
Select source folder	Lets you view a list of all available recovery points that may exist on your computer's local drives or on a specific drive.

Table 14-7   Select Recovery Point options when you view recovery points by
                    date *(continued)*

Option	Description
Map a network drive	Specifies a shared network folder path and assign it a drive letter. You can then browse the folder location for the recovery point file you want.
Browse	Lets you locate a recovery point on a local drive or a network folder.
Select a recovery point	Lets you select the recovery point to restore.
Recovery point details	Gives you additional information about the recovery point you want to restore.

Table 14-8   Select Recovery Point options when you view recovery points by file
                    name

Option	Description
View by - File name	Lets you view recovery points by their file name.
Recovery point folder and file name	Specifies a path and a file name of a recovery point.
Map a network drive	Specifies a shared network folder path and assign it a drive letter. You can then browse the folder location for the recovery point file you want.
Browse	Lets you locate a recovery point on a local drive or a network folder.
Recovery point details	Gives you additional information about the recovery point you want to restore.

See "Recovering files and folders by using Symantec System Recovery Disk "
on page 246.

Exploring files and folders on your computer by using Symantec System Recovery Disk

You can explore the files and folders on your computer from Symantec System Recovery Disk by using the **Explore My Computer** feature.

This feature uses the Recovery Point Browser and functions similar to Windows Explorer. You can browse the file structure of any drive that is attached to your computer from Symantec System Recovery Disk.

To explore files and folders on your computer by using Symantec System Recovery Disk

1   Start the computer by using the Symantec System Recovery Disk.

See "Booting a computer by using the Symantec System Recovery Disk" on page 228.

2   In the **Analyze** panel, click **Explore My Computer**.

See "Recovering files and folders by using Symantec System Recovery Disk " on page 246.

About using the networking tools in Symantec System Recovery Disk

If you store your recovery points on a network, you need access to the network. This access lets you restore your computer or your files and folders from Symantec System Recovery Disk. The Symantec System Recovery Disk includes a variety of networking tools that you can use to assist you with recovery.

Note: Additional computer memory might be required to recover your computer or files across a network.

See "Starting networking services" on page 249.

See "Using the pcAnywhere thin host for a remote recovery" on page 250.

See "Mapping a network drive from within Symantec System Recovery Disk" on page 252.

See "Configuring network connection settings" on page 253.

Starting networking services

If you need to start networking services, you can do so manually.

To start networking services

◆ On the **Network** panel in Symantec System Recovery Disk, click **Start My Networking Services**.

To verify the connection to the network, you can map a network drive.

See "Mapping a network drive from within Symantec System Recovery Disk" on page 252.

See "About using the networking tools in Symantec System Recovery Disk" on page 249.

Using the pcAnywhere thin host for a remote recovery

The Symantec System Recovery Disk includes a pcAnywhere thin host. It 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.

See "About using the networking tools in Symantec System Recovery Disk" on page 249.

Note: You cannot deploy a thin host to Symantec System Recovery Disk. The thin host can only be started from the Symantec System Recovery Disk to host a remote control session in Symantec System Recovery Disk. The thin host in Symantec System Recovery Disk does not support file transfers and cannot be used to add drivers for network or storage devices.

After you start the thin host from Symantec System 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 Symantec System Recovery Disk. You must use Symantec pcAnywhere to connect to the thin host.

See "Remotely connecting to the pcAnywhere thin host" on page 251.

To start the pcAnywhere thin host

◆ On the **Network** panel in Symantec System Recovery Disk, click **Start the pcAnywhere Thin Host**.

The networking services are started, if necessary. The thin host waits for a connection.

Remotely connecting to the pcAnywhere 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. This host is included in the Symantec System Recovery Disk. The host also must be available and waiting for a connection. When the host and the client computer are connected, the client computer can remotely manage a recovery. Or, the client computer can perform other tasks that are supported in Symantec System Recovery Disk.

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 pcAnywhere thin host

1   Ensure that the computer to be remotely managed (the host) has started in Symantec System Recovery Disk. Also, ensure that the pcAnywhere thin host is available and 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 log on 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 log on to the host on connection.
        If you do not include the logon information, you are prompted for it when you connect to the thin host.

   ■   Type the following log on 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.

You can prevent unauthorized users from tampering with your settings. You can also prevent users from trying to launch a session without your permission. To do so, you can 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 attempt to connect again.

6 Remotely perform the necessary tasks on the host computer.

The remote control session ends when the thin host is closed. It is also 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. The connection can help you verify the success of tasks that were performed in the recovery environment.

See "Using the pcAnywhere thin host for a remote recovery" on page 250.

See "About using the networking tools in Symantec System Recovery Disk" on page 249.

Mapping a network drive from within Symantec System Recovery Disk

If you started the networking services after you started the recovery environment, you can map a network drive. This mapping lets you browse to that drive and select the recovery point that you want to restore. Or, if you create backups from the recovery environment, you can select a destination that resides on a network location.

See "About using the networking tools in Symantec System Recovery Disk" on page 249.

If there is no DHCP server or the DHCP server is unavailable, you must provide a static IP address. You must also provide a subnet mask address for the computer on which you are running Symantec System Recovery Disk.

See "Configuring network connection settings" on page 253.

After you provide the static IP address and subnet mask address, you can enter the recovery environment. However, 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. Or, you can use the mapped network drive as a destination for recovery points that you create from within the recovery environment.

To map a network drive from within Symantec System Recovery Disk

1   In Symantec System Recovery Disk, on the **Network** panel, 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**

You can also map a network drive from within the **Recover My Computer** wizard or the **Back Up My Computer** wizard in Symantec System Recovery Disk.

See "Using the pcAnywhere thin host for a remote recovery" on page 250.

Configuring network connection settings

You can access the **Network Configuration** window to configure network settings while running in the Symantec System Recovery Disk environment.

To configure network connection settings

1   In the Symantec System Recovery Disk environment, click **Network**, and then click **Configure Network Connection Settings**.

2   If you are prompted to start networking services, click **Yes**.

See "About using the networking tools in Symantec System Recovery Disk" on page 249.

Getting a static IP address

You can restore a recovery point that is located on a network drive or share. Sometimes, however, you cannot map a drive or browse to the drive or share on the network to access the recovery point. The lack of an available DHCP service can cause such a failure. In such cases, 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.

See "Configuring network connection settings" on page 253.

See "About using the networking tools in Symantec System Recovery Disk" on page 249.

To get a static IP address

1   In the Symantec System Recovery Disk environment, click **Network**, and then click **Configure Network Connection Settings**.

2   In the **Network Adapter Configuration** dialog box, click **Use the following IP address**.

3   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.

4   Click **OK**.

5   Click **Close** to return to the recovery environment's main menu.

6   In the **Network** panel, click **Ping a Remote Computer**.

7   Type the address of the computer that you want to ping on the network segment.

8   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.

    If communication to the storage computer operates as expected, you can use the **Map Network Drive** utility to map a drive to the recovery point location.

See "Recovering a computer" on page 231.

Getting a static IP address if pinging 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.

See "Configuring network connection settings" on page 253.

See "About using the networking tools in Symantec System Recovery Disk" on page 249.

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.

    Return to the computer that is running the Symantec System Recovery Disk
    environment

3   In the **Network** panel of the Symantec Recovery Disk environment, click **Ping
    a Remote Computer** and use the IP address you wrote down.

See "Recovering a computer" on page 231.

Viewing the properties of a recovery point

You can view various properties of a recovery point by using the Recovery Point
Browser.

See "Viewing the properties of a drive within a recovery point" on page 256.

To view the properties of a recovery point

1   Do one of the following:

    ■   In Symantec System Recovery, on the **View** menu, click **Tools**. Click **Run
        Recovery Point Browser**.

    ■   On the Windows **Start** menu, click **Programs > Symantec System Recovery
        > Recovery Point Browser**.

2   In the Recovery Point Browser, in the tree panel, select the recovery point
    file name that you want to view.

3   Do one of the following:

    ■   On the **File** menu, click **Properties**.

    ■   Right-click on the recovery point file name, and then click **Properties**.

    See "Recovery Point Properties" on page 255.

Recovery Point Properties

The following table describes the information available on the **Recovery Point
Properties** dialog box. This dialog box is available from the **Recovery Point
Browser**.

Table 14-9   Recovery Point Properties

Property	Description
Description	Displays a user-assigned comment that is associated with the recovery point.
Size	Displays the total size (in megabytes) of the recovery point.
Created	Displays the date and time that the recovery point file was created.
Compression	Displays the compression level that is used in the recovery point.
Split across multiple files	Identifies whether the entire recovery point file is spanned over several files.
Password protected	Displays the password protection status of the selected drive.
Encryption	Displays the encryption strength that is used with the recovery point.
Version	Displays the version number that is associated with the recovery point.
Computer name	Displays the name of the computer on which the recovery point was created.
Restore Anyware	Identifies whether Restore Anyware was enabled for the recovery point.
Search engine support	Identifies whether you enabled search engine support for the recovery point.
Created by	Identifies the application (Symantec System Recovery) that was used to create the recovery point.

See

Viewing the properties of a drive within a recovery point

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

See

To view the properties of a drive within a recovery point

1 Do one of the following:

   ■ In Symantec System Recovery, on the **View** menu, click **Tools**. Click **Run Recovery Point Browser**.

   ■ On the Windows **Start** menu, click **Programs > Symantec System Recovery > Recovery Point Browser**.

2 In the Recovery Point Browser, in the tree panel, double-click the recovery point file name that contains the drive that you want to view.

3 Select the name of the drive.

4 Do one of the following:

   ■ On the **File** menu, click **Properties**.

   ■ Right-click on the drive name within the recovery point, and then click **Properties**.

   See "Driver properties within a recovery point" on page 257.

Driver properties within a recovery point

The following table describes the information available on the **Recovery Point Properties** dialog box. This dialog box is available from the **Recovery Point Browser** when you select a drive within a recovery point.

Table 14-10   Driver properties within a recovery point

Property	Description
Description	Displays a user-assigned comment that is associated with the recovery point.
Original drive letter	Displays the original drive letter that was assigned to the drive.
Cluster size	Displays the cluster size (in bytes) that is used in a FAT, FAT32, or NTFS drive.
File system	Displays the file system type that is used within the drive.
Primary/Logical	Displays the selected drive's drive status as either the primary partition or the logical partition.

Table 14-10   Driver properties within a recovery point *(continued)*

Property	Description
Size	Displays the total size (in megabytes) of the drive. This total includes used and unused space.
Used space	Displays the amount of used space (in megabytes) within the drive.
Unused space	Displays the amount of unused space (in megabytes) within the drive.
Contains bad sectors	Identifies whether there are any bad sectors on the drive.
Cleanly quiesced	Identifies whether the database application quiesced properly when a recovery point was created.

See "Viewing the properties of a drive within a recovery point" on page 256.

About the Support Utilities

The Symantec System Recovery Disk environment has several support utilities. Symantec Technical Support might ask you to use these utilities to troubleshoot any hardware issues that you encounter.

You might be required to supply the information that these utilities generate if you call Symantec Technical Support for help resolving problems.

Note: You should only use these tools as directed by Symantec Technical Support.

See "Recovering files and folders by using Symantec System Recovery Disk " on page 246.

Copying a hard drive

This chapter includes the following topics:

■ About copying a hard drive

■ Preparing to copy a hard drive

■ Copying one hard drive to another hard drive

About copying a hard 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 copy a larger hard drive to a smaller hard drive. The data on the drive that is copied must be at least 1/16th smaller in size than the total size of the new drive.

Some hard drives that you want to copy contain more than one partition. In such cases, 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 is used in another computer. The drivers that are used to run the hardware on one computer may not match the drivers on a second computer.

See "About recovering to a computer with different hardware" on page 243.

Preparing to copy a hard drive

Before you can copy hard drives, you must have the hardware configured correctly.

Table 15-1   Preparing to copy a drive

Action	Description
Prepare the computer	Do the following: ■ 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.
Arrange jumper settings	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 use cable select instead of jumper settings to determine the master and the slave drives.
Attach the new hard drive	Do the following: ■ 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. 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.
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.
Anchor the drive	Anchor the drive in the bay area according to the manufacturer's instructions.

Table 15-1   Preparing to copy a drive *(continued)*

Action	Description
Change the BIOS settings to recognize the new hard drive	Do the following: ■ 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 the slave drives. ■ Save the BIOS changes, and then exit. Your computer restarts automatically.

See "Copying one hard drive to another hard drive" on page 261.

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.

Some hard drives that you want to copy contain more than one partition. In such cases, you must copy the partitions 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.

To copy one hard drive to another hard drive

1   On the **View** menu, click **Tools**.

2   Click **Copy My Hard Drive**.

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

4   In the **Source Drive** panel, select the drive that you want to copy, and then click **Next**..

5   In the **Destination** panel, select the destination drive for the copy, and then click **Next**.

6   In the **Advanced Options** panel, set the copy options you want, and then click **Next**.

    See "Advanced options" on page 262.

7   Click **Finish** to begin the copy.

See "Preparing to copy a hard drive" on page 259.

Advanced options

The following table describes the options on the **Advanced Options** panel. This panel is available from the **Copy Drive Wizard**.

Table 15-2   Advanced options

Option	Description
Check source for file system errors	Checks the source drive for errors before you copy it. The source drive is the original drive.
Check destination for file system errors	Checks the destination drive for errors after you copy the drive. The destination drive is the new drive.
Resize drive to fill unallocated space.	Expands the drive to occupy the destination drive's remaining unallocated space.
Set drive active (for booting OS)	Makes 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 hard disk, and it must contain an operating system. When the computer boots, it reads the partition table of the first hard disk to find out which drive is active. It then boots from that location. If you cannot start up the computer from the drive, have a boot disk ready. You can use the Symantec System Recovery Disk. The **Set drive active** option is valid for basic disks only (not dynamic disks).
Disable SmartSector copying	Speeds up the copying process by only copying the clusters and sectors containing data. In high-security environments, you might want to copy all clusters and sectors in their original layout, regardless of whether they contain data. In such cases, this option should be deselected.
Ignore bad sectors during copy	Copies the drive even if there are errors on the disk.

Table 15-2   Advanced options *(continued)*

Option	Description
Copy MBR	Copies the master boot record from the source drive to the destination drive. Select this option if you intend to copy 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 the destination drive has partitions and you do not want to overwrite them.
Primary partition	Lets you make the destination (new) drive a primary partition.
Logical partition	Lets you make the destination (new) drive a logical partition inside an extended partition.
Drive letter	Lets you select the drive letter you want assigned to the partition.

Using the Symantec System Recovery Granular Restore Option

This chapter includes the following topics:

- About the Symantec System Recovery Granular Restore Option

- Best practices when you create recovery points for use with the Granular Restore Option

- Starting the Granular Restore Option

- What you can do with the Granular Restore Option

- Opening a specific recovery point

- Restoring a mailbox

- Restoring an email folder

- Restoring an email message

- Restoring SharePoint documents

- Restoring files and folders

About the Symantec System Recovery Granular Restore Option

The Granular Restore Option is an administrative tool that works with Symantec System Recovery to provide granular restore capabilities for the following applications:

■ Microsoft Exchange™ 2003, 2007, and 2010

Note: Microsoft Exchange 2007 requires a Windows 64-bit operating system. Microsoft Exchange 2010 requires Windows Vista SP2 64-bit or Windows Server 2008 64-bit.

■ Microsoft SharePoint® 2003, 2007, and 2010
■ File and folder data

Symantec System Recovery is used to create volume-level recovery points. Using the Granular Restore Option, you can open these recovery points and restore Microsoft Exchange mailboxes, folders, and individual messages. You can also restore Microsoft SharePoint documents, and unstructured files and folders.

See "Starting the Granular Restore Option" on page 268.

See "Opening a specific recovery point" on page 269.

See "What you can do with the Granular Restore Option" on page 268.

See "Best practices when you create recovery points for use with the Granular Restore Option" on page 266.

See "Restoring a mailbox" on page 270.

See "Restoring an email folder" on page 271.

See "Restoring an email message" on page 272.

See "Restoring SharePoint documents" on page 273.

Best practices when you create recovery points for use with the Granular Restore Option

When creating a recovery point, you should use the following guidelines:

■ Select the option to back up your computer, not the option to back up selected files and folders.
See "Defining a drive-based backup" on page 74.

- When you select which drives to back up, make sure that you select all of the drives on the system.
  See "How to identify drives for backup" on page 267.

- When you select the type of recovery point to create, you should select **Recovery Point Set** instead of **Independent Recovery Point**. This selection makes subsequent recovery points much smaller.
  See "Recovery point type options" on page 76.

- The Exchange or SharePoint server does not need to be turned off for a backup to run successfully. However, you should schedule the backup at a time when the server is less busy (for example, after midnight).
  See "Advanced Scheduling options" on page 81.

- If you use mount points, make sure that you select them for backup.

See "About the Symantec System Recovery Granular Restore Option" on page 266.

How to identify drives for backup

The recommended way to protect your Exchange server is to create a single backup job that contains all of the drives on your server. However, you can choose to run your backups at the storage group and message store levels. You should consider the following to ensure a successful backup:

Include the drive that contains your Exchange installation	Granular Restore Option uses the recovery point of the Exchange server to perform the restore operation. Therefore, you should routinely back up your Exchange server. When you create the recovery point, you should select the drive that contains your Exchange installation directory.
	For example, if you installed Exchange in the C:\Program File\Exchsrvr directory, make sure that you include the entire C drive in your recovery point.
Include the storage group for the message store that you want to back up	A storage group is a collection of message stores. Each storage group contains a transaction log that is used to buffer writes to the message stores. You must back up the drive that contains the storage group's log files for the message store that you want to protect.
	For example, suppose you have a storage group named *First Storage Group*. If the storage group contains a transaction log on E:\Exchsrvr\mdbdata, you should include the entire E drive as part of the recovery point. If you have multiple storage groups, you should back them up at the same time. If you want to back up your storage groups on different schedules, you still need to include Exchange in your backups.

Include the message stores that you want to protect	A message store is a database file that stores email. Message stores are subgroups of storage groups. When you create a recovery point for a message store, you must also include its storage group.
	For example, if you have a message store named *Message Store* (myserver) that is located on F:\Exchsrvr\mdbdata\Message Store (myserver).stm, you should include the entire F drive in your recovery point.

You can select a subset of drives when backing up a Microsoft SharePoint server. However, the recommended way is to protect the entire server. Unlike the method for Exchange, it is not necessary to back up the SharePoint binaries. You should, however, back up any volumes that contain SharePoint data.

See "Best practices when you create recovery points for use with the Granular Restore Option" on page 266.

Starting the Granular Restore Option

How you start Granular Restore Option depends on the version of Windows you use.

To start the Granular Restore Option

◆ Do one of the following:

- In Symantec System Recovery, on the **Tools** page, click **Run Granular Restore Option**.

- On the classic Windows taskbar, click **Start > Programs > Symantec System Recovery > Granular Restore Option**.

- On the Windows 2003, 2008, XP, Vista, or 7 taskbar, click **Start > All Programs > Symantec System Recovery > Granular Restore Option**.

See "What you can do with the Granular Restore Option" on page 268.

See "Opening a specific recovery point" on page 269.

What you can do with the Granular Restore Option

You can do the following tasks with the Granular Restore Option.

Table 16-1   Granular Restore Option tasks

Task	More information

■ Restore Exchange mail.
  ■ Open a specific recovery point.
  ■ Restore a mailbox.
  ■ Restore an email folder.
  ■ Restore or forward an email message.
	See "Restoring a mailbox" on page 270.
	See "Restoring an email folder" on page 271.
	See "Restoring an email message" on page 272.

■ Restore SharePoint documents.
  ■ Open a specific recovery point.
  ■ Search or browse for a lost document.
  ■ Restore a document.
	See "Restoring SharePoint documents" on page 273.

■ Restore unstructured files and folders.
  ■ Open one or more recovery points.
  ■ Search or browse for a lost file or folder.
  ■ Restore lost files and folders.
  ■ Restore a version of a file.
	See "Restoring files and folders" on page 274.

See "About the Symantec System Recovery Granular Restore Option" on page 266.

Opening a specific recovery point

You open recovery points so you can restore mailboxes, email folders and messages, SharePoint documents, and files and folders.

To open a specific recovery point

1   On the **View** menu, click **Tools**.

2   Click **Run Granular Restore Option**.

3   In the **Open Recovery Points** dialog box, select the option you want and then click **OK**.

    See "Open Recovery Points options" on page 270.

4   You can change the backup date that you view by selecting a different date in the upper right-hand corner.

See "What you can do with the Granular Restore Option" on page 268.

Open Recovery Points options

The following table describes the options on the **Open Recovery Points** dialog box. This dialog box is available when you run the Granular Restore Option.

Table 16-2   Open Recovery Points options

Option	Description
Use latest recovery points for this computer	Opens a recovery point using the latest recovery points from the computer on which you work.
Use alternate system index (.sv2i) file	Opens a recovery point using its system index file.
System index file name	Lets you specify a path and a file name of a system index file that you want to use for recovery.
Browse	Lets you browse to a path that contains a system index file. For example, you can browse to an external (USB) drive, a network location, or to removable media to select a system index file.
Use recovery points for another computer.	Opens a recovery point that resides on another computer.
Browse	Lets you browse to a path that contains recovery points. For example, you can browse to an external (USB) drive, a network location, or to removable media to select recovery points.
Computer Name	Identifies the names of recovery point files and virtual disk files in the specified path of another computer.

See "Opening a specific recovery point" on page 269.

Restoring a mailbox

A restored mailbox consists of all of the email that was contained in a user's mailbox when the recovery point was created. A recover mailbox is saved on the disk as a PST file.

You can use Microsoft Outlook to open and view the contents of the file. After a restored mailbox has been opened in Outlook, you can then drag email or folders back to their original locations.

Note: In many cases, it is easier to restore a user's entire mailbox than find a single message.

To restore a mailbox

1   On the **View** menu, click **Tools**.

2   Click **Run Granular Restore Option**.

3   In the **Open Recovery Points** dialog box, open the recovery point for the last known time that the mail was present on the Exchange server.

    See "Open Recovery Points options" on page 270.

4   Click **OK**.

5   On the **Exchange Mail** tab, from the list of mailboxes, select the mailbox you want to restore.

6   Right-click the mailbox, and then click **Recover Mailbox**.

7   Select the folder where you want to place the restored mailbox, and then click **Save**.

Note: If the size of the mailbox is large, you may want to copy it to a shared folder.

See "Restoring an email folder" on page 271.

See "Restoring an email message" on page 272.

Restoring an email folder

You can restore a single folder instead of an entire mailbox. For example, if a user needs a copy of a sent message, it may be quicker to restore only the Sent Items folder.

A restored folder is saved on the disk as PST file. You can use Microsoft Outlook to open and view the contents of the folder. After a restored email folder has been opened in Outlook, you can drag email or folders back to their original locations.

To restore an email folder

1. On the **View** menu, click **Tools**.

2. Click **Run Granular Restore Option**.

3. In the **Open Recovery Points** dialog box, open the recovery point for the last known time that the mail was present on the Exchange server.

   See "Open Recovery Points options" on page 270.

4. Click **OK**.

5. On the **Exchange Mail** tab, select the mailbox for the user who requested the restore.

6. In the folder list, right-click the folder you want to restore, and then click **Recover Folder**.

7. Select the folder where you want to place the restored folder, and then click **Save**.

See "Restoring an email folder" on page 271.

See "Restoring an email message" on page 272.

Restoring an email message

You can use the Granular Restore Option to restore individual email messages. You can save individual messages in an .msg file format on the disk, or you can forward them directly to a user. Use Microsoft Outlook to open and view the contents of a saved message file.

To restore an email message

1. On the **View** menu, click **Tools**.

2. Click **Run Granular Restore Option**.

3. In the **Open Recovery Points** dialog box, open the recovery point for the last known time that the mail was present on the Exchange server.

   See "Open Recovery Points options" on page 270.

4. Click **OK**.

5. Click the **Exchange Mail** tab, select the mailbox for the user who requested the restore.

6. Select the folder that contains the message you want to restore.

7   Select the message to restore.

Note: You can sort the list by clicking the column headers. You can also search the subject lines of the messages by entering a search term in the search field (near the message list). When you add or delete characters in the search box, it automatically changes the results.

---

8   To return the email message to the user, do one of the following:

■ If you have Microsoft Outlook installed, double-click the message to open it in Outlook. You can use Outlook to send the message back to its owner.

■ To forward the message in Outlook, right-click the message, and then click **Forward.**
Outlook opens a new message. The message that you want to forward is included as an attachment. You can then forward the message to the original owner.

■ To save the message to a disk, right-click the message, and then click **Recover Message**. Type the file name, and then click **Save**.
The email message is saved on the disk. You can use Outlook to open the message.

See "Restoring a mailbox" on page 270.

See "Restoring an email folder" on page 271.

Restoring SharePoint documents

Symantec System Recovery can be used to restore backed up documents on a Microsoft SharePoint server. SharePoint documents are restored to the local system. Use Microsoft SharePoint to place the document back on the SharePoint server if wanted.

To restore SharePoint documents

1   On the **View** menu, click **Tools**.

2   Click **Run Granular Restore Option**.

3   In the **Open Recovery Points** dialog box, open the recovery point for the last known time that the mail was present on the Exchange server.

See "Open Recovery Points options" on page 270.

4   Click **OK**.

5 On the **SharePoint Documents** tab, browse or search for the file that you want to restore.

Note: You can sort the list by clicking the column headers. You can enter a search term in the search field (near the documents list). When you add or delete characters in the search box, it automatically changes the results.

---

6 Click the file to view its contents or to restore it, and then select the check box beside it.

7 On the **Tasks** menu, click **Restore Files**, and then select the destination for the restore.

See "Restoring files and folders" on page 274.

See "Restoring a mailbox" on page 270.

See "Restoring an email folder" on page 271.

See "Restoring an email message" on page 272.

Restoring files and folders

Granular Restore Option can be used to restore unstructured files and folders. This feature is particularly useful if you need to search more than one recovery point (multiple backup dates) to find a missing file or folder.

To restore a file or folder

1 On the **View** menu, click **Tools**.

2 Click **Run Granular Restore Option**.

3 In the **Open Recovery Points** dialog box, open the recovery point for the last known time that the mail was present on the Exchange server.

See "Open Recovery Points options" on page 270.

4 Click **OK**.

5 On the **Files and Folders** tab, browse or search for the file that you want to restore.

6 You can view more than one recovery point at a time. To see a view of the file system that contains multiple recovery points, click **Versions**. Now select the versions that you want to view by checking them in the list.

You can sort the list by clicking the column headers. You can enter a search term in the search field (near the documents list). When you add or delete characters in the search box, the results change automatically.

7 Click the file to view its contents or to restore it, and then select the check box beside it.

8 On the **Tasks** menu, click **Restore Files**, and then select the destination for the restore.

Note: If you view multiple recovery points and more than one version of a file is available, you can expand the list of versions. Click the plus sign next to each file. After you select a file for restore, choose the version of the file that you want.

See "Restoring SharePoint documents" on page 273.

See "Restoring a mailbox" on page 270.

See "Restoring an email folder" on page 271.

See "Restoring an email message" on page 272.

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

Symantec System Recovery supports the use of Google Desktop for searching the file names that are contained in recovery points.

> **Note:** Symantec Backup Exec Retrieve is also supported, but your company's IT department needs to install it. When they install it, there is nothing you have to do to enable it. Ask your IT department for details.

When you enable search engine support, Symantec System Recovery creates a catalog of all the files that are contained in a recovery point. Search engines like Google Desktop use the catalog file to 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.

See "Enabling search engine support" on page 277.

Enabling search engine support

The following table summarizes the steps for enabling search engine support.

Table A-1   Enabling search engine support

Step	Action	Description
Step 1	Install a search engine	An organization's IT department installs Backup Exec Retrieve. 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 "Installing Google Desktop" on page 278.
Step 2	Enable Google Desktop support	A Google plug-in for Symantec 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 "Enabling Google Desktop support" on page 279.
Step 3	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 the files that are contained in the resulting recovery point. A search engine such as Google Desktop can then use the list to generate its own index. You can then use the index to perform searches by file name.
		See "Enabling search engine support for a backup job" on page 279.

Note: The generated list of files that search engines require for generating searchable indexes are appended to recovery points as they are created. Hence, recovery points that already exist when you enable this feature cannot be indexed. After you enable this feature, run each of your backups 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.

See "About using a search engine to search recovery points" on page 277.

Installing Google Desktop

You can download and install Google Desktop using the following steps.

To install Google Desktop

1   On the **Tasks** menu, click **Options**, and then click **Google Desktop**.

2   Click **Download Google Desktop from the Web** and follow the instructions for installation.

3   After completing the installation, click **OK** in the **Symantec System Recovery Options** window.

    For more information, visit desktop.google.com.

See "Enabling search engine support" on page 277.

Enabling Google Desktop support

After installing Google Desktop, you must enable the Google Desktop support feature. Enabling this feature automatically installs the Google plug-in for Symantec System Recovery. This plug-in is required for using Google Search to locate and recover files.

To enable Google Desktop support

1   On the **Tasks** menu, click **Options**, and then click **Google Desktop**.

2   Select **Enable Google Desktop File and Folder Recovery**.

    This option is not available if you do not have Google Desktop installed. Install Google Desktop, and then repeat this procedure.

3   Click **OK**.

4   Click **OK** to install the Google Plug-in.

See "Enabling search engine support" on page 277.

Enabling search engine support for a backup job

You can enable search engine support when you define new backup jobs. To enable search engine support for existing backup jobs, edit them.

To enable search engine support for a backup job

1   Start Symantec System Recovery.

2   Do one of the following:

    ■   Edit an existing backup job and select **Enable search engine support for Google Desktop and Backup Exec Retrieve** on the **Options** page of the wizard.

- Define a new backup job and select **Enable search engine support for Google Desktop and Backup Exec Retrieve** on the **Options** page of the wizard.

See "Enabling search engine support" on page 277.

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 locate and recover files using Google Desktop.

See "Enabling search engine support" on page 277.

To recover files using Google Desktop's Search Desktop feature

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 that contains the file you want to recover.

4   When the file opens in the associated application, on the **File** menu, click **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 and restoring files within a recovery point" on page 165.

Tips for finding a file using Google Desktop

If you do not find a file that is included in a recovery point that has search engine support enabled, do the following:

- Right-click the Google Desktop icon in the system tray. On the shortcut menu, click **Indexing**, and then click **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 that contains your recovery points (backup destination) is available.

For example, if your backup destination is on a USB drive, ensure that the drive is plugged in and the power is turned on. Or, if your backup destination is on a network, be sure that you are connected and logged on with the correct credentials.

■ Narrow your search results. Recovery point files use .v2i as their file extension. When you add the file extension to your search string, any results that are not found in a recovery point are eliminated. For example, you can add V2i to the search string "My Tune mp3 V2i" to find mp3 files only in recovery point files.

■ 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**.

See "Enabling search engine support" on page 277.

Backing up databases using Symantec System Recovery

This appendix includes the following topics:

- About backing up databases using Symantec System Recovery
- About backing up VSS-aware databases using Symantec System Recovery
- About backing up non-VSS-aware databases using Symantec System Recovery

About backing up databases using Symantec System Recovery

Symantec System Recovery enables you to back up both, Microsoft's Volume Shadow Copy Service (VSS)-aware and non-VSS aware databases. For backing up VSS-aware databases, Symantec System Recovery integrates with VSS to automate the backup process. While, for backing up non-VSS-aware databases, you can create manual or automatic cold or hot recovery points of the databases.

See "About backing up VSS-aware databases using Symantec System Recovery" on page 283.

See "About backing up non-VSS-aware databases using Symantec System Recovery" on page 284.

About backing up VSS-aware databases using Symantec System Recovery

Symantec System Recovery integrates with Microsoft's VSS to automate the process of backing up VSS-aware databases, such as the following:

- Exchange Server 2003 or later
- SQL Server 2005 or later
- Windows Server 2003-based domain controller or later

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, Symantec 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 during the backup. After the databases are quiesced, Symantec System Recovery takes the snapshot. VSS is then notified that a 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.

Symantec System Recovery supports Exchange Server 2003 or later, which implements VSS technology. However, if the database load is heavy, the VSS request might be ignored. Create recovery points at the lightest load time.

Be sure that you have installed the latest service packs for your given database.

Note: For backing up Exchange databases, additional backup applications are not needed to run with Symantec System Recovery.

See "About backing up non-VSS-aware databases using Symantec System Recovery" on page 284.

About backing up non-VSS-aware databases using Symantec System Recovery

With Symantec System Recovery, you can create manual cold backups, automatic warm backups, or hot backups of non-VSS-aware databases.

See "About creating a cold backup manually using Symantec System Recovery or Symantec System Recovery Disk" on page 285.

See "About creating a warm backup automatically using Symantec System Recovery" on page 286.

See "Creating a cold backup manually" on page 285.

See "Creating a warm backup automatically" on page 286.

About creating a cold backup manually using Symantec System Recovery or Symantec System Recovery Disk

A manual cold (or offline) backup ensures that all database transactions are committed to the hard disk. You can then use either Symantec System Recovery or the Symantec System Recovery Disk to create the recovery point, and then restart the database.

Creating a cold backup manually

The following table summarizes the steps for creating a cold backup manually using Symantec System Recovery or Symantec System Recovery Disk.

Table B-1   Creating a cold back manually

Step	Action	Description
Step 1	Stop the database	Manually stop the database you want to back up.
Step 2	Create a recovery point	Create a recovery point using either Symantec System Recovery or the Symantec System Recovery Disk. Do one of the following: ■ Use Symantec System Recovery to run a backup immediately using the **Run Backup** or **One-time Backup** feature. See "Running a one-time backup from Symantec System Recovery" on page 93. ■ Use the Symantec System Recovery Disk to create a one time cold backup. See "About running a one-time backup from Symantec System Recovery Disk" on page 94.
Step 3	Restart the database	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 immediately created from the virtual volume recovery point.

About creating a warm backup automatically using Symantec System Recovery

You can automate the creation of a warm backup of a non-VSS-aware database by running a command file in the backup job. Run this command file before data capture to stop (quiesce) the database momentarily and commit all transaction logs to the hard disk. Symantec System Recovery instantaneously snaps a virtual volume recovery point.

Run a second command file in the backup job to 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. As a result, there is a minimal number of log files created.

Creating a warm backup automatically

The following table summarizes the steps for creating a warm backup automatically using Symantec System Recovery.

Table B-2   Creating a warm backup automatically

Step	Action	Description
Step 1	Define a backup	Define a backup that includes the 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.
Step 2	Run the backup job	Using Symantec System Recovery, run the backup job that includes the command files.

See "About backing up non-VSS-aware databases using Symantec System Recovery" on page 284.

Creating a hot backup using Symantec System Recovery

If a cold or a warm backup is not possible in your organization, create a hot (or online) backup for backing up non-VSS-aware databases.

Symantec 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 backup

◆ Use Symantec System Recovery to create a recovery point without the need to stop or restart the database.

Symantec System Recovery instantaneously snaps a virtual volume recovery point from which the recovery point is created.

See "About backing up non-VSS-aware databases using Symantec System Recovery" on page 284.

Backing up Active Directory

This appendix includes the following topics:

- About the role of Active Directory

About the role of Active Directory

When protecting a domain controller with Symantec System Recovery, be aware of the following:

- If your domain controller is Windows Server 2003, it supports Microsoft Volume Shadow Copy Service (VSS). Symantec System Recovery automatically calls VSS to prepare the Active Directory database for backup.

- 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 that is contained in a recovery point is not updated automatically by the domain controller. Therefore, a computer that is recovered using a recovery point containing an outdated token cannot participate in the domain. For such a computer to participate in the domain it must be re-added to the domain by someone who has the proper credentials.
  In Symantec System Recovery, this trust token can be re-established automatically if the computer participates in the domain when the recovery process is started.

- In most cases, domain controllers should be restored non-authoritatively. Restoring domain controllers non-authoritatively prevents outdated objects in the Active Directory from being restored. Outdated objects are referred to as tombstones. Active Directory does 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 prevents 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/umi/V-269-16

Backing up Microsoft virtual environments

This appendix includes the following topics:

■ About backing up Microsoft virtual hard disks

■ About backing up and restoring Microsoft Hyper-V virtual machines

About backing up Microsoft virtual hard disks

Microsoft Windows 7/Server 2008 R2 now support the use of Virtual Hard Disks (VHDs). Microsoft does not support backing up a physical disk and a VHD on that physical disk in the same backup job. This limitation also applies to Symantec System Recovery. You cannot back up a physical disk and its VHD counterpart in the same backup job using Symantec System Recovery. Also not supported is the ability to back up a VHD that is hosted on or "nested" within another VHD. If you want to back up a physical disk and a VHD on that disk, you must create separate backup jobs for each disk.

Backing up a physical disk that hosts a VHD is supported as long as it is not included as another volume in the same backup. When a physical disk hosting a VHD is backed up, the VHD is treated as another file that is part of the physical disk backup.

VHDs can be attached and detached from their physical disk hosts (volumes). Microsoft recommends that you detach a VHD that is stored on a host volume before you back up. Not detaching a VHD before you back up a host volume can result in an inconsistent copy of the VHD in the backup. After you restore a host volume, you can re-attach the VHD file.

http://entsupport.symantec.com/umi/V-306-2

You can find more information on backing up VHDs on the Microsoft Web site.

http://technet.microsoft.com/en-us/library/dd440865(WS.10).aspx

Find information about backing up and restoring Microsoft Hyper-V virtual machines:

See "About backing up and restoring Microsoft Hyper-V virtual machines" on page 292.

About backing up and restoring Microsoft Hyper-V virtual machines

To create a backup of a Microsoft Hyper-V virtual machine, you must back up the volumes of the computer where the virtual machine is hosted. Create either a live backup or a system state backup of the host machine. You cannot back up or restore a specific virtual machine. A live backup is created while the virtual machine is running (hot backup).

A system state backup is created in any of the following conditions:

- The guest operating system on the virtual machine is not running (cold backup).

- The Hyper-V VSS integration component is not installed in the virtual machine.

Note: Symantec System Recovery is unable to back up cluster shared volumes. Because volumes in such a configuration are accessible to each of the clustered Hyper-V host computers, a given volume cannot be locked for backup . However, clustered disks can be backed up by Symantec System Recovery because one host has exclusive access to the disk.

To create a backup of a running virtual machine, the following conditions must be met:

- The guest operating system must be running.

- The guest machine must be running Windows Server 2003 or later.
  If the guest machine is running Winows 2000, Windows XP 32- or 64-bit, you can only create a system state backup (cold backup).

- The Hyper-V VSS integration component must be installed on each virtual machine to be backed up.
  If you move a virtual machine from Virtual Server 2005 to Hyper-V, first uninstall the Virtual Server 2005 integration component from the virtual machine. After you Virtual Server 2005 integration component, you can install the Hyper-V VSS integration component.

■ The guest virtual machine should be configured to only use basic disks, not dynamic disks.
 This configuration is the default for installing a Windows virtual machine.

■ All the volumes on the fixed disks must support the creation of snapshots.

If you perform a backup when these conditions are not met, Symantec System Recovery creates a system state recovery point that is crash-consistent. A crash-consistent recovery point captures the virtual machine as if it had experienced a system failure or power outage.

To restore a virtual machine, you must restore the recovery point of the host computer. The host computer recovery point must include the volume that holds the virtual machine you want to restore. You cannot restore a specific virtual machine.

To know about the limitations of Hyper-V when backing up databases on virtual machines, refer to the Symantec Knowledge Base:

http://entsupport.symantec.com/umi/V-306-2

Find information about backing up Microsoft virtual hard disks:

See "About backing up Microsoft virtual hard disks" on page 291.

http://entsupport.symantec.com/umi/V-306-2

Using Symantec System Recovery 2011 and Windows Server 2008 Core

This appendix includes the following topics:

- About Symantec System Recovery 2011 and Windows Server 2008 Core

- Installing Symantec System Recovery 2011 on Windows Server 2008 Core using commands

About Symantec System Recovery 2011 and Windows Server 2008 Core

Windows Server 2008 Core does not include the traditional graphical user interface (GUI) that is available with other versions of Windows. It is installed and managed primarily using commands at the command line interface.

Although Symantec System Recovery 2011 can be installed on Windows Server 2008 Core, it is an agent only install. Windows Server 2008 Core does not support Microsoft .NET. Therefore, the Symantec System Recovery GUI cannot be installed. Symantec System Recovery is supported on Windows Server 2008 Core by a headless agent only. You can install Symantec System Recovery 2011 using commands at the command line. You can also install (push) the agent from a remote machine.

One-to-one management is the only supported method for backing up and restoring a Windows Server 2008 Core machine. This means, after you install the agent on a Windows Server 2008 Core machine, connect to it from a remote machine running one of the following:

- Symantec System Recovery 2011

- Symantec System Recovery Management Solution

Before installing the agent remotely on a Windows Server 2008 Core machine, you must configure the firewall to allow access to the server. By default, the firewall is configured to allow no access to the server.

For more information on configuring the firewall on a Windows Server 2008 Core machine, see the Microsoft Web site.

Windows-on-Windows 64-bit (WoW64) is a subsystem of the Windows operating system and is required for running 32-bit applications on 64-bit versions of Windows. It is installed by default and is included on all 64-bit versions of Windows. If you have uninstalled WoW64 on a Windows Server 2008 Core R2 machine, you must reinstall it before installing Symantec System Recovery 2011.

See "Installing Symantec System Recovery 2011 on Windows Server 2008 Core using commands" on page 296.

Installing Symantec System Recovery 2011 on Windows Server 2008 Core using commands

The following options exist for installing Symantec System Recovery 2011 on a Windows Server 2008 Core system. They are

- Full install with GUI support
  See "Running a full install with GUI support" on page 296.

- Full silent install with logging
  See "Running a full silent install with logging" on page 297.

- Agent-only silent install with logging
  See "Running an agent-only silent install with logging" on page 297.

Running a full install with GUI support

The following table summarizes the steps for installing Symantec System Recovery 2011 using the option for full install with GUI support.

| Table E-1 | Installing Symantec System Recovery 2011 using the option for full install with GUI support |
| | |

Step	Action	Description
Step 1	Run `Browser.exe`	On the Symantec System Recovery 2011 CD, browse to and run `Browser.exe`. A graphical environment (GUI) is launched where you complete the remainder of the installation.
Step 2	Complete installation	Complete the installation by following the steps in the installation wizard. Even though the full Symantec System Recovery is installed, only the agent is needed and used on Windows Server 2008 Core.

See "Installing Symantec System Recovery 2011 on Windows Server 2008 Core using commands" on page 296.

Running a full silent install with logging

The following are the steps for installing Symantec System Recovery 2011 using the option for full silent install with logging.

To install Symantec System Recovery 2011 using the option for full silent install with logging

1   On the Symantec System Recovery 2011 CD, change to the Install directory.

2   Run the following command:

```
Setup.exe /s /v"/qn /l*v %temp%\SSRInstall.log"
```

Even though the full Symantec System Recovery is installed, only the agent is needed and used on Windows Server 2008 Core.

See "Installing Symantec System Recovery 2011 on Windows Server 2008 Core using commands" on page 296.

Running an agent-only silent install with logging

The following are the steps for installing Symantec System Recovery 2011 using the option for agent-only silent install with logging.

To install Symantec System Recovery 2011 using the option for agent-only silent install with logging

1   On the Symantec System Recovery 2011 CD, change to the Install directory.

2   Run the following command:

```
Setup.exe /s /v"/qn AddLocal=Agent,Shared,SecurityShortCut /l*v
%temp%\SSRInstall.log"
```

See "Installing Symantec System Recovery 2011 on Windows Server 2008 Core using commands" on page 296.

Index