Norton Ghost 15.0 User's Guide

symantec™

Norton Ghost 15.0 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, the Symantec Logo, Norton, Norton AntiVirus, LiveUpdate, pcAnywhere, and SmartSector are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Microsoft, Windows, Windows NT, Windows Vista, MS-DOS, Hyper-V, and the Windows logo are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries. VeriSign® is a registered trademark of Verisign, Inc.

VMware, the VMware "boxes" logo and design are registered trademarks or trademarks of VMware, Inc..

Gear Software is a registered trademark of GlobalSpec, Inc.

Google and Google Desktop are trademarks of Google, Inc.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 Norton Ghost™

This chapter includes the following topics:

About Norton Ghost

Norton Ghost provides advanced backup and recovery for your computer. Protect any kind of data you keep on your computer by making a backup of your computer's entire hard disk. Or, limit your backup to include only those files and folders that mean the most to you.

You can schedule backups to capture your changes automatically as you work from day to day. Or start a backup manually at any time. You can also easily configure Norton Ghost to run a backup in response to specific events. For example, a backup can run when a particular application is started. Or, a backup can run when a specified amount of new data is added to the drive.

When you experience a problem with your computer, you can restore a file, folder, or an entire drive. This recovery process returns your computer to a previous, functional state with the operating system, applications, and data files intact. Or, if you accidentally delete a personal file, get it back with a few steps.

Using easy-to-follow wizards, you can set up fast and reliable backup jobs and have them run while you continue to work. Or, schedule your backups to run after hours when your computer is idle.

When disaster strikes, Norton Ghost helps you recover your computer from the effects of many common problems, including

- Virus attacks: Damage might be done before a virus is quarantined.
- Faulty software installations: Some software can negatively affect your computer's performance, and slow it down to the point that programs or documents require too much time to open. But when installed, removing a program might not recover unintentional damage by the installation.
- Hard drive failure: Data can become corrupted on your system drive (typically C), making it impossible to start your operating system
- Files accidentally deleted or overwritten: Accidental deletion of files is common, but often costly.
- Corrupted files: Individual files and folders can become corrupted by viruses, or when a program used to modify them encounters an error.

What is new in Norton Ghost

Norton Ghost 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 1-1 What is new Norton Ghost

Feature	Description
Improved support for virtual formats	Norton Ghost now includes support for the following virtual platforms: ■ VMware ESX 3.5i and 4.0i ■ VMware ESX 3.5 and 4.0
Improved platform support	Norton Ghost now includes support for the following platforms: ■ Windows 7 ■ Windows Vista with SP2 (includes Home Basic, Home Premium, Business-Retail, and Ultimate)

Table 1-1 What is new Norton Ghost *(continued)*

Feature	Description
Create recovery points from within Symantec Recovery Disk	You can now create independent recovery points using the new Back Up My Computer feature in Symantec Recovery Disk. Sometimes known as a cold backup or offline backup, you can create recovery points of a partition without the need to install Norton Ghost or its Agent. See "About running a one-time backup from Symantec Recovery Disk" on page 76.
Convert recovery points to virtual disks using a schedule	You can now create schedules to convert recovery points to VMware Virtual Disk and Microsoft Virtual Disks, or directly to a VMware ESX 3.5 server. See "Defining a virtual conversion job" on page 147.
Support for Microsoft Hyper-V	You can now convert recovery points to Hyper-V format and also import recovery points to a Hyper-V server.
Support for Blu-ray disc media	Back up your computer directly to Blu-ray, DVD, or CD. Or, you can copy recovery points to Blu-ray, DVD, or CD.
Fully enabled 60-day trial	If you choose to delay installation of the product license, all features still remain enabled during the 60-day trial period. The 60-day trial period begins when you do a particular task. See "When you delay licensing " on page 20.

Hiding or showing the Advanced page

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

Note: When you refer to the documentation while using 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 product interface. From that point on, follow the remaining steps of each procedure.

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

To hide or show the Advanced page

1. Start Norton Ghost.
2. On the View menu, click **Show Advanced Page** to hide or show the Advanced page.

Getting more information about Norton Ghost

To learn more about Norton Ghost, visit the Help and Support page. Depending on which version and language of the product you have installed, the Help and Support page includes one-click access to more information. The page also includes access to the product help system, the product User's Guide. It also includes access to the Symantec Knowledge Base where you can find troubleshooting information.

To access Help and Support

1. Start Norton Ghost.
2. On the Home page, click **Help > Help and Support**.

Installing Norton Ghost

This chapter includes the following topics:

Before you install

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

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

System requirements

The following table lists the system requirements for Norton Ghost to function properly.

Table 2-1 Minimum system requirements

Component	Minimum requirements
Operating system	The following Windows 32- or 64-bit operating systems are supported: ■ Windows 7 ■ Windows Vista Ultimate ■ Windows Vista Business ■ Windows XP Professional/Home (SP2 or later) ■ Windows XP Media Center (SP2 or later)
RAM	The following are the memory requirements for each component of Norton Ghost: ■ Norton Ghost Agent: 512 MB ■ Norton Ghost user interface and Recovery Point Browser: 512 MB ■ Symantec Recovery Disk: 1 GB (dedicated) ■ LightsOut Restore: 1 GB
Available hard disk space	The following are hard disk space requirements for Norton Ghost and other areas: ■ 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. See “Best practices for backing up” on page 50. ■ 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. Norton Ghost 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/support/recorders/index.cfm You can look up information about your writer if you know the name of the manufacturer and model number of your writer.
Software	The Microsoft .NET Framework 2.0 or later is required to run Norton Ghost. If .NET Framework is not already installed, you are prompted to install it after Norton Ghost is installed and your computer is restarted.
Virtual platforms (for converted recovery points)	The following virtual platforms are supported: ■ VMware Workstation 4, 5, and 6 ■ VMware ESX 3.0, 3.5, and 4.0 ■ VMware ESXi 3.5 and 4.0 ■ 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

About supported file systems and removable media

Norton Ghost supports the following file systems and removable media:

Supported file systems

Norton Ghost 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 Norton Ghost 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

Norton Ghost also lets you save recovery points to most USB devices, 1394 FireWire devices, REV, Jaz, Zip drives, and magneto-optical devices.

About disabled features

Norton Ghost 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 Norton Ghost.

When you delay licensing

If you choose to delay installation of the license key, all features in Norton Ghost remain enabled during the 60-day grace period.

Symantec Recovery Disk, a component of Norton Ghost, is available with no trial period or evaluation. However, you need a valid license key to use the following features in Symantec Recovery Disk:

- Back Up My Computer wizard

See “About running a one-time backup from Symantec Recovery Disk” on page 76.

The 60-day grace period of Norton Ghost 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 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

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

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

See “Activating Norton Ghost later” on page 24.

Installing Norton Ghost

Before you begin, you should review the requirements and scenarios for installing Norton Ghost.

See “System requirements” on page 17.

Note: During the installation process, you might be required to restart the computer. You should ensure proper functionality after the computer restarts. You can do this by logging on again using the same user credentials that you used to log on when you installed Norton Ghost.

Warning: The Symantec Recovery Disk CD provides the tools that you need to recover your computer. How you received Symantec Recovery Disk depends on the version of the product that you purchased. For example, Symantec Recovery Disk is included with your product either on a separate CD, or on your product CD. Be sure you store the CD in a safe place.

To install Norton Ghost

1. Log on to your computer using either the Administrator account or an account that has administrator privileges.
2. Insert the Norton Ghost product CD into the media drive of the computer.

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

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

   where <drive> is the drive letter of your media drive.
4. In the CD browser panel, click **Install Norton Ghost**.
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 or deselect the options you want installed, and then click **Install Now**.
     Installation options include:

Backup and Recovery Service	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.
User Interface	Installs the product user interface that is required for interacting with the Norton Ghost Service. Agent Deployment– Allows the computer on which you have installed Norton Ghost to deploy the Norton Ghost Agent to other computers for remote recovery management.

CD/DVD Support	Required for backing up directly to CD/DVD, and for creating a custom Symantec Recovery Disk CD. A CD/DVD burner is required to use this feature.
LiveUpdate	Keeps your Symantec software up-to-date with the latest product updates.

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 Norton Ghost until after you restart your computer.

Completing the installation

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

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

To complete the installation

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 Norton Ghost.

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 Norton Ghost.

- Click **Activate later** to delay the activation of your license. After the trial period ends, the product will no longer work.
  See "When you delay licensing " on page 20.
- If Norton Ghost is a trial version and you want to purchase a license key, click **Symantec Global Store**.

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 Desktop version of Norton Ghost.)
- 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, Norton Ghost 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.

5 Click **Finish**.

Activating Norton Ghost later

If you do not activate Norton Ghost 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 Norton Ghost later

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

2 Follow the on-screen prompts.

About setting up your first backup

Unless you deselected the **Run Easy Setup** check box during the setup wizard, the **Easy Setup** window appears. If you do not run **Easy Setup** during the setup wizard, it appears the first time you open the **Run or Manage Backups** window.

When the **Easy Setup** window is displayed, you can accept the default drive and file and folder backup settings. Or, you can click any of the settings to edit them.

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

Updating Norton Ghost

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 Norton Ghost

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

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

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

About uninstalling Norton Ghost

When you upgrade Norton Ghost from a previous version of the product, the install program automatically uninstalls the previous versions. If needed, you can manually uninstall the product.

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

Chapter 3

Ensuring the recovery of your computer

This chapter includes the following topics:

About ensuring the recovery of your computer

If Windows fails to start or it does not run normally, you can recover your computer by using the Symantec Recovery Disk CD. 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 help ensure that you have the drivers that you need to recover your computer, you can use the **Run Driver Validation** tool available on the Symantec Recovery Disk. The driver validation tool compares hardware drivers on the Symantec Recovery Disk CD with the drivers that are 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.

See "If driver validation fails" on page 28.

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

Testing Symantec Recovery Disk

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

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

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

- You cannot start Symantec Recovery Disk.
  See "To configure a computer to boot from a CD" on page 175.
- 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 Recovery Disk.

See "If driver validation fails" on page 28.

To test Symantec Recovery Disk

1. Run the driver validation tool to test whether Symantec Recovery Disk works with the network cards and storage devices on the computer.
2. Start your computer using the Symantec Recovery Disk CD.

   See "Starting a computer by using Symantec Recovery Disk" on page 174.
3. When you have started Symantec Recovery Disk, do one of the following:
   - If you want to store recovery points on a network, run a mock restore of a recovery point that is stored on a network to test the network connection.
   - If you want to store recovery points on a computer, run a mock restore of a recovery point that is stored locally to test the local hard drive connection.

If driver validation fails

The driver validation test verifies whether the drivers for all storage devices and network cards in use by the computer are available in Symantec Recovery Disk. If the drivers are available on the recovery disk, you receive a validation message. 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 Recovery Disk. Therefore, if the recovery points that are required for recovering your computer are stored on a network or a local hard drive, you might not have access to them.

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

See "Creating a custom Symantec Recovery Disk CD" on page 29.

Creating a custom Symantec Recovery Disk CD

Even if driver validation succeeds and your Symantec Recovery Disk CD appears to work, you should create a custom Symantec Recovery Disk CD. A custom CD 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.

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

To create a custom Symantec Recovery Disk CD

1. Attach and turn on all storage devices and network devices that you want to make available.
2. Start Norton Ghost.
3. Insert the Symantec Recovery Disk CD into your media drive.

   If necessary, specify the path or browse to the media drive in which you placed the Symantec Recovery Disk CD.
4. Click **Tasks > Create Custom Recovery Disk CD**.
5. Click **Next**.

6 Specify the following:

Disk label	Type the name that you want to use for the Symantec Recovery Disk label.
Burn Symantec Recovery Disk to CD/DVD	If you want to save your customized Symantec Recovery Disk to media, select this option and then in the list box, select the media burning device that you want to use.
Save a copy of the custom Symantec Recovery Disk (CD/DVD image file)	If you want to save your customized Symantec Recovery Disk as an .iso file, select this option, and then specify the path to where you want to save the resulting file.

7 Click **Next**.

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

9 On the Startup Options pane, select the default keyboard layout, display language, and time zone from the respective lists.

10 Click **Next**.

11 On the Options pane, do the following:

Automatically start network services	Select this option if you want networking to start automatically when you recover the computer through LightsOut Restore.
Dynamic IP	Click this option to connect 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	Click this option to connect 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

Select this option if you want the Symantec pcAnywhere thin host to start automatically when you start Symantec Recovery Disk.

Click **Configure** to specify pcAnywhere log on credentials and the following optional parameters:

- Host name

  In the Host name box, 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

  To encrypt the data stream between the host and remote computer, in the Encryption level list, select one of the following:
  - None

    No encryption of the data stream occurs between the host and remote computer.
  - pcAnywhere

    Scrambles 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.
  - Symmetric

    Encodes and decodes data using a cryptographic key.

    This option is available on any Windows operating system that supports the Microsoft CryptoAPI.

12 Click **Next**.

13 On the License Setup pane, specify how you want to enable licensed features in the customized Symantec Recovery Disk (such as the cold imaging feature called Back Up My Computer).

14 Click **Finish**.

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

See "Testing Symantec Recovery Disk" on page 28.

Chapter 4

Getting Started

This chapter includes the following topics:

- About key product components
- How you use Norton Ghost
- Starting Norton Ghost
- Configuring Norton Ghost default options

About key product components

Norton Ghost includes two key components: the program itself, and the Symantec Recovery Disk CD.

Table 4-1 Key product components

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

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

Key Component	Description
Symantec Recovery Disk CD	The Symantec Recovery Disk CD is used to start your computer in the recovery environment. If your computer's operating system fails, use Symantec 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 Recovery Disk is either included on your product CD, or as a separate CD. You should place the CD that contains Symantec Recovery Disk in a safe place. See "About recovering a computer" on page 173.

How you use Norton Ghost

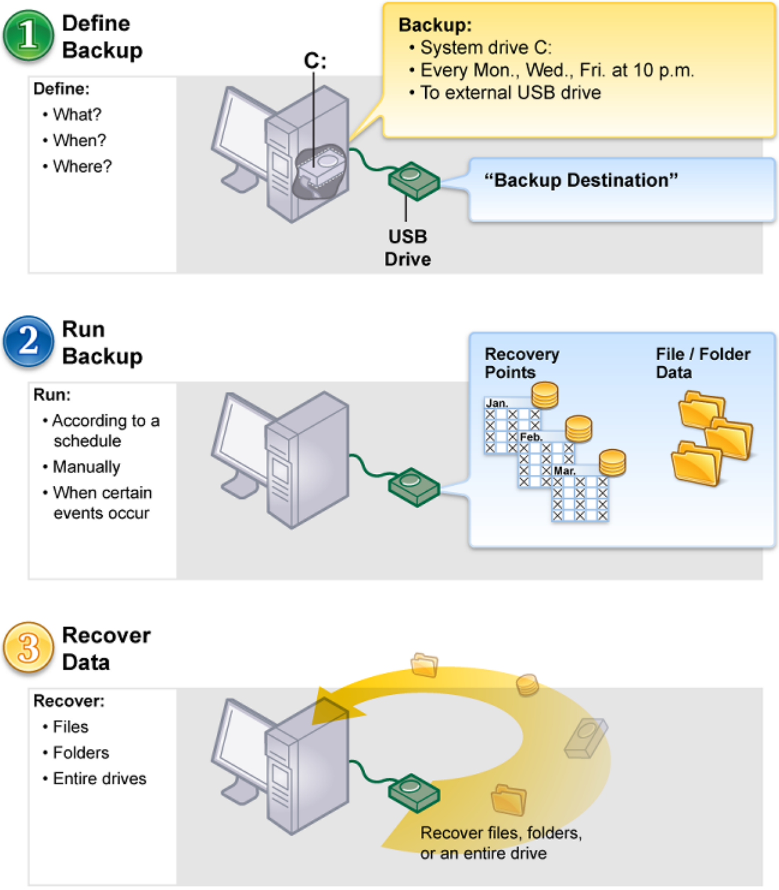
While Norton Ghost does the work of backing up your files, folders, or entire drives, you need to tell Norton Ghost what to backup, when to back it up, and where to put the backed up data.

Using Norton Ghost 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 Norton Ghost



Starting Norton Ghost

Norton Ghost 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 Norton Ghost. You can also open Norton Ghost from the Windows Start menu.

To start Norton Ghost

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

- On the classic Windows taskbar, click **Start > Programs > Norton Ghost > Norton Ghost 15.0**.
- On the Windows taskbar, click **Start > All Programs > Norton Ghost > Norton Ghost 15.0**.
- In the Windows system tray, double-click the **SymantecNorton Ghost 15.0** tray icon.
- In the Windows system tray, right-click the Norton Ghost tray icon, and then click **Open Symantec Norton Ghost 15.0**.

Configuring Norton Ghost default options

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

Options	Description
General	Specify a default location where a backup will create and store recovery points and file and folder backup data. If the location you choose is on a network, you can enter your user authentication information. See "Selecting a default backup destination" on page 38.
Performance	Lets you specify a default speed for backup or recovery processes. When you move the slider closer to Fast, it increases the speed at which the program backs up or recovers your computer. If you choose a slower speed it could improve the performance of your computer, especially if you work on your computer during a backup or recovery. **Note:** During a backup or recovery, you have the option to override this default setting to fit your needs at the time. You can also configure network throttling to limit the effects of backups on network performance. See "Adjusting the effect of a backup on computer performance" on page 39. See "Enabling network throttling" on page 39.
Tray Icon	You can turn on or off the system tray icon. You can also specify whether to show only error messages when they occur, or to show both error messages and other information, such as the completion of a backup. See "Adjusting default tray icon settings" on page 40.

Options	Description
File Types	Lets you manage file types and file type categories, which are used as a method for selecting the types of files you want included in a file and folder backup. See "Managing file types" on page 41.
Google Desktop	If Google Desktop is installed on your computer when you install Norton Ghost, you have the option of enabling Google Desktop file and folder recovery. When you enable this feature, you can search for files (by file name) inside a recovery point that was created with search engine support enabled. If Google Desktop is not installed on your computer when you install Norton Ghost, you have the option of clicking a link to the Web site where you can download and install Google Desktop for free. See "About using a search engine to search recovery points" on page 201.
External Drives	Delete or rename the unique names you have given to external drives used as backup and Offsite Copy destinations. See "Using nicknames for external drives" on page 43.
Configure FTP	Specify default FTP settings to be used with Offsite Copy. See "Configuring default FTP settings for use with Offsite Copy" on page 44.
Log File	Lets you specify the types of product messages to log (errors, warnings, and information), where to store the log file, and set a maximum file size for the log file. See "Logging Norton Ghost messages" on page 44.
Event Log	Lets you specify the types of product messages to log (errors, warnings, and information) in the Windows event log. See "Logging Norton Ghost messages" on page 44.
SMTP E-mail	If you want a history of actions taken by Norton Ghost, or of error messages and warnings, you can choose to save them in a log file on your computer, or to have them emailed to an address you specify. See "Enabling email notifications for product (event) messages" on page 46.

Options	Description
SNMP Trap	If you have a Network Management System (NMS) application, you can enable SNMP Traps support to send notifications to you NMS application. See "About SNMP traps" on page 122.

To configure Norton Ghost default options

1 Start Norton Ghost.

2 Click **Tasks > Options**.

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

Selecting a default backup destination

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

To select a default backup destination

1 In Norton Ghost, on the menu bar, click **Tasks > Options**.

2 Click **General**.

3 Select **Prepend computer name to backup data file names**.

   This is especially useful if you back up more than one computer to the same drive. For example, you might back up a laptop and a desktop computer to the same USB or network drive. By prepending the computer name to each backup data file name, you can more easily identify which backup data files belong to which computer.

4 Select **Save backup files to a unique subfolder** if you want Norton Ghost to create a new subfolder that will serve as your backup destination.

   Note: The new subfolder is given the same name as your computer. For example, if your computer name is "MyLaptop", the new subfolder would be named \MyLaptop.

5 Enter a path to a folder where you want to store recovery points and file and folder backup data, or click **Browse** to look for a location.

You cannot use an encrypted folder as your backup destination. If you want to encrypt your backup data to prevent another user from accessing it, refer to the Advanced options when you define or edit a backup.

6 If you entered the path to a location on a network, enter the user name and password required to authenticate to the network.

7 Click **OK**.

Adjusting the effect of a backup on computer performance

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

However, you can actually change the speed of the backup as a way of minimizing the impact of Norton Ghost on your computer while you work.

To adjust the effect of a backup on computer performance

1. In Norton Ghost, on the menu bar, click **Tasks > Options**.
2. Click **Performance**.
3. If you want to improve your computer's speed performance, move the slider bar closer to **Slow**.
4. If you want the backup to complete more quickly, move the slider bar closer to **Fast**.
5. Click **OK**.

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

See “Adjusting the speed of a backup” on page 94.

Enabling network throttling

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

Network performance is affected by many variables. Consider the following issues 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?

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. Then, if necessary, enable this feature and set the Maximum network throughput to a setting that matches the circumstances.

To enable network throttling

1. In Norton Ghost, on the menu bar, click **Tasks > 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 that Norton Ghost can send per second.
5. Click **OK**.

Adjusting default tray icon settings

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

To adjust default tray icon settings

1. In Norton Ghost, on the menu bar, click **Tasks > Options**.
2. Click **Tray Icon** and select one of the following:

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

3. Click **OK**.

Managing file types

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

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

To create a new file type and extensions

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

To edit a file type and extensions

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

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

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

1. In Norton Ghost, on the menu bar, click **Tasks > Options**.
2. Select a file type in the File types column.

   You cannot delete a default file type. You can delete all but one extension of a default file type, and you can add additional extensions to a default file type.
3. Click the **Remove a file type** (-) button , and then click **OK**.

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

Using nicknames for external drives

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

To help you manage these destinations, Norton Ghost lets you assign a nickname to each external drive. Doing so does not change the drive label, but is for use only when you are accessing those drives from within Norton Ghost.

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

However, by associating unique nicknames to each drive, then as you use the drive with Norton Ghost, the nicknames you assigned appear in various locations in Norton Ghost.

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

For example, if you assigned the nickname, "Cathy Read" to one drive, and "Thomas Read" to a second drive, their nicknames appear in Norton Ghost whenever the drives are plugged in to your computer.

See “About Offsite Copy” on page 81.

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

To remove or edit external drive nicknames

1. In Norton Ghost, on the menu bar, click **Tasks > Options**.
2. Under **Destinations**, click **External Drives**.
3. Select an external drive from the list and then do one of the following:
    - Click **Remove** to delete the nickname associated with the external drive.
    - Click **Rename** to edit the nickname.

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. Norton Ghost serves as an FTP client to copy your recovery points to a remote FTP server as a secondary backup of your critical data.

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

To configure default FTP settings for use with Offsite Copy

1 In Norton Ghost, on the menu bar, click **Tasks > Options**.

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

3 Refer to the following table when making changes:

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

Logging Norton Ghost 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: Norton Ghost logging, and the Windows application log.

From the Options page, you can configure both methods.

To log Norton Ghost messages

1. In Norton Ghost, on the menu bar, click **Tasks > Options**.
2. Under Notifications, click **Log File**.
3. Click the **Select the priority and type of messages** list and select the priority level at which a message should be logged.

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

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

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

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

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

1. In Norton Ghost, on the menu bar, click **Tasks > Options**.
2. Under Notifications, click **Event Log**.

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

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

4 Select one or more of the following options:

- Errors
- Warnings
- Information

5 Click **OK**.

Enabling email notifications for product (event) messages

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

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

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

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

To enable email notifications for product (event) messages

1 In Norton Ghost, on the menu bar, click **Tasks > Options**.

2 Under Notifications, click **SMTP E-mail**.

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

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

4 Select one or more of the following options:

- Errors
- Warnings
- Information

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

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

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

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

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

9 Enter your SMTP user name and password.

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

10 Click **OK**.

Best practices for backing up your data

This chapter includes the following topics:

About backing up your data

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

- Define a backup
- Run the backup
  See “How you use Norton Ghost” on page 34.

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.

About choosing a backup type

There are two types of backups available:

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

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

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

See “Before you back up” on page 51.

Best practices for backing up

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

- Before you back up
- During a back up
- When a back up is finished

About backups

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

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

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

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

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

Before you back up

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

Schedule back ups when you know your computer will be turned on.	Your computer must be turned on and Windows must be running at the time a back up occurs. If not, any scheduled back ups are skipped until the computer is turned on again. You then are prompted to run the missed back up. See "About choosing a backup type" on page 50.
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 "About selecting a backup destination" on page 56.

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 81.
Give nicknames to your external drives to help you easily identify them	You can assign a nickname to each external drive to help keep track of where your backup data is stored for each computer you back up. Because drive letters can change each time you unplug and plug an external drive into your computer, a nickname ensures that you can always know which drive you are using when you are running Norton Ghost. Using a nickname does not change the volume label of a drive. A nickname simply helps you identify the drive when using Norton Ghost. And the nickname sticks with the drive, so that if you plug the drive into a second computer running another copy of Norton Ghost, the nickname appears. **Note:** You might also consider placing a sticky label on each drive that matches the nickname that you have assigned. See “Using nicknames for external drives” on page 43.
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 81.
Run back ups on a regular and frequent basis.	When you define your back ups, 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 97. See “Defining a drive-based backup” on page 60.

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.

When you define a backup, you should select the option to verify the recovery point to ensure that the recovery point can be used to recover lost data.

See “About choosing a backup type” on page 50.

During a back up

If you are working at your computer and a back up starts to run, you might notice that the performance of your computer slows down. Norton Ghost requires significant system resources to run a back up. If slowing occurs, you can reduce the speed of the back up to improve computer performance until you are finished working.

See “Adjusting the speed of a backup” on page 94.

When a back up is finished

After a back up 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.

For file and folder backups, click **Recover My Files** from either the Home or Tasks pages. Then click **Search** to display the latest version of all the files that are included in your backup.

See “About opening files and folders stored in a recovery point” on page 163.

Review the Status page to verify that backups have happened and to identify any potential problems.	Periodically review the Status page. You can also review the events log on the Advanced page. The event log records events when they occur, backups and any errors that might have occurred during or after a backup. If you do not see the Advanced page tab, click **View** > **Show Advanced Page**. **Note:** Backup status and other messages are also conveyed in the system tray. So you do not even need to start the product to identify the status of your backups. See "Verifying that a backup is successful" on page 95.
Manage storage space by eliminating old backup data.	Delete outdated recovery points to make more hard disk space available. Also, reduce the number of file versions that are created by file and folder backups. See "Managing recovery point storage" on page 137. See "About managing file and folder backup data" on page 154.
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 139.

Additional tips about backups

Consider the following tips when you run a defined backup:

- Norton Ghost does not need to be running for a scheduled backup to start. After you define a backup, you can close Norton Ghost.
- The computer that is being backed up must be turned on and Windows must be started.
- All defined backups are saved automatically so that you can edit them or run them later.

- Do not run a disk defragmentation program during a backup. Doing so will significantly increase the time that it takes to create the recovery point and might cause unexpected system resource issues.
- If you have two or more drives that are dependent on each other, you should include both drives in the same backup. This provides the safest protection.
- Include multiple drives in the same defined backup to reduce the total number of backups that must be run. Doing so minimizes interruptions while you work.
- Use the Progress and Performance feature to reduce the impact of a backup on your computer's performance. For example, if a scheduled backup starts while you are in the middle of a presentation, you can slow down the backup to give more processing resources back to your presentation program.
- The power management features on a computer can conflict with Norton Ghost during a backup.

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

After defining your backup job

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

After you define a backup and schedule it to run, you can close Norton Ghost. The program does not need to be running for a backup to start.

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

Viewing the properties of a backup job

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

To view the properties of a backup job

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

About selecting a backup destination

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

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

The following table contains information that you need to consider when selecting a backup destination.

Table 5-1 Selecting a backup destination

Backup destination	Information to consider
Local hard drive, USB drive, or FireWire drive (recommended)	The benefits of this option are as follows: ■ Fast backup and recovery ■ Can schedule unattended backups ■ Inexpensive because drive space can be overwritten repeatedly ■ Off-site storage is possible ■ Reserves hard drive space for other uses Although you can save the recovery point to the same drive that you are backing up, it is not recommended for the following reasons: ■ As the number or size of recovery points grows, you will have less disk space available for regular use. ■ The recovery point is included in subsequent recovery points of the drive, which increases the size of those recovery points. ■ If the computer suffers a catastrophic failure, you may not be able to recover the recovery point you need, even if you save it to a different drive on the same hard disk.

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

Backup destination	Information to consider
Network folder	If your computer is connected to a network, you can save your recovery points and file and folder backup data to a network folder. Backing up to a network folder typically requires that you authenticate to the computer that is hosting the folder. If the computer is part of a network domain, you must provide the domain name, user name, and password. For example, domain\username. If you are connecting to a computer in a workgroup, you should provide the remote computer name and user name. For example: remote_computer_name\username.
CD-RW/DVD-RW	When you save backup data to removable media, it is automatically split into the correct sizes if the backup spans more than one media. If more than one drive is being backed up, the recovery points for each drive are stored independently on the media, even if there is space to store recovery points from multiple drives on the same media. The scheduling of backups is not available when this option is used. **Note:** Using CD-RWs or DVD-RWs as your recovery point storage location is not the best option because you will be required to swap disks during the process.

The following table describes the advantages and disadvantages of different types of backup destinations.

Table 5-2 Advantages and disadvantages of backup destinations

Backup destination	Advantages	Disadvantages
Hard drive (recommended)	■ Fast backup and recovery ■ Can schedule unattended backups ■ Inexpensive because drive space can be overwritten repeatedly	■ Uses valuable drive space ■ Vulnerable to loss if the hard drive fails

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

Backup destination	Advantages	Disadvantages
Network drive (recommended)	■ Fast backup and recovery ■ Can schedule unattended backups ■ Inexpensive because drive space can be overwritten repeatedly ■ Protection from local hard drive failure ■ Off-site storage (through existing network backup strategies)	■ Must have supported network interface card drivers to restore from Symantec Recovery Disk ■ Must understand and assign the appropriate rights for users who will run backups and restore data
Removable media (local)	■ Protection from hard drive failure ■ Ideal for off-site storage ■ Reserves hard drive space for other uses	

About backing up dual-boot computers

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

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

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

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

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

Backing up entire drives

This chapter includes the following topics:

- About defining a drive-based backup
- Defining a drive-based backup
- Compression levels for drive-based backups
- Running a one-time backup from Norton Ghost
- About running a one-time backup from Symantec Recovery Disk
- About Offsite Copy
- How Offsite Copy works

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 points or recovery point set names are appended with 001.v2i, 002.v2i, and so forth. Recovery point set names are appended with _i001.iv2i, _i002.iv2i, and so forth. For example, if your base recovery point is called CathyReadF001.v2i, the first incremental recovery point is called CathyReadF001_i001.iv2i.

See "Defining a drive-based backup" on page 60.

Defining a drive-based backup

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

To define a drive-based backup

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

   If you have not yet defined a backup, the Easy Setup dialog appears instead.
3. Click **Back up my computer**, and then click **Next**.
4. Select one or more drives to back up, and then click **Next**.

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

   If you do not see a drive that you expected to see, select **Show Hidden Drives**.
5. 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 62.
6. Select the recovery point type that you want the backup to create.

   See "Recovery point type options" on page 63.
7. Click **Next**.
8. On the Backup Destination panel, select the desired options.

   See "Backup destination options" on page 64.

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

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

See “About Offsite Copy” on page 81.

10 Click **Next**.

11 On the Options panel, set the recovery point options you want.

See “Recovery point options” on page 64.

12 (Optional) Click **Advanced**, set the advanced options you want, and then click **OK** to return to the Options panel.

See “Advanced options for drive-based backups” on page 70.

13 (Optional) If you want to run command files during the recovery point creation process, click **Command Files**, set the command file options, and then click **OK** to return to the Options panel.

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

See “About running command files during a backup” on page 68.

14 Click **Next**.

15 Do one of the following:

- If you chose a recovery point set as your recovery point type earlier in step 6 above, skip to the next step.
- If you chose an independent recovery point as your recovery point type, select one of the following options in the **Automatically create a recovery point**list, click **Next**, review the options you have selected, then click **Finish**.

No Schedule	Runs the backup only when you run it yourself, manually.
Weekly	Runs the backup at the time and on the days of the week that you specify. When you select this option, the Select the days of the week to protect box appears.
Monthly	Runs the backup at the time and on the days of the month that you specify. When you select this option, the Select the days of the month to protect box appears.

Only run once	Runs the backup one time on the date and at the time you specify. When you select this option, the Create a single recovery point box appears.

16 If you want the backup to run automatically according to a schedule, select Schedule, enter a start time, and select the days of the week when the backup should run.

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

17 (Optional) Click the **Custom** button and specify 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.

18 For advanced scheduling options, such as setting up event triggers that start the backup in response to specific events, click **Advanced** and configure the desired options.

See “Advanced scheduling options” on page 66.

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

20 (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.

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

Related Drives options

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 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 backup 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 backup an attached VHD that is nested within another attached VHD.

See “About backing up Microsoft virtual hard disks” on page 205.

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 Norton Ghost does not work with locked data drives. Instead, you must unlock the bitlocked drive before you can backup it up.

Generally, you should accept the preselected option **Add all related drives (recommended)**. Doing so can help you with a successful recovery, should you ever need to perform a restore in the future. If you deselect certain related drives you may experience an incomplete recovery or an unsuccessful recovery.

Recovery point type options

Recovery point set and Independent recovery point are the two recovery point type options that are available. Each option type is described in the table below.

Table 6-1 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.

Backup destination options

The following table describes the options on the Backup Destination Page.

Table 6-2 Backup destination options

Option	Description
Folder field	Indicates the location where you want to store the recovery points. If Norton Ghost detects that this location does not have enough available space, it alerts you. You should choose another location that has more space.
Edit	The Edit button only becomes active if you have selected a backup destination that is on a network. If the backup destination is on a network, you can click the Edit button to bring up a dialog where you can specify the necessary user name and password for network access. This also applies if you want to save the recovery point on a network share. See "About network credentials" on page 68.
Customize recovery point file names	Allows you to rename the recovery point. To rename a recovery point click **Rename** and then type a new file name. Default file names include the name of the computer followed by the drive letter.
Add	Allows you to add up to two Offsite Copy destinations. Offsite Copy automatically copies your latest recovery points each time a backup completes to either a portable storage device, such as an external drive, or to a remote server either through a local area network connection or to a remote FTP server. See "About Offsite Copy" on page 81.

Recovery point options

The following table describes the recovery point options on the Options page.

Table 6-3 Recovery point options

Options	Description
Name	Type 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 Recovery Disk.
Compression	Select one of the following compression levels for the recovery point.: ■ None ■ Standard ■ Medium ■ High See "Compression levels for drive-based backups" on page 74. The results can vary depending on the types of files that are saved in the drive.
Verify recovery point after creation	Select this option to automatically test whether a recovery point or set of files is valid or corrupt.
Limit the number of recovery point sets saved for this backup	Select this option to limit the number of recovery point sets that can be saved for this backup. You can limit the number of recovery point sets to reduce the risk of filling up the hard drive with recovery points. Each new recovery point set replaces the oldest set on your backup destination drive. This option only appears 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 Recovery Disk.

Table 6-3 Recovery point options *(continued)*

Options	Description
Enable search engine support	Select this option to let a search engine, such as Google Desktop, index all of the file names that are contained in each recovery point. By indexing the file names, you can then use your search engine to locate files you want to restore. This option is for NTFS file systems only. See "About using a search engine to search recovery points" on page 201. **Note:** This option does not appear if you create a recovery point using the **Back Up My Computer** feature in Symantec Recovery Disk.
Include system and temporary files	Select this option to include 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 Recovery Disk.
Advanced	See "Advanced options for drive-based backups" on page 70.
Command Files	See "About running command files during a backup" on page 68.
Description text box	Type a description for the recovery point. The description can be anything that helps you further identify the recovery point's contents.

Advanced scheduling options

The following table describes the advanced scheduling options.

Table 6-4 Advanced scheduling options

Option	Description
Schedule (Backup Time)	Do one or more of the following: ■ Click **Schedule**, and then select the days and a start time for when the backup should run. ■ Select **Run more than once per day** if you frequently edit data that you want to protect. Also, specify the maximum time that should occur between backups and the number of times per day that the backup should run. ■ Click the **Automatically optimize** list, and then select how often optimization should occur to help manage the disk space that is used by your backup destination. ■ Click the **Start a new recovery point set** list and select how frequently a new recovery point set should be started. Click **Custom** to customize the option you select.
Event Triggers (General) (ThreatCon Response)	Select the type of events that should automatically start the backup. See "Enabling event-triggered backups" on page 96.

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.

About network credentials

If you are connecting to a computer on a network, you are required to enter the user name and password for network access, even if you have previously authenticated to the network. This is because the Norton Ghost 15.0 service runs as the local System account.

When entering network credentials, the following rules apply:

- If the computer you want to connect to is on a domain, you would enter the domain name, user name, and password. For example: domain\username
- If you are connecting to a computer in a workgroup you would enter 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 at this dialog because the service runs in a different context and cannot recognize the mapped drive.

By going to the Tools menu and selecting Options, you can set a default location, including network credentials. Then when you create future jobs, the dialog will default to the location you specified. Another option would be to create a specific "backup" user account for the enterprise and configure the Norton Ghost 15.0 service to use this account.

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 Norton Ghost with other backup routines that you might be running on the computer. You can also use command files to integrate with other applications that use a drive on the computer.

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

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

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

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

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

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 Norton Ghost before you use them during a backup.

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

The following table describes the stages of recovery point creation.

Table 6-5 Recovery point creation stages

Stage	Description
Run before snapshot creation	This stage occurs after a backup has started and before a recovery point is created. You can run a command during this stage to prepare for the recovery point creation process. For example, you can close any open applications that are using the drive. **Note:** If you use this option, be sure the command file has an error recovery mechanism built into it. If the computer has one or more services that must be stopped at this stage (such as stopping a non-VSS aware database or a resource intensive application), and the command file does not contain any form of error recovery, one or more of the stopped services may not be restarted. An error in the command file can cause the recovery point creation process to stop immediately. No other command files will run. See "How you use Norton Ghost" on page 34.
Run after snapshot creation	This stage occurs after a snapshot is created. Running a command during this stage is typically a safe point for allowing services to resume normal activity on the drive while continuing the recovery point creation. Because the snapshot takes only a few seconds to create, the database is in the backup state momentarily. A minimal number of log files are created.
Run after recovery point creation	This stage occurs 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.

Advanced options for drive-based backups

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

Table 6-6 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. 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.
Disable SmartSector™ Copying	SmartSector technology speeds up the copying process bycopying 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. Lets you copy used and unused hard-disk sectors. This option increases process time and usually results in a larger recovery point.
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 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: ■ Low (8+ character password) ■ Medium (16+ character password) ■ High (32+ character password)

Editing advanced backup options

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

To edit advanced backup options

1. On the Home or Tasks page, click **Run or Manage Backups**.
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 70.
6. Click **Next** three times, and then click **Finish**.

About recovery point encryption

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

You can also encrypt recovery points that were created with earlier versions of Symantec LiveState Recovery or Norton Ghost. 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 6-7 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, Norton Ghost 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.

Verifying the integrity of a recovery point

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

- Norton Ghost 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 70.

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**.

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**.

Compression levels for drive-based backups

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

The following table describes the available compression levels.

Table 6-8 Compression levels

Compression level	Description
None	Use this option if storage space is not an issue. However, if the backup is being saved to a busy network drive, high compression may be faster than no compression because there is less data to write across the network.
Standard (recommended)	This option uses low compression for a 40 percent average data compression ratio on recovery points. This setting is the default.
Medium	This option uses medium compression for a 45 precent average data compression ratio on recovery points.

Table 6-8 Compression levels *(continued)*

Compression level	Description
High	This option uses high compression for a 50 percent average data compression ratio on recovery points. This setting is usually the slowest method. When a high compression recovery point is created, CPU usage might be higher than normal. Other processes on the computer might also be slower. To compensate, you can adjust the operation speed of Norton Ghost. This might improve the performance of other resource-intensive applications that you are running at the same time.

Running a one-time backup from Norton Ghost

You can use One Time Backup to quickly define and run a backup that creates an independent recovery point from Norton Ghost. 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 Recovery Disk to create one time cold backups.

See "About running a one-time backup from Symantec Recovery Disk" on page 76.

To run a one-time backup from Norton Ghost

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 62.
5. In the Backup Destinations panel, select the appropriate options.

   See "Backup destination options" on page 64.
6. Click **Next**.

7 On the Options panel, select the appropriate options.

See "Recovery point options" on page 64.

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 CommandFiles folder, you may need to click **Back**, and then **Next** to see the files in each stage's list.

See "About running command files during a backup" on page 68.

10 Click **Next**.

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

About running a one-time backup from Symantec Recovery Disk

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

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 anytime during the backup so you have a complete recovery point.

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

- A level of corruption prevents you from starting Windows on the computer.
- Norton Ghost 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 server or desktop is severely damaged, you can use the Symantec Recovery Disk CD to back up what remains of the system. Then, you can recover what you can later, after you restore an independent recovery point.

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

- You use the original, shipping version of the Symantec Recovery Disk CD to create a backup of a computer that does not have Norton Ghost installed.
- The computer that you intend to back up using the original, shipping version of the Symantec Recovery Disk has an unlicensed installation of Norton Ghost.
- You create a custom Symantec Recovery Disk CD on a computer that has an unlicensed installation (60-day trial) of Norton Ghost. You then use the custom Symantec Recovery Disk CD to create a backup of a computer that does not have an installation of Norton Ghost.

  See "Creating a custom Symantec Recovery Disk CD" on page 29.
- You choose not to add a license key at the time you create the customized Symantec Recovery Disk CD.

Running a one-time backup from Symantec Recovery Disk

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

To run a one-time backup from Symantec 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 Recovery Disk CD on the computer you want to back up.

   See "Starting a computer by using Symantec Recovery Disk" on page 174.
3. On the **Home** panel, click **Back Up My Computer**, and then click **Next**.
4. If prompted, enter a valid license key, and then click **Next**.
5. Select one or more drives that you want to back up, and then click **Next**.

6 In the **Backup Destination** panel, set the options you want, then click **Next**.

Folder field	Lets you browse to and specify the location where you want to store the independent recovery point.
Map a network drive	Lets you map 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.
Recovery point file names field	Lets you edit the recovery point file name. To do this, select a drive, click **Rename**, type a new file name, and then click **OK**.

7. In the **Options** panel, set the desired compression level for the recovery point.

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

8. If you want to verify whether the recovery point is valid after its creation, select **Verify recovery point after creation**.
9. In the **Description** text box, type a description that you want associated with the recovery point.
10. Click **Advanced**.
11. In the **Advanced options** panel, set the options you want, and then click **OK**.

Divide into smaller files to simplify archive	You can split the recovery point into smaller files and specify the maximum size (in MB) for each file. For example, if you plan to copy a recovery point to ZIP disks from your backup destination, specify a minimum file size of 100 MB, according to the size of each ZIP disk.
Disable SmartSector copying	SmartSector technology speeds up the copying process bycopying 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. Lets you copy used and unused hard-disk sectors. This option increases process time and usually results in a larger recovery point.
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 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: ■ Low (8+ character password) ■ Medium (16+ character password) ■ High (32+ character password)

12 Click **Next**.

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

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

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 copies your latest, complete recovery points to either a portable storage device, a remote server in your network, or to a remote FTP server.

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

See "How Offsite Copy works" on page 81.

See "About using external drives as your Offsite Copy destination" on page 82.

See "About using a network server as your Offsite Copy destination" on page 84.

See "About using an FTP server as your Offsite Copy destination" on page 85.

How Offsite Copy works

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

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

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 p.m. and configured an external drive as an Offsite Copy destination. However, when you leave the office at 5:30 p.m., you take the drive with you for safe keeping. When the backup job completes at 6:20 p.m., Norton Ghost 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. Norton Ghost detects the presence of the Offsite Copy destination drive and automatically begins copying your recovery points.

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

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

See “About using external drives as your Offsite Copy destination” on page 82.

See “About using a network server as your Offsite Copy destination” on page 84.

See “About using an FTP server as your Offsite Copy destination” on page 85.

See “To define a drive-based backup” on page 60.

See “Editing backup settings” on page 95.

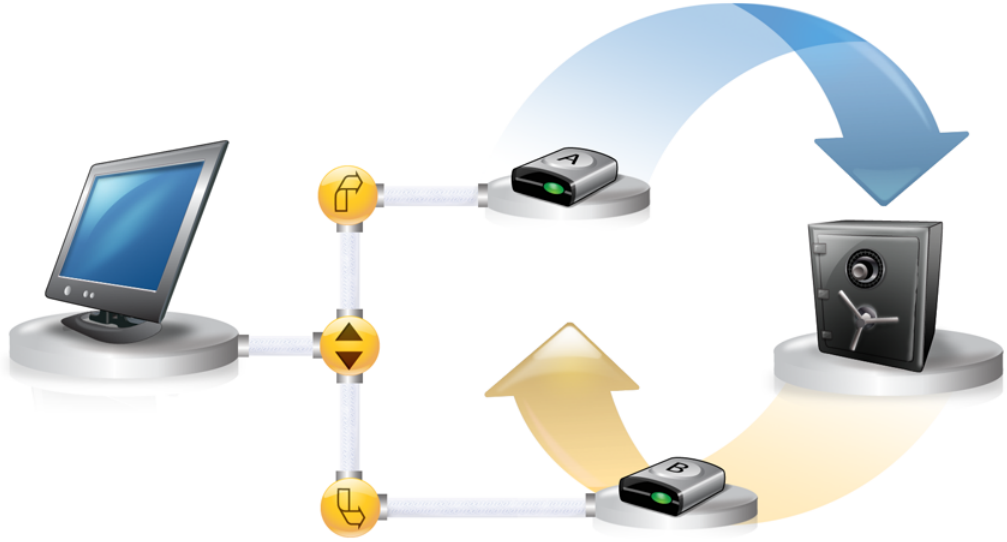
About using external drives as your Offsite Copy destination

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

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

See “About recovery point encryption ” on page 72.

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



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

On Wednesday morning, you bring drive B to the office. You plug in drive B and Norton Ghost detects that drive B is an Offsite Copy destination. Norton Ghost 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 nickname, to each drive. Then place matching physical labels on each external drive to help you manage the task of swapping the drives.

See “Using nicknames for external drives” on page 43.

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.

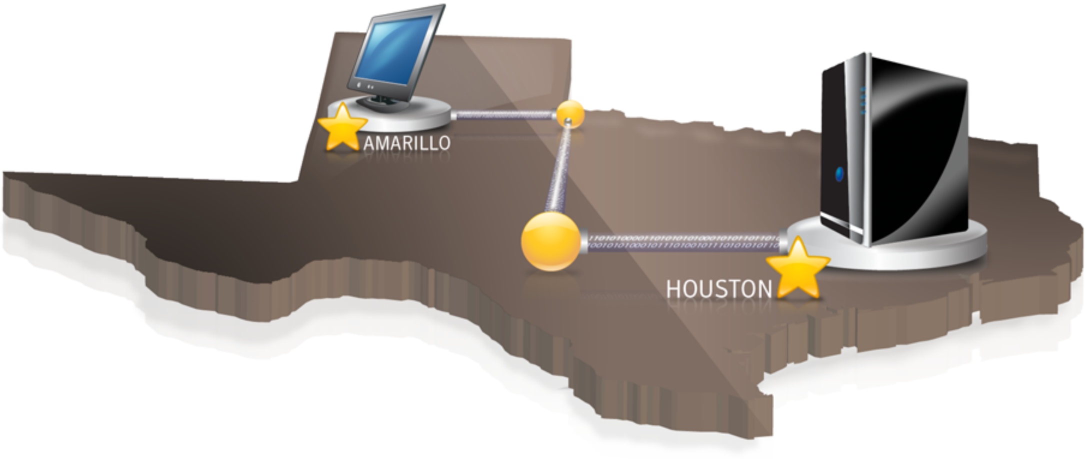
Using external drives as your Offsite Copy destination ensures that you have a copy of your backup data stored at two separate, physical locations.

About using a network server as your Offsite Copy destination

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

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

If the remote server becomes unavailable for a period of time, Offsite Copy copies all recovery points that were created since the last connection. If there is no room to hold all of the recovery points available, Offsite Copy removes the oldest recovery points from the network server. In turn, it makes room for the newest recovery points.



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 Norton Ghost in order for this method to work correctly. When Offsite Copy is configured correctly, it copies recovery points to the directory that you specified on the FTP server. If the server becomes unavailable for a period of time, Offsite Copy copies all recovery points that were created since the last connection. If there is no room to hold all of the recovery points available, Offsite Copy removes the oldest recovery points 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 44.

Backing up files and folders

This chapter includes the following topics:

Defining a file and folder backup

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

To define a file and folder backup

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

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

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

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

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

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

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

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

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

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

8 To add or edit advanced options, click **Advanced** and do any of the following:

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

See "About folders that are excluded by default from file and folder backups" on page 89.

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

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

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

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

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

See Table 6-4 on page 67.

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

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

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

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

About folders that are excluded by default from file and folder backups

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

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

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

See “Defining a file and folder backup” on page 87.

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

Chapter 8

Running and managing backup jobs

This chapter includes the following topics:

Running an existing backup job immediately

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

You can run an existing backup at any time.

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

See "Running a one-time backup from Norton Ghost" on page 75.

Norton Ghost can be configured to run a backup automatically when an event occurs on your computer, such as installing a new software program.

See "Enabling event-triggered backups" on page 96.

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

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

See "Editing a backup schedule" on page 97.

To run an existing backup immediately from the system tray

1. On the Windows desktop, right-click the Norton Ghost 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 Norton Ghost and define a backup.

To run an existing backup immediately from within Norton Ghost

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

Running a backup with options

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

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

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

See "Editing a backup schedule" on page 97.

See "Editing backup settings" on page 95.

To run a backup with options

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

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

   See "Backup options" on page 93.
5. Click **OK** to run the backup job and create the recovery point type you selected.

Backup options

Incremental recovery point of recent changes, New recovery point set, and Independent recovery point are the three options that are available. Each option type is described in the table below.

Table 8-1 Backup options

Options	Description
Incremental recovery point of recent changes	Select this option if the backup already has a base recovery point created and you want to simply capture changes made to the drive since the last backup.
New recovery point set	Select this option if you want to start a completely new recovery point set. When you select this option, a base recovery point is created.

Table 8-1 Backup options *(continued)*

Options	Description
Independent recovery point	Select this option to create an independent recovery point, which is a complete snap shot of your entire drive. To specify an alternate backup location, click **Browse**.

Adjusting the speed of a backup

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

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

To adjust the 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 as quickly as possible and you are not doing extensive work on your computer, drag the slider toward **Fast**.
3. When you are finished, click **Hide** to dismiss the Progress and Performance dialog box.

Stopping a task

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

To stop the current task

◆ Do one of the following:
   - On the Tools menu, click **Cancel the Current Operation**.
   - On the Tools menu, click **Progress and Performance**, and then click **Cancel Operation**.

- On the Windows system tray, right-click the Norton Ghost tray icon, and then click **Cancel the Current Operation**.

Verifying that a backup is successful

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

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

See "Monitoring backup protection from the Status page" on page 118.

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

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

See "Verifying the integrity of a recovery point" on page 73.

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.

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

   See "Defining a drive-based backup" on page 60.

   See "Defining a file and folder backup" on page 87.

Enabling event-triggered backups

Norton Ghost can detect certain events and run a backup when they occur.

For example, to protect your computer when you install new software, Norton Ghost can run a backup 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 Norton Ghost to automatically run a backup when the following events occur:

- Any application is installed.
- A specified application is started.
- Any user logs on to Windows.
- Any user logs off of Windows.
- The data that was added to a drive exceeds a specified number of megabytes. This option is unavailable for file and folder backups.

To enable event-triggered backups

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

About Symantec ThreatCon

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 Symantec ThreatCon trigger for a selected backup job, Norton Ghost 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 Symantec ThreatCon is started automatically. You then have a recovery point to use to recover your data should your computer become affected by the latest threat.

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

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

Editing a backup schedule

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

To edit a backup schedule

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

Turning off a backup job

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

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

See "Deleting backup jobs" on page 97.

To turn off a backup job

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

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

Deleting backup jobs

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

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

See "Managing recovery point storage" on page 137.

To delete backup jobs

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

Adding users who can back up your computer

You can use the Security Configuration Tool to control which users on your computer can access and configure key features of Norton Ghost.

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

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

   On Windows Vista, click **Start > All Programs > Symantec > Security Configuration Tool**.
2. Click **Add**.
3. In the Enter the object names to select box, type the names of the users or groups you want to add.
4. Click **OK**.
5. To delete users or groups, select a user or group, and then click **Remove**.
6. Click **OK** to apply your changes and close the Security Configuration Tool.

To configure access rights for users or groups

1 On the Windows taskbar, click **Start > Programs > Symantec Norton Ghost > Security Configuration Tool**

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

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

3 Choose from the following options:

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

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

Chapter 9

Backing up remote computers from your computer

This chapter includes the following topics:

About backing up other computers from your computer

Norton Ghost lets you connect to, and back up a second computer 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 Norton Ghost 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. When you do, the Norton Ghost product interface changes to reflect the status of the remote computer. At any time, you can switch back to manage your local computer.

Adding computers to the Computer List

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

To add computers to the Computer List

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

To add a local computer

1. On the Norton Ghost menu bar, click **Computers** > **Add Local Computer**.
2. Click **OK**.

To remove a computer from the Computer List

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

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

Deploying the Norton Ghost Agent

You can deploy the Norton Ghost 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 Norton Ghost.

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

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

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

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

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

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

1. On the Windows taskbar, right-click **Start**, and then click **Explore**.
2. On the **Tools** menu, click **Folder Options > View**.

3 On the **View** tab, scroll to the end of the list and verify that the **Use simple file sharing** check box is not selected, and then click **OK**.

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

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 will automatically restart at the end of the installation wizard.

To deploy the Norton Ghost Agent

1 On the Norton Ghost menu bar, click **Computers** > select a computer from the menu.

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

2 Click **Deploy Agent**.

3 In the Deploy Norton Ghost Agent dialog box, specify the administrator user name (or a user name that has administrator rights) and the password.

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

For example, type *RemoteComputerName\UserName*

4 If you want to restart the computer when the agent installation is finished, click **Reboot when finished**.

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

5 Click **OK**.

To manually install the Norton Ghost Agent

1 Insert the Norton Ghost product CD into the media drive of the computer.

The installation program should start automatically.

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

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

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

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

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

3 In the CD browser panel, click **Install Norton Ghost**.

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

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

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

7 Click **Next**.

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

9 Click Norton GhostService, and then click **This feature will be installed on local hard drive**.

This feature is the agent.

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

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

Using the Norton Ghost Agent

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

See “About managing the Norton Ghost Agent through Windows Services” on page 106.

See “Controlling access to Norton Ghost ” on page 111.

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

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

To use the Norton Ghost Agent

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

  - Right-click the Norton Ghost tray icon, and then click **Reconnect** to restart the service automatically.
    You cannot run a backup until the service is running.
  - If Norton Ghost is installed on the computer, double-click the Norton Ghost 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 Norton Ghost installed, right-click the Norton Ghost tray icon to display a menu of common Norton Ghost Agent tasks.

About managing the Norton Ghost Agent through Windows Services

The Norton Ghost Agent is a Windows service that runs in the background.

It provides the following:

- Locally running scheduled backup jobs, even when there are no users, or an unprivileged user, logged on to the computer
- Allows administrators to remotely back up computers throughout an enterprise from Norton Ghost running on another computer.

See “Using the Norton Ghost Agent ” on page 105.

To use the features of Norton Ghost, the Norton Ghost Agent must be started and properly configured. You can use the Windows Services tool to manage and troubleshoot the agent.

Note: To manage the Norton Ghost Agent, you must be logged on as a local administrator.

You can manage the Norton Ghost Agent in the following ways:

- Start, stop, or disable the Norton Ghost Agent on local and remote computers.
  See “Starting or stopping the Norton Ghost Agent service” on page 108.
- Configure the user name and password that is used by the Norton Ghost Agent.
  See “Controlling access to Norton Ghost ” on page 111.

- Set up recovery actions to take place if the Norton Ghost Agent fails to start.
  For example, you can restart the Norton Ghost Agent automatically or restart the computer.
  See "Setting up recovery actions when the Norton Ghost Agent does not start" on page 109.

About 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 Norton Ghost Agent. You should view the most recent log entries in the Events tab for more information about the potential causes of the problem.
Verify that the Norton Ghost Agent starts without user intervention.	The Norton Ghost Agent is configured to start automatically when Norton Ghost starts. You can view the status information to verify that the Norton Ghost 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 Norton Ghost Agent is starting automatically by looking in Services. You can check the status and restart the service if necessary. If the Startup type is set to automatic, you should restart the agent. See "Starting or stopping the Norton Ghost Agent service" on page 108.
Use caution when changing default settings for the Norton Ghost Agent.	Changing the default Norton Ghost Agent properties can prevent Norton Ghost from running correctly. You should use caution when changing the default Startup type and Log On settings of the Norton Ghost Agent. It is configured to start and log on automatically when you start Norton Ghost .

Opening Windows Services

There are several methods you can use to open Windows Services to manage the Norton Ghost Agent.

To open 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 Norton Ghost (the name of the agent).

   Its status should be **Started**.

   See "Starting or stopping the Norton Ghost Agent service" on page 108.

Starting or stopping the Norton Ghost Agent service

To start, stop, or restart the Norton Ghost 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 Norton Ghost Agent service for the following reasons:

Start or Restart	You should start or restart the agent if Norton Ghost is unable to connect to the Norton Ghost Agent on a computer, or you cannot reconnect from Norton Ghost.
Restart	You should restart the agent after you change the user name or password that you use to log on to the Norton Ghost Agent service, or you used the Security Configuration Tool to give additional users the ability to back up computers. See "Controlling access to Norton Ghost " on page 111.
Stop	You can stop the agent if you believe it is causing a problem on the computer, or you want to temporarily free memory resources. If you stop the agent, you also prevent all of your drive-based backups and file and folder backups from running.

If you stop the Norton Ghost Agent service and then start Norton Ghost, the agent restarts automatically. The Status changes to Ready.

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

To start or stop the Norton Ghost 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 **Norton Ghost**.
5. On the **Action** menu, select one of the following:
   - Start
   - Stop
   - Restart

Setting up recovery actions when the Norton Ghost Agent does not start

You can specify the computer’s response if the Norton Ghost Agent fails to start.

To set up recovery actions when the Norton Ghost 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 Norton Ghost Agent must run successfully before the fail count is reset to zero.

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

7 Click **OK**.

Viewing Norton Ghost Agent dependencies

The Norton Ghost 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 Norton Ghost Agent fails to start, check the dependencies to ensure that they are installed and that their Startup type is not set to Disabled.

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

The top list box on the Dependencies tab displays services that are required by the Norton Ghost Agent to run properly. The bottom list box does not have any services that need the Norton Ghost Agent to run properly.

The following table lists the services that are required by the Norton Ghost Agent to run properly, along with their default startup setting.

Table 9-2 Required services

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

To view Norton Ghost Agent dependencies

1 In the **Services** window, under **Name**, click **Norton Ghost**.

See "Opening Windows Services " on page 108.

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

3 Click the **Dependencies** tab.

Controlling access to Norton Ghost

You can use the Security Configuration Tool to allow or deny users and groups the necessary permissions to access the Norton Ghost Agent , or to the full Norton Ghost user interface.

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

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

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

Table 9-3 Permission options

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

Table 9-3 Permission options *(continued)*

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

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

To add users and groups

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

To change permissions for a user or a group

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

To remove a user or group

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

Running Norton Ghost using different user rights

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

To perform Run As from Windows

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

- On the Windows taskbar, click **Start > Program Files > Norton Ghost**.
  Right-click **Norton Ghost**, and then click **Run As**.
  In the **Run As** dialog box, click **The following user** to log onto with another account.
  In the User Name and Password boxes, type the account name and password that you want to use, and then click **OK**.
- On the Windows taskbar, click **Start > All Programs > Norton Ghost > Norton Ghost**.
  Click **Yes** when prompted to add the required privileges.
  Enter the password for an administrator account, and then click **OK**.

Chapter 10

Monitoring the status of your backups

This chapter includes the following topics:

About monitoring backups

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

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

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

Rescanning a computer’s hard disk

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

When you use Refresh, Norton Ghost scans all attached hard disks for any configuration changes. It also updates information on removable media, media drives, basic drives, file systems, and hard drive letters.

To rescan a computer’s hard disks

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

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

Monitoring backup protection from the Home page

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

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 being calculated, or you have not yet licensed your product. Either wait a few seconds for the status to display, or make sure that you have licensed your copy of the product.
🚫	No backup protection assigned	The drive that displays this icon is not monitored for backup status; or, it is monitored for errors only. However, there are no errors to report. Use the Customize status reporting feature on the Status page to change the status report setting.

Monitoring backup protection from the Status page

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

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

Refer to the following table for the meaning of each icon 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 the backup ran and that an independent recovery point was created. 🛢 Indicates that the backup is unavailable. 🛢✗ Indicates that the backup did not run as scheduled. This problem could occur if an error prevents the backup from running or if you manually cancel a backup before it completes. 🛢 Indicates a drive-based backup 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 the backup ran and that an incremental recovery point was created. Indicates that the backup is unavailable. ✗ Indicates that the backup did not run as scheduled. This problem could occur if an error prevents the backup from running or if you manually cancel a backup before it completes. Indicates that the backup is scheduled to run at a future time.

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

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

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

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

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

- Use the scroll bar at the bottom of the calendar to scroll backward or forward in time.

About SNMP traps

You must install and configure the Windows SNMP service on your computer in order for SNMP traps to work from Norton Ghost.

By default, Norton Ghost is not enabled to send traps to NMS managers. You can configure Norton Ghost 15.0 to send SNMP traps for different priority and notification types.

To configure Norton Ghost to send SNMP traps

1. From the Tools menu, click **Options**, and then click the Notifications tab.
2. Under Notifications are sent to the following, click **SNMP trap**, and then click **Properties**.
3. In the SNMP Trap Notification Properties dialog, you can select the priority and type of notifications that you want for generating the traps. You can also select the version of SNMP traps to be sent (V1 or V2). Make your selections, and then click **OK**.

   Norton Ghost 15.0 will now send SNMP traps to all of the destinations set in the Windows SNMP agent.

About the Norton Ghost management information base

The Norton Ghost management information base (MIB) is an enterprise MIB, and contains the Norton Ghost 15.0 SNMP trap definitions. All NMS applications have options to load a MIB, and the Norton Ghost 15.0 MIB can be loaded using any of those options. Even without loading the MIB, the NMS applications will still receive and display the traps, but they will not be displayed in informative text. The .MIB file, named BESR_MIB.MIB, is located in the Support folder on the Norton Ghost product CD.

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

You can configure how Norton Ghost reports the status of a particular drive (or all file and folder backups).

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

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

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

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

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

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

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

2 Click **Customize status reporting**.

3 Select one of the following options:

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

4 Click **OK**.

Viewing drive details

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

You can view the following drive details:

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

To view drive details

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

   If the Advanced page is not visible on the Primary Navigation Bar, click **View > Show Advanced Page**.

2. In the Drive column, select a drive.
3. Review the Details section below the Drives table.

Improving the protection level of a drive

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

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

See “Best practices for backing up” on page 50.

To improve the protection level of a drive

1 On the Status page, select a drive that requires attention from the Drives column.

2 In the Status section at the bottom of the page, right-click the backup you want to 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, 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 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, 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 file and folder backup data).

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. By selecting a drive that is assigned to an existing backup, you have access to this short-cut method for starting the Define Backup Wizard from the Status page.

Manage Backup Destination

Opens the Manage Backup Destination dialog, 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 window, where you can specify if you want status reporting, and the type of status reporting.

See “Editing backup settings” on page 95.

About using event log information to troubleshoot problems

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

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

See “Logging Norton Ghost messages” on page 44.

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

The following information is included in the event log:

Type	Indicates if the event is an error message or other information, such as the successful completion of a backup job.
Source	Identifies if the message was generated by Norton Ghost or another program.
Date	Displays the exact date and time that a selected event occurred.
Description	Offers additional details about an event that can help you troubleshoot problems that might have occurred.

Chapter 11

Exploring the contents of a recovery point

This chapter includes the following topics:

About exploring recovery points

You can use Norton Ghost to explore files in a recovery point by assigning it a drive letter that is visible from Windows Explorer.

You can perform the following tasks on the assigned drive:

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

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

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

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

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

You do not need to mount a drive to restore the files or folders 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 being created, edited, or deleted at the time.

See “Exploring a recovery point through Windows Explorer” on page 130.

See “Dismounting a recovery point drive” on page 133.

See “Viewing the drive properties of a recovery point” on page 133.

Exploring a recovery point through Windows Explorer

When you explore a recovery point, Norton Ghost mounts the recovery point as a drive letter and opens it in Windows Explorer.

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

To explore a recovery point through Windows Explorer

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

Mounting a recovery point from Windows Explorer

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

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

To mount a recovery point from Windows Explorer

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

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

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 either by saving them using the application associated with them, or by using the Recover Files button in the Recovery Point Browser.

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

Note: You cannot view 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 unavailable if you select a program file that has a .exe, .dll, or .com file extension.

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, select a drive in the tree panel (on the left).

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

5 Do one of the following:

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

About using a search engine

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

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

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

See “To define a drive-based backup” on page 60.

See “About using a search engine to search recovery points” on page 201.

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 in Windows Explorer

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

To dismount a recovery point drive in Recovery Point Browser

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

Viewing the drive properties of a recovery point

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

Description	A user-assigned comment that is associated with the recovery point.
Original drive letter	The original drive letter that was assigned to the drive.
Cluster size	The cluster size (in bytes) of the FAT, FAT32, or NTFS drive.
File system	The file system type used within the drive. For example, FAT, FAT32, or NTFS.
Primary/Logical	The selected drive's status as either a primary partition or a logical partition.
Size	The total size (in 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 there are any bad sectors on the drive.
Cleanly quiesced	Indicates whether the database application quiesced properly when a recovery point was created.

To view the drive properties of a recovery point

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

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.

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

About how backup data works

Norton Ghost offers two backup methods:

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

About drive-based backups

When you run a drive-based backup, a snapshot 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 that is used to restore your computer back to the way it was when the recovery point was created.

The types of recovery points are as follows:

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

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

About file and folder backups

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

File and folder backups let you select individual files or folders to back up. You can also specify a file type to back up and let Norton Ghost locate and back up all files of the type you specified. For example, if you have Microsoft Word documents stored at several locations on your computer, Norton Ghost 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 types unique to the software you use.

Norton Ghost also keeps multiple versions of the same files for you, so that 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.

Managing recovery point storage

Norton Ghost includes several features that help you manage your backup data. The key is to prevent backup data from taking lots of hard disk space on your computer. And, to also provide adequate backup protection in the event that you need to recover your computer, files, or folders.

See "Defining a virtual conversion job" on page 147.

See "Running a one-time virtual conversion" on page 141.

To manage recovery point storage manually

1. On the Tools page, click **Manage Backup Destination**.
2. From the Manage Backup Destination window, you can do any of the following tasks:
   - Clean Up
     See "Cleaning up old recovery points" on page 138.
   - Move
     See "Moving your backup destination" on page 157.
   - Settings
     See "Automating management of backup data" on page 156.
   - Delete
     See "Deleting a recovery point set" on page 138.
     See "Deleting recovery points within a set" on page 139.
   - Copy
     See "Making copies of recovery points" on page 139.
   - Explore
     See "About exploring recovery points" on page 129.

Cleaning up old recovery points

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

See "Automating management of backup data" on page 156.

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

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

See "Opening and restoring files within a recovery point" on page 131.

See "About exploring recovery points" on page 129.

To clean up old recovery points

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

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

Deleting a recovery point set

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

Note: 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 Tools page, click **Manage Backup Destination**.
2. Select the recovery point set that you want to delete, and then click **Delete**.

3 Click **Yes** to confirm the deletion.

4 Click **OK**.

Deleting recovery points within a set

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

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

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

See "Opening and restoring files within a recovery point" on page 131.

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

To delete recovery points within a set

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

2 Select the recovery point set that you want to delete, and then click **Delete**.

3 Do one of the following:

- To automatically delete all but the first and last recovery point in the set, click **Automatic**.
- To manually select which recovery points in the set to delete, click **Manual**, and then select the recovery points you want to delete.
- To delete all the recovery points in the set you selected, click **Delete all recovery points in the set**.

4 Click **OK**.

Making copies of recovery points

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

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

To make copies of recovery points

1. On the Tools page, click **Manage Backup Destination**.
2. Select a recovery point set or an independent recovery point, and then click **Copy**.
3. Select which recovery point to copy, and then click **OK**.
4. On the Welcome page of the Copy Recovery Point Wizard, click **Next**.
5. Select the recovery point that you want to copy.

   Recovery point sets appear as single recovery points. Select **View all recovery points** to display all incremental recovery points that are included within the recovery point sets.
6. Click **Next**.
7. Do one of the following:
   - In the **Folder** box, type the path to which you want to copy the recovery point.
   - Click **Browse** to locate the folder to which you want to copy the recovery point, and then click **OK**.
8. Select a level of compression for the copies of the recovery points.

   See "Compression levels for drive-based backups" on page 74.
9. If you want to verify whether a recovery point is valid after the copy is complete, select **Verify recovery point after creation**.
10. Click **Advanced**, and then select from the following options.

Divide into smaller files to simplify archiving	You can split the recovery point into smaller files and specify the maximum size (in MB) for each file. For example, if you plan to copy a recovery point to ZIP disks from your backup destination, specify a file size of 100 MB or less, according to the size of each ZIP disk.

Use password

This option sets a password on the recovery point. Passwords can include standard characters, not extended characters, or symbols. (Use characters with an ASCII value of 128 or lower.)

A user must type this password before they can restore a backup or view the contents of the recovery point.

Use AES encryption

You can encrypt your recovery point data to add another level of protection to your recovery points.

You can choose from the following encryption levels:

- Low (8+ character password)
- Medium (16+ character password)
- High (32+ character password).

11 Click **OK**.

12 Click **Next**, 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 138.

Running a one-time virtual conversion

You can use Norton Ghost to convert recovery points of a physical computer to VMware Virtual Disk, 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, and 6
- VMware ESX Server 3.0, 3.5, 3.5i, 4.0, and 4.0i
- 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 147.

To run a one-time recovery point conversion to virtual disk

1. On the Tasks page, 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 one of the following alternative recovery point sources:

Date

Displays all of the discovered recovery points in the order in which they were created.

- If no recovery points are discovered, the table is empty. In such cases, you can select an alternate date by using the drop-down calendar.
- Select a recovery point from the list.

File name

Lets you browse to another recovery point location. For example, you can browse an external (USB) drive, network location, or removable media to select a recovery point (.v2i) or incremental recovery point (.iv2i) file.

Select this option, and then do the following:

- Click **Browse**, locate and select a recovery point, and then click **Open**.
- If you selected a recovery point that is stored on a network, type your network credentials.
  See "About network credentials" on page 68.

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.

Or, you can select an alternate system index file (.sv2i) that resides elsewhere, such as a network location. 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.

Select this option, and then do one of the following:

- Click **Use latest recovery points for this computer**.

  The list of drives, source files (.v2i and .iv2i files), and dates comes from the most current system index file (.sv2i) that is located in the recovery point storage location on your computer.
- Click **Use alternate system index (*.sv2i) file** .

  Click **Browse**, locate and select an alternate system index file (.sv2i), and then click **Open**.

  If you selected a system index file that is stored on a network, type your network credentials.

  See “About network credentials” on page 68.

  Select the recovery points that you want to convert in the list box.

4 Click **Next**.

5 Do one of the following based on the virtual disk format and version (if applicable) that you selected:

If you selected VMware Virtual Disk or Microsoft Virtual Disk as the conversion format.	■ Folder for virtual disks Type the path to the folder where you want to place the virtual disk files. ■ Browse Click **Browse** to locate the folder in which you want to place the virtual disk files. ■ Network Credentials If you selected a virtual disk folder location on a network, type your network credentials. ■ Create one virtual disk per volume Select this option to 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. This option is not available if the volumes are on separate disks. ■ Rename To edit the name of the resulting virtual disk file, select the file name in the list near the bottom of the pane. Click **Rename**, and then type the new file name.

If you selected VMware ESX Server as the conversion format.	■ ESX server name or IP address Type the name of the server or the server's IP address. ■ ESX Server Credentials In the ESX Server Credentials group box, type a valid administrator user name that has sufficient rights. Type a valid password. ■ Destination for the virtual disks Type the path to the folder where you want to place the virtual disk files. ■ Rename To edit the name of the resulting virtual disk file, select the file name in the list near the bottom of the pane. Click **Rename**, and then type the new file name. Click **Next**. ■ Temporary location for conversion Type the name of the server or the server's IP address that you can use as a temporary location for files. ■ Temporary Location Credentials If you selected a temporary location for files on a network, type a valid administrator user name that has sufficient rights. Type a valid password.

6 Click **Next**.

7 Select one or more of the following options:

Run Windows Mini-Setup

Select this option (default) to run 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, by way of the wizard, 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, including accepting the End–User License Agreement, entering the Product Key, user name, and company name are automatically applied 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 ensures that the computer is recovered to its original state prior to recovery.

For more detailed information about Mini-Setup. you can perform a search for "Mini-Setup" on the Microsoft Help and Support Web site.

Split virtual disk into 2 GB (.vmdk) files	Select this option if you want to 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 (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.

8 Click **Next**.

9 Review the summary of the choices you made.

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

10 Click **Finish**.

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, and 6
- VMware ESX 3.0, 3.5, and 4.0
- VMware ESXi 3.5 and 4.0
- 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

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 virtual conversion" on page 141.

See "Viewing the properties of a virtual conversion job" on page 153.

See "Viewing the progress of a virtual conversion job" on page 153.

See "Editing a virtual conversion job" on page 153.

See "Running an existing virtual conversion job immediately" on page 153.

See "Deleting a virtual conversion job" on page 154.

To define a virtual conversion job

1. On the Tasks page, click **Run or Manage Virtual Conversions**.
2. On the toolbar, click **Define New**.
3. Click the virtual disk type (and version, if applicable) that you want to create, and then click **Next**.
4. Do one of the following:
   - Click **Use latest recovery points for this computer**.
     The list of drives, source files (.v2i and .iv2i files), and dates comes from the most current system index file (.sv2i) that is located in the recovery point storage location on your computer.
   - Click **Use alternate system index (*.sv2i) file** .
     Click **Browse**, locate and select an alternate system index file (.sv2i), and then click **Open**.
     If you selected a system index file that is stored on a network, type your network credentials.
     See "About network credentials" on page 68.
     Select the recovery points that you want to convert in the list box.
5. Click **Next**.
6. Do one of the following based on the virtual disk format and version (if applicable) that you selected:

If you selected VMware Virtual Disk or Microsoft Virtual Disk as the conversion format.	■ Folder for virtual disks Type the path to the folder where you want to place the virtual disk files. ■ Browse Click **Browse** to locate the folder in which you want to place the virtual disk files. ■ Network Credentials If you selected a virtual disk folder location on a network, type your network credentials. ■ Rename To edit the name of the resulting virtual disk file, select the file name in the list near the bottom of the pane. Click **Rename**, and then type the new file name.

If you selected VMware ESX Server as the conversion format.	■ ESX server name or IP address Type the name of the server or the server's IP address. ■ ESX Server Credentials In the ESX Server Credentials group box, type a valid administrator user name that has sufficient rights. Type a valid password. ■ Destination for the virtual disks Type the path to the folder where you want to place the virtual disk files. ■ Rename To edit the name of the resulting virtual disk file, select the file name in the list near the bottom of the pane. Click **Rename**, and then type the new file name. Click **Next**. ■ Temporary location for conversion Type the name of the server or the server's IP address that you can use as a temporary location for files. ■ Temporary Location Credentials If you selected a temporary location for files on a network, type a valid administrator user name that has sufficient rights. Type a valid password.

7 Click **Next**.

8 Type a name for the conversion job. Or, you can use the default name.

9 Select one or more of the following options.

Run Windows Mini-Setup

Select this option (default) to run 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, by way of the wizard, 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, including accepting the End–User License Agreement, entering the Product Key, user name, and company name are automatically applied 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 ensures that the computer is recovered to its original state prior to recovery.

For more detailed information about Mini-Setup. you can perform a search for "Mini-Setup" on the Microsoft Help and Support Web site.

Split virtual disk into multiple 2 GB (.vmdk) files

Select this option if you want to 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 (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.

10 Click **Next**.

11 In the Conversion Time panel, select one of the following, and then click **Next**:

No Schedule

Select this option to run the conversion only when you run it yourself, manually.

Weekly

Select this option to run the conversion at the specified start time and on the days of the week that you select.

- **Run more than once per day**
  Select this option if you want to convert recovery points multiple times throughout a day, and then specify the following options:
  - **Time between conversions**
    Select the amount of time to elapse before the next conversion.
  - **Number of times**
    Specify the number of times that you want the conversion to occur, beginning from the specified start time.

Monthly

Select this option to run the conversion at the time and on the days of the month that you specify.

Only run once

Select this option to run the conversion one time on the date and at the time that you specify.

12 If you want to run the new conversion job immediately, click **Run conversion now**.

13 Click **Finish**.

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 page, 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**.

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 page, 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**.

Viewing the progress of a virtual conversion job

You can view the progress of a virtual conversion 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 page, click **Run or Manage Virtual Conversions**, and then on the View menu, click **Progress and Performance**.

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 page, 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**.

Deleting a virtual conversion job

You can delete conversion jobs you no longer need or use.

When you delete a 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 page, 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.

About managing file and folder backup data

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

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

Viewing how much file and folder backup data is stored

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

To view how much file and folder backup data is stored

1. On the Tools page, 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.

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 required, especially if the files are large, as is often the case with audio and video files.

To limit the number of file versions to keep

1. On the Tools page, click **Manage Backup Destination**.
2. Click **Settings**.
3. 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**, and then specify a limit to the total amount of disk space that can be used for both recovery points and file and folder backup data.

   See "Automating management of backup data" on page 156.
5. Click **OK**.

Manually deleting files from your file and folder backup

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

To manually delete files from your file and folder backup

1. On the Home or Tasks page, click **Recover My Files**.
2. Do one of the following:
   - In the Find files to recover box, type the file name of the file that you want to delete, and then click **Search**.

- If you don't know the name of the file, click **Search** to return a list of all of the files that have been backed up, and then browse for the file.

3 Click **View All Versions** to display all versions of each file that exist in the file and folder backup data.

4 Select one or more files that you want to delete.

5 Right-click, and then click **Delete**.

Finding versions of a file or folder

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

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

See "Limiting the number of file versions to keep" on page 155.

To find versions of a file or folder

1 Open Windows Explorer.

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

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

Automating management of backup data

Norton Ghost 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 that exceed the threshold. If you do not specify a threshold, Norton Ghost notifies you when the disk reaches 90 percent of its total capacity.

To automate management of backup data

1 On the Tools page, 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**, and then drag the slider to limit the total amount of disk space that can be used for your recovery points and your file and folder backup data.

4 Do one of the following:

- 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 Norton Ghost to manage the backup data automatically, without prompting you.
  If you select this option, Norton Ghost 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**.

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

To move your backup destination

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

2 In the Manage Backup Destination window, in the Drives 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 file and folder backup data is found at the original backup destination.

10. Click **OK**.

Chapter 13

Recovering files, folders, or entire drives

This chapter includes the following topics:

About recovering lost data

Norton Ghost can restore lost files, folders, or entire drives by using recovery points or file and folder backup data.

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

Recovering files and folders by using file and folder backup data

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

Norton Ghost includes a search tool to help you locate the files that you want to recover.

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

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

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

5. Click **Recover Files**.
6. In the Recover My Files dialog box, do one of the following:
   - Click **Original folders** to restore your files to the same folder where they existed when they were backed up.
     If you want to replace the original files, 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 (or the files of the same names that are currently stored at that location) with the files that you are restoring.

- Click **Recovered Files folder on the desktop** to restore your files to a Recovered Files folder on your Windows desktop.

  Norton Ghost creates this folder during the restore.
- Click **Alternate folder** and type the path to the location in which you want to restore your files.

7 Click **Recover**.

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

9 Click **OK**.

Recovering files and folders using a recovery point

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

To recover files and folders using a recovery point

1 On the Home or Tasks page, click **Recover My Files**

2 In the left pane of the Recover My Files window, select **Recovery Point** as the search method.

3 If you want to use a different recovery point than the one selected for you in the Recovery Point box, click **Change**.

Note: If Norton Ghost cannot locate any recovery points, the Select Recovery Point dialog box opens automatically.

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

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

Filename

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

Select this option, and then do the following:

- Click **Browse**, locate and select a recovery point (.v2i file), and then click **Open**.
- If you select a network location, type your network credentials.
  See “About network credentials” on page 68.
- Click **Finish**.

System

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

Select this option, and then do the following:

- Click **Browse**, locate and select a recovery point (.sv2i), and then click **Open**.
- If you select a network location, type your network credentials.
  See “About network credentials” on page 68.
- Select each recovery point that you want to recover.
  If necessary, add, change, or remove recovery points from the list.
- Click **Finish**.

4 In the Find files to recover box, type the whole name or partial name of a file or folder that you want to restore, and then click **Search**.

For example, type **recipe** to return any file or folder that includes the word recipe in its name such as Chocolate Cheesecake Recipes.doc, Cathy Read Recipes.xls, Recipes for Success.mp3, and so forth.

5 In the Files to restore list, select the files that you want to restore by using one of the following methods:

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

6 Click **Recover Files**.

7 In the Recover My Files dialog box, do one of the following:

- Click **Original folders** to have your files restored in the original folder where they existed when they were backed up.
  If you want to replace the original files, select **Overwrite existing files**. If you do not select this option, a number is added to the filename, leaving the original file untouched.

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

- Click **Recovered Files folder on the desktop** to have your files restored to a new folder that is created on your Windows desktop called Recovered Files.
- Click **Alternate folder** and specify the path to an alternate location where you want your files restored.

8 Click **Recover**.

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

10 Click **OK**.

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 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 131.

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 Norton Ghost 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 129.

Recovering a secondary drive

If you lose data on a secondary drive, you can use an existing recovery point for that drive to restore the data. A secondary drive is a drive other than the drive on which your operating system is installed.

Note: You can recover your system drive (typically, drive C).

For example, if your computer has a D drive and the data has been lost, you can restore the D drive back to an earlier date and time.

See “About recovering a computer” on page 173.

To recover a drive, you must have a recovery point that includes the drive that you want to recover. If you are not sure, review the Status page to determine what recovery points are available.

See “Monitoring backup protection from the Status page” on page 118.

Note: Before you proceed, close any applications and files that are open on the drive that you want to restore.

Warning: When you recover a drive, all of the data on the drive to which you are restoring the recovery point is replaced by the data in the recovery point. Any changes that you made to the data on a drive after the date of the recovery point you use to recover it are lost. For example, if you created a new file on the drive after you created the recovery point, the new file is not recovered.

To recover a drive

1. On the Tasks page, click **Recover My Computer**.
2. Select a recovery point, and then click **Recover Now**.
3. Click **OK**.
4. Click **Yes**.

To customize the recovery of a drive

1. On the Tasks page, click **Recover My Computer**.
2. Select a recovery point, and then click **Recover Now**.
3. Click **Custom** to start the Recover Drive Wizard.
4. Click **Next**.

5 Do one of the following:

- To use the recovery point that is selected, click **Next**.
- Click **Browse** to select a different recovery point, and then click **Next**.
  If you need to access recovery points on a network that requires user authentication, enter your user name and password, and then click **Next**.

6 Select the drive that you want to restore, and then click **Next**.

If the drive does not have enough space available to restore a recovery point, press **Shift** and then select multiple, contiguous destinations that exist on the same hard disk.

7 If the recovery point is password-protected, in the Password box, type the password and then click **OK**.

8 Select the desired restore options.

The options that are available depend on the restore destination that you have selected.

See "Recovery options" on page 165.

9 Click **Next** and review your selections.

10 Click **Finish**, then click **Yes**.

If the wizard cannot lock the drive to perform the recovery in Windows (typically, because the drive is in use by a program), make sure the drive is not in use by closing any files or applications that might be using it, and then click Retry.

If the Retry option fails, click Ignore to tell Windows to attempt to force a lock on the drive. If Ignore fails, you might be prompted to insert the Symantec Recovery Disk CD and manually start the recovery environment so that you can complete the recovery. When the recovery is finished, the computer restarts automatically.

Recovery options

The options you can specify for the recovery are described in the table below.

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 required for the recovery to complete.

Option	Description
Check for file system errors	Checks the restored drive for errors after the recovery point is restored.
Resize restored drive	Automatically expands the drive to occupy the target drive's remaining unallocated space.
Set drive active (for booting OS)	Makes the restored drive the active partition (for example, the drive from which the computer starts). You should select this option if you are restoring the drive on which your operating system is installed.
Restore original disk signature	Restores the original, physical disk signature of the hard drive. Disk signatures are part of all Windows operating systems that Norton Ghost 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 restoring a recovery point to a new, empty hard disk.
Partition type	Sets the partition type as follows: ■ Primary partition: Because hard disks are limited to four primary partitions, select this type if the drive will have four or less partitions. ■ Logical partition: Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of your hard disk.
Drive letter	Lets you assign a drive letter to the partition.

Restoring using LightsOut Restore

You must install a fully licensed version of Norton Ghost before you can perform a restore using the LightsOut capability. There is no trial or evaluation period for this feature.

The Norton Ghost LightsOut Restore feature enables administrators to restore a computer from a remote location, regardless of the state the computer is currently in, so long as its file system is intact. This option provides a way to boot the Symantec recovery environment from a folder on the operating system partition. This option has been developed around the concepts of pcAnywhere, the Windows boot menu, and hardware devices such as RILO and DRAC, which allow an administrator to remotely control a system during the boot process (including the selection of items from a Windows boot menu). Depending on your hardware configuration, you can use LightsOut Restore to complete a system restoration on a remote server via a Web browser, using your server's remote connection capabilities, and the Symantec recovery environment. By using this option, you save the time it takes to physically visit the computer to perform the restore.

When LightsOut Restore is set up, it installs a Symantec recovery environment directly to the file system on the system partition, and places a Symantec recovery environment boot option within the Windows boot menu. Whenever this boot menu option is selected, the system will boot directly to the Symantec recovery environment using the files installed on the system partition.

Note: The LightsOut feature requires at least 1 gigabyte of memory to run.

Once LightsOut Restore has been set up and the boot menu option has been added, you can use a hardware device to remotely connect to the system. When you are connected, you can power on or reboot the system and select the recovery environment from the boot menu. The system then boots to the recovery environment.

By default, when the recovery environment boots as part of LightsOut Restore, it automatically starts a pcAnywhere thin host (this can be changed through the LightsOut Restore wizard). You can then use pcAnywhere to connect to the thin host and remotely use the recovery environment to restore files or entire partitions.

Summary of the LightsOut Restore process

The following is a summary of the basic LightsOut Restore process.

1. Install pcAnywhere on a central system that will be used for management (such as a helpdesk computer).

2. Ensure that all servers can be managed remotely through a hardware device such as RILO or DRAC.

3. Install Norton Ghost on servers that need to be protected, and then create the desired recovery points.

4. Run the LightsOut Restore wizard by going to the Windows Start menu and selecting Programs > Symantec > Norton Ghost 15.0. This installs the Symantec recovery environment to the local file system, and creates an entry in the Windows boot menu that can be used to boot to this environment.

5. When either file or system recovery is needed, use the RILO or DRAC device to connect to the remote server and either power on or reboot the system.

6. During the remote server boot process, select the Symantec recovery environment from the boot menu. The remote server will then proceed to boot to the Symantec recovery environment (at which point, connection through RILO or DRAC will be lost). As the Symantec recovery environment starts, a pcAnywhere thin host will automatically start (unless this was disabled through the LightsOut Restore wizard).

7. Use pcAnywhere to connect to the remote server pcAnywhere thin host.

8. Through pcAnywhere, use the recovery environment to restore individual files, or entire partitions.

Starting the LightsOut Restore Wizard

If you have not already licensed Norton Ghost, the first time you run the LightsOut Restore wizard, you will be prompted to install a license file or a product license key.

Starting the LightsOut Restore Wizard

1. From Windows, click **Start > All Programs > Symantec > Norton Ghost 15.0 > LightsOut Restore Setup**.
2. If the product is not licensed, the Install License File dialog appears. Do one of the following:
   - If you have a license file, browse to its location.
   - If you have the serial number that came with Norton Ghost, click **Get License**.
   - If you do not have a license file, click **Buy Now** to purchase the product.
   - If you received a product license key, enter the key in the appropriate fields.
3. Depending on which option you clicked in the previous step, click **Activate**, or click **Later**.
4. You might be asked to specify the source location of a Symantec Recovery Disk. You can use your Norton Ghost product CD. Specify the location, and then click **Next**.

5 At the Options dialog, you can specify the amount of time that the boot menu is displayed. The default is 10 seconds.

If you leave the Enable Symantec pcAnywhere check box selected, networking will automatically start, and pcAnywhere will be loaded. If you clear this check box, pcAnywhere will not be automatically started.

6 Select the type of IP address you want to use, and then click **Next**.

7 You might be shown a list of network and storage drivers that are not supported in the Symantec recovery environment. Select the box next to the network driver that you would like to copy from your current Windows installation to the Symantec recovery environment, review the list of missing storage drivers, and then click **Next**.

8 Browse to the locations of your missing storage and network driver files.

Note: The location for missing network and storage drivers should point to a path that contains the fully extracted installation package for the desired driver. If you have more than one missing storage driver, you must rerun the LightsOut Restore wizard for each missing driver. Also, the drivers you select should be compatible with Windows Server 2003.

9 Click **Next**.

10 The summary screen with the options you selected is displayed. Click **Back** if you need to change the options, or if you are satisfied with your selections, click **Finish**.

The files are copied from the Symantec Recovery Disk. When the copying has completed, a dialog displays, indicating that LightsOut Restore successfully installed.

11 Click **OK**.

LightsOut Restore options for Symantec Recovery Disk

The table below describes the LightsOut Restore options for Symantec Recovery Disk.

Option	Description
Automatically start network services	Select this option if you want networking to start automatically when you recover the computer through LightsOut Restore.

Option	Description
Dynamic IP	Select this option to connect to a network without the need for additional network configuration. You can click this option if you know there will be a DHCP server available on the network at the time you restore.
Static IP	Click this option to connect to a network with a particular network adapter and specific address settings. You should click this option if you know there will be no DHCP server (or the DHCP server will be unavailable) when you recover.
Automatically start Symantec pcAnywhere	Select this option if you want the Symantec pcAnywhere thin host to start automatically when you start the Symantec recovery environment. Useful for troubleshooting a system recovery. Click **Configure** to specify pcAnywhere log on credentials and the following optional parameters: ■ Host name In the Host name box, 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 To encrypt the data stream between the host and remote computer, in the Encryption level list, select one of the following: ■ None No encryption of the data stream occurs between the host and remote computer. ■ pcAnywhere Scrambles 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. ■ Symmetric Encodes and decodes data using a cryptographic key. This option is available on any Windows operating system that supports the Microsoft CryptoAPI.

Reconfiguring Using the LightsOut Restore Wizard

You can run the LightsOut Restore wizard again if you need to reconfigure your options.

Reconfiguring Using the LightsOut Restore Option Wizard

1. From Windows, click **Start > All Programs > Symantec > Norton Ghost 15.0 > LightsOut Restore Setup**.
2. Make your desired changes in the wizard screens, and then click **Finish**.
3. Click **Yes** if you want to recopy all of the files, or click **No** to only make the changes necessary for updating your system.

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 recover your computer using the Symantec Recovery Disk CD 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 secondary drive (which is any drive other than your system drive, or the drive where your operating system is installed), you can restore the drive within Windows.

The Symantec Recovery Disk CD lets you run a recovery environment that provides temporary access to Norton Ghost recovery features. For example, you can access the Recover My Computer Wizard to restart the computer into its previous, usable state.

Note: If you purchased Norton Ghost from your computer manufacturer, some features in the recovery environment might not be available. For example, if the manufacturer installed the recovery environment on your computer's hard disk. Your manufacturer might also assign a keyboard key for the purpose of starting the recovery environment.

When you restart your computer, watch for instructions on your computer monitor, or refer to your manufacturer's instructions.

Starting a computer by using Symantec Recovery Disk

The Symantec Recovery Disk CD lets you start a computer that can no longer run the Windows operating system. Symantec Recovery Disk is included with Norton Ghost. When you boot your computer using the Symantec Recovery Disk CD, a simplified version of Windows starts that runs a recovery environment. In the recovery environment, you can access the recovery features of Norton Ghost.

Note: Depending on which version of the product you have purchased, Symantec Recovery Disk is either included on your product CD, or as a separate CD. You should place the CD containing Symantec Recovery Disk in a safe place. See *If driver validation fails* in the *Norton Ghost™ User's Guide*.

Note: Symantec Recovery Disk requires a minimum of 512 MB of RAM to run. If your computer's video card is configured to share your computer's RAM, you might need more than 512 MB of RAM.

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

To start a computer by using Symantec 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 Recovery Disk might not detect it.

2. Insert the Symantec Recovery Disk CD into the media drive of the computer.

   If Norton Ghost was installed by your computer manufacturer, the recovery environment already could be installed on your computer's hard drive. Either watch your computer monitor after the computer restarts for on-screen instructions, or refer to your manufacturer's documentation.

3. Restart the computer.

   If you cannot start the computer from the CD, you might need to change the startup settings on your computer.

   See "Configuring a computer to boot from a CD" on page 175.

4. As soon as you see the prompt **Press any key to boot from CD**, press a key to start Symantec 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 Recovery Disk, and your computer will restart.

Configuring a computer to boot from a CD

To run Symantec Recovery Disk, you must be able to start your computer using a CD.

To configure a computer to boot from a CD

1. Turn on your computer.

2. As the computer starts, watch the bottom of the screen for a prompt that tells you how to access the BIOS setup.

   Generally, you need to press the Delete key or a function key to start your computer's BIOS setup program.

3 In the BIOS setup window, select Boot Sequence, and then press **Enter**.

4 Follow the on-screen instructions to make the CD or DVD device be the first bootable device in the list.

5 Put your Symantec Recovery Disk CD into the CD drive, and then restart your computer.

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

6 Save the changes and exit the BIOS setup to restart the computer with the new settings.

7 Press any key to start Symantec Recovery Disk.

When you start your computer with the Symantec Recovery Disk CD in the drive, you will see a prompt telling you to **Press any key to boot from CD**. If you do not press a key within five seconds, your computer will attempt to start from the next bootable device listed in the BIOS.

Note: Watch carefully as the computer starts. If you miss the prompt, the computer will need to be restarted again.

How to prepare to recover a computer

You should scan your hard disk to check it for corrupted data or surface damage before recovering your computer.

You should scan your computer for viruses before you attempt to recover. You can run a virus scan using Symantec Recovery Disk.

See “Scanning for viruses” on page 176.

See “Checking a hard disk for errors” on page 178.

Scanning for viruses

If you suspect that your computer was damaged by a virus or other threat, you should run a virus scan before you restore your computer.

To scan for viruses

1 On the Analyze panel, click **Scan for Viruses**.

2 Select one of the following:

Use the virus definitions currently available	Select this option to use the definitions that are included on the Symantec Recovery Disk CD.
Use Update Locator virus definitions folder	Select this option if you downloaded the latest virus definitions to a disk.

See "Locating the latest virus definitions" on page 177.

Locating the latest virus definitions

The Symantec Recovery Disk CD includes virus definitions. However, to help protect your computer from the latest threats, you should use the latest virus definitions that are available. The Update Locator locates the latest virus definitions that are available from Symantec. You must run the Update Locator on a working computer that has Internet access. You can save the virus definitions to a disk and then use them on the troubled computer.

Note: Depending on which version of the product you have purchased, Symantec Recovery Disk is either included on your product CD, or as a separate CD. You should place the CD containing Symantec Recovery Disk in a safe place. Should you lose the CD, you can create a new one if you have a CD burner. See *If driver validation fails* in the *Norton Ghost User's Guide*.

To locate the latest virus definitions

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

The installation program should start automatically.

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

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

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

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

- Right-click the Start button, and click **Properties**.
- On the **Start Menu** tab, click **Customize**.

- Scroll down and select **Run command**.
- Click **OK**.

3 Click **Run Update Locator**.

4 Click **Find and retrieve virus definitions**.

If more recent virus definitions are not found, you can still scan for viruses on your damaged computer by using the virus definitions that are on the Symantec Recovery Disk CD. However, the computer might not be protected from new viruses or threats.

5 When prompted, click **OK**.

6 Do one of the following:

- Insert a floppy disk into the floppy disk drive.
- Insert a blank, writable CD or DVD into the computer's CD or DVD recordable drive.

7 Locate the newly created Update Locator Virus Definitions folder on your computer's desktop and copy it to the blank disk.

Checking a hard disk for errors

If you suspect that your hard disk is damaged, you can examine it for errors.

To check a hard disk for errors

1 In the Analyze panel, click **Check Hard Disks for Errors**.

2 Select the drive that you want to check.

3 Select any of the following options.

Automatically fix file system errors	Fixes errors on the selected disk. When this option is not selected, errors are displayed but are not fixed.
Find and correct bad sectors	Locates bad sectors and recovers readable information.

4 Click **Start**.

Recovering a computer

You can restore your computer from within the recovery environment. If you have a recovery point for the hard drives that you want to recover, you can fully recover your computer or other hard drive back to the state it was in when the recovery point was created.

See "Recovering a computer from a virtual disk file" on page 183.

To recover a computer

1 Start the computer by using the Symantec Recovery Disk CD.

  See "Starting a computer by using Symantec Recovery Disk" on page 174.

2 On the Home panel, click **Recover My Computer**.

  If your recovery points are stored on a CD or DVD and you only have one CD/DVD drive, you can eject the Symantec Recovery Disk CD now. Insert the CD or DVD that contains your recovery points.

3 On the Welcome page of the wizard, click **Next**.

4 Do one of the following:

  - If Symantec Recovery Disk located recovery points, proceed to step 6
  - If Symantec Recovery Disk did not locate any recovery points, proceed to the next step.

5 In the View recovery points by list, select one of the following options:

  Date

  Displays all of the discovered recovery points in the order in which they were created.

  If no recovery points were discovered, the table is empty. If such cases, you can search all local drives on the computer or browse to find a recovery point.

  In the Select source folder list, do one of the following:

  - Click **All local drives** to view a list of all available recovery points that may exist on your computer's local drives.
  - Click **Browse** to locate a recovery point on a local drive or a network folder.

  File name

  Lets you browse to another location to select a recovery point file (.v2i).

  Select this option, and then click **Browse**. Locate and select a recovery point file (.v2i), and then click **Open**.

  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 file you want.

System	This type of recovery operation uses a system index file (.sv2i) to restore a computer that has multiple drives. A system index file reduces the amount of time that is needed to restore the drives. When a recovery point is created, a system index file is saved with it. The system index file contains a list of the most recent recovery points, which includes the original drive location of each recovery point Select this option, and then click **Browse**. Locate and select a system index file (.sv2i), and then click **Open**.

6 Click **Next**.

7 In the Drives to Recover panel, select each recovery point that you want to recover.

If necessary, add or remove recovery points from the list.

If you are recovering your computer, select the drive on which Windows is installed. On most computer systems, this drive is the C drive. In the recovery environment, the drive letters and labels might not match what appears in Windows. You might need to identify the correct drive based on its label, the name assigned to it, or by browsing the files and folders in the recovery point.

8 Do the following:

- 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 Restore pane.
  See “Edit target drive and options” on page 181.
- Set the following:

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 required for the recovery to complete.

See “Recovering files and folders using Symantec Recovery Disk ” on page 187.

9 Click **Next** to review the recovery options that you selected.

10 Select **Reboot when finished** if you want the computer to restart automatically after the recovery process finishes.

11 Click **Finish**.

12 Click **Yes** to begin the recovery process.

Edit target drive and options

The following table describes the options that are available on the Edit Target Drive and Options page after booting to the Symantec Recovery Disk CD.

Options	Description
Delete Drive	Delete a selected drive in the list to make space available to restore your recovery point. 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.
Undo Delete	If you delete a drive and then change your mind, click **Undo Delete** to return the drive to the list.
Resize drive after recover (unallocated space only)	Select a disk (or volume label) that you want to resize after the recovery point is restored. Then, select this option and specify the new size in megabytes. The size must be greater than the identified size of the disk that you selected in the list.
Partition type	Sets the partition type as follows: ■ Primary partition: Because hard disks are limited to four primary partitions, select this type if the drive will have four or less partitions. ■ Logical partition: Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of your hard disk.
Check for file system errors after recovery	Checks the restored drive for errors after the recovery point is restored.

Options	Description
Set drive active (for booting OS)	Makes the restored drive the active partition (for example, the drive from which the computer starts). You should select this option if you are restoring the drive on which your operating system is installed.
Restore original disk signature	Restores the original, physical disk signature of the hard drive. Disk signatures are part of all Windows operating systems that Norton Ghost 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 restoring a recovery point to a new, empty hard disk.

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 physical hard disk to see which primary partition is active. It then starts the boot program from the boot sector of the active partition. This option is recommended only for advanced users and is available only if you restore a whole drive in the recovery environment. Select this option if any of the following situations are true: ■ You are restoring a recovery point to a new, empty hard disk. ■ You are restoring a recovery point to the original drive, but the drive's partitions were modified since the recovery point was created. ■ You suspect that a virus or some other problem has corrupted your drive's master boot record.

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 other hard drive back to the state it was in when the original virtual disk was created.

See “Defining a virtual conversion job” on page 147.

See “Running a one-time virtual conversion” on page 141.

See “Recovering a computer” on page 178.

To recover a computer from a virtual disk file

1. Start the computer by using the Symantec Recovery Disk CD.

   See "Starting a computer by using Symantec Recovery Disk" on page 174.

2. On the Home panel, click **Recover My Computer**.

3. On the Welcome page of the wizard, click **Next**.

4. In the View recovery points by list, select **Filename** and then do the following:

   - Click **Browse**.
   - Locate and select a virtual disk file (.vmdk or .vhd), and then click **Open**.
   - 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.

5. Click **Next**.

6. Select the target drive where you want to restore the virtual disk.

7. 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.

8. Click **Next**.

9. Select the options that you want to perform during the recovery process.

   See "Virtual disk recovery options" on page 185.

   The options that are available depend on the target drive that you selected earlier.

10. Click **Next** to review the recovery options that you selected.

11. Select **Reboot when finished** if you want the computer to restart automatically after the recovery process finishes.

12. Click **Finish**.

13. Click **Yes** to begin the recovery process.

Virtual disk recovery options

The following table describes the recovery options that are available when you recover a virtual disk.

Option	Description
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.
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)	Select this option and specify the new drive size in megabytes.
Partition type	Sets the partition type as follows: ■ Primary partition: Because hard disks are limited to four primary partitions, select this type if the drive has four or less partitions. ■ Logical partition: Select this type if you need more than four partitions. You can have up to three primary partitions, plus any number of logical partitions, up to the maximum size of your hard disk.
Set drive active (for booting OS)	Makes the restored drive the active partition (for example, the drive from which the computer starts). You should select this option if you restore the drive on which your operating system is installed.

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 Norton Ghost 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.
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, physical hard disk to see which primary partition is active. It then starts the boot program from the boot sector of the active partition. This option is recommended only for advanced users and is available only if you restore a whole drive in the recovery environment. Select this option if any of the following situations are true: ■ You 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.

Recovering files and folders using Symantec Recovery Disk

You can use the Symantec Recovery Disk CD to start your computer and to restore files and folders from within a recovery point.

To recover files and folders using Symantec Recovery Disk

1. Start the computer by using the Symantec Recovery Disk CD.

   See “Starting a computer by using Symantec Recovery Disk” on page 174.

2. Click **Recover**, and then click **Recover My Files**.

3. Do one of the following:

   - If Symantec Recovery Disk cannot locate any recovery points, you are prompted to locate one. In the Open dialog box, navigate to a recovery point, select one, and then click **Open**.
   - If Symantec Recovery Disk finds recovery points, select a recovery point from the list, and then click **OK**.

   Note: If you have trouble finding the recovery points in a network location, in the File name box, type the name of the computer and share that holds your recovery points. For example, \\computer_name\share_name.

   If you are still having problems, try entering the computer's IP address.

   See “About using the networking tools in Symantec Recovery Disk” on page 188.

4. In the tree view pane of the Recovery Point Browser, double-click the drive that contains the files or folders that you want to restore to expand it.

5. In the content pane of the Recovery Point Browser, do one of the following to select the files or folders that you want to restore.

To select all items	Press **Ctrl+A.**
To select a group of files that are next to each other	Select the top file, press **Shift**, and then select the last file in the list.
To select a group of files that are not next to each other	Press **Ctrl** as you select the files.

6 Click **Recover Files**.

Where possible, the Recover Items dialog box automatically completes the Restore to this folder box with the original path from which the files originated.

If the original location does not include a drive letter you must type the drive letter at the beginning of the path.

Note: While in the recovery environment, drive letters and labels might not match what appears in Windows. You might have to identify the correct drive based on its label, which is the name assigned to it.

7 If the original path is unknown or you want to restore the selected files to a different location, click **Browse** to locate the destination.

8 Click **Recover** to restore the files.

9 Click **OK** to finish.

Exploring files and folders on your computer using Symantec Recovery Disk

You can explore the files and folders on your computer from the recovery environment by using the Explore My Computer feature.

This feature uses the Recovery Point Browser and functions similarly to Windows Explorer. You can browse the file structure of any drive that is attached to your computer from the recovery environment.

To explore files and folders on your computer using Symantec Recovery Disk

◆ In the Analyze pane, click **Explore My Computer**.

About using the networking tools in Symantec Recovery Disk

If you store your recovery points on a network, you need access to the network to restore your computer or your files and folders fromSymantec Recovery Disk.

Note: Additional computer memory might be required to recover your computer across a network.

See “Starting networking services” on page 189.

See “Using the pcAnywhere thin host for a remote recovery” on page 189.

See “Mapping a network drive from within Symantec Recovery Disk” on page 191.

See “Configuring network connection settings” on page 192.

Starting networking services

If you need to start networking services, you can do so manually.

To start networking services

◆ On the Network panel, click **Start My Networking Services**.

  To verify the connection to the network, you can map a network drive.

  See “Mapping a network drive from within Symantec Recovery Disk” on page 191.

Using the pcAnywhere thin host for a remote recovery

The Symantec Recovery Disk CD 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.

Note: You cannot deploy a thin host to Symantec Recovery Disk. The thin host can only be started from the Symantec Recovery Disk CD to host a remote control session in Symantec Recovery Disk. The thin host in Symantec 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 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 Recovery Disk. You must use Symantec pcAnywhere to connect to the thin host.

To start the pcAnywhere thin host

1 On Network panel, in the recovery environment, click **Start the pcAnywhere Thin Host**.

2 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 that is included in the Symantec Recovery Disk CD, and it must be waiting for a connection. When connected, the client computer can remotely manage a recovery or perform other tasks that are supported in Symantec 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 the recovery environment. Also, ensure that the pcAnywhere thin host is waiting for a connection.
2. Obtain the IP address of the thin host computer.
3. On the client computer, in Symantec pcAnywhere, configure a remote connection item.

   For more information, see the *Symantec pcAnywhere User's Guide*.

   Note: You do not need to choose to automatically logon 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 logon 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.

To prevent unauthorized users from tampering with your settings or trying to launch a session without your permission, set a password for your remote connection item.

This option is available in the Remote Properties window on the Protect Item tab. The thin host does not support encryption.

5 In pcAnywhere, start the remote control session.

If the connection attempt is unsuccessful, the thin host must be restarted on the host computer before you 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, when the thin host computer is restarted, or when the remote control session is ended.

After the host computer starts Windows, the client computer can deploy and connect a thin host on the computer to verify the success of tasks that were performed in the recovery environment.

Mapping a network drive from within Symantec Recovery Disk

If you started the networking services after you started the recovery environment, you can map a network drive. This 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.

If there is no DHCP server or the DHCP server is unavailable, you must provide a static IP address and a subnet mask address for the computer on which you are running Symantec Recovery Disk.

See “Configuring network connection settings” on page 192.

After you provide the static IP address and subnet mask address, you can enter the recovery environment. However, because there is no way to resolve computer names, when you run the Recover My Computer Wizard or the Recovery Point Browser, you can only browse the network by using the IP addresses to locate a recovery point. You can map a network drive so that you can locate the recovery points more effectively. 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 Recovery Disk

1 Do one of the following:

- On the left side of the recovery environment window, click **Home**, and then in the right pane click **Map a Network Drive**.

- On the left side of the recovery environment window, click **Network**, and then in the right pane 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 the recovery environment.

Configuring network connection settings

You can access the Network Configuration window to configure basic network settings while running in the recovery environment.

To configure network connection settings

1 In the recovery environment main window, click **Network**, and then click **Configure Network Connection Settings**.

2 If you are prompted to start networking services, click **Yes**.

Getting a static IP address

If you want to restore a recovery point that is located on a network drive or share, but you are unable to map a drive or browse to the drive/share on the network (usually caused by the lack of an available DHCP service), you can assign a unique static IP address to the computer that is running the recovery environment. You can then map to the network drive or share.

To get a static IP address

1 In the Network Adapter Configuration box, click **Use the following IP address**.

2 Specify a unique IP address and subnet mask for the computer that you want to restore.

Be sure that the subnet mask matches the subnet mask of the network segment.

3 Click **OK**.

4 Click **Close** to return to the recovery environment's main menu.

5 In the Network pane, click **Ping a Remote Computer**.

6. Type the address of the computer that you want to ping on the network segment.
7. Click **OK**.

   If you specified a computer name or a computer name and domain as the address method, make note of the IP address that is returned from the computer that you pinged.

   If communication to the storage computer is operating as expected, you can use the Map Network Drive utility to map a drive to the recovery point location.

Getting a static IP address if 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.

To get an IP address if the ping is unsuccessful

1. On the computer that contains the recovery point that you want to restore, at a DOS prompt, type the following command, and then press **Enter**.

   ipconfig /all
2. Write down the IP address that is displayed.
3. Return to the computer that is running the recovery environment and run the utility Ping Remote Computer with this IP address.

About viewing properties of recovery points and drives

You can view the properties of recovery points and the drives that are contained in them. For example, you can view the recovery point's description, size, and compression level. You can also view the name of the computer on which the recovery point was created.

- Viewing the properties of a recovery point
- Viewing the properties of a drive within a recovery point

Viewing the properties of a recovery point

You can view various properties of a recovery point by using the Recovery Point Browser. The following properties are available for viewing:

Description	A user-assigned comment associated with the recovery point
Size	The total size (in megabytes) of the recovery point
Created	The date and time that the recovery point file was created
Compression	The compression level that is used in the recovery point
Split across multiple files	Whether the entire recovery point file is spanned over several files
Password protected	The password protection status of the selected drive
Encryption	The encryption strength that is used with the recovery point
Version	The version number associated with the recovery point
Computer name	The name of the computer on which the recovery point was created
Search engine support	If you enabled search engine support for the recovery point, this property is displayed.
Created by	Identifies the application (Norton Ghost) that was used to create the recovery point.

To view the properties of a recovery point

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

Viewing the properties of a drive within a recovery point

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

Description	A user-assigned comment associated with the recovery point.
Original drive letter	The original drive letter that was assigned to the drive.
Cluster size	The cluster size (in bytes) that is used in a FAT, FAT32, or NTFS drive.
File system	The file system type that is used within the drive.

Primary/Logical	The selected drive's drive status as either the primary partition or the logical partition.
Size	The total size (in megabytes) of the drive. This total includes used and unused space.
Used space	The amount of used space (in megabytes) within the drive.
Unused space	The amount of unused space (in megabytes) within the drive.
Contains bad sectors	Indicates if there are any bad sectors on the drive.
Cleanly quiesced	Indicates whether the database application quiesced properly when a recovery point was created.

To view the properties of a drive within a recovery point

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

About the Support Utilities

The recovery environment has several support utilities that Symantec Technical Support might ask you to use to troubleshoot any hardware issues that you encounter.

You might be required to supply the information that is generated by these utilities if you call Symantec Technical Support for help resolving problems.

Note: You should only use these tools as directed by Symantec Technical Support.

Copying a drive

This chapter includes the following topics:

About copying a drive

You can use the Copy Drive feature to copy your operating system, applications, and data from one hard drive to another hard drive.

You can even copy a larger hard drive to a smaller hard drive if the data on the drive being copied is at least 1/16th smaller in size than the total size of the new drive.

If the hard drive that you want to copy contains more than one partition, you must copy the partitions one at a time to the new hard drive.

You can use the Copy Drive feature when you upgrade to a larger hard drive or when you add a second hard drive. You should not use the Copy Drive feature to set up a hard drive that will be used in another computer. The drivers that are used to run the hardware on one computer will likely not match the drivers on a second computer.

Preparing to copy drives

Before you can copy drives, you must have the hardware configured correctly.

To prepare to copy drives

1 Do all of the following:

- Prepare the computer.
- Get the manufacturer's directions for installing the drive.
- Shut down the computer, and then disconnect the power cord.
- Discharge electricity by touching a grounded metal object.
- Remove the computer cover.

2 Change the jumper settings on the hard drive to make the new hard drive the slave drive, or connect it as the slave drive if you are using cable select instead of jumper settings to determine the master and slave drives.

3 Do the following to attach the new hard drive:

- Connect the cable so that the colored stripe on the edge lines up with the I/O pins on the motherboard.
  The motherboard is marked Pin1 or 1 where the colored stripe should go.
- Connect the other end of the cable to the back of the hard drive, and match the striped edge with the I/O pin position on the drive itself.
  The I/O pin is usually on the side closest to the power supply.

4 Attach the power connector to the new hard drive.

Make sure that the angled edge of the plastic connector lines up with the angled edge of the pin socket.

5 Anchor the drive in the bay area according to the manufacturer's instructions.

6 Do the following to change the BIOS settings to recognize the new hard drive:

- Open the BIOS setup. As the computer starts, watch the computer screen for instructions on how to open the BIOS setup.
- Select Auto Detect for both the master and slave drives.
- Save the BIOS changes, and then exit.
  Your computer will restart automatically.

Copying one hard drive to another hard drive

After you install a new hard drive, you can copy your old hard drive to the new one. The new hard drive does not need to be formatted.

If the hard drive that you want to copy contains more than one partition, you must copy each partition, one at a time, to the new hard drive.

If the power or the hardware fails while you copy the data, no data is lost from the source drive. However, you must restart the copying process.

To copy one hard drive to another hard drive

1 On the Tools page, click **Copy My Hard Drive**.

2 Complete the steps in the wizard to copy the drive.

The wizard steps you through the process of selecting the right drive to copy, selecting the destination drive, and selecting the options for copying the data from one drive to another.

About drive-to-drive copying options

When you copy a drive from one hard drive to another, you can use the drive-to-drive copying options.

The following table describes the options for copying from one hard drive to another.

Table 15-1 Drive-to-drive copying options

Option	Description
Check source for file system errors	Check the source drive for errors before you copy it. The source drive is the original drive.
Check destination for file system errors	Check the destination drive for errors after you copy the drive. The destination drive is the new drive.
Resize drive to fill unallocated space.	This option automatically expands the drive to occupy the destination drive's remaining unallocated space.
Set drive active (for booting OS)	Make the destination drive the active partition (the drive from which the computer starts). Only one drive can be active at a time. To boot the computer, it must be on the first physical hard disk, and it must contain an operating system. When the computer boots, it reads the partition table of the first physical hard disk to find out which drive is active. It then boots from that location. If the drive is not bootable or you are not certain if it is, have a boot disk ready. You can use the Symantec Recovery Disk CD. The Set drive active option is valid for basic disks only (not dynamic disks).
Disable SmartSector copying	The SmartSector technology from Symantec speeds up the copying process by only copying the clusters and sectors that contain data. However, in a high-security environments, you might want to copy all clusters and sectors in their original layout, regardless of whether they contain data.

Table 15-1 Drive-to-drive copying options *(continued)*

Option	Description
Ignore bad sectors during copy	This option copies the drive even if there are errors on the disk.
Copy MBR	This option copies the master boot record from the source drive to the destination drive. Select this option if you are copying the C:\ drive to a new, empty hard drive. You should not select this option if you want to copy a drive to another space on the same hard drive as a backup. You should also not select this option if you want to copy the drive to a hard drive that has existing partitions that you do not want to replace.
Destination partition type	Click Primary partition to make the destination (new) drive a primary partition. Click Logical partition to make the destination (new) drive a logical partition inside an extended partition.
Drive letter	Select the drive letter you want assigned to the partition from the Drive letter list

Appendix A

Using a search engine to search recovery points

This appendix includes the following topics:

- About using a search engine to search recovery points
- Enabling search engine support
- Recovering files using Google Desktop's Search Desktop feature

About using a search engine to search recovery points

Norton Ghost supports the use of Google Desktop for searching file names that are contained in recovery points.

When you enable search engine support, Norton Ghost creates a catalog of all of the files that are contained in a recovery point. Search engines like Google Desktop use the catalog file generate an index. You can then search for files by name. Google Desktop does not index the content of files. It only indexes the file names.

Enabling search engine support

To use this feature with a search engine such as Google Desktop, you must do all of the following:

Install a search engine	You can download and install Google Desktop for free from the Internet. Visit desktop.google.com. See "To install Google Desktop" on page 202.

Enable Google Desktop support	A Google plug-in for Norton Ghost is required before you can use Google Search to locate and recover files. The plug-in is installed for you automatically when you enable this feature. See "To enable Google Desktop support" on page 202.
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 "To enable search engine support for a backup job" on page 203.

Note: Recovery points that already exist when you enable this feature cannot be indexed. This restriction is because the generated list of files that search engines require for generating searchable indexes are appended to recovery points as they are created. 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.

To install Google Desktop

1. Start Norton Ghost.
2. Click **Tasks > Options > Google Desktop**.
3. Click **Download Google Desktop from the Web** and follow instructions for installation.
4. When installed, click **OK** in the Norton Ghost Options window.

   For more information, visit desktop.google.com.

To enable Google Desktop support

1. Start Norton Ghost.
2. Click **Tasks > Options > Google Desktop**.
3. Select **Enable Google Desktop File and Folder Recovery**.

4. Click **OK**.

   This option is not available if you do not have Google Desktop installed. Install Google Desktop, and then repeat this procedure.

5. Click **OK** to install the Google Plugin.

To enable search engine support for a backup job

1. Start Norton Ghost.
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.

Recovering files using Google Desktop's Search Desktop feature

If you have correctly set up and enabled support for Google Desktop, you can search recovery points to located and recover files using Google Desktop.

See "Enabling search engine support" on page 201.

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, click **File > Save As** to save the recovered file.

   You can also right-click the search result and click Open to open the recovery point in the Recovery Point Browser.

   See "Opening and restoring files within a recovery point" on page 131.

About finding a file using Google Desktop

If you are certain that your file is included in a recovery point that has search engine support enabled, but the file is not found, do the following:

- Right-click the Google Desktop icon in the system tray and click **Indexing > Re-Index**.

  Re-indexing can take a significant amount of time. Be sure to wait until it completes before attempting to search again.

- Right-click the Google Desktop icon in the system tray and click **Preferences**.

  Under Search Types, verify that Web history is checked. This option must be checked or Google Desktop cannot index the content of your recovery points.

- Verify that the drive that contains your recovery points (backup destination) is available.

  For example, if your backup destination is on a USB drive, be sure that the drive is plugged in and that the power is turned on. Or, if your backup destination is on a network, be sure you are connected and logged in with the correct credentials.

- Adding **v2i** to the search string to narrow down the number of search results. For example, if you search for My Tune mp3, add v2i so that the search string is **My Tune mp3 v2i**.

  Recovery point files use .v2i as their file extension name. When you add it to the search string it eliminates any results that are not found in a recovery point.

- If your backup destination is on a network drive, be sure to add the location to the Search These Locations setting in Google Desktop Preferences.

About backing up Microsoft virtual environments

This appendix includes the following topics:

About backing up Microsoft virtual hard disks

Microsoft Windows 7 now supports 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 Norton Ghost. You cannot back up a physical disk and its VHD counterpart in the same backup job using Norton Ghost. 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 you do not include the VHD as another volume in the same backup. If you backup a physical disk that hosts a VHD, 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

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. To do this, 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 when the guest operating system on the virtual machine is not running (cold backup) or the Hyper-V VSS integration component is not installed in the virtual machine.

Note: Norton Ghost is unable to back up clustered 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 Norton Ghost because one host has exclusive access to the disk.

To create a backup of a running virtual machine, the following conditions must be met:

If you attempt to perform a backup when the conditions above are not met, Norton Ghost 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.

http://entsupport.symantec.com/umi/V-306-2

Index