Symantec Ghost Implementation Guide

symantec™

Symantec Ghost Implementation 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 11.5

Legal Notice

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

The Licensed Software and Documentation are deemed to be commercial computer software 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
20330 Stevens Creek Blvd.
Cupertino, CA 95014

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

Additional enterprise services

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

Enterprise services that are available include the following:

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

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

Consulting Services Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each 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

Appendix M Diagnostics 619

Appendix N User Migration supported applications 623

Section 1

Getting Started

Chapter 1

Introducing Symantec Ghost

This chapter includes the following topics:

About Symantec Ghost

Symantec Ghost reduces costs and overhead associated with installing software applications and operating systems.

It makes PC management and deployment issues easier and more cost effective. Functionality, including computer configuration management, computer and user migration, and incremental backup, defines Symantec Ghost as the solution for PC management.

Symantec Ghost can make complete backups of disks and partitions. It copies system files that other backup utilities miss, making it a useful tool for disaster recovery operations.

Symantec Ghost includes the following features:

Create image files of and restore computers	Use Symantec Ghost to create image files of and restore computers. Computers can be backed up to a network or to a wide range of hard drives and removable media, including CD/DVD drives, FireWire and USB hard drives, ZIP, and JAZ drives.

Hardware and software inventory

Manage hardware and software inventory from the centralized Console.

Create detailed reports from fully customizable filters and views.

Create dynamic folders to manage a group of target computers based upon hardware or software attributes to streamline operating system migration.

Client staging area

Any directory on a client computer which is preserved during clone operations. A staging area can be used to store Ghost image files, Autoinstall packages and Ghost User Migration packages.

Preserve the contents of a selected directory during a restore, keeping a local backup and recovery image file.

Manage computers

Remotely manage all client computers from a central Console and execute tasks on client computers from the Console or from the client.

Multicast file transfer

Transfer all files, including installation packages, using the multicasting functionality from the Console. Reduce network traffic by sending an individual file to multiple recipients simultaneously. Flexible file transfer lets you specify where a file transfer goes.

Retire disks

Wipe disks to U.S. Department of Defense standards using GDisk.

Transfer user data

Capture user files, application settings, and operating system settings from a computer and transfer them onto another computer or onto a reimaged computer.

Ghostcasting

Use the GhostCasting feature to clone computers efficiently and to help minimize the impact on network traffic.

AutoInstall

Create executable programs that install software packages.

File system support

Back up, restore, or clone FAT, FAT32, NTFS, and Linux Ext2/3 file systems.

Image file editing

Edit FAT, FAT32, NTFS, and Linux image files by using Ghost Explorer.

Restore individual files

Restore individual files from an image file by using Ghost Explorer.

SID-changing capability

Change SIDs using the Symantec Ghost utility Ghost Walker. Symantec Ghost also supports Microsoft Sysprep.

Stand-alone post-clone configuration client

Apply configuration settings to a computer directly. The stand-alone post-clone configuration lets you run a post-clone configuration without the Console.

Disk and partition management	Run GDisk from DOS or from a command shell in Windows to manage partitions and disks.
OmniFS utility	Manipulate files and directories in a locally attached NTFS or FAT file system.
GhRegEdit utility	Edit the Windows registry from DOS or WinPE by using the executable programs GhRegEdt and GhRegEdit32.
Tutorials	View the set of tutorials that are included in Symantec Ghost to provide a demonstration of the most commonly used features.

What's new in Symantec Ghost

Symantec Ghost 11.5 includes the following features:

WinPE PreOS Support	Both the console, and the standard tools include WinPE 2.0 in addition to PC-DOS. This greatly improves hardware compatibility.
DeployAnywhere	The new hardware-independent imaging feature allows a single image to be deployed to diverse hardware, and obtain the necessary drivers from a centrally managed driver database.
Hot Imaging	Images may be created hot, using Volume Snapshot, from both the Ghost Console and the standard tools.
Machine Erase	The Console has a task to perform the secure erase of a computer for decommissioning, or prior to re-imaging.
Support for VMDK and V2i/PQI images	VMDK virtual disk, Symantec Backup Exec System Recovery (V2I) and Symantec Deploy Center (PQI) images can be deployed directly from the Console and from Ghost.
Native Linux versions of Ghost tools	Native Linux versions of the Ghost executable and standard tools are provided, along with a bundled Linux distribution (ThinStation) for use when creating boot packages.
New Software and File Actions Interface	You can specify the order in which to perform file transfer, command execute and AI package deployment task steps in the Ghost Console. The ability to transfer folders to clients, retrieve files from clients, and obtain return codes when running command actions is also provided.
Improved Sysprep Interface	The interface for creating sysprep unattend files has been improved.

User Migration Application Content IDE

A User Migration content development tool which allows advanced users to create their own application migration definitions is provided.

Components of Symantec Ghost

Symantec Ghost includes a number of products and utilities that you can install. Install components that are required on your server and client computers.

Symantec Ghost Console

The Symantec Ghost Console is a Windows server-based application for remote management of computers.

Using the Symantec Ghost Console, IT managers can group targeted computers for a task and initiate the process from the Console.

Symantec Ghost Console client

The Symantec Ghost Console client enables remote control from the Symantec Ghost Console. The Console client includes a Windows agent and a Ghost partition. You can install the client on Windows Vista/XP/2000 computers. The Windows agent lets the computer start from the Ghost partition when necessary, and it coordinates the tasks that you start from the Console.

Symantec GhostCast Server

The GhostCast Server lets you deliver an image file to multiple computers simultaneously through a single, IP multicast transmission. A multicast transmission can minimize the impact on network traffic. The GhostCast Server sends and receives images to or from one or more computers. This method of delivery usually is faster than accessing a mapped network drive.

Symantec Ghost Boot Wizard

You use the Symantec Ghost Boot Wizard to create boot packages. A boot package can be a boot disk, a Ghost image file, an ISO image, or a Preboot eXecution Environment (PXE) image. You use boot packages for cloning operations. For example, you can create a boot disk for GhostCasting or create a boot image for use with PXE applications or the Microsoft Remote Installation Service. The Symantec Ghost Boot Wizard helps you locate the drivers that you need to create a boot package.

Symantec Ghost AutoInstall

Symantec Ghost AutoInstall has two components, AI Builder and AI Snapshot, that let you create and customize an application image, which you can deploy to your target workstation or workstations.

Symantec Ghost executable program

The Symantec Ghost executable program (Ghost.exe) lets you back up, restore, and clone computers. The Ghost.exe executable program has a small footprint with minimal conventional memory requirements. You can run it from a boot-disk set or from a hard drive. Symantec Ghost can restore a computer from an image file that contains Windows XP and a full installation of Microsoft Office in less than one minute.

A Linux version of the Ghost executable is available.

Note: The performance tests were performed on P4, 7,200 RPM hard drive.

The Ghost executable program includes the following versions:

Ghost.exe	Runs in DOS.
Ghost32.exe	Runs in Microsoft Windows Vista/XP/PE/2000. You can use Ghost32.exe to create image files on hard drives that are accessible from these operating systems or that can make a connection with the GhostCast Server. **Note:** To create an image file of the boot drive with Ghost32, you run Ghost32 in Windows PE.
ghost	Runs in Linux.

Symantec User Migration Wizard

The Symantec User Migration Wizard is an application that lets you migrate the settings and files from one computer to another.

You can run the wizard on the source and the destination computer to perform the following tasks:

Create and restore a migration package	A migration package contains data that is collected from a client computer. The package consists of application settings, user files and folders, and registry entries. You use the migration package after you update a user's computer to restore the user's application settings and personal data files. **Note:** A package contains only the settings that are associated with a software application. It does not include the application.
Run a peer-to-peer transfer	You can simultaneously run Symantec User Migration on a source computer and a destination computer. This operation copies application settings, user files and folders, and registry entries from a source computer to a destination computer.

Symantec User Migration does not remove anything from the source computer. User settings, files and folders, and registry entries are copied to the destination computer or migration package.

If you installed an updated version of an application that Ghost supports, the restore step updates the user settings. For example, if your destination computer has a more current version of a Microsoft Windows operating system, then your operating system settings are upgraded and applied to the new computer. Taskbar settings and screen saver settings appear on the new computer as they were set on the old computer.

See "About supported applications" on page 624.

There are two ways that you can install the Symantec User Migration Wizard:

From the Symantec Ghost installation CD	Select Install Tools and Utilities > Install User Migration Wizard.
From the Ghost Console server	The installation files are located in \Program Files\Symantec\Ghost\SUMWizardInstall.

The Symantec User Migration Wizard documentation includes online help (`SUMWizard.chm`, located in the \Program Files\Symantec\Ghost folder) and the *Symantec User Migration Guide* (`SUM User Guide.pdf`, located on the Symantec Ghost installation CD).

GhConfig tool

The GhConfig tool lets you apply configuration settings directly to a computer. You can use this feature to apply post-clone configuration settings without using the Symantec Ghost Console.

A Linux version of this utility is available.

Ghost Walker

Ghost Walker lets you assign unique security identifiers (SIDs) to restored and cloned Microsoft Windows Vista/XP/2000 workstations. The SID is an important part of the Windows Vista/XP/2000 security architecture. It provides a unique identifier for the computers that are attached to your network.

Ghost Walker includes the following versions:

Ghost Walker	Runs in DOS
Ghost Walker 32	Runs from the command line in a WinPE operating system

Ghost Explorer

Ghost Explorer lists all of the files and directories that are within an image file. You can add, recover, and delete individual directories and files to or from an image file.

GDisk

A Linux version of this utility is available.

GDisk is a complete replacement for the FDISK and FORMAT utilities that allows the following:

- FAT and NTFS file system formatting
- Batch mode operation
- Hiding and unhiding of partitions
- Secure disk wiping to U.S. DoD requirements
- Extensive partition reporting

Unlike FDISK, which uses interactive menus and prompts, GDisk is command-line driven and offers faster configuration of a disk's partitions.

Table 1-1 lists the GDisk versions that are available.

Table 1-1 GDisk versions

Version	Description
GDisk.exe	Runs in DOS
GDisk32.exe	Runs from the command line in a Windows operating system

Table 1-1 GDisk versions *(continued)*

Version	Description
gdisk	Runs in Linux

GhRegEdit

GhRegEdit is a utility for editing the Windows registry.

A Linux version of this utility is available.

Table 1-2 lists the GhRegEdit versions that are available.

Table 1-2 GhRegEdit versions

Version	Description
GhRegEdt.exe	Runs in DOS
GhRegEdit32.exe	Runs from the command line in a Windows operating system.
ghregedit	Runs in Linux

OmniFS

OmniFS is a general-purpose utility for manipulating files and directories in a locally attached NTFS, Linux, or FAT file system (including FAT hidden partitions).

A Linux version of this utility is available.

Table 1-3 lists the OmniFS versions that are available.

Table 1-3 OmniFS versions

Version	Description
OmniFS.exe	Runs in DOS
OmniFS32.exe	Runs from the command line in a Windows operating system
omnifs	Runs in Linux

Chapter 2

Understanding Symantec Ghost

This chapter includes the following topics:

The Symantec Ghost partition

For the Symantec Ghost Console to execute tasks on client computers, you must have a Ghost partition on the client. There are two types of partitions that you can create on client computers. A client computer requires one of the following:

Virtual partition

Once you install the Console client remotely or from the CD, Symantec Ghost creates the virtual partition automatically when a task that requires a computer to restart in the PreOS is executed.

Ghost boot partition

Installing the Ghost boot partition is more complicated and time consuming than creating the virtual partition. It involves creating a boot package and then an image file to restore onto the client computer.

The Ghost boot partition is used on client computers that have one of the following:

- A version previous to 7.5 of the Console client for Symantec Ghost installed.
- No operating system installed. You can create a Ghost boot partition that contains the Console client, which then connects to the Console.

  Note: You can also connect to a computer that has no operating system installed by using a PXE Server.

  See "Using 3Com Boot Services and Symantec Ghost" on page 40.

See "About boot partitions" on page 591.

You can check the Ghost partition settings for each client computer. You can also set the virtual partition parameters globally from the Symantec Ghost Console.

See "About setting up the virtual partition" on page 91.

Using the virtual partition to connect to the Console

The virtual partition is created on client computers that have an operating system installed but do not have the Ghost boot partition installed.

The operating system on the client computer creates a nonfragmented, contiguous file that is formatted as a FAT 16 partition. The DOS network drivers and the DOS operating system are copied to the file. The Master Boot Record (MBR) and the partition table point to the file and see it as an active partition. When the task ends, the MBR is reassigned to point back to the host's operating system.

Note: The partition table in the MBR shows if a disk is partitioned into up to four primary partitions or three primary partitions and one extended partition.

If a client computer uses static IP, the same static IP address is used in the virtual partition.

The support for virtual partitions has the following limitations:

- Compressed NTFS drives on Windows Vista/XP/2000/NT are not supported.
- The support of dynamic disks is limited to simple dynamic disks.

- Spanned, striped, and RAID-5 volumes are not supported.
- GPT disks are not supported.

Client staging area

The client staging area is a scenario that brings together Symantec Ghost features to let you do the following:

- Store Ghost image files, Autoinstall packages, Ghost User Migration packages, and other files locally on a client computer.
  You can remotely create a directory on a client computer and transfer files from the Console by using multicasting technology.
  See "Transferring files to client computers" on page 133.
  See "Local deployment of Console resources" on page 109.
  See "Setting the default data transfer properties" on page 82.
- Restore a computer or migrate a computer to Windows Vista by using the files stored locally in the client staging area, reducing network traffic.
  See "Local deployment of Console resources" on page 109.
- Preserve user data and settings.
  You can create a user-migration package to preserve the files that are on a client computer when you perform a restore operation from an image file. The package and the image file are preserved in the client staging area.
  See "Preserving files and folders on client computers" on page 124.

Choosing a method to create an image file

There are several ways to create an image and restore it onto a computer. Which of the following methods you choose depends on how many computers you are restoring, the operating system installed, and the functions required:

Stand-alone computer	You can use the Symantec Ghost executable to back up one drive or partition to an image file on another drive or partition. You can create an image file on a computer or between computers through an LPT/USB, mapped network drive or a network connection. This process is fast and efficient. It requires only a boot package that includes Ghost.exe and the relevant drivers. In a peer-to-peer operation, the Symantec Ghost executable is run on each computer from a boot package. You use the Symantec Ghost Boot Wizard to create the boot package.

Over a network by using GhostCast	You can use the GhostCast Server on a server computer and run the Symantec Ghost executable on the client computers to create an image file. You can then restore a number of computers simultaneously. The Symantec Ghost executable is used on each client computer from a boot package created with the Symantec Ghost Boot Wizard.
Console task	The Console draws on the functionality of Ghost.exe and GhostCasting but offers many more functions. A task is created that can be run concurrently with other tasks. After the task is complete, you can apply configuration settings to the computer.

Using 3Com Boot Services and Symantec Ghost

The Symantec Ghost OEM version of 3Com Boot Services is included with Symantec Ghost. This lets you install a PXE server.

The PXE server is useful for the following:

- Connecting a client computer with no operating system installed to the Console Server or the GhostCast Server.
  You can perform Console or GhostCast operations, including installing the Console client on the client computer.
- Disaster recovery.

The 3Com Boot Services functionality is not detailed in the Symantec Ghost documentation.

For more information, see the 3Com Boot Services documentation, which is included on the product CD.

See “Creating a TCP/IP Network Ghost Client Boot Image” on page 271.

Where to find more information

Each application includes guides and online help.

Note: The guides are also available on the Symantec Ghost Solution Suite CD.

Symantec Ghost documentation includes the following guides in PDF format:

Symantec Ghost Implementation Guide

Symantec User Migration Implementation Guide

You can also find more information about Symantec Ghost on the Symantec Ghost user forums at the following URL:

http://forums.symantec.com/discussions/forum.jspa?forumID=109

Chapter 3

Installing Symantec Ghost

This chapter includes the following topics:

- About installing Symantec Ghost
- Before you install
- System requirements
- Installing Symantec Ghost Console
- Installing the Console client
- Installing the Configuration Client Stand-alone
- Installing Symantec Ghost Standard Tools
- Installing Symantec Ghost Standard Tools for Linux
- Installing the User Migration Wizard
- Installing 3Com Boot Services
- Post-installation tasks

About installing Symantec Ghost

There are a number of ways to install Symantec Ghost depending on how you want to use it and the setup of the computer on which it is being installed.

How to install Symantec Ghost AutoInstall is covered separately.

See "How Ghost AutoInstall works" on page 389.

Before you install

Symantec Ghost includes a number of software packages. They are listed as follows with details of what you need to install and where you need to install it:

Symantec Ghost Console

Install on the server computer from which you plan to remotely back up, restore, clone, and configure other workstations. Installs all components of Symantec Ghost on the server except for the Console client, AI Snapshot, and the Symantec User Migration Wizard.

Symantec Ghost Console client

Install on your workstations to enable communication between your workstations and the Symantec Ghost Console. You can install the client from either the CD or from the Console.

Symantec Ghost Configuration Client (Standalone)

Install on a workstation that is not to be managed by the Symantec Ghost Console. Install this client to apply configuration settings after a restore or clone using Ghost.exe if you are joining the computer to a domain.

See "About performing applying post-clone configuration changes from the command-line" on page 355.

Symantec Ghost Standard Tools

Install when the Console is not required. Install all components of Symantec Ghost except for the Console server and client, and the Symantec User Migration Wizard.

Linux versions of the Ghost executable and the standard tools (except Ghost Walker) are available.

Symantec User Migration Wizard

Install on a client computer on which you want to create a migration package or run a peer-to-peer migration operation.

AutoInstall

Install on the computer on which you want to create packages to install applications.

See "Installing Ghost AutoInstall on the model computer" on page 391.

The *Symantec Ghost Solution Suite Getting Started* guide includes common scenarios for using Symantec Ghost and details which components must be installed for each scenario.

System requirements

The minimum hardware and software requirements to run Symantec Ghost vary according to the components you install.

Symantec Ghost Console and Standard Tools

The minimum requirements for running the Symantec Ghost Console are as follows:

- Pentium III processor
- 1024 x 768 screen resolution
- 512 Mb of RAM
- One of the following:
  - Windows Server 2008
  - Windows Vista Business/Enterprise/Ultimate
  - Windows Server 2003 Standard/Enterprise SP1
  - Windows Server 2003 R2 Standard/Enterprise
  - Windows XP Professional SP2
  - Windows 2000 Professional/Server SP4

Note: Symantec Ghost has been tested with the service packs listed above. We recommend that you install the latest service packs available from Microsoft.

Ghost executable

You can run Ghost.exe on a computer with the following minimum requirements:

- IBM PC computer or 100% compatible
- Pentium processor
- 16 MB RAM
- VGA monitor
- Microsoft-compatible mouse recommended
- One of the following:
  - PC DOS as included with Symantec Ghost
  - MS DOS

You can run Ghost32.exe on a computer with one of the following operating system requirements:

- Windows Vista(Business/Enterprise/Ultimate)/XP/Server 2003/2000 Professional

- Windows Preinstallation Environment (WinPE)

You can run Ghost32 on all 64-bit Windows operating systems except for WinPE 64-bit. Ghost32 does not support WinPE 64-bit because WinPE 64-bit does not include WOW64.

A 64-bit executable, Ghost64.exe, is provided with Ghost Solution Suite 2.5. This can be used in 64-bit WinPE environments and on 64-bit Windows systems.

Symantec Ghost supports Ghost32 on the following WinPE versions:

Windows XP SP2	Version 2004
Windows 2003 SP1	Version 2005
Windows Vista	Version 2.0

A Linux version of the Ghost executable is also provided.

Symantec Ghost Console client and Configuration client

The minimum requirements for running the Symantec Ghost Console client or the Configuration client are as follows:

- Networked computer with Windows Vista(Business/Enterprise/Ultimate)/XP/Server 2003/2000 Professional
- Single boot system
  Symantec Ghost does not support dual-boot computers. You cannot install the Console client or the Configuration client on Apple Mac computers.
- Can have more than one physical disk, but backup functionality supports the first physical disk only
- DOS drivers for network card
  See “Selecting the boot package type” on page 263.
- If you want to run WinPE as the PreOS on the Console client computer, you must have at least 256 MB RAM.

AutoInstall and Incremental Backups have the following support limitations:

- On x64 platforms, you can only capture 32-bit applications.
- You cannot capture 64-bit applications.

The minimum requirements for executing the user migration feature are as follows:

- Computer with Windows Vista(Business/Enterprise/Ultimate)/XP Professional/2000

Symantec Ghost Boot Wizard

The minimum requirement for using the Symantec Ghost Boot Wizard to modify WinPE images is:

- Computer with Microsoft Core XML Services (MSXML) 6.0 or later

Note that you can install and run the Ghost Boot Wizard on a computer that does not meet this requirement, but you cannot run any process that uses `PEImg.exe` (part of PETools). For example, modifying a WinPE image with new Windows network or disk drivers. `PEImg.exe` depends on Microsoft Core XML Services (MSXML) 6.0 or later.

Symantec User Migration Wizard

The minimum requirements for running Symantec User Migration Wizard is:

- Computer with Windows Vista(Business/Enterprise/Ultimate)/XP Professional/2000

Symantec User Migration does not support server platforms.

See "Symantec User Migration Wizard" on page 33.

Symantec User Migration Content IDE

The minimum requirement for running the Symantec User Migration Content IDE is:

- Computer with Microsoft .NET Framework 2.0 or later

Note that you can install the User Migration Content IDE on a computer that does not meet this requirement, but you cannot start the application until you have installed Microsoft .NET Framework 2.0 or later.

For more information see *.NET Framework 2.0 SDKs, Redistributables & Service Packs* on the Microsoft web site:

http://msdn2.microsoft.com/en-us/netframework/aa731542.aspx

Supported backup media

In addition to saving a backup to a secondary partition or an internal hard disk, Symantec Ghost can also save a backup to the following external media devices:

- CD-R/RW
- DVD+RW/-RW/+R/-R
- USB 1.1/2.0 hard drive and CD/DVD recordable devices

- FireWire (IEEE) 1394 hard drive and CD/DVD recordable devices
- Atapi tape (QIC157) devices
- SCSI tape
- A second computer using a peer-to-peer connection
- Mapped network drive
- ZIP drive
- JAZ drive

File systems supported for back up, restore, and cloning tasks

File systems supported for back up, restore, and cloning tasks are as follows:

- All FAT
- All NTFS
- EXT2/3
  See “Supported configurations” on page 561.

Ghost lets you backup. restore, and clone Windows 64-bit operating systems. You can back up, restore, and clone disks that have AMD 64-bit processors or that have Intel EM64T processors.

Support for GPT disks

The GUID partition table (GPT) is a standard for formatting a partition on a disk. It replaces the master boot record (MBR) disk format. GPT is part of the Extensible Firmware Interface (EFI) standard, which is intended to replace PC BIOS.

GPT uses logical block addressing and has the following features:

- It allows up to 128 primary partitions and, therefore, does not support extended partitions.
- It allows a volume size that is greater than 2 TB.
- It can be used as a storage volume on an x64-based platform

Symantec Ghost supports GPT-formatted disks using the following executable programs:

- Ghost
- Ghost32
- Ghost64
- ghost for Linux

- GhDplyAw32
- GDisk
- GDisk32
- GDisk64
- gdisk for Linux
- Ghost Walker
- Ghost Walker 32
- GhConfig
- GhConfig32
- GhConfig64
- ghconfig for Linux
- GhRegEdit
- GhRegEdit32
- GhRegEdit64
- ghregedit for Linux
- OmniFS
- OmniFS32
- OmniFS64
- omnifs for Linux

Support for RAID disks

Symantec Ghost supports all imaging operations for RAID disks using Ghost32 if the RAID disk complies with all of the following conditions:

- The source or destination disk is a hardware RAID array disk.
- The disk is accessible from the host operating system.

The pre-OS must be Windows Preinstallation Environment (WinPE).

RAID software-level drives are not supported. The ability to successfully back up other types of RAID-array configurations depends on the specific computer model, driver controller, hard drive, and RAID implementation.

Support for PQI and V2I images

PQI and V2I images are supported as a source (but not as a destination) in all cloning operations. They can be mounted as read-only disks that can be used by Ghost and all the Ghost tools (such as GDisk, GhRegEdit, OmniFS, etc.).

If you want to use this feature, you must have `v2DiskLib.dll` in the same directory as Ghost.exe.

Support for virtual disks

Ghost allows virtual disks to be treated as images. You can clone a computer to a virtual disk (create a vmdk file instead of a .gho file), and you can restore a computer from a vmdk file.

Installing Symantec Ghost Console

You must have administrator privileges on the Console computer to install Symantec Ghost Console. When you install Symantec Ghost Console, the Standard Tools are automatically installed.

To install the Symantec Ghost Console

1. Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive.
2. In the Symantec Ghost Solution Suite installation window, click **Install Symantec Ghost**.
3. Click **Install Ghost Console and Ghost Standard Tools**.
4. In the Symantec Ghost Server 11.5 - InstallShield Wizard dialog box, click **Next**.
5. Accept the terms of the license agreement, then click **Next**.
6. Read the licensing information, check **I have read and understood the above information**, then click **Next**.
7. In the User Information window, verify that the user and organization names are correct.
8. Click **Next**.
9. In the Destination Folder dialog box, do one of the following:
   - Confirm the installation location.
   - To select a different installation location, click **Change**.
10. Click **Next**.

11 In the Custom Setup window, click **Next**.

12 Click **Install**.

See “Post-installation tasks” on page 58.

Installing the Console client

You can install the Console client in either of the following ways:

- Install the Console client remotely from the Symantec Ghost Console.
  You can install the Console client on computers that run Windows Vista/XP/2000. You cannot remotely install the Console client on Windows XP Home computers.
- Manually install the Console client on a workstation from the Symantec Ghost CD.

You can also use 3Com DynamicAccess Boot Services to run the Console client from the network.

See “Using 3Com Boot Services and Symantec Ghost” on page 40.

Once you have installed the Console client, confirm that the client appears in the Symantec Ghost Console.

See “Managing Symantec Ghost Console client computers” on page 77.

Preparing a Windows Vista/XP client for remote installation

Before you remotely install the Console client on Windows Vista/XP computers you must verify that the following conditions are set:

Windows XP SP2 computers

When you install the Console client on a Windows XP SP2 computer, verify the following settings:

- If the Windows Firewall is turned on, then you must verify that File and Printer Sharing is added to the Firewall Exceptions list.

  See “To add File and Printer Sharing to the Exceptions List on a Windows XP SP2 computer” on page 53.
- If a firewall other than Windows Firewall is turned on, then you might need to allow the following ports:

  For UDP: 137 and 138

  For TCP: 139 and 445
- The administrator user account on the client computer must have a password.
- You must ensure that simple file sharing is turned off.

  See “To alter the client computer's security settings on a Windows XP SP2 computer ” on page 52.

Windows Vista computers

When you install the Console client on a Windows Vista computer, verify the following settings:

- If the Windows Firewall is turned on, then you must verify that File and Printer Sharing is added to the Firewall Exceptions list.

  See “To add File and Printer Sharing to the Exceptions List on a Windows Vista computer” on page 53.
- If a firewall other than Windows Firewall is turned on, then you might need to allow the following ports:

  For UDP: 137 and 138

  For TCP: 139 and 445
- The administrator user account on the client computer must have a password.
- If the client computer belongs to a workgroup, you must either turn on the built-in Administrator account, or turn off the User Account Control.

  See “To turn on the built-in Adminstrator account” on page 53.

  See “To disable the User Account Control” on page 53.

To alter the client computer's security settings on a Windows XP SP2 computer

1. On the client computer, on the Windows taskbar, click **Start > All Programs > Accessories > Windows Explorer**.
2. In Windows Explorer, on the Tools menu, click **Folder Options**.
3. On the View tab, under Advanced Settings, uncheck **Use simple file sharing**.
4. Click **OK**.

To add File and Printer Sharing to the Exceptions List on a Windows XP SP2 computer

1. On the client computer, click **Start > Run**.
2. In the Run dialog box, type **Firewall.cpl**.
3. Click **OK**.
4. On the Windows Firewall dialog box, on the Exceptions tab, verify that **File and Printer Sharing** is checked.
5. Click **OK**.

To add File and Printer Sharing to the Exceptions List on a Windows Vista computer

1. On the client computer, click **Start**.
2. In the Start Search field, type **Firewall.cpl**.
3. On the Windows Firewall dialog box, click **Change settings**.
4. On the Exceptions tab, verify that **File and Printer Sharing** is checked.
5. Click **OK**.

To turn on the built-in Adminstrator account

1. On the client computer, log on as an user that has adminstrator rights.
2. On the Control Panel, click **Classic View**.
3. Click **Adminstrative Tools**.
4. Click **Computer Management**.
5. Click **System Tools > Local Users and Groups > Users**.
6. Double-click the Administrator user.
7. Uncheck **Account is disabled**.
8. Click **OK**.
9. Right-click **Adminstrator** and click **Set Password**.
10. Set a password for the Administrator account and click **OK**.

To disable the User Account Control

1. On the client computer, log on as an user that has administrator rights.
2. On the Control Panel, click **User Accounts**.
3. Click **Turn User Account Control on or off**.
4. Uncheck **Use User Account Control (UAC) to help protect your computer**.
5. Click **OK**.
6. Restart the computer.

Remotely installing the Console client

Once you have installed the Symantec Ghost Console, you can perform remote client installations.

If the Ghost Console is running on a Windows Vista computer and you are having problems installing the Console client to clients, then verify that the LAN Manager authentication level setting on the Console computer is the same setting as the setting on your client computers. The Console computer setting might be incompatible with the setting on your client computers. The default level in Windows Vista is Send NTLMv2 response only.

Note: On the client computer, the share C$ must be shared for administrative purposes to allow remote client installation.

Note: In order to be able to uninstall a client remotely, the Console must contain the actual name of the client and not an older name. To ensure this, run a Refresh task on the client to update the client name in the Console.

To remotely install the Console client

1. On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Console**.
2. On the Tools menu, click **Remote Client Install**.
3. In the Remote Client install dialog box, do one of the following:
   - Select the computers to include in the client installation, then click **Add >>**.
     You can select multiple computers under different domains.
   - Click **Add...**, then type the computer domain or workgroup and name.
     You can add a group of computers in a workgroup that have the same administrative credentials. If you have computers with different administrative credentials for a workgroup, then each computer or group of computers must be added separately.
4. In the Enter client domain and machine name dialog box, in the User name field, do one of the following:
   - Type the administrator name for the domain.
   - Type the user name for a computer under the workgroup.
     If you are adding a single computer then you can type the fully qualified user name, for example, machinename\username.

This account must have administrator rights for the computer that you selected.

5 In the Password field, type the password for the account.

6 Click **OK**.

7 Click **Install**.

Manually installing the Console client

You can install the Console client directly on a client computer from the installation CD.

To install the Console client manually

1 Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive of the client computer.

2 In the Symantec Ghost Solution Suite installation window, click **Install Symantec Ghost**.

3 Click **Install Ghost Console Client**.

4 In the Symantec Ghost Managed Console Client 11.5 - InstallShield Wizard window, click **Next**.

5 Accept the terms of the license agreement, then click **Next**.

6 In the Connect to server window, type the computer name of the Ghost Console server.

If you leave this field empty, then the client connects to the first Ghost Console that it finds.

7 Click **Next**.

8 In the Destination Folder dialog box, do one of the following:

- Confirm the installation location.
- To select a different installation location, click **Change**.

9 Click **Next**.

10 Click **Install** to start the installation process.

Installing the Configuration Client Stand-alone

You should install the Configuration Client Standalone on a client computer only if you do not plan to use the Console to manage the computer, and you only intend to perform post-clone configuration tasks on the computer.

To install the Configuration Client (stand-alone)

1. Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive.
2. In the Symantec Ghost Solution Suite installation window, click **Install Symantec Ghost**.
3. Click **Install Ghost Configuration Client (Standalone)**.
4. In the Symantec Ghost Configuration Client (Standalone) 11.5 - InstallShield Wizard window, click **Next**.
5. Accept the terms of the license agreement, then click **Next**.
6. In the Destination Folder window, do one of the following:
   - Confirm the installation location.
   - To select a different installation location, click **Change**.
7. Click **Next**.
8. Click **Install** to start the installation process.

Installing Symantec Ghost Standard Tools

Install Standard Tools to use the Ghost executable program, Ghost Boot Wizard, Ghost Walker, GhostCast Server, GDisk, OmniFS, User Migration Explorer, GhConfig, GhRegEdit, and Ghost Explorer.

To install Symantec Ghost Standard Tools

1. Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive.
2. In the Symantec Ghost Solution Suite installation window, click **Install Symantec Ghost**.
3. Click **Install Ghost Standard Tools**.
4. Click **Next**.
5. In the Symantec Ghost Configuration Client (Standalone) 11.5 - InstallShield Wizard window, click **Next**.
6. Accept the terms of the license agreement, then click **Next**.
7. Do one of the following:
   - Confirm the installation location.
   - To select a different location for the installed files, click **Change**.
8. Click **Next**.

9 In the Custom Setup window, click **Next**.

10 Click **Install** to start the installation.

Installing Symantec Ghost Standard Tools for Linux

Linux versions of the following Ghost standard tools are supplied on the installation CD:

- ghost
- ghregedit
- ghconfig
- omnifs
- gdisk

There is no Linux version of Ghost Walker or the Ghost Client.

Note: The Linux tools must run as root.

To install Symantec Ghost Standard Tools for Linux

1 Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive.

2 Open the Linux folder, and copy the file `LinuxTools.tgz` to your Linux computer.

3 Extract the Linux tools to the appropriate location.

Installing the User Migration Wizard

Install the User Migration Wizard on a client computer to transfer user files and application settings.

To install Symantec Ghost User Migration Wizard

1 Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive.

2 In the Symantec Ghost Solution Suite installation window, click **Install Tools and Utilities**.

3 Click **Install User Migration Wizard**.

4 Click **Next**.

5 Accept the terms of the license agreement, then click **Next**.

6 Do one of the following:

- Confirm the installation location.
- To select a different location for the installed files, click **Change**.

7 Click **Next**.

8 Click **Install** to start the installation.

Installing 3Com Boot Services

The Symantec Ghost version of 3Com Boot Services was developed before Microsoft released Windows Vista. Therefore, Symantec Ghost does not support 3Com Boot Services on Windows Vista.

To install 3Com Boot Services

1 Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive.

2 In the Symantec Ghost Solution Suite installation window, click **Install Tools and Utilities**.

3 Click **Install 3Com Boot Services PXE Server**.

4 In the 3Com Boot Services for Symantec Ghost Corporate Edition dialog box, follow the on-screen prompts to complete the installation.

Post-installation tasks

After installing the Symantec Ghost Console you must register Symantec Ghost. Other post-installation tasks that you may want to do include the following:

- About activating Symantec Ghost
- Updating Symantec Ghost
- About upgrading Symantec Ghost
- Uninstalling Symantec Ghost
- Creating Console Service accounts

About activating Symantec Ghost

You activate Symantec Ghost Console by a license.

Until you activate your license for Symantec Ghost, your use of the Console is restricted as follows:

- You can run tasks on the Console for no more than 30 days after installation.
- You can attach a maximum of 10 clients.

After you activate your license, Symantec Ghost tracks the number of client computers that are attached to the Console. It alerts you when you have installed 90 percent of your licensed clients.

See “Activating Symantec Ghost” on page 59.

Activating Symantec Ghost

Before you can activate Symantec Ghost, you need the following materials:

License file	The license file includes the license key that is required to activate the product. For more information, see the instructions on your license certificate.

Obtaining a license file

To obtain a license file, you must have the serial number that is printed on your license certificate. The format of the serial number is a letter that is followed by 10 digits.

For example:

F8573329133

Symantec sends you the file by email as a .zip file attachment. You should ensure that your email program is configured to allow incoming .zip file attachments.

Note: License files are digitally signed. You should not attempt to modify the license file.

To obtain a license file

1. On the Internet, go to the following URL:

   https://licensing.symantec.com

   Your Web browser must support 128-bit encryption to view the site.

2. Follow the on-screen instructions to complete the registration process.

3. When you receive the email message from Symantec that contains the license file, save the license file to a location that is easily accessible.

   The file is delivered as a .zip file attachment. You must extract the file contents from the .zip file. The license file has a .slf extension.

Importing a license file

You must add your license file to activate Symantec Ghost. If you purchase additional licenses, you receive an additional license file.

To add a license file

1. In the Symantec Ghost Console, on the Help menu, click **Register Console > Add Symantec License File**.
2. In the Symantec Ghost Registration Screen window, click **Browse**.
3. In the Open dialog, select the license file (.slf) that you want to import, and then click **Open**.
4. Click **OK**.

Updating Symantec Ghost

LiveUpdate provides Symantec Ghost with updates. It connects to Symantec sites for the following:

- Provide free updates to fix defects and provide additional features to the Symantec Ghost program. LiveUpdate connects to Symantec by the Internet to see if updates are available for Symantec Ghost.
- Update the Symantec Ghost Console if there is a new version. When you update the Symantec Ghost Console you receive the updated client version of the software. The client automatically updates when a task is run.

Symantec may provide updates for Symantec Ghost. Symantec does not charge for these updates. However, your normal Internet access fees apply.

To update Symantec Ghost using LiveUpdate

1. On the Console server, do one of the following:
   - On the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Console**.
   - On the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Explorer**.
2. On the Help menu, click **LiveUpdate**.
3. Follow the on-screen instructions.

About upgrading Symantec Ghost

Symantec Ghost can be upgraded from Symantec Ghost 8.0 or later.

When the Symantec Ghost Console is upgraded or updated, the Console client is updated automatically when a task is run for the client computers.

Note: Due to design changes in the Symantec Ghost Console, Windows Vista/XP/2000 client computers appear as NT4 computers when you first open the Configuration settings window. If you refresh the configuration details from the Symantec Ghost Console, the operating system information displays correctly.

See “Setting Configuration properties” on page 130.

Uninstalling Symantec Ghost

Before remotely uninstalling a client computer, note the following:

- If a client computer is part of a task or a Console resource, the Console does not remove the computer record. After you uninstall the client, you should remove the client computer from any Console task or resource, and then delete it.
- In case configuration details on a client computer have changed since the client was installed, refresh the configuration details from the Symantec Ghost Console.
  See “Setting Configuration properties” on page 130.
- If the Symantec Ghost Console server is on a Windows XP computer, you must alter the server’s computer security settings.
  See “Preparing a Windows Vista/XP client for remote installation” on page 51.

You can also uninstall the Console client on the client computer.

To remotely uninstall a client computer

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Open the folder containing the computer for which you want to uninstall the client.
3. Select the computer.
4. On the Tools menu, click **Client Uninstall**.
5. Click **Yes**.

To uninstall the Console client on the client computer

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. In the Control Panel window, double-click **Add or Remove Programs**.
3. Click **Symantec Ghost Console Client**.
4. Click **Remove**.

To uninstall Symantec Ghost Console

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. In the Control Panel window, double-click **Add or Remove Programs**.
3. Click **Symantec Ghost Console and Standard Tools**.
4. Click **Remove**.

Creating Console Service accounts

During installation, a service is installed called the Configuration Server. This service is responsible for task execution and client communication. One of its roles is to create and remove computer accounts in Windows domains if computers are added to domains during the execution of a task. The Configuration Server is also required when you are changing a computer name or taking an image of a computer that belongs to a domain. To perform this role, a Console Service user account must be created in the domain.

The Configuration Server logs on as this user. The user does not have interactive logon rights and does have the rights to create computer accounts in the domain.

When a Console Service account is created on the domain, the domain is now supported for Configuration Server operations.

You can either create a Console Service account from the Symantec Ghost Console or create a Console Service account manually.

Note: You must set some rights for the account. The user of the Console Service account must have the authority to create an account in the domain.

To create Console Service accounts from the Symantec Ghost Console

1. On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Console**.
2. Do one of the following:
   - On the Tools menu, click **Supported Domains List**.
   - In the First Time Run window, click **Domains**.
     This option is available only when you run the Console for the first time.
3. Click **Add**.
4. Do one of the following to add a domain to the list of supported domains:
   - In the Domain field, type a domain name.
   - Click **Browse** to select a domain.

5. Do one of the following:
   - Check **Create account in the domain**, then type a user name and password to create a Console Service account on the domain.
   - Uncheck **Create account in the domain**.
     You must have previously created a user account on the domain.
6. Click **OK**.

Editing the Console Service account

To increase security, you might want to use the administration tools in Windows to change the password for this the Console Service user account. You must then edit the Console Service account password through the Ghost Console. If you change the user name, you must remove from the supported domains list any domains that have previously been added with this user. You then must add the domains to the new Console Service account.

To edit the Console Service account

1. On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Console**.
2. On the Tools menu, click **Supported Domains List**.
3. In the Domain Administration dialog box, click **Edit**.
4. In the User Name field, type the Console Service account name.
5. In the Password field, type the Console Service password.
6. Click **OK**.
7. Click **Close**.

Removing a domain account

Removing a domain from the Symantec Ghost Console does not remove an account from the domain, only from the Symantec Ghost Console database.

To remove a domain account from the Symantec Ghost Console database

1. On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Console**.
2. On the Tools menu, click **Supported Domains list**.
3. In the Domain Administration dialog box, select the domain to remove.
4. Click **Remove**.

Section 2

Managing computers from the Console

- Managing computers and configuration resources
- Creating tasks
- Executing and scheduling tasks
- Incremental backup regimes and rollbacks
- Migrating users
- Using Client Inventory
- Additional Console options

Chapter 4

Managing computers and configuration resources

This chapter includes the following topics:

About the Symantec Ghost Console

The Symantec Ghost Console lets you do the following:

- Define and execute tasks that automate the restoration of computers from image files

- Create backups
- Save user data
- Transfer files and folders to client computers
- Retrieve files from client computers
- Execute commands on client computers
- Deploy AutoInstall (AI) packages
- Alter the configuration settings on a Console client computer, or a group of Console client computers
- Obtain and view hardware and software inventory data for Client computers
- Migrate user settings
- Run the Microsoft Sysprep application
- Organize and manage your client computers, image files, configuration sets, and other resources required to complete these tasks

Starting the Symantec Ghost Console

The Symantec Ghost Console lets you organize and manage your client computers. You can set up and maintain the image files, configuration sets, and other resources you require. You can also perform tasks such as creating image files, restoring computers, cloning from image files, and configuration updates.

The Console might lose its connection with the database when the Console computer comes back from Windows Standby. If the Console loses its connection with the database, you might need to restart the Console computer. To avoid this issue, you can deactivate Windows Standby on the Console computer.

Note: The Symantec Ghost Console runs in Windows Vista/XP/2000/2003/2008 only.

To open the Symantec Ghost Console

◆ On the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Console**.

Setting properties from the Console

Table 4-1 describes the four groups of properties that you can set globally from the Symantec Ghost Console.

Table 4-1 Global properties

Properties	Description
Console preferences	Settings for the Console, including showing and hiding panes and user messages, and setting the location on the Console server to store backup images and user packages. See "Setting Symantec Ghost Console options" on page 244. See "Setting the location for backup images" on page 166. See "Setting the storage location for user packages" on page 201.
Client properties	Default settings for Client computers. Some of these settings, such as client heartbeat and virtual partition PreOS type, can be overridden at the client level. Other settings, such as client warning and client user interface can only be set globally on the Console. See "Setting the default client heartbeat interval" on page 82. See "Setting the Virtual Partition PreOS" on page 91. See "Setting Symantec Ghost Console options" on page 244.
Data Transfer properties	Default settings for data transfer to and from the Console, and the transfer mode. These can be overridden by each subnet, and again by each task. See "Setting the default data transfer properties" on page 82.
Inventory properties	Default inventory settings. You can show or hide the collected data sets in the Inventory folder, and can specify the default inventory views that apply to a computer when it is detected by the Console. See "Showing the Collected Data folder" on page 209. See "Setting the default Inventory views for new client computers" on page 221.

About Symantec Ghost Console resources

The Symantec Ghost Console contains all the resources that are available for you to use with Symantec Ghost. These include the client computers that you are managing, the tasks you can execute, and the data that is used by the tasks. You can add and remove Symantec Ghost Console resources, and can organize them to suit your requirements.

Table 4-2 describes the Symantec Ghost Console resources.

Table 4-2 Symantec Ghost Console resources

Resource folder name	Description
Machine Groups	This folder contains all the client computers detected by the Console. These resources contain information on each computer's configuration and setup. You can set up groups of computers and you can apply a task to all the computers in the group at the same time. See "Setting up computer groups" on page 79.
Dynamic Machine Groups	This folder contains the dynamic machine groups that you have set up. A dynamic machine group is the result of a filter applied to a computer group, and contains the computers in the target group that match the filter conditions. Each dynamic machine group is treated as a virtual computer group, and can be used as the target of a task. See "Setting up dynamic machine groups" on page 237.
Network	This folder contains all the client computers detected by the Console, grouped by subnet. You can set the network properties for each subnet, to suit your requirements and deal with any network limitations. See "Setting properties for a subnet" on page 84.
Tasks	This folder contains the definitions of tasks that you can run on the client computers. You can create new tasks and modify existing ones. For each task you can define the task steps (such as restore from an image file, or update configuration settings) and the target computer group. See "About tasks" on page 107.
Executed Template tasks	This folder contains tasks that have been executed without being saved. The executed template task can be executed again but none of the settings can be modified. See "About template tasks" on page 108.
Configuration Resources	This folder contains the image definitions and other resources that tasks require. These include computer configuration settings, AI packages, Sysprep configurations, migration templates, and migration packages. See "Configuration Resources" on page 71.

Table 4-2 Symantec Ghost Console resources *(continued)*

Resource folder name	Description
Backup Regimes	This folder contains the definitions of the backups you are making for each client computer. Each computer has its own backup regime, which specifies the backup parameters and whether the backup is scheduled or initiated manually. If the backups are scheduled, the backup regime includes the task and schedule details. See "About incremental backups and backup regimes" on page 165.
Inventory	This folder contains the resources that are used for collecting and displaying inventory information for client computers. These include filters, views, reports, and collected data sets. See "Inventory resources" on page 72.

Configuration Resources

Table 4-3 describes the resources stored in the Configuration Resources folders.

Table 4-3 Configuration Resources folders

Folder name	Description
AI Packages	Stores definitions of AutoInstall (AI) packages. These AI packages are executable files stored in a location that is accessible from the Console server. See "Deploying AutoInstall packages" on page 140.
Configurations	Stores sets of registry parameters. These may be configuration sets for individual computers, or configuration templates for computer groups. See "Setting up configuration sets" on page 96.
Images	Stores information about the image files that are available for cloning tasks. These image files are stored in a location that is accessible from the Console server. See "About image definitions" on page 110.
Sysprep Configurations	Stores the Sysprep configurations.
User Migration Templates	Stores the migration templates that are available for User Migration tasks. See "Creating user migration templates" on page 178.

Table 4-3 Configuration Resources folders *(continued)*

Folder name	Description
User Migration Packages	Stores the migration packages that you save on the Console in a User Migration task. Symantec Ghost stores the migration packages on either the Console server or on the client computer. Only the migration packages that are stored on the Console server are shown in this folder. Migration packages are used in User Migration Restore tasks. See "Managing user packages" on page 199.

Inventory resources

Table 4-4 describes the resources stored in the Inventory folders.

Table 4-4 Inventory folders

Folder name	Description
Collected Data	Stores collected data sets. Each data set defines the Windows Management Interface (WMI) class and properties that are collected from client computers and stored in the inventory database. This folder is hidden by default. See "Managing collected data sets" on page 209.
Filter	Stores the filters that are used in reports and dynamic machine groups. See "Creating and maintaining filters" on page 223.
Report	Stores report definitions. You can create and run reports to extract data from the inventory database. See "Creating and running reports" on page 232.
View	Stores view definitions. You can use views to display selected properties for each client computer, or to display property values in a report. See "Viewing inventory information" on page 216.

Managing Symantec Ghost Console resources

The Symantec Ghost Console resource folders contain the image file definitions, task definitions, configuration sets, and other resources that are available for you to use. You can organize and manage these resources as you want, using a standard set of console options. These options are the same for all resource folders. You can set up the folder structure and move resources within them. You can also view details of Symantec Ghost Console resources, rename them, and delete any that are not part of any task definition.

These procedures are common to most resources. Any exceptions are identified in the appropriate sections.

See "Setting the resource folder view mode" on page 73.

See "Creating new folders" on page 73.

See "Moving Symantec Ghost Console resources" on page 74.

See "Renaming Symantec Ghost Console resources" on page 75.

See "Deleting Symantec Ghost Console resources" on page 75.

See "Viewing Symantec Ghost Console resource properties" on page 76.

Setting the resource folder view mode

You can set the view mode for each resource folder. The view modes are the same as those available in Microsoft Windows Explorer, and the view names are self-explanatory.

To set the resource folder view mode

1 In the Symantec Ghost Console, in the left pane, select the folder for which you want to set the view mode.

2 In the right pane, do one of the following:

- Right-click, click **View**, then click the appropriate option.
- On the View menu, click the appropriate option.

The selected view mode is applied to all subfolders in the Symantec Ghost Console resource folder.

Creating new folders

You can set up the sub-folder structure within each Symantec Ghost Console resource folder, by creating the new folders that you require.

The exceptions to this rule are Dynamic Machine Groups, Network, and Executed Template Tasks. All dynamic machine groups and subnets are stored in the root folder, and you cannot create any subfolders.

To create a new folder

1 In the Symantec Ghost Console, in the left pane, select the folder in which you want to create a new subfolder.

2 In the right pane, do one of the following:

- Right-click, then click **New Folder**.
- On the File menu, click **New > Folder**.

3 Type the new folder name.

The name can be anything you want, up to a maximum of 80 characters, but it cannot be the same as another folder at the same level.

4 Press **Enter** or click anywhere in the Symantec Ghost Console, to confirm the new folder name.

Moving Symantec Ghost Console resources

You can move resources within your folder structure, and organize them to suit your requirements. You move resources by copying or cutting them from one folder, and then pasting them into another folder.

When you move a folder, all resources and subfolders it contains are also moved.

The following restrictions apply to organizing some Symantec Ghost Console resources:

- Network resources (client computers) cannot be moved. The subnet groups are read from your network, and cannot be modified via the Symantec Ghost Console.
- Machine Groups may contain only one copy of a client computer in each top-level group. A top-level group is a folder directly under the Machine Groups folder, and includes all its subfolders.
- Backup Regimes and Dynamic Machine Groups cannot be copied. These folders may contain only one instance of each resource.

To move Symantec Ghost Console resources

1 In the Symantec Ghost Console, in the left pane, expand the folder that contains the resources or folders that you want to move.

2 Do one of the following:

- Right-click the resource or folder, then click **Copy** or **Cut**.
- Select the resources or folders that you want to move then, on the Edit menu, click **Copy** or **Cut**.

Copy creates a new instance of the selected item, leaving the original intact. Cut moves the selected item, removing it from the original location.

3 Open the folder to which you want to move the selected resources or folders.

4 Do one of the following:

- Right-click, then click **Paste**.
- On the Edit menu, click **Paste**.

The selected resources or folders are moved immediately.

You can also use the keyboard shortcuts Ctrl+X, Ctrl+C, and Ctrl+V.

Renaming Symantec Ghost Console resources

You can rename Symantec Ghost Console resources and folders if necessary. You may use any names you want, but you cannot use the same name for two items in the same folder. Folder names must be unique at each level of the folder structure. There are two exceptions: Computers and Collected Data Sets must have unique names. You cannot use the same name for two different computers, or for two collected data sets, anywhere in the Console.

If the resource is a pointer to an external object, such as a client computer or an image file, renaming it simply changes the name in the Symantec Ghost Console. If there are two or more instances of the resource, all instances are renamed. The name of the external object is not affected.

To rename Symantec Ghost Console resources

1 In the Symantec Ghost Console, in the left pane, expand the folder that contains the resources or folder that you want to rename.

2 Do one of the following:

- Right-click the resource or folder, then click **Rename**.
- Select the resource or folder that you want to rename then, on the File menu, click **Rename**.

3 Type the new name.

The name can be anything you want, up to a maximum of 80 characters.

4 Press **Enter** or click anywhere in the Symantec Ghost Console, to confirm the new name.

Deleting Symantec Ghost Console resources

You can delete any folders or Symantec Ghost Console resources that you are no longer using. When you delete a folder, everything inside that folder is also deleted.

You cannot delete anything that is being used by another Symantec Ghost Console resource. For example, you cannot delete a migration template or a computer group that is being used by a task.

If the Symantec Ghost Console resource is a pointer to an external object, such as a client computer or an image file, deleting it simply removes it from the Symantec Ghost Console. The external object is not affected. There is one exception to this rule: when you delete a user package, the external user package file is also deleted.

Client computers are different from other Console resources. When you delete a client computer from the Console, its backup regime is deleted automatically. However, if the computer is still running the Console Client software and is still on the network, the Console detects it and automatically restores it to the Default computer group folder.

Note: When you delete Symantec Ghost Console resources, you cannot restore them again.

To delete Symantec Ghost Console resources

1. In the Symantec Ghost Console, in the left pane, expand the folder that contains the resources or folder that you want to delete.
2. Do one of the following:
   - Right-click the resource or folder, then click **Delete**.
   - Select the resources or folder that you want to delete, then on the File menu, click **Delete**.
   - Press **Delete**
3. Click **Yes** to confirm the deletion.

   The selected resources or folder are deleted immediately.

Viewing Symantec Ghost Console resource properties

You can open a Symantec Ghost Console resource to view its properties. The properties may be descriptive details of the resource, such as an image definition, or they may be the complete set of resource data, such as a migration template.

If necessary, you can make changes to specific resource properties. Each resource has a different set of procedures, so they are not described here. For more information, refer to the section that describes the resource that you want to modify.

Note: You cannot modify a resource if it is being used by an active task.

To view Symantec Ghost Console resource properties

1. In the Symantec Ghost Console, in the left pane, expand the folder that contains the resource for which you want to view properties.
2. In the right pane, do one of the following:
   - Double-click the resource.
   - Right-click the resource, then click **Properties**.
   - Select the resource, then on the File menu, click **Properties**.
3. In the Properties window, view the properties of the resource.

   If necessary, you can make changes to the properties.
4. Click **OK**.

Managing Symantec Ghost Console client computers

The Symantec Ghost Console stores a record for every client computer that it detects. A client computer is detected by the Symantec Ghost Console once the Console client software is installed and set up to connect to that particular Symantec Ghost Console. If there are two or more Symantec Ghost Consoles on the network, each detects its own client computers and ignores the others.

The new client computer automatically appears in the Machine Groups Default folder and in the Network folder, under the subnet on which the client was detected. The default computer name is a combination of the computer name and the last logged-on user name. If DOS is the only operating system that is installed on the client computer, the computer name matches the adapter address of the computer.

The software version and status of each client computer is represented pictorially.

The top half of the Symantec Ghost Console client icon provides client software version information:

A yellow screen	The client computer has the current software version installed.
An exclamation mark in the screen	The client computer does not have the current software version installed.

The bottom half of the Console client icon provides client status information:

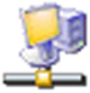
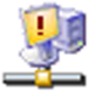
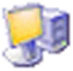
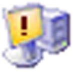
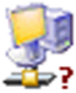
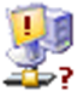
A solid cable — The client computer is online.

No cable — The client computer is offline or unavailable.

A question mark to the right of the cable — The client heartbeat has been set to zero, so the client computer status is unknown.

Table 4-5 displays the Console client computer icons.

Table 4-5 Console client computer icons

	Current software version	Old software version
Online		
Offline or unavailable		
Status is unknown		

You can organize the Symantec Ghost Console client computers into groups. This lets you maximize efficiency by running a task on all the computers in a group at the same time.

See "Setting up computer groups" on page 79.

You can set up the Symantec Ghost Console client computers to suit your requirements. There are several levels at which you can set client computer properties:

Global defaults — These are set in the Symantec Ghost Console, and apply automatically to all clients, unless overridden by network or individual client property settings.

These include properties such as client heartbeat interval, data throughput limits, and virtual partition DOS type.

See "Setting default client and data transfer properties" on page 81.

Network defaults	These are set for each subnet, and apply automatically to all client computers on the subnet, unless overridden by individual client property settings or at the task level. These include properties such as client heartbeat interval, and data throughput limits. See "Setting properties for a subnet" on page 84.
Individual client properties	These are set for each Console client computer. These include client configuration parameters, virtual partition settings, backup regimes, and inventory settings. See "Setting Symantec Ghost Console client computer properties" on page 85.

Setting up computer groups

Grouping computers lets you distinguish among computers with different user requirements. For example, you could create a group of Console client computers for students and a group for teachers. You could then run a task to restore the appropriate image file onto the student computers, and then run another task to restore another image file onto the teacher computers.

Computer group information is stored in folders under the top-level Machine Groups folder in the Symantec Ghost Console. You can have a hierarchy of subgroups under the main groups so that a subgroup can be selected for a task, or you can apply a task to a main group that includes the subgroups.

For example, you might have an Administration folder, and beneath that, an HR folder and a Payroll folder. A computer can be added to any one of these three groups. A task can be applied to either the HR group or the Payroll group. To execute the task for both HR and Payroll, select the Administration folder. The task executes for both the HR group and the Payroll group as well as any computers that are grouped in the Administration folder.

Creating computer groups

The Symantec Ghost Console detects its client computers on the network and automatically adds them to the Default group in the Machine Groups folder. You can use this group if you want, or you can create new computer groups to suit your requirements.

To create a computer group

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group folder in which you want to place the new computer group.
3. Do one of the following:
   - In the Machine Groups pane, right-click, then click **New Folder**.
   - On the File menu, click **New > Folder**.
4. Type a name for the new computer group.
5. Press **Enter** or click anywhere in the Symantec Ghost Console to confirm the name.

   The new group is added to the computer group hierarchy. You can now add computers to this group.

About adding computers to groups

All the client computers must belong to a computer group. By default, all computers are added to the Default group. You can copy or move the computers into other groups as appropriate. A computer may belong to two or more different groups.

There are some restrictions for adding computers to a group as follows:

- You cannot copy or move a computer into the Machine Groups folder. This folder is not a computer group, instead it is a container for your computer groups.
- A computer group may contain only one copy of a computer. Each computer group includes all its subfolders. Therefore each computer may appear only once under each main folder. (A main folder is a folder immediately below the Machine Groups folder.)

To move computers to groups, use the Cut, Copy and Paste options.

See “Moving Symantec Ghost Console resources” on page 74.

About renaming a computer

You can rename a computer for easy identification. The name changes in the Symantec Ghost Console only. The name of the computer is not affected anywhere else. You cannot rename a computer using the same name as another computer in the same folder.

To rename computers, use the Rename option.

See “Renaming Symantec Ghost Console resources” on page 75.

Removing a computer from a computer group

You can remove a computer from a computer group when it is no longer needed. If you have two copies of the same computer in different groups, removing one copy does not remove the other.

To remove a computer from a group, use the Delete option.

See “Deleting Symantec Ghost Console resources” on page 75.

Remember that the Console automatically detects all client computers on the network. You can remove a computer from all computer groups but, if the computer still exists as a client on the network, the Symantec Ghost Console will detect it and add it back to the Default computer group.

If you want to remove a computer from the Symantec Ghost Console, you need to remove the client software, and the Symantec Ghost boot partition (if it exists), before removing the computer from the last group.

To remove a computer from the Symantec Ghost Console

1. Uninstall the client software from the computer.
2. If the client computer is using the Ghost boot partition rather than the virtual partition, remove the boot partition.

   See “Removing the Symantec Ghost boot partition from a client computer” on page 96.
3. Remove the computer from the computer groups in the Symantec Ghost Console.

Setting default client and data transfer properties

You can set default client and data transfer properties in the Console. These settings apply automatically to all client computers and subnets detected by the Symantec Ghost Console. They are used unless you set the subnet, individual computer, or task properties to override them.

You can set the following default client and data transfer properties:

- Client heartbeat interval
  See “Setting the default client heartbeat interval” on page 82.
- Data transfer mode and data throughput limits
  See “Setting the default data transfer properties” on page 82.

Setting the default client heartbeat interval

The client heartbeat interval determines the frequency with which update messages are sent by each client computer to the Symantec Ghost Console. You can change the frequency to reduce network traffic. This can be useful if computers are networked over a WAN.

The default interval set in the Symantec Ghost Console is used for all client computers, unless specifically overridden by the settings for subnet or client.

See "Setting properties for a subnet" on page 84.

See "Setting the client computer heartbeat interval" on page 88.

To set the default client heartbeat interval

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. In the Options window, click the Client tab.
3. Under Client Heartbeat, in the Interval field, type the number of seconds between client update messages.
4. Click **Apply**.

Setting the default data transfer properties

The default data transfer properties determine the data throughput limits and data transfer mode for the entire network. These defaults apply to all subnets and all tasks, unless specifically overridden by the settings for a subnet or a task.

See "Setting properties for a subnet" on page 84.

See "Setting network properties" on page 117.

You can set the following default data transfer properties:

Data throughput limits

You can control how much network bandwidth is used when transferring image files (in a Clone task) and data files (in a Transfer Files task) across the network. By using this functionality, you avoid overloading the network with GhostCasting traffic.

You can set data throughput limits for each subnet, and for each task. The lowest limit is used in each case.

See "Controlling the amount of network bandwidth used" on page 375.

Data transfer mode	You can set the data transfer mode depending on your network hardware setup. Used in conjunction with the network bandwidth limits, you can optimize the way in which image files, data files, and AI packages are transferred over your network. You can set the data transfer mode for each subnet and for each task. The subnet setting overrides the default, and the task setting overrides both the subnet and default.

Table 4-6 lists the data transfer modes that you can select.

Table 4-6 Data transfer modes

Transfer mode	Description
Unicast	Deployment to a single client
Multicast	Simultaneous deployment of an image file or data files to many computers
Direct broadcast	Selective deployment based on direct broadcast for subnet

See "Setting the data transfer mode" on page 373.

To set the default data transfer parameters

1 In the Symantec Ghost Console, on the Tools menu, click **Options**.

2 In the Options window, click the Data Transfer tab.

3 To set the maximum data transfer rate for transferring files or backing up a computer to an image file on the Symantec Ghost Console server, check **Create**, then type the number of megabytes per minute.

4 To set the maximum data transfer rate for transferring files or restoring a computer from an image file on the Symantec Ghost Console server, check **Restore**, then type the number of megabytes per minute.

5 To set the default data transfer mode, under Data Transfer Mode, select the appropriate option:

- Multicast
- Direct Broadcast
- Unicast

6 Click **Apply**.

Setting properties for a subnet

The Network folder contains all the client computers detected by the Symantec Ghost Console, grouped by subnet. If necessary, you can set the properties for each subnet. You may want to do this to work around the limitations of a particular subnet.

By default, all client computers in each subnet use the default properties set in the Symantec Ghost Console. The settings you make for a subnet override the default values but, in turn, may be overridden by the settings for a particular client computer or task.

You can set the following properties for each subnet:

Client heartbeat interval

This overrides the default client heartbeat interval, but is overridden by the setting for individual client computers.

See "Setting the default client heartbeat interval" on page 82.

See "Setting the client computer heartbeat interval" on page 88.

Data throughput limits

You can set default data throughput limits, and set limits for each task. If the limits are set in two or more places, the lowest limit is used.

Data transfer mode

You can set the default data transfer rate and mode for each task.

See "Setting the default data transfer properties" on page 82.

See "Setting network properties" on page 117.

See "Controlling the amount of network bandwidth used" on page 375.

To set properties for a subnet

1 In the Symantec Ghost Console, in the left pane, expand the **Network folder**.

2 In the Network pane, do one of the following:

- Right-click the subnet for which you want to set properties, then click **Properties**.
- Click the subnet for which you want to set properties then, on the File menu, click **Properties**.

The global default values set via the Console are not reflected in the Properties for *Subnet name* window. The values that you see are hardcoded, and may not be the current default settings.

3 In the Properties for *Subnet name* window, to set the time interval between client update messages, check **Client Heartbeat Interval**, then type the number of seconds.

4 To set the maximum data transfer rate for restoring a computer from an image file on the Symantec Ghost Console server, check **Transmit Limit**, then type the number of megabytes per minute.

5 To set the maximum data transfer rate for backing up a computer to an image file on the Symantec Ghost Console server, check **Receive Limit**, then type the number of megabytes per minute.

6 To set the data transfer mode for the subnet, under Data Transfer Mode, select the appropriate option from the following list:

- Multicast
- Directed Broadcast
- Unicast

7 Click **OK**.

Setting Symantec Ghost Console client computer properties

You can view and change the properties for each Symantec Ghost Console client computer.

Table 4-7 lists and describes the client properties.

Table 4-7 Client computer properties

Client computer property	Description
Name	The computer name.
Last image file used to restore the computer	The image file used to restore the computer, if one was used.
Default configuration settings for the client computer	This is the last known configuration for the client computer. The actual configuration may have changed since the client was detected or last updated. You can modify the default configuration if necessary, by editing the settings or copying them from another computer. See "Maintaining the default client configuration settings" on page 89.

Table 4-7 Client computer properties *(continued)*

Client computer property	Description
Heartbeat interval	The client heartbeat interval determines the frequency with which update messages are sent by the client computer to the Symantec Ghost Console. This setting overrides both the global default (set in the Symantec Ghost Console) and the subnet setting. See "Setting the client computer heartbeat interval" on page 88.
Whether or not the Symantec Ghost boot partition is installed	If the Symantec Ghost boot partition is detected, it is used. Otherwise, the virtual partition is used.
The template to use for creating the virtual partition	A network driver template is required for a virtual partition. Symantec Ghost usually automatically selects a default template that is based on the client hardware. If there is no net.drv template for the network card that is installed on the client, then Symantec Ghost selects the Universal Packet Driver as the template. You can change the selection if necessary. For example, if you have an unusual hardware configuration, you can create and use your own custom template. For DOS/NT clients, you must manually select a template. See "Setting the DOS network driver template" on page 93.
The PreOS version installed on the virtual partition	This PreOS version is used for any operation that runs under the PreOS when a task is executed on the client computer. See "Setting the PreOS version for a client computer" on page 94.
Version of the Symantec Ghost Console client software on the computer	If the product version is older than the client, both the client and product version numbers are shown. This can occur when an upgrade is only partially completed.
Details of the backups created for this computer	The name of the backup regime to which the computer belongs, and the list of backups currently stored on the Symantec Ghost Console server. Each backup is identified by date and time, and whether it is a baseline or incremental backup. See "Viewing computer backups" on page 171.

Table 4-7 Client computer properties *(continued)*

Client computer property	Description
Hardware and software inventory information for this computer	The Inventory information is a list of computer properties and their values. You can set up the list to include any properties that you want. See "Viewing inventory information for client computers" on page 221.

To view Symantec Ghost Console client computer properties

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group that contains the computer that you want to view.
3. In the Machine Groups pane, do one of the following:
   - Double-click the computer.
   - Right-click the computer, then click **Properties**.
   - Select the computer, then on the File menu, click **Properties**.
4. In the Properties for *Computer name* window, view the properties for the client computer.

   The Properties for *Computer name* window has several tabs:

   General
   This tab contains the client computer name, adapter address, PCI location, machine ID and the name of the image file used to install the client software.

   Configuration
   This tab contains the default configuration information, and lets you edit the configuration parameters or copy them from another computer.

   Client
   This tab contains the client heartbeat interval, whether or not the client has the Symantec Ghost Boot Partition installed, and the software version information. If the client is using the virtual partition, the DOS version and the template used for creating the virtual partition are shown.

   Backups
   This tab contains details of the incremental and baseline backups created for this computer.

   Inventory
   This tab contains hardware and software inventory information for this computer.

Setting the client computer heartbeat interval

The client heartbeat interval determines the frequency with which update messages are sent by the client computer to the Symantec Ghost Console. The interval you set here overrides both the default set in the Symantec Ghost Console, and the setting for the client's subnet.

If you set the client heartbeat to 0, the client computer has no heartbeat. No update messages are sent by the client computer, and its status is indicated on the Symantec Ghost Console as Unavailable. An unavailable client is still a valid target for a task.

See "Setting the default client heartbeat interval" on page 82.

See "Setting properties for a subnet" on page 84.

To set the client computer heartbeat interval

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group that contains the computer that you want to change.
3. In the Machine Groups pane, do one of the following:
   - Double-click the computer.
   - Right-click the computer, then click **Properties**.
   - Select the computer, then on the File menu, click **Properties**.
4. In the Properties for *Computer name* window, click the Client tab.

   The global default values set via the Console, or the subnet values set in the Network Properties window, are not reflected in the Properties for *Computer name* window. The values you can see are hardcoded, and may not be the current default settings.
5. Check **Heartbeat interval** to set the heartbeat interval for this computer.
6. Specify the heartbeat interval, by typing the appropriate number of seconds.
7. Click **OK**.

Changing a client computer name

You can change a client computer name if necessary.

To change a client computer name

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group that contains the computer that you want to change.
3. In the Machine Groups pane, do one of the following:
   - Double-click the computer.
   - Right-click the computer, then click **Properties**.
   - Select the computer, then on the File menu, click **Properties**.
4. In the Properties for *Computer name* window, click the General tab.
5. In the Name box, type the new computer name.
6. Click **OK**.

Maintaining the default client configuration settings

The Symantec Ghost Console reads the client configuration settings when the client is first detected. These settings are stored in the Symantec Ghost Console. They are not updated automatically if the client computer configuration is changed. This lets you restore the original client configuration settings if required.

To restore the default configuration settings to a client, you need to execute a Configuration task on the client computer. When you set up the Configuration step of the task, select the Default setting.

See "Setting Configuration properties" on page 130.

You can edit the default settings, or copy them to match those on another computer.

When you apply new configuration settings to a computer, the last known configuration shown in the computer's Properties window is not automatically updated. You need to execute a Configuration Refresh task to read the new configuration from the computer.

See "Setting up tasks" on page 119.

To view or edit the default configuration settings

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group that contains the computer that you want to change.

3 In the Machine Groups pane, do one of the following:

- Double-click the computer.
- Right-click the computer, then click **Properties**.
- Select the computer, then on the File menu, click **Properties**.

4 In the Properties for *Computer name* window, click the Configuration tab.

The Last known machine configuration panel shows the configuration that was read from the client computer when the Console first detected it, or when the last Configuration Refresh task was run on it. It is not necessarily the same as the default configuration.

5 To change or view the configuration, click **Edit**.

In the Properties for *Computer name* Default Configuration window, you can change settings as needed.

See “Setting up configuration sets” on page 96.

6 Click **OK**.

7 Click **OK**.

To copy default configuration settings from another computer

1 In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.

2 Expand the computer group that contains the computer that you want to change.

3 In the Machine Groups pane, do one of the following:

- Double-click the computer.
- Right-click the computer, then click **Properties**.
- Select the computer, then on the File menu, click **Properties**.

4 In the Properties for *Computer name* window, click the Configuration tab.

5 To copy the default configuration from another computer, click **Copy**.

In the Select Source window, select the computer from which you want to copy the configuration.

6 Click **OK**.

7 Click **OK**.

About setting up the virtual partition

Each client computer uses a Symantec Ghost boot partition or a virtual partition. To see the type of partition used on each computer, open the computer's Properties window and, on the Client tab, look under PreOS Client Settings.

If any Symantec Ghost Console clients are using a virtual partition, you can set up the virtual partition to suit your requirements. You can specify the default PreOS version to use, and add or edit files as appropriate. The same settings are used for all client computers.

See "Setting the Virtual Partition PreOS" on page 91.

See "Editing files in the virtual partition" on page 92.

You can set the driver template and DOS version for each client computer. The DOS version setting at the client level overrides the default set on the Console.

See "Setting the DOS network driver template" on page 93.

See "Setting the PreOS version for a client computer" on page 94.

Setting the Virtual Partition PreOS

You can choose the default PreOS to use in the virtual partition. This PreOS version is written to the virtual partition of each client computer as part of a task, and used for rebooting the client computer when required.

Both PC-DOS and WinPE are available, both of which are supplied with Symantec Ghost. The default is WinPE. If you want to use DOS, but your computers don't run under PC-DOS, you need to use MS-DOS instead.

Two versions of Win PE are supplied with Symantec Ghost: WinPE, which is designed to run on 256 MB RAM computers, and WinPE-512, which is designed to run on 512 MB computers. Win PE-512 includes more drivers and packages. You need to select the version that you want to use as the default Win PE. You do this in the Windows PE Editor window in the Ghost Boot Wizard.

See "Setting up different versions of Windows PE" on page 259.

Note: MS-DOS is not supplied with Symantec Ghost. You need to obtain an MS-DOS licence, and use the Ghost Boot Wizard to load it before you can use it.

The PreOS version you specify here is the default version for all clients. You can choose a different PreOS version for individual clients, by changing the client property settings.

See "Setting the PreOS version for a client computer" on page 94.

Note: When Symantec Ghost boots a client into WinPE from the virtual partition, it boots into the WinPE Ramdisk environment, removes the virtual partition from the partition table, and restores the partition table and MBR to exactly what was in the operating system before booting into WinPE. It attempts to return the drive letters to what they were in the operating system, with the exception of X:, which is dedicated to the WinPE ramdisk. As soon as the client reboots from WinPE it should go back to the main operating system.

Note: If the client computer has a Ghost Boot Partition installed from an earlier version of Ghost, and you select WinPE as the PreOS, the client uses a virtual partition for WinPE instead of the existing Ghost Boot Partition.

Ghost always reformats (recreates) the Ghost Boot Partition each time the client enters it. This allows the Ghost Boot Partition to be more easily changed for a client.

To set the default PreOS

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. In the Options window, on the Client tab, under Virtual Partition default PreOS, select the PreOS that you want to use:
   - Win PE
   - Win PE-512
     These are the default Win PE versions that are supplied with Symantec Ghost. If you have created any custom versions, they are also listed.
   - PC-DOS
   - MS-DOS
     The MS-DOS option is available only if MS-DOS is available on the Symantec Ghost Console server.
3. Click **Apply**.

Editing files in the virtual partition

The virtual partition can be configured to use a different file or a different setting for a parameter. For example, the IP address or receive mode.

The following settings can be configured from the Symantec Ghost Console:

- PreOS selection: WinPE, PC-DOS, or MS-DOS
- NIC driver

To change other parameters you must add files to the virtual partition or edit the appropriate files, for example, one of the following:

- `Wattcp.cfg`
- `Config.sys`
- `Autoexec.bat`

Setting the DOS network driver template

When the client computer starts in the virtual partition, it uses a template that contains the DOS network drivers that match the client computer's hardware. This template is usually selected automatically by Symantec Ghost when the Symantec Ghost Console first detects the client computer.

Note: If the client computer appears in the Console with the MAC address (adapter address), no template is automatically selected.

If no template is selected, you must make the selection manually before you include the client computer in a task. If a computer with no template is included in a task, the task may fail.

If necessary, you can change the setting for computer groups, or individual client computers.

To set the DOS network driver template for a computer group

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. In the Machine Groups pane, right-click the computer group, then click **Set DOS Template**.
3. In the Browse for template dialog box, select the one that you want.

   The list displays all of the templates that are included with the Symantec Ghost Boot Wizard. You can add and modify a template if necessary.
4. Click **OK**.

To set the DOS network driver template for a client computer

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group that contains the computer that you want to change.
3. In the Machine Groups pane, do one of the following:

- Double-click the computer.
- Right-click the computer, then click **Properties**.
- Select the computer, then on the File menu, click **Properties**.

4 In the Properties for *Computer name* window, click the **Client** tab.

5 In the Network Settings when using Virtual Partition field, specify one of the following options:

- If you want to use the default chosen by the Console, click **Use Suggested Template** and select a template from the drop-down list. The drop-down list displays the templates that are suggested by the Symantec Ghost Console as it connects with the client. If there are no suggested templates, then you must select a template manually.
- If you want to use a different template, click **Use Manually Selected Template**, then click **Browse**.
  The Browse for template dialog box displays all of the templates that are included with the Symantec Ghost Boot Wizard. You can select one of these templates, or add and modify a template.

6 Click **OK**.

Setting the PreOS version for a client computer

You can select the PreOS to install when the virtual partition is created on the client computer. The setting you make here overrides the default setting in the Symantec Ghost Console.

If necessary, you can change the setting for computer groups, or individual client computers.

See “Setting the Virtual Partition PreOS” on page 91.

Note: If the client computer has a Ghost Boot Partition installed from an earlier version of Ghost, and you select WinPE as the PreOS, the client uses a virtual partition for WinPE instead of the existing Ghost Boot Partition.

Ghost always reformats (recreates) the Ghost Boot Partition each time the client enters it. This allows the Ghost Boot Partition to be more easily changed for a client.

To set the PreOS version for a computer group

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. In the Machine Groups pane, right-click the computer group, then click **Set Virtual Partition PreOS**.
3. In the Set Virtual Partition PreOS dialog box, in the drop-down list, select the PreOS that you want to use:
   - Win PE
   - Win PE-512
     These are the default Win PE versions that are supplied with Symantec Ghost. If you have created any custom versions, they are also listed.
   - PC-DOS
   - MS-DOS
     This option is available only if MS-DOS is available on the Symantec Ghost Console server.
4. Click **OK**.

To set the PreOS version for a client computer

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group that contains the computer that you want to change.
3. In the Machine Groups pane, do one of the following:
   - Double-click the computer.
   - Right-click the computer, then click **Properties**.
   - Select the computer, then on the File menu, click **Properties**.
4. In the Properties for *Computer name* window, click the Client tab.
5. In the Virtual Partition PreOS drop-down list, select the version that you want to use.

   You have the following choices:
   - Default
     Use the PreOS version that is specified as the default in the Symantec Ghost Console.
   - Win PE
   - Win PE-512

These are the default Win PE versions that are supplied with Symantec Ghost. If you have created any custom versions, they are also listed.

- PC-DOS
- MS-DOS
  This option is available only if MS-DOS is available on the Symantec Ghost Console server.

6 Click **OK**.

Removing the Symantec Ghost boot partition from a client computer

Once the Symantec Ghost boot partition is installed, it remains on the client computer until you remove it. It is not affected by removing the client software, or most cloning tasks.

If you want to remove the Ghost boot partition, you need to run a cloning task that overwrites it on the client.

To remove the Symantec Ghost boot partition from a computer

1 Create a task that includes a cloning step.

See "Setting up tasks" on page 119.

2 In the Properties for *Task name* window, on the Clone tab, click **Advanced**.

3 In the Advanced Ghost Options window, check **Overwrite Ghost Boot Partition**.

4 Click **OK**.

5 Execute the task on the client computer.

See "Executing tasks" on page 149.

Setting up configuration sets

A configuration set is a group of registry settings that is saved and stored in the Symantec Ghost Console. These settings can be applied to client computers after an image restore task or as a separate configuration task.

There are several types of configuration sets as follows:

Default configuration set

These configuration sets are read directly from the client computers, and are stored on the Symantec Ghost Console server. Each default configuration set applies only to the computer from which it was read, so they are not shown in the Configurations folder, and cannot be applied to any other computers. You can view and change the default configuration set for each computer, by using the Edit option in the computer's Properties window.

Custom configuration set

These configuration sets are stored in the Configurations folder, and must be applied to individual client computers. You can create new custom configuration sets, and modify them to suit your requirements. Each configuration set contains the settings for a single computer.

Template configuration set

These configuration sets are stored in the Configurations folder, and must be applied to groups of computers. They are very similar to custom configuration sets, but have the Allow Template Settings option checked. You need to specify extra settings, such as an IP address range rather than a single IP address, and use wildcard characters in computer-specific properties such as computer names.

When you apply a custom or template configuration set, the settings it contains are applied to the target computer or computer group. Any gaps in the configuration set (where you have disabled the settings) are filled using either the default configuration set for each target computer, or the settings currently on the target computer, whichever you specify in the configuration task.

Note: If you want to preserve any settings on the target computers, you must disable the corresponding settings in the custom or template configuration set that you are using. Specifying a null setting, such as a blank description, is usually treated as a valid setting, and is applied to the target computers.

You must also ensure the default configuration is up to date by running a configuration refresh task before the configuration task.

Creating a new configuration set

You can create as many new custom and template configuration sets as you want.

To create a new configuration set

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **Configurations** folder, then select the folder in which to store the new configuration set.
3. In the Configurations pane, do one of the following:

- Right-click, then click **New Configuration**.
- On the File menu, click **New > Configuration**.

4 In the Properties For New Configuration Set window, type the name for the new configuration set.

The name can be anything you want, up to a maximum of 50 characters, but it must not be the same as another in the same folder.

5 In the Target OS field, select the operating system that this configuration applies to from the following:

- Windows 98
- Windows NT4
- Windows 2000/XP/Vista

6 If you want to create a configuration set template, check **Allow template settings**.

Leave this unchecked if you want to create a custom configuration set.

A template can be applied to a group of computers, but a custom configuration set can be applied to individual computers only.

7 If you want to export settings, click **Export**, select the location in which you want to save the file, type a file name, and then click **Save**.

You can export the configuration settings of a computer to a text file, which you can then use when you apply configuration changes with the Ghconfig tool. This option is enabled only if the configuration set is not a template.

See "Applying a post-clone configuration from the command-line" on page 356.

8 Set the configuration properties.

The properties are listed in the left pane. Click a property to open the corresponding window, and make the appropriate changes.

See "Viewing or modifying configuration sets " on page 98.

9 When you have set all the configuration properties you require, click **OK**.

Viewing or modifying configuration sets

You can open a configuration set to view at any time. For example, you may want to check the content of a configuration set before you use it in a Configuration task. You can modify configuration sets to suit your requirements.

Some characters are not allowed in computer names, domain names, and workgroup names in Windows. Although the Symantec Ghost Console lets you enter these characters, you should verify that the characters are allowed by the target operating system. The following characters might not be allowed:

!#@%&()-.^_{}~

To view or modify a configuration set

1 In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.

2 Expand the **Configurations** folder, then select the folder that contains the configuration set that you want to view.

3 In the Configurations pane, do one of the following:

- Double-click the configuration set.
- Right-click the configuration set, then click **Properties**.
- Select the configuration set, then on the File menu, click **Properties**.

4 In the Properties for *Configuration set name* window, view the configuration properties, then make any appropriate changes.

The configuration properties that you can modify are as follows:

Computer Name	See "Specifying the computer name" on page 99.
Workgroup/Domain membership	See "Specifying the computer workgroup or domain" on page 100.
TCP/IP Settings	See "Applying IP addresses" on page 101.
Default Gateway	See "Setting the default gateway" on page 102.
DNS Configuration	See "Setting the DNS Configuration" on page 103.
WINS Configuration	See "Setting the WINS server address" on page 103.
Novell NetWare Client	See "Applying Novell NetWare client configuration details" on page 104.

5 Click **OK**.

Specifying the computer name

You can specify a computer name and description to apply to the target computer. If you specify a computer name in a configuration set template, you must include at least one asterisk (*) wildcard character. When the configuration set template is applied to a computer group, the wildcard characters are replaced with a number that is unique to each computer. For example, if you create computers for the Administration department, you may set this field to Admin *****.

Note: The number of asterisk (*) wildcard characters specifies the number of digits. You must include sufficient digits for the number of computers in the target group. For example, if there are 10 computers, you must include at least two asterisk (*) wildcard characters.

To specify the computer name

1. In the Properties for *Configuration set name* window, in the left pane, click **Computer Name**.
2. If you want the computer name to be applied as part of the configuration, check **Apply Computer name**.
3. In the space provided, type the computer name.

   If the configuration set is a template, the computer name must contain at least one asterisk (*) wildcard character.
4. If you are setting up a Windows Vista/XP/2000 configuration, and you want the NetBIOS computer name to be applied as part of the configuration, check **Apply NetBIOS Computer name**.

   By default, this name is the same as the computer name.
5. If you want to use a different name, check **Override name**, then in the space provided, type the NetBIOS computer name.

   If the configuration set is a template, the NetBIOS computer name must contain at least one asterisk (*) wildcard character.
6. If you want the computer description to be applied as part of the configuration, check **Apply Computer description**.
7. In the space provided, type the computer description.

Specifying the computer workgroup or domain

You can specify a workgroup or domain to apply to the target computers.

To specify the computer workgroup or domain for Windows Vista/XP/2000 computers

1. In the Properties for *Configuration set name* window, in the left pane, click **Workgroup/Domain Membership**.
2. If you want the computer to be added to a workgroup or domain as part of the configuration, check **Apply Member of**.

3 To add the computer to a workgroup, select **Workgroup**, then type the workgroup name.

To add the computer to a domain, select **Domain**, then complete the following steps.

4 Click the drop-down list, then select the appropriate domain.

If the domain you want isn't in the list, you can add it.

See "To add a new domain to the list" on page 101.

5 If you want to add the computer to an Active Directory container in the domain, check **Add to Active Directory Container**.

The Console must be a member of the domain.

6 Specify the Active Directory container by doing one of the following:

- Type the path to the container, relative to the domain.
- Click **Browse**, then select the container from the list of those available on the domain.
  You must be logged on to the domain to be able to browse for a container.

7 If you want to preserve any computers that are already in a container, uncheck **Move computers that are currently in a container**.

If you leave this checked, all computers are placed in the specified container.

To add a new domain to the list

1 In the Properties for *Configuration set name* window, in the Workgroup/Domain Membership page, click **Domains**.

2 In the Add Domain window, click **Browse**, then select the domain you want to add.

3 If the Symantec Ghost Console does not have an account in the selected domain, check **Create Console Service Account in the domain**, then in the Name and Password boxes, type the appropriate name and password.

4 Click **OK**.

The Symantec Ghost Console service account is validated on the selected domain and then the new domain is added to the list in the Domain field.

Applying IP addresses

You can specify the IP addresses to apply to the target computers. If you are setting up a configuration set template, you can specify a range of IP addresses. The computers in the target group are assigned consecutive addresses starting from the beginning of the range.

You can use DHCP to assign a dynamic IP address, or you can assign a static IP address.

Note: You must ensure that the address range for a template is consistent with the number of computers in the target computer group. If the range is too small, the configuration task fails.

To apply IP addresses

1. In the Properties for *Configuration set name* window, in the left pane, click **TCP/IP Settings**.
2. Specify whether the target computers use dynamic or static IP addresses:
   - To use dynamic IP addresses, select **Target machine uses DHCP server to obtain the IP Address**.
   - To use static IP addresses, select **Target machine has static IP address**.
     If you are using static IP addresses, follow the next three steps to specify the address information.
3. If you want to assign new IP addresses to the target computers, check **Apply IP Address**.
4. If you are setting up a configuration for a single computer, type the IP address.

   If you are setting up a configuration template, in the From and To boxes, type the IP address range for a computer group.
5. In the Subnet Mask box, type the subnet mask.

Setting the default gateway

You can set the default gateway address.

To specify default gateway information

1. In the Properties for *Configuration set name* window, in the left pane, click **Default Gateway**.
2. Check **Apply Default Gateway**.
3. If you need to add a new address, click **Add**.
4. In the Default Gateway IP Address dialog box, type the address.
5. Click **OK**.

   The new address is added to the list.

6 If you want to change any address on the list, select it, then click **Edit**, and make the appropriate changes.

7 If you want to remove an address from the list, select it, then click **Delete**.

Setting the DNS Configuration

You can set the DNS configuration.

To specify DNS configuration information

1 In the Properties for *Configuration set name* window, in the left pane, click **DNS Configuration**.

2 Check **Apply DNS Domain**, then type the domain name.

3 Check **Apply DNS Server Addresses**.

4 If you need to add a new address, click **Add**.

5 In the DNS Server IP Address dialog box, type the address.

6 Click **OK**.

The new address is added to the list.

7 If you want to change any address on the list, select it, then click **Edit**, and make the appropriate changes.

8 If you want to remove an address from the list, select it, then click **Delete**.

9 If necessary, rearrange the list by clicking **Move Up** or **Move Down** to move the selected address by one place.

Setting the WINS server address

You can set the Windows Internet Naming Service (WINS) server address.

To set the WINS server address

1 In the Properties for *Configuration set name* window, in the left pane, click **WINS Configuration**.

2 Check **Apply WINS Server**.

3 If you need to add a new address, click **Add**.

4 In the WINS Server IP Address dialog box, type the address.

5 Click **OK**.

The new address is added to the list.

6 If you want to change any address on the list, select it, then click **Edit**, and make the appropriate changes.

7 If you want to remove an address from the list, select it, then click **Delete**.

8 If necessary, rearrange the list by clicking **Move Up** or **Move Down** to move the selected address by one place.

Applying Novell NetWare client configuration details

You can specify the default Novell NetWare logon information to apply to target computers.

You can set the client computer's default Novell NetWare logon information. Novell NetWare client information can only be applied to client computers that are running the Novell NetWare client.

Table 4-8 shows the versions of Novell NetWare clients supported by Symantec Ghost.

Table 4-8 Supported versions of Novell NetWare clients

Client OS	Novell NetWare version
Windows 2000/XP	Novell NetWare clients version 4.7 and later.

Note: There must be a successful logon to a Novell server from the client or from the model computer before you can apply the configuration details.

The Novell client must be installed before the Ghost client is installed.

When executing tasks on a Windows 2000 client computer, the client will be unable to reboot if it is in the Novell NetWare logon window. It must be logged on or in the Windows Ctrl+Alt+Del logon window.

To specify Novell NetWare client information

1 In the Properties for *Configuration set name* window, in the left pane, click **Novell NetWare Client**.

2 Check **Apply Novell NetWare Client Settings**.

3 In the NetWare Tree box, type the NetWare tree.

4 In the NetWare Context box, type the NetWare context.

5 In the Preferred Server box, type the Novell NetWare preferred server.

6 In the Novell Username box, type the Novell user name.

Erasing and decommissioning client computers

You can erase and decommission a client computer directly from the Console. When you do this, you can choose the security level of the data erasing process: the default is a single pass that writes zeros to the disk, but the secure erase option makes six passes and writes a pattern of zeros and ones. This overwrites the partition's data area before deleting the partition and then wipes the entire disk, partitions, partition table, MBR, and all used and unused space.

You also have the option to recycle the license of the decommissioned computer for use on another computer. Alternatively, you can leave the client intact, which preserves the license and the Ghost partition on the computer. This lets the computer boot up after its disk has been wiped, and resume contact with the Ghost server. You may then run a clone task to restore a new image to the computer.

When you run the Erase Machine task on a client computer, it boots into the PreOS through the virtual partition and runs the appropriate gdisk commands to wipe the hard drive clean of data. If the remove client option is selected, it also reclaims the Ghost license from the client before the system is decommissioned and removes the entry of the client from the Ghost server database.

Note: The Erase Machine task timeout is 48 hours. This is because the secure disk wipe process involves multiple passes over the disk, which can be slow to complete on a large disk. The Console has no contact with the client during this process, and must wait until the disk wipe has been completed. Most other Console tasks have a timeout of about 20 minutes.

To securely erase a computer

1. In the Ghost Console, on the Tools menu, click **Erase Machine**.
2. In the Task Name box, type a suitable name for the erase machine task.

   The erase machine task runs in the same way as any other Console task, and the results are displayed in the task log.
3. In the Target Machine Group or Machine box, specify the computer or computer group that you want to erase.
4. Under Disks to Wipe, specify the appropriate option:

   System Disk

   All Disks (Except USB/FW)

   All Disks

5 If you want to perform the full DoD disk wipe, check **Secure Erase (6-Pass)**.

If you leave this option unchecked, the default quick wipe (single pass) is performed.

6 If you want to recycle the Ghost license from the client to use on another computer, check **Remove Client**.

This erases the Ghost partition on the client computer, and deletes the client from the Console database, freeing up its license for another computer.

If you leave this option unchecked, the Ghost partition is preserved on the client computer, and the client remains in the Console database.

7 Click **Execute**.

Chapter 5

Creating tasks

This chapter includes the following topics:

About tasks

A task is a set of instructions that are carried out by the Symantec Ghost Console. You can create a task to perform any of the following actions on a client computer:

- Create an image file
- Restore an image file
- Apply configuration settings
- Capture and restore user files, application settings, and registry settings
- Install and uninstall AutoInstall packages
- Transfer files and folders between clients and the Ghost server
- Run commands

You can initiate a task from the Ghost Console server or from a client computer.

Creating and executing a Ghost Console task

The Ghost Console lets you manage all of your cloning tasks. There are a number of steps involved in creating and executing such tasks.

To create and execute a Console task

1. Install the Console client software on all client computers.

   See "Installing the Console client" on page 51.

2. Group the Console client computers to create a specific set of target computers to receive the task.

   See "Setting up computer groups" on page 79.

3. Create the task and set up the appropriate task steps.

   See "Setting up tasks" on page 119.

4. Execute the task for a computer or group of computers.

   See "Executing tasks" on page 149.

5. Review the Task Log to check the status of executed tasks.

   See "To view the Task Log" on page 242.

About template tasks

You can create and save a task that does not have all of the required information, which you can use as follows:

- When you create a template task, you can complete most of the fields and then save the task. The minimum requirement for a template task is a task name. You can run the task later after you add the required information.
- You can run a template task from the command line or from a batch file with flexible parameters.

Information that is required but not completed is marked by the following icon: ℹ

Before you can run the task, you must add the required information. If you run the task from the command line, then you can include the required information in the command line. Information that is marked by an icon indicates that the task tab is incomplete. You cannot start a template task from the client computer or schedule a template task.

You can run a template task without saving it. If you run a template task without saving it, then the task is automatically saved in the Executed Template Tasks folder. The Executed Template Tasks folder is emptied on a schedule that is set in the Ghost Console options.

Local deployment of Console resources

The Ghost Console resources are normally stored on the Symantec Ghost Console server, and they are transferred to the client computers when they are used in a task. However, you can store image files, migration packages, and AI packages locally on your client computers. These resources are usually large files. You can store these files on the client computers and run them locally to reduce the load on the network. For example, if you run a clone task to load an image file to a group of computers, it is more efficient to store the image file locally on each computer. If you store the image file on the Console server, the image file must be transferred over the network to every computer in the group when you run the task.

When you create an image file or a migration package, you can choose to store the file locally on the client computer or in the default location on the Console server.

Note: If you store a migration package locally on a client computer, the package does not appear in the Symantec Ghost Console, and you cannot access it from the Console. You must know the name of the migration package and its location on the client computer to use the migration package in a task.

When you restore settings and files from a local migration package, the migration package is automatically preserved on each client computer. If you want to remove it, you must delete it manually.

When you restore a client computer from an image file, you have the option of preserving selected files. By default, the image file is preserved but all other files on the client computer are overwritten. You can choose the files to preserve, and specify which partition they are to be stored in. You may need to do this to preserve a migration package or other resources that are stored on the client computer.

Creating an image of a computer

An image create task lets the Symantec Ghost Console create an image file of a client computer. Image create tasks can be created, copied, changed, and reused as required.

To create an image of a computer

1. Set up the model computer.

   See “Creating a model computer” on page 110.

2. Create the image definition.

   See “Creating image definitions” on page 111.

3. Create the image create task.

   See “Creating an image create task” on page 114.

4. Execute the image create task.

   See “Executing tasks” on page 149.

Creating a model computer

A model computer is used as a template for client computers. This is the first step in creating a Symantec Ghost model image. Set up a computer with the Windows version and all of its drivers installed and configured as you want all of your computers configured. If the computers are to be controlled from the Symantec Ghost Console, install the Console client executable on the model computer.

About image definitions

Image definitions contain details of image files created by Symantec Ghost. Each image definition is a pointer to an image file stored on the Symantec Ghost Console server or on a client machine. The image definition lets you access and manage the image file via the Symantec Ghost Console and use it in a clone task.

You need to provide an image definition for each image create task. You can do this before creating the task, by creating an image definition with no associated image file, or as part of the task creation process. The image create task creates a new image file, and stores it as specified in the image definition.

Image files may be Ghost images (.gho files) or VMWare Disk images (.vmdk files). Note that .vmdk files do not have a Description field, and cannot be used in Ghost Explorer.

You can also create new image definitions for existing image files. For example, you may have some image files that were created elsewhere and manually loaded on to the Symantec Ghost Console server. To add these image files to the Console resources, and make them available for use in restore tasks, you must create image definitions for them.

When an image definition is associated with an image file, it contains the following information:

- Name and location of the image file
- Image file status
- Details of the image file as follows:
  - Partition number
  - Type
  - Original size of the partitions
  - Size of data
- Description of the image file.
  This does not apply to VMWare Disk images.

When an image definition does not have an image file associated with it, or the image file is stored on a client computer, it contains only the name and location of the image file. This is the location to which the image file is saved when the image definition is used in an image create task.

Creating image definitions

You can create image definitions for new images, before the image file itself has been created. You need to do this before you can execute an image create task. You can also create image definitions for image files that already exist on the Symantec Ghost Console server. For example, you may have some image files that were created elsewhere and manually loaded on to the Symantec Ghost Console server.

To create a new image definition

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **Images** folder, then select the folder in which to store the new image definition.
3. In the Images pane, do one of the following:
   - Right-click, then click **New Image**.
   - On the File menu, click **New > Image**.
4. In the Properties For New Image window, in the Name box, type the name for the new image.

   The name can be anything you want, up to a maximum of 50 characters, but it must not be the same as another image definition in the same folder.

5. If you want to save the image file on the client computer, check **Image is located on the Client Machine**, then specify the image file location.

   See "To set the image file location on a client computer" on page 112.

   If you want to save the image file on the Symantec Ghost Console server, or you are creating a definition for an image file that is already stored on the Symantec Ghost Console server, leave this option unchecked, then specify the image file location.

   See "To set the image file location on the Symantec Ghost Console server" on page 113.

6. Click **OK**.

   The new image definition is added to the Images folder.

To set the image file location on a client computer

1. In the Properties For New Image window, under Location, click **Edit**.
2. In the Path to Image File on Client window, under Volume Identifier, select one of the following:

   - Drive letter: Type the drive letter.
   - Volume label: Type the volume label.

3. In the Path box, type the path and name of the image file.

   You do not need to include the file extension. It is automatically appended to the file name when you save the image definition. The default, .gho, is used if you don't specify an image file type.

4. In the Image Type box, specify the image file type.

   Image files may be Ghost images (.gho files) or VMWare Disk images (.vmdk files).

5. Click **OK**.

   If you use this image definition in an image create task, a new image file is created and stored with the specified name and location on the client computer.

   If you use this image definition in a clone task, the task looks for an image file at the specified location and name on each client computer. The Symantec Ghost Console does not validate the path when you create an image definition, so you must ensure that the image file name and location that you type are correct.

To set the image file location on the Symantec Ghost Console server

1 In the Properties For New Image window, under Location, click **Browse**, then do one of the following:

If you are creating a definition for a new image file	1 Select the folder in which you want to store the image file, then type the file name. You do not need to include the file extension in the name. It is automatically appended to the file name when you save the image definition. 2 Specify the image file type. Image files may be Ghost images (.gho files) or VMWare Disk images (.vmdk files). The default, .gho, is used if you don't specify an image file type.
If you are creating a definition for an image file that is already stored on the Symantec Ghost Console server	Select the image file. The file information appears in the Properties for New Image window.

2 If you selected an image file on the Symantec Ghost Console server, you can change the image file description. You cannot change any other details.

Managing image definitions

The Images folder contains the image definitions that you have created and are available for you to use in Recover tasks. The Console provides standard options to help you organize these image definitions as you wish. These options allow you to set up the folder structure, and move items within it as appropriate. You can also rename items, and delete any items that you don't need.

See "Managing Symantec Ghost Console resources" on page 72.

Note: An image definition cannot be deleted if it is part of a task definition.

If you delete an image definition, you are only removing it from the Console. The image file is not affected.

Viewing image details

You can view details of the image associated with each image definition.

To view image details

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **Images** folder, then select the folder that contains the image definition that you want to view.
3. In the Images pane, do one of the following:
   - Double-click the image definition.
   - Right-click the image definition, then click **Properties**.
   - Select the image definition then, on the File menu, click **Properties**.
4. In the Properties for *Image name* window, view the image properties.

   These include image status, and the type and size of each partition.
5. If you want to view full details of the image file, click **Launch Ghost Explorer**.

   This applies only to Ghost image (.gho) files. You cannot view VMWare Disk image (.vmdk) files with Ghost Explorer.

   See "Using Ghost Explorer" on page 323.

Creating an image create task

An image create task is applied to the model computer, and includes the definition of the image file to be created. When you create an image create task, you must select the computer from which to take the image, specify the image definition that is to be associated with it, and optionally set the network and Sysprep parameters.

You can generate an image file without saving the image create task in the Symantec Ghost Console. The procedure is the same as for creating an image create task, but you execute the task immediately to generate the image file from the target computer.

To create an image create task

1. In the Symantec Ghost Console, in the left pane, expand the **Tasks** folder.
2. Expand the folder in which to store the new image create task.
3. In the Tasks pane, do one of the following:
   - Right-click, then click **New Image Create Task**.
   - On the File menu, click **New > Image Create Task**.

4 In Properties for New Task dialog box, in the Name box, type the name for the new image create task.

The name can be anything you want, up to a maximum of 50 characters, but it must not be the same as another task in the same folder. This step is not relevant if you are not saving the image create task.

5 Set the following image create properties on each tab:

General	Specifies the general properties such as the task name, and the drive and partition on the source computer. See "Setting general image create task properties" on page 115.
Network	Sets the data transfer mode and data throughput limits to optimize the way image files are transferred over your network. See "Setting network properties" on page 117.
Sysprep	Facilitates restoring of image files on computers that have different hardware configurations. See "Creating an image with Sysprep" on page 465.

6 Do one of the following:

- To save the task, click **Save**.
  The new task is added to the Tasks folder.
- To run the task, click **Execute**.
  The task runs immediately and is saved in the Executed Template Tasks folder. The lower pane of the Console shows the progress of the task.

Setting general image create task properties

The general image create task properties include the task name, and the drive and partition on the source computer. You can change any of these properties later if necessary.

Symantec Ghost supports "Hot Imaging", which is the ability to capture an image of a computer without leaving Windows. The captured image is based on volume snapshots. If capturing a volume snapshot is unsuccessful, you have the option to automatically revert to using traditional preOS imaging. This feature is available only for clients running Windows XP and Vista. It is not available for clients that are running Windows 2000, nor is it available for clients that are running a server OS, such as Windows 2003.

If you want to create an image from a .v2i, .iv2i (both Backup Exec System Recovery), .pqi (Deploy Center Library), or .vmdk (VMWare Disk) image file, you need to mount the appropriate file as a disk on the source computer. You do this using the Advanced option to add the /ad=filename switch to the Ghost command line. Any mounted image files are given sequential drive IDs starting with 50 (first ID is 50, second is 51, etc.) in the Source Drive box where you select the appropriate drive.

To set general image create task properties

1. In the Properties for *Task Name* window, on the General tab, in the Name box, type a name for the task.

   The name of the task must be unique and can use up to a maximum of 50 characters.

2. Under Source machine, click **Browse**, then from the hierarchy of client computers, select the computer from which you want to take the image, then click **OK**.

   You can select only one computer for an image create task.

3. If necessary, in the Source Drive box, specify the appropriate drive number.

   Any mounted image files are given sequential drive IDs starting with 50.

4. If you want to extract the image of a particular partition on the target computer, check **Partition operation**, then in the Source partition box, type the source partition number.

5. Under Image, in the Name box, click **Browse**, then from the hierarchy of image definitions, select the image definition that you want to use, then click **OK**.

   If the image definition does not yet exist, you can create it now. To do this, select the Images folder, then click **New** to open the Properties for New Image window.

   See “Creating image definitions” on page 111.

6. Under Compression, select the compression level that you want to use from the following list:

   - None
   - Fast
   - High

   The default is fast compression.

   See “Image files and compression” on page 314.

7. If you want the ability to execute the task from the client computer, check **Allow Client Initiation**.

8. Set the authorization password that the client must type in order to execute the task. To do this, click **Set Password**, then type a suitable password.

   The client computer users are prompted to type this password when they try to execute the task.

   See “Initiating a task from a client computer” on page 154.

9. If necessary, check **Remove machine from Domain before taking an image**.

   You must remove the computer from its domain if you are going to roll out the image file to a number of computers. This is not necessary if you are using Sysprep, as Sysprep does this automatically.

10. If you want to enable hot imaging, check **Clone using Volume Snapshot (Hot Imaging)**.

11. If appropriate, check **Fallback to PreOS cloning if cloning using Volume Snapshot failed**.

12. If you want to add any options to the image create task using the command line, click **Advanced**.

    In the Advanced Ghost Options window, add the following information:

    - In the Additional Options for Ghost Command Line box, type the command line switches that you want to use.
      If you want to create an image from a .v2i, .iv2i (both Backup Exec System Recovery), .pqi (Deploy Center Library), or .vmdk (VMWare Disk) image file, you need to mount the appropriate file as a disk on the source computer. You do this by adding the /ad=*image file name* switch to the Ghost command line.

    - If you want to include the Ghost Boot partition in the image, check Include Ghost Boot Partition.
      This is not recommended, and you should do it only when necessary.
      See “To add Advanced features for cloning” on page 127.

Setting network properties

You can set the data transfer mode and data throughput limits to suit your requirements. You can change these settings globally, for a multicast session, and for a task.

See “Optimizing data transfer over the network” on page 118.

You can choose to include target computers that are shut down when the task is executed. This only applies to computers that support Wake on LAN (WOL).

See “Enabling Wake on Lan (WOL)” on page 118.

Optimizing data transfer over the network

You can set the data transfer mode to optimize the use of your network hardware setup. Used in conjunction with the network bandwidth limits, you can optimize the way image files are transferred over your network. The settings you make for a task override the Symantec Ghost Console default settings and the subnet default settings.

See “Setting the default data transfer properties” on page 82.

See “Setting properties for a subnet” on page 84.

To set data transfer mode and network bandwidth limits

1. In the Properties for *Task name* window, click the **Network** tab.
2. To set the data transfer mode for the task, check Data transfer mode, then select one of the following options:
   - Multicast
   - Directed broadcast
   - Unicast
3. To set the maximum data transfer rate between the client computer and the Console server, check **Data throughput limit**, then type the number of megabytes per minute.

Enabling Wake on Lan (WOL)

You can enable Wake on Lan (WOL) to include computers that are shut down when the task is executed. This only applies to computers that support WOL.

Computers must meet the following specifications:

- The motherboard must support WOL.
- The NIC must support WOL.
- There must be a wire connecting the motherboard WOL port to the NIC WOL port.
- The WOL feature must be enabled in BIOS Power Management.
- The connection light on the back of the NIC must be lit when the computer is turned off.

To enable Wake on Lan

1. In the Properties for *Task name* window, in the Network tab, check **Use WOL when executing a task**.
2. If you want to turn off the computers that were started, once the task is executed, check **Shut down machines when task is finished**.

Setting up tasks

A task is a set of instructions carried out by the Symantec Ghost Console, applied to one or more client computers. A task may contain one or more steps.

Table 5-1 lists the available task steps.

Table 5-1 Task steps

Task step	Description
Clone	Restores a specified image file onto a client computer, or group of computers. See "Setting Clone properties" on page 122.
Deploy Anywhere	Retargets an image that has been restored to a client computer that has different hardware from the model computer from which the image was created. See "Setting up the Deploy Anywhere task step" on page 127.
Configuration	Applies the specified configuration settings to the client computers. See "Setting Configuration properties" on page 130.
Refresh Configuration	Reads the configuration from client computers and updates their default configuration settings in the Console. There are no properties to set.
Refresh Inventory	Gathers inventory information from client computers and updates the Inventory database on the Console server. There are no properties to set.
User Migration: Capture	Captures user files, application settings, and registry settings from client computers and stores them in user packages. See "Capturing user data" on page 189.

Table 5-1 Task steps *(continued)*

Task step	Description
User Migration: Restore	Restores user files, application settings, and registry settings from user packages to client computers. See "Restoring user data" on page 195.
Software and File Actions	Installs and uninstalls AutoInstall packages on client computers, transfers files and folders to client computers, retrieves files from client computers, and executes commands on client computers. See "Setting up software and file actions in a task" on page 132.

Creating a task

You can create new tasks and set them up to suit your requirements. Task definitions are stored in the Symantec Ghost Console, and can be managed in the same way as other Console resources.

A task always includes the following components:

General properties, that specify the task name, the steps to include and the target computers.	The target of the task may be a single computer, a machine group, or a dynamic machine group (which is a group of computers that have specified properties, such as a certain amount of available disk space). See "Setting up computer groups" on page 79. See "Setting up dynamic machine groups" on page 237. See "To create a task" on page 121.
Network properties, that specify the data transfer mode and data throughput limits for the task.	See "Setting network properties" on page 117.

The other task steps are optional. You can choose the steps that you want to perform for each task, and set them up to suit your requirements.

If the target of the task is a dynamic machine group, the task icon has a small triangle on the upper left side. If the task is a template task, the task icon is marked as follows:

To create a task

1. In the Symantec Ghost Console, in the left pane, expand the **Tasks** folder.
2. Expand the folder in which to store the new task.
3. In the Tasks pane, do one of the following:
   - Right-click, then click **New Task**.
   - On the File menu, click **New > Task**.
4. In the Properties For New Task window, on the General tab, in the Name box, type the name for the new task.

   The name can be anything you want, up to a maximum of 50 characters, but it must not be the same as another task in the same folder.
5. Under Task Steps, check the task steps that you want to include in this task.

   You must include at least one step in a task.

   When you uncheck a step, the corresponding tab is hidden. Only the tabs relevant to the selected steps are shown.
6. Under Refresh Steps, check the refresh steps that you want to include in this task.

   These steps have no tab associated with them, as you do not need to set any properties.
7. Under Target Machine Group/Machine, click **Browse**, then select the computer, machine group, or dynamic machine group to which you want to apply the task, then click **OK**.
8. If you want the ability to execute the task from the client computer, under Client Initiated Task, check **Allow Client Initiation**.

   You must complete all of the required information in the task before this option is available.
9. Click **Set password**, and then, in the Client Initiation dialog box, type the authorization password that the client user must provide to run the task.

   You must retype the password in the box below to confirm the password. The client users are prompted to type this password when they try to run the task.

   See "Initiating a task from a client computer" on page 154.
10. If you want to override the default network properties for this task, on the Network tab, make the appropriate settings.

    See "Setting network properties" on page 117.

11 On each of the remaining tabs, set the properties for each step that you have included in the task.

For a list of tabs, and references to where you can find complete descriptions, see Table 5-1.

12 Do one of the following:

- To save the task, click **Save**.
  The new task is added to the Tasks folder and is available for use.
- To run the task, click **Execute**.

Setting Clone properties

The Clone step lets you restore image files to client computers. Symantec Ghost lets you restore a computer from any of the following image types: Ghost (.gho), VMWare Disk (.vmdk), Backup Exec System Recovery (.v2i, .iv2i), DeployCenter Library (.pqi).

You can restore an image file to a single computer, or restore the same image to all the computers in a computer group. If you have saved an image file locally on each of the target computers using the same name and location, you can restore them all in a single task.

See "Local deployment of Console resources" on page 109.

Note: If a client computer has had a previous local clone, it may have a File Preservation Metadata File (`FPMFILE`*n*`.DAT`) present in the Ghost boot partition. If such a file exists, you need to remove it before you attempt to reimage the computer. If the file is present, the clone step will fail. You can use a Command execution task to delete the file (the recommended method), or you can delete it manually.

Note: When you restore the same image to multiple computers, they all have the same name, which is the name of the model computer from which the image was created. To correct this, you need to include a configuration step in the task to change the name of each restored client computer. You use a template configuration set for this.

To set Clone properties

1 In the Properties for *Task name* window, click the Clone tab.

2 In the Destination drive box, type a drive number, if required.

3 If you want to restore a single partition in the image file to a particular partition on the target computers, check **Partition restore**, then type a destination partition number.

4 Under Image, click **Browse**, then select the image that you want to restore, then click **OK**.

If the image definition does not yet exist, you can create it now. To do this, click the **Images** folder, then click **New** to open the Properties for New Image window.

See "Creating image definitions" on page 111.

5 If you want to restore a single partition in the image file, under Source partition, select the appropriate partition from the drop-down list.

If the image file does not yet exist, no partitions are defined. You can type a Source Partition number instead.

6 To change the SID on each target computer, check **Use Ghost Walker to perform a SID Change on the target machine**. This option is applicable only if you are cloning a Windows Vista/XP/2000 operating system.

See "Using Ghost Walker" on page 452.

7 If you want to preserve certain files on the target computers, set the file preservation options.

See "Preserving files and folders on client computers" on page 124.

8 If you want to add more advanced features to the task using the command line, set the advanced feature options.

See "Adding Advanced features for cloning" on page 126.

Determining the hard-disk order

If you have multiple types of hard disks on a computer, the BIOS can order them differently than Windows does. The BIOS also orders the disk based on which type of device was used to start the computer. Ghost uses the hard-disk number that is assigned by BIOS. If you have multiple types of hard disks on a computer, you can run Ghost.exe to determine the order of the disks.

Warning: Windows Vista does not order the hard disks on a computer consistently after the computer is restarted or in alignment with the BIOS order. Therefore, the disk order on a Windows Vista computer might vary when the computer is restarted.

To determine the hard-disk order

1. On the client computer, at the command prompt, type the following command to start the client in the boot partition:

   ngctw32 -recovery

2. In the boot partition, type **Ctrl+X** to exit the DOS client.
3. Run Ghost.
4. In Ghost, click **Quit** to exit.

   After you exit Ghost, you can use Ghreboot to restart the computer to Windows.

5. At the command prompt, type the following command to exit the virtual partition:

   ngctdos -hide

Preserving files and folders on client computers

By default, restoring from an image file overwrites every file on the destination partition of the client computer, except the image file if it is stored locally.

During a restore task you can choose to overwrite the image file, or preserve files and folders that you want to keep on the destination partition of the client computer.

Table 5-2 shows some examples of the way in which you can use this feature.

Table 5-2 File preservation examples

Method	Description
Preserve client computer data files and folders.	You can select data files and folders from any of the partitions that are overwritten by the restore operation, but all files are preserved on a single partition. If necessary, to avoid name collisions when preserving files and folders from different partitions, specify the destination name and path for each file or folder.
Save the image file locally.	If you are performing a Clone operation from an image file stored locally, you can preserve the image file.

Table 5-2 File preservation examples *(continued)*

Method	Description
Create and restore a migration package in a single task.	You can combine a User Migration Capture operation, a Clone operation, and a User Migration Restore operation in one task. If you plan to store the package locally, you must preserve the package during the clone operation. You preserve the package in the same way that you preserve other data files on the client computer. You must specify the path and name of the migration package that you want to preserve. When you run the task, the migration package is created and saved on the client computer. The task then preserves the migration package when the client is restored with an image file. Then the User Migration settings are restored on the client.

Any files that are restored from the image with the same name and location as the preserved files are overwritten by the preserved files. To prevent this you can rename files when you select them to preserve.

You can also run file preservation using command-line switches.

See "About Symantec Ghost switches" on page 521.

To set file preservation options

1. In the Properties for *Task name* window, on the Clone tab, click **Preserve**.
2. If you are restoring from a locally deployed image file, it is preserved by default. If you want to overwrite it, uncheck **Preserve Image File**.

   If you want to move or rename the image file you must add the image file to the list of files to preserve.

   See "To add a file to the list" on page 126.
3. Specify the files and folders that you want to preserve by adding them to the list.

   See "To add a file to the list" on page 126.
4. If you need to remove a file or folder from the list, select it, then click **Delete**.
5. In the File Preservation Options window, in the Preservation Partition box, type the number of the partition in which you want the specified files and folders to be stored.

   The preserved files and folders are stored in the partition chosen after the restore operation.
6. Click **OK**.

To add a file to the list

1. In the File Preservation Options window, click **Add**.
2. In the Add File To Preserve window, under Volume Identifier, select one of the following:
   - Drive letter: Type the drive letter.
   - Volume label: Type the volume label.
3. In the Path box, type the full path and name of the file or folder that you want to preserve.
4. Specify what action you want to take if the selected file does not exist in the specified location on the client computer.
   - To halt the task, check **Fail if path doesn't exist**.
     You may want to select this option for important files, to ensure that the task does not run unless they are preserved.
   - To ignore the missing file and continue, leave the option unchecked.
     Any missing files that are ignored are not preserved.
5. If you want to store the file in a different location, or under a different name, in the Rename To box, type the appropriate path and file name.

   If you are preserving files from more than one source partition, you can change the name and path for each file. You may need to do this to avoid collisions or prevent overwriting files that were restored from the image.

   If you leave this box empty, the file is preserved with its original name and location.
6. Click **OK**.

   The file name and path details are added to the list.

Adding Advanced features for cloning

You can set more options for the cloning task using the command-line switches. You can also choose to overwrite the Ghost boot partition, if one exists on the client computer, and you no longer need it.

The command-line switches that you can use for file preservation are as follows:

-preserve	Duplicates the functionality of the File Preservation Options window.
-preserveifexists	Duplicates the functionality of the File Preservation Options window.

-preservedest	Duplicates the functionality of the File Preservation Options window.
-preservedimagedeleteafterclone	Duplicates the functionality of the File Preservation Options window.
-unpreserveimage	
-recover	
-rfile	

See “About Symantec Ghost switches” on page 521.

Warning: The syntax of your command is not checked when the task runs. Therefore, review these instructions carefully to avoid crashing or errors. The consequences of an error could be serious.

To add Advanced features for cloning

1. In the Properties for *Task name* window, on the Clone tab, click **Advanced**.
2. In the Advanced Ghost Options window, in the Additional Options for Ghost Command Line box, type the extra commands.

   See “About Symantec Ghost switches” on page 521.
3. If you want to overwrite the Symantec Ghost DOS boot partition on the client computer, check **Overwrite Ghost Boot Partition**.

   If the image that you are restoring contains a Symantec Ghost DOS boot partition, this option is always checked. The partition in the image must overwrite the corresponding partition in the client computer.

   If the image does not contain a Symantec Ghost DOS boot partition, you can select this option to remove the Ghost boot partition from the client computer.
4. Click **OK**.

Setting up the Deploy Anywhere task step

The Deploy Anywhere feature lets you retarget an image to suit a computer that has different hardware from the model computer from which the image was created. This lets you deploy a generic image to a range of different computers and perform a retargetting of the clients, rather than requiring a separate image for each client hardware set.

You may want to include the Deploy Anywhere task step immediately after the Clone step, to deploy an image and retarget it for the clients in a single task.

Alternatively, you may want to keep the Deploy Anywhere step as a stand-alone task so that you do not have to repeat the Clone step when all that needs to be done is update a few missing drivers.

The Deploy Anywhere task step performs the following actions on each client computer:

- Boots the computer to Win PE.
- Performs the Evaluation step. This searches the computer for all of the required drivers. It starts by asking the hardware what drivers are required, and then finds out what is available on the client.
- If any of the required drivers are not available, a list of missing drivers is passed back to the Console.
- The Console pulls the requested drivers out of the Deploy Anywhere driver database and sends them down to the client.

  If the client cannot be supplied with all of its required drivers, the task fails on that client. Details of all required drivers are shown in the Task log, along with the task status.

  The task failure is handled as specified in the Task Failure Option setting in the Deploy Anywhere task step, which is either leave the client in Win PE, or attempt to boot it up to Windows.

  If the task fails because required drivers are missing, you need to add the missing drivers to the database, and then run the Deploy Anywhere task step again to get them transferred to the client.
- When the client has all the required drivers available, the Retargetting step is performed. This installs all the new drivers and makes any other necessary changes.
- When the retargetting is completed successfully, the client is booted up to Windows.

  If the task fails for any reason, the failure is handled as described above.

The drivers in the Ghost Deploy Anywhere driver database are available for use by the Deploy Anywhere feature when retargetting a client computer, and by the Ghost Boot Wizard when modifying a Win PE version. You can add new drivers to the Ghost Deploy Anywhere driver database if necessary.

The DeployAnywhere feature has some limitations that you need to be aware of:

- You cannot deploy an image that was created from a member of a domain. This is because of a limitation on retrieving the domain user account from the sysprep answer file.

  To work around this limitation, you need to run a configuration step in the Console task to join the domain.

- If you created an image from a member of a workgroup, there is a limitation on retrieving the name of the workgroup from the sysprep answer file. The default name "TempWorkGroup" is used instead.

  To work around this limitation when you deploy the image, you need to run a configuration step in the Console task to join the appropriate workgroup.
- When you deploy an image, it does not generate a unique computer name on each computer to which the image is deployed.

  You need to include a configuration step in the Console task, to ensure that a unique computer name can be applied on each cloned machine.

To set the Deploy Anywhere task failure option

1 In the Properties for *Task name* window, on the Deploy Anywhere tab, under Task Failure Option, do one of the following:

To leave the client computer in Win PE	Check **Remain in PreOS if Deploy Anywhere fails**.
To attempt to boot the client computer to Windows	Uncheck **Remain in PreOS if Deploy Anywhere fails**.

2 Click **Save**.

To add a new driver to the Ghost Deploy Anywhere driver database

1 In the Properties for *Task name* window, on the Deploy Anywhere tab, under Manage Driver Library, click **Manage Drivers**.

2 In the Windows Driver Database Editor window, select the tab to which you want to add the new driver: Network Drivers, or Storage Drivers.

3 Click **Add New Driver**.

4 In the New Windows Driver window, select the driver that you want to add and specify the appropriate driver details:

Location	The folder in which the driver is located. Type the folder path, or click **Browse** and select it.
Friendly Name	A suitable name for the driver. This is used in the Ghost Deploy Anywhere driver database and displayed in the Windows PE Drivers window.
Applicable OS	Specify the operating systems that the driver supports by checking the appropriate check boxes.

5 Click **OK**.

The new driver is added to the list in the Windows Driver Database Editor window.

6 Click **OK**.

Setting Configuration properties

The Configuration step lets you apply configuration settings to client computers.

There are several ways to do this as follows:

Default configurations can be applied to each computer.	The default configuration settings are read from each computer when it first connects to the Symantec Ghost Console. You can view and edit these settings in the computer's Properties window. See "Maintaining the default client configuration settings" on page 89.
A template configuration set can be applied to each computer in a group.	This applies the same configuration settings to each computer in the target group. Any computer-specific settings, such as the computer name or IP address, are adjusted automatically to ensure they are unique.
Custom configuration sets can be applied to each computer.	This applies a configuration set to each computer in the target group. You can choose which configuration set to apply to each computer. If the target of the task is a dynamic machine group, the target computers are not identified until the task is run, so you cannot assign custom configuration sets. You must apply a template or the default configuration settings.

Custom and template configuration sets may not contain all the settings required. You can fill any gaps from the default configuration set for each computer, or you can preserve the configuration settings that are currently on each computer.

Note: If you use the default configuration set to fill gaps in a custom or template configuration set, you must run a configuration refresh task to update the default configuration for each computer before you run the configuration task.

To check the Configuration settings before running the task, view the task scenario.

See "Viewing task details" on page 146.

To apply default configurations to target computers

- In the Properties for *Task name* window, on the Configuration tab, select **Default**.

To apply a configuration template to target computers

1. In the Properties for *Task name* window, on the Configuration tab, select **Template**.
2. Click **Browse**, then in the Select Configuration window, select the template that you want, then click **OK**.

   If you want to view the settings in a template before selecting it, double-click the name to open its Properties window.
3. If you want to fill any gaps in the template with the default configuration settings for each computer, check **Use default settings**.

   If you leave this option unchecked, any gaps in the template configuration set are filled with the settings currently on each computer.

To apply a custom configuration to target computers

1. In the Properties for *Task name* window, on the Configuration tab, select **Custom**.
2. Click **Customize** to open the Custom Configuration window.

   The target computer or computer group folder appears in the left pane, and the Configuration Resources folder appears in the right pane.
3. For each computer to which you want to apply custom configuration settings, in the Configuration Resources folder, select the configuration set and drag it onto the computer.

   If you want to view the settings in a custom configuration set before selecting it, double-click the name to open its Properties window.

   The icon for the configuration set appears below the computer to which it is assigned.
4. If you want to remove a custom configuration set and leave the computer without one assigned, right click the configuration set name, then click **Delete**.
5. Click **OK** to close the Custom Configuration window.
6. If you want to fill any gaps in the custom configuration sets with the default configuration settings for each computer, check **Use default settings**.

   If you leave this option unchecked, any gaps are filled with the settings currently on each computer.

Setting up software and file actions in a task

You can include a number of software and file actions in a task.

The available actions are:

- Install an AI package
- Uninstall an AI package
- Transfer files and folders
- Retrieve a file
- Execute a command.

The actions are performed in the order in which they are listed.

To set up software and file actions in a task

1. In the Properties for *Task name* window, click the **Software and File Actions** tab.
2. Create the software and file actions that you want to include in the task, and place them in the appropriate order.

   You can do any of the following:

To add a new action	Click **Add**.
To modify an existing action	In the Action pane, select the appropriate action and then click **Modify**.
To copy an action	In the Action pane, select the appropriate action and then click **Duplicate**. This lets you create a new action by modifying the settings in an existing one, rather than creating the action from scratch.
To delete an action	In the Action pane, select the appropriate action and then click **Delete**.
To move an action in the list	In the Action pane, select the appropriate action and then click **Move Up** or **Move Down** to move the action up or down one place.

3. Click **Save**.

Transferring files to client computers

You can transfer files and folders from the Symantec Ghost Console server to the operating system or the Ghost partition of the client computer. If you transfer the files to the virtual partition, then the files remain there only while the task is being executed.

You need to select the files and folders that you want to transfer, and specify where to transfer them.

If you transfer files by multicast, you might encounter the following issues:

- When you transfer files to multiple clients by multicast, there is a 20-second delay between each file transfer. Therefore, the task might take longer to run than expected.
- The Ghost Console supports only one multicast file transfer at a time. Multicast file transfers do not run simultaneously.

Warning: Do not attempt to transfer files to the My Documents folder on the client computer in a file transfer task. If you want to move any files to the My Documents folder, use the User Migration feature. User Migration automatically handles the directory mapping required.

See “About migrating users” on page 175.

Note: You may want to hide the folders that contain transferred files on the client computers to prevent the computer users from accessing them. To hide a folder, you need to add the following Execute Command action to the task:

“attrib” +h [pathname]

where [pathname] is the full path and name of the folder that you want to hide, and the target of the command is the Target OS of the client computer.

See “Executing Commands” on page 137.

To set up the list of files to transfer to the client computers

1. In the Properties for *Task name* window, click the **Software and File Actions** tab.
2. Do one of the following:

To add a new file transfer action	1 Click **Add**. 2 In the Deploy Actions window, click **Transfer Files and Folders**. 3 Click **Next**.
To modify an existing file transfer action	In the Action pane, select the appropriate action and then click **Modify**.

3. In the Transfer Files and Folders window, set up the list of files and folders that you want to transfer.

To add a group of files to the list	1 Click **Add Files**. 2 In the browser, go to the folder containing the files that you want to include in the group, select the files, then click **Open**. The selected files are added to the list.
To add a folder to the list	1 Click **Add Folder**. 2 In the browser, go to the folder that you want to include in the group, and then click **OK**. The selected folder is added to the list.
To remove files or folders from the list	Select the appropriate files or folders, and then click **Delete**.

4. Specify where you want to transfer the files and folders by clicking one of the following:

Transfer to the Target Operating System	The destination is the specified path on the client computer's file system.
Transfer to the Ghost Partition	The destination is the Ghost boot partition. If the client is using a virtual partition, the files will remain there only while the task is being executed.

5. In the Destination box, specify the destination path for all the files and folders in the list.

   See "To set the destination path for a group of files" on page 135.

6. Click **Next**.

7 Specify the file transfer action name by clicking one of the following:

Default Name	Use the default name that is shown.
Custom Name	Use the name that is specified in the adjacent box. Type the appropriate name.

8 If appropriate, check **Continue task if the files fail to transfer**.

9 Click **Finish**.

The file transfer action is added to the list in the Software and File Actions tab.

To set the destination path for a group of files

1 In the Transfer Files and Folders window, under Destination, click **Edit**.

2 In the Path on Client Machines window, under Volume Identifier, select one of the following:

- Drive letter: Type the drive letter.
- Volume label: Type the volume label.

3 In the Path box, type the destination path for the group of files.

4 Click **OK**.

The path is added to the Destination box.

Retrieving files from client computers

You can retrieve files from client computers and store them in a specified location on the Ghost server. You can use variables to differentiate files that are retrieved from different clients in the same task.

There are four variables that you can use in a destination path:

- MachineId - our internal unique id for the machine
- Filename - the name of the source file (without any drive or path information)
- FileBase - the same as Filename, but without an extension
- FileExt - the file extension.

You specify variables in a destination path or file name by surrounding them with curly braces, for example **{Filename}**. Variables are not case-sensitive. When you select a destination path in the Console, the default file name is `{FileBase} ({MachineId}).{FileExt}`. This appends the client computer ID to the file that was retrieved from it. You can modify the default to suit your requirements. For example, you may want to place retrieved files in separate subdirectories for each client computer.

To retrieve files from client computers

1. In the Properties for *Task name* window, click the **Software and File Actions** tab.
2. Do one of the following:

To add a new retrieve file action	1 Click **Add**. 2 In the Deploy Actions window, click **Retrieve a File**. 3 Click **Next**.
To modify an existing retrieve file action	In the Action pane, select the appropriate action and then click **Modify**.

3. In the Retrieve Files window, under File Name, specify the file that you want to retrieve.

   See "To specify the file to retrieve" on page 137.
4. Specify where you want to retrieve the file from by clicking one of the following:

Retrieve from the Target Operating System	The file location is the specified path on the client computer's file system.
Retrieve from the Ghost Partition	The file location is the Ghost boot partition.

5. In the Destination File box, specify the destination path and file name:
   - Click **Browse** and then, in the Browse for Folder dialog, select the appropriate destination folder and then click OK.
     The path, and the variables that define the default file name, are shown in the Destination File box. The default file name is `{FileBase}({MachineId}).{FileExt}`, which appends the client computer ID to the file that was retrieved from it.
   - Make any necessary changes to the path and file name.
     You typically use variables to differentiate files that are retrieved from different clients in the same task. You specify a variable in a destination path or file name by surrounding it with curly braces, as in the default file name shown above.

6 Click **Next**.

7 Specify the retrieve file action name by clicking one of the following:

Default Name	Use the default name that is shown.
Custom Name	Use the name that is specified in the adjacent box. Type the appropriate name.

8 If appropriate, check **Continue task if the files are not retrieved**.

9 Click **Finish**.

The retrieve file action is added to the list in the Software and File Actions tab.

To specify the file to retrieve

1 In the Retrieve Files window, under File Name, click **Edit**.

2 In the File Path window, under Volume Identifier, select one of the following:

- Drive letter: Type the drive letter.
- Volume label: Type the volume label.

3 In the Path box, type the full path and file name, including the file extension, of the file that you want to retrieve.

4 Click **OK**.

The specified file path is added to the File Name box.

Executing Commands

Commands are executed in the operating system or the Symantec Ghost partition.

You can specify the acceptable return codes, to ensure that the command action performs to your requirements. Any return codes that are not defined as successful or warning codes are treated as failure codes. You can also specify the action name and whether or not the task is to continue if the action fails.

Note: Using GDisk in the Command step lets you alter partitions during a task.

See “About GDisk” on page 471.

To set up command actions

1. In the Properties for *Task name* window, click the **Software and File Actions** tab.
2. Do one of the following:

To add a new command action	1 Click **Add**. 2 In the Deploy Actions window, click **Execute a Command**. 3 Click **Next**.
To modify an existing command action	In the Action pane, select the appropriate action and then click **Modify**.

3. In the Command box, type the command syntax.

   You must include the full path of the command and any necessary command arguments.
4. If you want to add a command to the list, select the target of the command.

Execute command in the Target Operating System	Execute the command in the operating system. You must include the full path for the command. The path is as follows: C:\Program Files\Symantec\Ghost\Incoming
Execute command in the Ghost Partition	Execute the command in the Ghost partition. You must include the full path for the command. The path is as follows: C:\Ghost\Incoming

5. Click **Next**.
6. If appropriate, check **Wait for the command to finish executing before continuing the task**.
7. Specify the return codes that you want to define as Successful and Warning.

   In the Successful Return Codes and the Warning Return Codes boxes, type the appropriate return codes, separated by commas.

8 Specify the command action name by clicking one of the following:

Default Name	Use the default name that is shown.
Custom Name	Use the name that is specified in the adjacent box. Type the appropriate name.

9 If appropriate, check **Continue task if the command fails to execute**.

10 Click **Finish**.

The command action is added to the list in the Software and File Actions tab.

Using a command to access UNC paths

The Command action operates in the local system security context, which does not usually have access to network resources. To allow the local system security context to access network resources, you need to grant access permission for each computer on which the command will be executed. You can do this by granting the client computers on which the command will execute permission to access those network resources.

Note: Granting read access is probably sufficient for most purposes. However, for initial testing, you may want to start with higher access rights in order to confirm correct operation of the command, and then restrict the access rights later.

Granting a specific machine object permission to access a specific network share does have security implications. If you have any concerns, please discuss this scenario with your site security officer prior to implementation.

Mapped network drives are available only in a user context, so you will not have access to mapped network drives when using a Command action.

For example, if you wanted to execute the following command on some client computers:

\\*MyServer**MyShare**MyApplication.exe MyArgument1 MyArgument2 MyArgument3...*

you would grant the client computers access to *MyServer**MyShare*.

To grant the client computers access to the shared folder

1 On *MyServer*, open Windows Explorer and right-click *MyShare*.

2 Click **Properties** and then, in the Properties window, select the Security tab.

3 Click **Add**, and then click **Object Types**.

4 Click **Computers**, and then specify the appropriate client computers.

You can also paste a list of computers, or optionally click **Advanced** to search for computers by name.

5 Click **OK**.

Deploying AutoInstall packages

AutoInstall (AI) packages let you automate the process of installing and uninstalling applications on client computers. You create the AI packages with Symantec Ghost AutoInstall.

You deploy AI packages to the client computers by including Install AI Package and Uninstall AI Package actions as part of a task that you run from the Symantec Ghost Console. When you set up the actions, you select which AI packages to install and uninstall.

Note: When you create an AI package, you have the option to include an Uninstall command. If you want to be able to uninstall a package from the Symantec Ghost Console in an Uninstall AI Package action, you must include the Uninstall command when you create it.

To deploy AI packages

1 Create the AI package definitions that you require.

See “Creating AI package definitions” on page 141.

2 Create the AI packages you require.

See “How Ghost AutoInstall works” on page 389.

3 Store the AI package files in the appropriate places.

You can store AI package files on the Console server, a shared network drive, an HTTP location, or on the client computer.

If you want to minimize the use of network bandwidth, you can store a copy of each file on every client computer.

See “Storing AI packages” on page 141.

4 Create AI package definitions for the AI package files that you want to use.

See “Creating AI package definitions” on page 141.

5 Create the appropriate task, and add the Install AI Package and Uninstall AI Package actions.

See "Setting up an Install or Uninstall AI Package action" on page 144.

6 Execute the task.

See "Executing tasks" on page 149.

Storing AI packages

AI packages can be stored on the Symantec Ghost Console server, at an HTTP location, on a network share, or locally on each client computer.

See "Local deployment of Console resources" on page 109.

Packages located on a non-UNC (Universal Naming Convention) path are transferred and installed from the client. Packages located on a UNC path are accessed over the network. However, should this fail, these packages are transferred to the client.

The client uses HTTP protocols to access the packages stored at HTTP locations.

If packages are stored on Windows 2000 network shares, other computers cannot access the packages. To enable access, edit the registry on the computer on which the share exists, adding the name of the share to the following registry location:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares

Client computers can then access this share.

Warning: This workaround creates an open share, which does not require a username or password to connect. This is a potential security threat.

Creating AI package definitions

AI packages may be stored on the Symantec Ghost Console server, at an HTTP location, on a network share, or locally on each client computer. To make an AI package available for deployment, you need to create an AI package definition for it. To deploy an AI package, you add the appropriate AI package definition to a Deploy AI Package task.

Each AI package definition contains the name and location of an AI package and, if the package is stored on the Symantec Ghost Console server, it also contains the GUID. The available AI package definitions are stored in the AI Packages folder in the Symantec Ghost Console.

To create a new AI package definition

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **AI Packages** folder, then expand the folder in which to store the new AI package definition.
3. In the AI Packages pane, do one of the following:
   - Right-click, then click **New AI Package**.
   - On the File menu, click **New > AI Package**.
4. In the Properties For New AI Package window, in the Name box, type the name for the new AI package definition.

   The name can be anything you want, up to a maximum of 50 characters, but it must not be the same as another AI package definition in the same folder.
5. If the AI package file is stored on the client computer, check **Package is located on the Client Machine**, then specify the AI package file location.

   See "To specify the AI package file location on a client computer" on page 142.

   If the AI package file is stored on the Console server, a network share, or an HTTP location, leave this option unchecked, then specify the AI package file location.

   See "To specify the AI package file location on the Console server" on page 143.
6. If the package is located on an HTTP path, click **Validate** to verify that the package is a valid AI Package.

   If the package is a valid AI Package, then the Package GUID appears.
7. Click **Launch AI Builder** to start AI Builder and verify the package, if appropriate.
8. Click **OK**.

   The new AI package definition is added to the AI Packages folder.

To specify the AI package file location on a client computer

1. In the Properties For AI Package window, under Location, click **Edit**.
2. In the Path to AI Package on Client window, under Volume Identifier, select one of the following:
   - Drive letter: Type the drive letter.
   - Volume label: Type the volume label.

3 In the Path box, type the full path and name of the AI package file.

4 Click **OK**.

The AI package file name and location are added to the Location box.

Note: When you use this AI package definition in a Deploy AI Package task, the task looks for an AI package file at the specified location and name on each client computer. The Symantec Ghost Console does not validate the path for each client computer when you create an AI package definition. It is up to you to ensure that the package file exists on each client computer in the correct location.

To specify the AI package file location on the Console server

1 In the Properties For AI Package window, under Location, click **Browse**.

2 In the browser, select the AI package file on the Console server.

3 Click **Open**.

The AI package file name and location are added to the Location box, and the package GUID is shown.

Managing AI package definitions

The AI Packages folder contains the AI package definitions that you have created and are available for you to use in Install AI Package actions. The Symantec Ghost Console provides standard options to help you organize AI package definitions. These options allow you to set up the folder structure, and move definitions within it as appropriate. You can also rename definitions, and delete any definitions that you don’t need.

See “Managing Symantec Ghost Console resources” on page 72.

Note: An AI package definition cannot be deleted if it is part of a task definition.

If you delete an AI package definition, you are only removing it from the Console. The AI package file is not affected.

Viewing AI package details

You can view details of the AI package associated with each AI package definition.

To view AI package details

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **AI Packages** folder, then expand the folder that contains the AI package definition that you want to view.
3. In the AI Packages pane, do one of the following:
    - Double-click the package definition.
    - Right-click the package definition, then click **Properties**.
    - Select the package definition, then on the File menu, click **Properties**.
4. In the Properties for *AI package name* window, you can view details such as the package location and GUID.

    The name and location of the package appears. The package can be stored on the Symantec Ghost Console server, on the client computer, on a network share, or at an HTTP location.
5. If you want to view full details of the AI package, click **Launch AI Builder**.

    See "How Ghost AutoInstall works" on page 389.

Setting up an Install or Uninstall AI Package action

You deploy AI packages to client computers by running an Install AI Package action in a task. When you set up the action, you select the target computers, and specify which AI packages to install.

You may not be able to uninstall all the AI packages that you have installed. In the following cases you cannot uninstall an AI package:

The package does not include an Uninstall command.	When each package is built, you have the option to include an Uninstall command. If you do not include this command, you cannot uninstall the package in a Deploy AI Package task. If you want to check whether or not a package includes an Uninstall command, open the package with AI Builder and view its contents.
The package has been rebuilt with a new identifying number (GUID).	The new package cannot uninstall any software that was installed with the package prior to the rebuild. The application checks the GUID to ensure that the same package is used to uninstall software as the one used to install it.

If an AI package does not include an Uninstall command, or if the package has been rebuilt with a new GUID, you must use some other means to uninstall the software from the client computers.

The connection from a client to the Ghost Console might be slow if you use an HTTP connection. You should confirm that the HTTP connection has been successful before you start a second HTTP task.

To set up an Install or Uninstall AI Package action

1 In the Properties for *Task name* window, click the **Software and File Actions** tab.

2 Do one of the following:

To add a new install or uninstall AI package action	1 Click **Add**. 2 In the Deploy Actions window, click **Install an AI package** or **Uninstall an AI package**, whichever is appropriate. 3 Click **Next**.
To modify an existing install or uninstall AI package action	In the Action pane, select the appropriate action and then click **Modify**.

3 In the Install AI Packages or Uninstall AI Packages window, under Package Name, click **Browse**, and then select the AI package that you want to install or uninstall.

4 Specify the Install or Uninstall AI Package action name by clicking one of the following:

Default Name	Use the default name that is shown.
Custom Name	Use the name that is specified in the adjacent box. Type the appropriate name.

5 If appropriate, check **Continue task if the package fails to (un)install**.

6 Click **Finish**.

The Install AI Package or Uninstall AI Package action is added to the list in the Software and File Actions tab.

7 Do one of the following:

To save the task	Click **Save**. The new task is added to the Tasks folder and is available for use.
To run the task	Click **Execute**. The task runs immediately and is saved in the Executed Template Tasks folder. The lower pane of the Console shows the progress of the task.

Viewing task details

You can check the details of a task before you execute it, by viewing a Task Scenario. When you view a task scenario, the Symantec Ghost Console validates the properties and settings of the selected task and displays full details of each step, including any possible reasons for failure.

The Task Scenario includes the following information:

- The steps in the task, and the order in which they are performed
- The number of computers in the target group
- The name of each computer in the target group
- The network settings for data transfer mode and data throughput limit
- Details of each step in the task

This is essentially the information that has been set on each tab of the Properties for *Task name* window. The settings for each step are validated and, if any possible reasons for failure are found, a warning message is displayed.

The task scenario details are displayed in an instance of your default browser, letting you use the browser functions to save the HTML, print it, or send it to an email address. You can view multiple task scenarios simultaneously - each scenario opens a new browser.

To view task details

1 In the Symantec Ghost Console, in the left pane, expand the **Tasks** folder.

2 In the Tasks pane, do one of the following:

- Open the task that you want to view, then in the Properties for *Task Name* window, on the General tab, click **Task Scenario**.
- Select the task that you want to view, then on the View menu, click **Task Scenario**.
- Right-click the task, then click **Task Scenario**.

The Symantec Ghost Console validates the properties and settings of the selected task. This may take a few moments.

When the validation is complete, a browser opens, displaying the task scenario details.

If the Console finds an obvious reason why the task would fail, such as having no computers in the target group, or no image file for a restore step, it stops the validation immediately. The task scenario shows the task information up to the point of failure, where a warning message is shown. No further information is shown. You must modify the task to correct the problem, and generate the task scenario again.

Chapter 6

Executing and scheduling tasks

This chapter includes the following topics:

- Executing tasks
- Scheduling tasks

Executing tasks

Once defined, tasks can be executed at any time. You can execute tasks on a scheduled basis, from the Symantec Ghost Console or from the client.

See "Executing a task from the Symantec Ghost Console" on page 150.

See "Executing a recovery task" on page 153.

See "Initiating a task from a client computer" on page 154.

See "Initiating a task from the command line" on page 155.

You can view tasks that are currently executing in the bottom pane of the Symantec Ghost Console.

See "Setting Symantec Ghost Console options" on page 244.

All tasks are logged. If any problems occur, you can access the logs from the Console.

See "Monitoring Symantec Ghost Console activity" on page 241.

A task may fail to execute if the correct network drivers are not found. If the task log indicates a failure for this reason, amend the computer properties to use the correct template.

See "Managing Symantec Ghost Console client computers" on page 77.

Executing a task from the Symantec Ghost Console

You can execute a task manually at any time from the Symantec Ghost Console. You can run tasks concurrently.

Before tasks are executed, the following information is checked:

- The validity of an image file to be restored.
- Whether or not a target computer is included in more than one task.
  If you run two tasks that have the same target computer, the first task executes for that computer. The second task does not start.

Table 6-1 lists the task execution modes available from the Symantec Ghost Console.

Table 6-1 Task execution modes

Mode	Description
Execute	You can use this mode for any task. The task is executed immediately, and uses the network settings in the task definition. See "Executing a task manually" on page 150.
Advanced Execute	You can use this mode only for cloning tasks. This mode lets you override the data-transfer mode and the data-throughput limit that are defined in the task. The network settings apply only for this instance, and they do not change the task definition. You can also use this mode to set the logging parameters for the GhostCastChange SIDs using the Symantec Ghost utility Ghost Walker. Symantec Ghost also supports Microsoft Sysprep. server. You can set the logging parameters on the GhostCast server. You can use the GhostCast server's logs to diagnose problems if the data transfer is slow. See "Executing a Clone task manually" on page 151.
Execute as Recovery Task	You can use this mode to recover from a failed task. See "Executing a recovery task" on page 153.

Executing a task manually

You can execute a task manually. You can execute a saved task from the Tasks folder or from the Executed Template Tasks folder. You also can execute a saved task or an unsaved task from the task's Properties dialog box.

After you run a template task it is saved in the Executed Template Tasks folder. Any task information that you had to add is also saved in the task. The original template task is left unchanged in the Tasks folder. If you try to execute a template task that has incomplete information then the Properties dialog box opens and you are prompted to complete the missing information first.

To execute a task manually from a task folder

1. In the Symantec Ghost Console, in the left pane, expand one of the following:
   - The **Tasks** folder
   - The **Executed Template Tasks** folder
2. Expand the folder that contains the task that you want to execute.
3. Right-click the task, then click **Execute Task**.
4. In the confirmation dialog box, click **Yes**.

To execute a task manually from the task's Properties dialog box

1. In the Symantec Ghost Console, in the left pane, expand one of the following:
   - The **Tasks** folder
   - The **Executed Template Tasks** folder
2. Expand the folder that contains the task that you want to execute.
3. Double-click the task.
4. In the Properties dialog box, click **Execute**.

If they are enabled in the Console, start task and end task confirmation messages are displayed. These are for your information only, and do not control the task execution.

The Active Task pane (the bottom pane of the Symantec Ghost Console) shows the progress of the task as it executes.

If you want to enable or disable the confirmation messages, or hide the Active Task pane, you can do so in the Ghost Console options.

See "Setting Symantec Ghost Console options" on page 244.

Executing a Clone task manually

You can override the network settings in the task definition, and can set the logging parameters for the GhostCast server. The network settings apply only for this execution, and do not change the task definition. The logging parameters are set on the GhostCast server. You may want to use the GhostCast server logs to diagnose problems if the data transfer is very slow.

See “About GhostCasting” on page 363.

To execute a clone task manually

1. In the Symantec Ghost Console, in the left pane, expand one of the following:
   - The **Tasks** folder.
   - The **Executed Template Tasks** folder.
2. Expand the folder that contains the clone task that you want to execute.
3. Do one of the following:
   - Right-click the task, then click **Advanced Execute**.
   - Select the task, then on the File menu, click **Advanced Execute**.
4. In the Task Execution Options window, if you want to log the task, check **Log Data Transfer Information**.
5. If you are logging the task, specify the logging properties:
   - Under Log Level, in the drop-down list, select the event level that you want to log.
   - In the Log File box, type the full path and name of the log file to use, or click **Browse** to select it.
6. If you want to set the data transfer mode for the task, check **Data Transfer Mode**, then select one of the following:
   - Multicast
   - Directed Broadcast
   - Unicast
7. To set the maximum data transfer rate between the Console server and the client computer, check **Data throughput limit**, then type the number of megabytes per minute.

   The data transfer settings replace the corresponding settings on the Network tab in the task definition.
8. Click **OK**.
9. In the confirmation dialog, click **Yes**.

The Active Task pane (the bottom pane of the Symantec Ghost Console) shows the progress of the task as it executes.

Executing a recovery task

If a clone task that includes preserved files fails and the client is left in the Ghost partition unable to start in Windows, you can execute a recovery task that is a simplified version of the failed task. A recovery task attempts to restore those clients on which the original task failed and recover the preserved files that were specified in the original task. It does not attempt any steps previous to the clone step.

To execute a recovery task

1. In the Symantec Ghost Console, in the left pane, expand one of the following:
   - The **Tasks** folder.
   - The **Executed Template Tasks** folder.
2. Expand the folder that contains the clone task that you want to execute.
3. Do one of the following:
   - Right-click the task, then click **Execute as Recovery Task**.
   - Select the task, then on the File menu, click **Execute as Recovery Task**.
4. In the Properties for Recovery Task window, make any necessary changes.

   If the recovery task is in the Executed Template Task folder, then you cannot change the task.
5. Click **OK**.

   The task starts immediately. There is no confirmation message. The Active Task pane shows the progress of the task as it executes.

Canceling a task that is executing

You can cancel a task that is currently executing. In order to do this, you need to have the Active Task pane of the Console displayed. If necessary, enable the Active Task pane in the Console by clicking View > Active Task Pane.

When you cancel a task, Symantec Ghost does not stop the task immediately. It continues executing the task until it can hand over control to the client computer. This ensures that all the client computers are left in a stable state.

Note: Any in-progress file transfer must be completed before the task can stop. This may take a few minutes for large files such as images or AI packages.

To cancel a task that is executing

1. In the Symantec Ghost Console, in the Active Task pane, right-click the task that you want to cancel.
2. Click **Cancel**.
3. In the confirmation dialog, click **Yes**.
4. In the message dialog, click **OK**.

   The process may take a few minutes.

Initiating a task from a client computer

A task can be initiated from the client computer if Allow Client Initiation is checked in the task definition and Enable Client User Interface is checked in the Console Options window on the Client tab. All the resources that are used by a client-initiated task must reside on either the client computer or on the Console computer.

If a task is set up to run from a client, then you can initiate the execution of the task from the client computer. End users can execute tasks, or administrators can execute tasks immediately from the client without having to return to the Console server.

Both global and task settings must allow for client-initiated tasks.

See “Creating a task” on page 120.

See “Setting Symantec Ghost Console options” on page 244.

Note: You cannot initiate a template task or a task that targets a computer in a Dynamic Machine Group from the client computer.

Warning: Unless a password is required to execute the task, there is no confirmation required. The task executes immediately.

To initiate a task from a client computer

1. On the client computer, click the Symantec Ghost Client icon.
2. On the pop-up menu, select the task to execute.
3. In the Password box, type the password for the task.

   If no password was set in the Symantec Ghost Console task window, then this window does not appear.

Initiating a task from the command line

You can initiate a task from the command line in the Console server or from the command line in a client computer. You cannot initiate a template task from a client computer.

To initiate a task from the Console server command line

- In the Console server command line, type:

  ngcons.exe /e taskname

To initiate a task from the client command line or a batch file

- In the client command line or batch file, type:

  ```
  ngctw32.exe -initiate taskname [password]
  ```

  You must include the task name in this command and the password, if required. There is no notification if the task has succeeded or failed.

Console command-line switches

You can run a task from the command line by using command-line switches. Each switch corresponds to a Ghost Console object. Any parameters that you type in the command line override the parameters that are saved in the task definition. For example, you can use a command-line switch to run a task on a different target computer than the one that is specified in the task definition.

Every task that you run from the command line is saved in the Executed Template Tasks folder. Any errors or warnings that occur as the task runs are logged in the ConsoleLog.txt file. You can use this file to help diagnose any problems that occurred. The ConsoleLog.txt file is saved in the installation directory.

If a resource is stored in a folder, you must include the full path to the resource in the command line, for example: "My Configurations\Win2k\config".

Table 6-2 lists the switches that you can use with a template task.

Table 6-2 Task command-line switches

Switch	Task type	Description
/t target_name	All task types	The target computer or machine group. You must type the computer name or machine group name exactly as it appears in the Ghost Console. You can specify a dynamic machine group. You must specify the full path to the computer or machine group, for example: AKSITE\SALES\SMITH_A, but you do not need to include the _username section of the computer name.
/dd 1	Clone	The destination drive. The default value is drive one. This switch corresponds to the Destination Drive setting in a Clone task.
/dp 1	Clone	The destination partition. This switch is used only for partition operations. This switch corresponds to the Destination Partition setting in a Clone task.
/sp 1	Clone	The source partition. This switch is used only for partition operations. This switch corresponds to the Source Partition setting in a Clone task.
/img image_name	Clone	The image definition name. This name corresponds to the Image Name setting in a Clone task.

Table 6-2 Task command-line switches *(continued)*

Switch	Task type	Description
/conf 1|2:template_name	Configuration	The configuration set. The parameters for this command are as follows: ■ 1: The default configuration set. This switch corresponds to the default configuration setting in a Configuration task. ■ 2: The template configuration set. this switch corresponds to the template configuration setting in a Configuration task. ■ template_name: The name of the configuration set resource. You cannot apply custom configuration sets from the command line.
/tfd 1|2|3:c:\folder_path	Transfer files	The directory to which the files are transferred. The parameters are as follows: ■ 1: The Ghost partition. ■ 2: A specified path. This switch must be used with the /tfs switch. You can use multiple pairs of the /tfs switch and the /tfd switch.
/tfs c:\source_path	Transfer files	The source directory for the files in a file transfer task. This switch must be used with the /tfd switch. You can use multiple pairs of the /tfs switch and the /tfd switch.

Table 6-2 Task command-line switches *(continued)*

Switch	Task type	Description
/cmd 1:c:\command.exe 2:\c:\command.exe	Execute Command	The command that you want to execute. The parameters are as follows: ■ 1: Runs the command in the target operating system. ■ 2: Runs the command in the Ghost partition.
/cmdarg "/batchfile 1"	Execute Command	A batch file that contains the command arguments that you want to use with the /cmd switch. You can use multiple pairs of /cmd and /cmdarg.
/ai 1:ai_package 2:ai_package2	Deploy AI Package	Deploys an AutoInstall package. The parameters are as follows: ■ Ai_package: The name of the AutoInstall package resource name. ■ 1: Installs the package. ■ 2: Removes a package. You can use this switch multiple times.
/mcn package_name	User Migration: Capture	The name of the user-migration package that you want to create. This name corresponds to the package name that is specified in the User Migration: Restore task.
/mt template_name	User Migration: Capture	The name of the user-migration template. This switch corresponds to the Migration Template setting in the User Migration: Capture task. You can use this switch multiple times.

Table 6-2 Task command-line switches *(continued)*

Switch	Task type	Description
/mrn package_name	User Migration: Restore	The name of the migration package that you want to restore. This name corresponds to the package name that is specified in the User Migration: Capture task.
/s script.txt		The path name and file name of the script that you want to run. The script should include the commands and switches that you want to use. You must type each command on a separate line. Use # at the beginning of the line to signify a comment. For example, the following script runs a task named Test on the Default machine group and applies the my_template configuration set. /e test /t Default /conf 2:my_template

Scheduling tasks

You can schedule tasks to run automatically from the Symantec Ghost Console.

Backup regimes may include scheduled backup tasks. Backup task schedules are very similar to scheduled tasks.

You can set up a schedule for a task at any time. A task may have two or more schedules, but each schedule may contain only one task.

The procedure for setting up a backup schedule is identical to that for a task. The only difference is that there is no Scheduler window in which to view the entire list of backup task schedules.

Note: You cannot schedule a template task.

To create a schedule for a task

1. In the Symantec Ghost Console, on the View menu, click **Scheduler**.
2. In the Symantec Console Scheduler, on the Task menu, click **New Task**.
3. In the Select Task window, select the task that you want to schedule, then click **OK**.
4. In the Ghost Console Scheduled Tasks window, on the Task tab, set the schedule task properties.

   See "Setting the schedule task properties" on page 160.
5. In the Ghost Console Scheduled Tasks window, on the Schedule tab, specify the schedule details.

   See "Specifying schedule details" on page 161.
6. Click **OK**.

   The new task is added to the list in the Scheduler.

Setting the schedule task properties

You can specify the properties for the task that is being scheduled.

To set the schedule task properties

1. In the Ghost Console Scheduled Tasks window, on the Task tab, in the Run box, view the schedule task executable name.
2. In the Comments box, type any appropriate comments for the scheduled task.

   For example, you can identify each backup regime.
3. In the Run as box, type the user name of the person who is running the task.

   The default is the logged on user.
4. Click **Set Password**.
5. In the Password box, type your password.
6. In the Confirm Password box, type your password again to confirm that it is entered correctly.

7 Click **OK**.

A password must be set for scheduled tasks to execute. The password is validated when the task runs.

8 If you need to enable the schedule, check **Enabled**.

This option lets you enable or disable the schedule without deleting it or losing any of the schedule details. If you don't want the scheduled task to run, uncheck **Enabled**. When you want the scheduled task to run again, check **Enabled** to restore it.

A disabled scheduled task is indicated on the schedule list as Next Run Time = never. All the enabled tasks show the next run time, as set in the schedule.

Specifying schedule details

There are a number of different schedule types. You need to select the schedule type that you want, and then specify the appropriate details.

You can have multiple schedule types for the same scheduled task. Details of all schedules are shown on the Schedule tab, and you can add or delete them as required. Multiple schedule tasks are only one entry on the Scheduler list.

Table 6-3 describes the available schedule types

Table 6-3 Schedule types

Type	Description
Daily	The scheduled task is run at a specified time each day. You need to specify the time.
Weekly	The scheduled task is run at a specified time on particular days of each week. You need to specify the time and the days of the week.
Monthly	The scheduled task is run at a specified time on particular days of each selected month. You need to specify the time and the days of the month, and select the appropriate calendar months.
Once	The scheduled task is run at a specified date and time. You need to specify the date and time.
At System Startup At Logon When Idle	These schedule types are not relevant to client computers. Do not use them.

To specify the schedule details

1. In the Ghost Console Scheduled Tasks window, click the Schedule tab.
2. Under Schedule Task, select the schedule type from the following list, then set the appropriate details:

Daily	See "To set up a daily schedule" on page 162.
Weekly	See "To set up a weekly schedule" on page 162.
Monthly	See "To set up a monthly schedule" on page 162.
Once	See "To set up a once-only schedule" on page 163.

3. If you want to set up two or more schedules for the same task, check **Show Multiple Schedules**.
4. Click **New** to add each new schedule, then specify the appropriate details.

   Repeat step 2 for each new schedule.
5. If you want to delete a schedule, select it in the list, then click **Delete**.

To set up a daily schedule

1. In the Start Time box, type the time at which the task should start.
2. If you don't want to run the task every day, but at regular intervals of two or more days, in the Every X days box, type the number of days.

To set up a weekly schedule

1. In the Start Time box, type the time at which the task should start.
2. If you don't want to run the task every week, but at regular intervals of two or more weeks, in the Every X weeks box, type the number of weeks.
3. Under Schedule Task Weekly, select the days of the week on which the task should run.

To set up a monthly schedule

1. In the Start Time box, type the time at which the task should start.
2. Under Schedule Task Monthly, specify the day of the month on which the task should run. You can set either of the following:
   - The number of the day, such as the 17th or 23rd.
   - The number of a particular weekday, such as the second Monday.
3. Click **Select Months**, then select the calendar months on which the task should run.

To set up a once-only schedule

1. In the Start Time box, type the time at which the task should start.
2. In the Run On box, select the date on which to run.

Viewing or modifying a schedule

You can view details of scheduled tasks and make any necessary changes to the schedule.

To view or modify a schedule

1. In the Symantec Console Scheduler, do one of the following:
   - Double-click the task that you want to change.
   - Right-click the task, then click **Properties**.
   - Select the task, then on the Task menu, click **Properties**.
2. In the Properties window, make the changes.

   See "Scheduling tasks" on page 159.

Chapter 7

Incremental backup regimes and rollbacks

This chapter includes the following topics:

About incremental backups and backup regimes

Incremental backups ensure that personal or company information that is stored on client computers is retrievable. The Symantec Ghost Console lets you schedule incremental backups, create them manually, and roll them back as required.

The backup regime contains a number of settings that determine how and when a backup is completed. This allows for the regular scheduling of a backup.

The first backup of a client computer is stored as the baseline image. Each subsequent backup is an incremental image. Only the changes made since the last backup are stored. However, if the changes are too large to be stored as an incremental image, a new baseline image is created and stored.

A full baseline image is automatically created when the size of an incremental backup image is equal to or greater than 2 gigabytes. A baseline is also automatically created when fundamental changes such as the following examples are made:

- Installation of service packs
- Installation of Microsoft applications
- Installation of drivers
- Changes to files that are protected by the operating system

You should create a new baseline image after every five incremental images. You can specify a maximum time between the creation of baseline images.

Symantec Ghost saves the incremental backups as AI Snapshot.exe files. You should not manually run an incremental backup.

Note: Creating a backup of a Windows 2000 computer which has a mapped network drive may fail with a client timeout error. This is because the backup process boots into Windows to create a baseline snapshot and then waits for the password in order to reconnect to the network. To work around this limitation, you should disable the "Reconnect at logon" option for mapped network drives before creating the backup.

Incremental backup platform support

You can deploy any incremental backup that you have created with a version of Symantec Ghost previous to 11.5.

Incremental backups of 64-bit operating systems are not supported.

Setting the location for backup images

You can specify the location in which to store the backup images. You might need to change this location to ensure there is enough disk space available for the images. The default location is as follows:

C:\Documents and Settings\All Users\Application Data\Symantec\Ghost\Backups\

To set the location for backup images

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. On the Preferences tab, under Backup Regime, specify the location in which you want to store the backup images.

   You can type the full directory path, or click Browse to select it from the file system.
3. Click **Apply**.

Setting up backup regimes

Each backup regime contains a number of settings that determine how and when a backup image is completed. You can create a backup regime for each client computer and may modify them at any time.

Backup images are stored in the directory specified in the Console Options dialog box. You can set the location of this directory to suit your requirements.

See “Setting the location for backup images” on page 166.

To create a new backup regime

1. In the Symantec Ghost Console, in the left pane, expand the **Backup Regimes** folder.
2. Select the parent folder in which to place the new backup regime.
3. Do one of the following:
   - In the Backup Regimes pane, right-click, then click **New Backup Regime**.
   - On the File menu, click **New > Backup Regime**.
4. In the Properties for New Backup Regime window, on the Properties tab, specify the properties.

   See “Setting backup regime properties” on page 168.

   Steps 5 and 6 apply only if you are scheduling the backup. If you don’t set up a schedule, you must execute the backup manually.
5. On the Task tab, type the schedule task details.

   You must set the user name and password that authorizes the backup task to run on the Console server.

   See “Setting the schedule task properties” on page 160.

6. On the Schedule tab, type the schedule details.

   The client becomes temporarily unavailable to the end-user when you take a backup image. You should consider scheduling the backup regime to occur during off-peak times.

   See “Specifying schedule details” on page 161.

7. Click **OK**.

Setting backup regime properties

The backup regime properties include the name of the computer being backed up, the minimum number of days to keep backups, and whether or not the backups are scheduled.

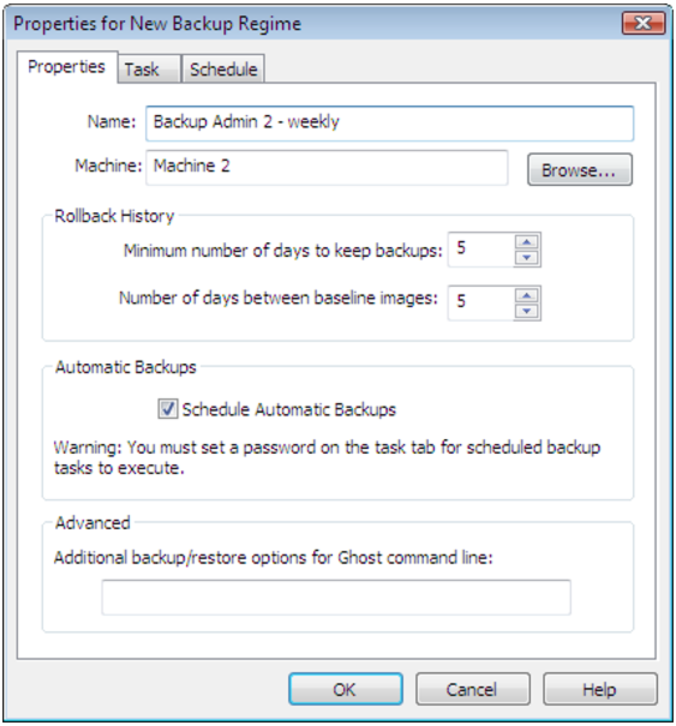
Incremental and baseline images are deleted as a set, so a particular backup image may not be deleted immediately after the minimum number of days to keep it has expired. A backup image is not deleted until all dependent images are deleted.

If you have a baseline image and several incremental images that rely on the baseline, nothing is deleted until the most recent incremental backup is older than the specified minimum number of days to keep backups. Once the most recent incremental backup passes the minimum number of days, the entire set of backups (baseline image and all dependent incremental images) is deleted.

Note: Any deletion based on the minimum number of days to keep backups setting occurs only after a new backup has been created successfully.

To set backup regime properties

1. In the Properties for *Backup Regime name* window, on the Properties tab, in the Name box, type a name for the backup.

   Name: Backup Admin 2 - weekly

   Machine: Machine 2

   Rollback History

   Minimum number of days to keep backups: 5

   Number of days between baseline images: 5

   Automatic Backups

   ☑ Schedule Automatic Backups

   Warning: You must set a password on the task tab for scheduled backup tasks to execute.

   Advanced

   Additional backup/restore options for Ghost command line:

2. Click **Browse** to select the computer to be included in the backup regime.

   Each computer can only be placed in one backup regime.

3. Under Rollback History, in the Minimum number of days to keep backups box, type the required number of days to set a time before which backup information cannot be deleted.

   If you set this to 0, then the backups are never removed.

4. In the Number of days between baseline images box, type the number of days after which to create a new baseline image.

5 Under Automatic Backups, check **Schedule Automatic Backups** to create or edit the schedule for automatic backups.

When this option is checked, the Task and Schedule tabs become available, letting you set up the schedule to suit your requirements.

See “Setting the schedule task properties” on page 160.

See “Specifying schedule details” on page 161.

6 Under Advanced, in the Additional backup/restore options for Ghost command line box, type any additional command-line options.

See “About Symantec Ghost switches” on page 521.

Warning: The syntax of your command is not checked when the task runs. Therefore, review these instructions carefully to avoid crashing or errors. The consequences of an error could be serious and you could lose data.

Viewing or modifying backup regimes

A backup regime is a set of properties associated with a particular computer that specify how backups for the computer are created and maintained. These properties include how long the backup information is saved, whether automatic backups are scheduled, and any additional command-line options.

You can view details of each backup regime and make any necessary changes.

To view or modify a backup regime

1 In the Symantec Ghost Console, in the left pane, expand the **Backup Regimes** folder.

2 In the Backup Regimes pane, do one of the following:

- Double-click the backup regime that you want to modify.
- Right-click the backup regime that you want to modify, then click **Properties**.
- Select the backup regime that you want to modify, then on the File menu, click **Properties**.

3 In the Properties for *Backup Regime name* window, view the backup regime properties, then make any appropriate changes.

See “Setting backup regime properties” on page 168.

4 Click **OK**.

Creating a backup manually

Backup regimes are usually scheduled to create backups at regular intervals. However, once you have created a backup regime for a computer, you can create a backup at any time. You may want to create a manual backup to ensure a new baseline image is created for a computer at a particular time.

Note: The maximum size of a backup image is 2 gigabytes. If you attempt to create an incremental backup larger than this, a baseline backup is created instead.

To create a backup manually

1. In the Symantec Ghost Console, in the left pane, expand the **Backup Regimes** folder.
2. In the Backup Regimes pane, do one of the following:
   - Right-click the backup regime for the computer that you want to back up, then click **Backup Now**.
   - Select the backup regime for the computer that you want to back up, then on the File menu, click **Backup Now**.
3. If you want to create a new baseline image, in the Backup Now dialog, check **Force new baseline image**.

   If this option is not checked, the backup is performed as defined on the Properties tab of the backup regime.
4. In the Comments box, type any notes that you want to accompany the backup.

   Notes are stored in the Properties window for the computer on the Backup tab.
5. Click **OK**.

Viewing computer backups

You can view details of all the backups that have been created for a computer.

To view computer backups

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Open the machine group that contains the client computer for which you want to view backups.
3. In the Machine Groups pane, do one of the following:

- Double-click the computer for which you want to view backup details.
- Right-click the computer for which you want to view backup details, then click **Properties**.
- Select the computer for which you want to view backup details, then on the File menu, click **Properties**.

4 In the Properties for *Computer name* window, on the Backups tab, view the backup details for the computer.

The details include whether the backup is a baseline or incremental image, the time at which it was created, the backup status, and any comments that may have been entered.

Restoring a computer

Client computers can be rolled back to a successful baseline or incremental image backup at any time.

When you restore a computer from a backup, the restore is performed in safe mode. This restores user files only. The operating system files and registry files are not restored.

Safe mode is intended to help you retrieve your data from a damaged and possibly unusable operating system. It does enough to give you a usable bootable system from which you can retrieve your files, but does not restore everything. Therefore some applications may not function correctly after a safe-mode restore.

Note: You cannot cancel or undo a restore once it has started.

To restore a computer

1 In the Symantec Ghost Console, in the left pane, expand the **Backup Regimes** folder.

2 In the Backup Regimes pane, right-click the backup regime for the computer that you want to receive the rollback, then click **Restore**.

3 In the list of backups, select the one to roll back.

The status of each backup is indicated as follows:

- Success: The computer in this backup was successfully backed up.
- Failed: The computer in this backup failed to back up.

4 In the bottom pane, you can view the status of the backup.

The status for the computer is as follows:

- OK: This computer was successfully backed up.
- Unfinished: This computer did not complete the back up or is currently running the back up.

5 Click **Safe Mode restore (non-system files only)** to restore user files only.

The operating system files and registry files are not restored.

6 Click **OK**.

Chapter 8

Migrating users

This chapter includes the following topics:

About migrating users

You can capture a user’s personal files and settings from a computer, save them to a migration package, and restore the package to the same computer or to another computer. During a user migration you can perform tasks that preserve a user’s personal setup and reset applications with mandatory or personal configurations. You can use migration tasks to quickly move a user from one computer to another.

If you installed an updated version of an application that Ghost supports, the restore task updates the user settings.

You can capture and restore the following user information:

User settings	You can capture desktop and application settings. For example, you can capture the following settings: ■ The default printer that is selected in Microsoft Word ■ A user's screen saver or desktop wallpaper settings ■ A user's Internet settings See “About supported applications” on page 624.

Folders and files	You can capture entire folders or individual files from any Windows-accessible partition on the computer. For example, the My Documents folder.
Registry entries	You can capture individual registry entries, keys, or user hives.

Note: You should restore a migration package to a target computer that is running the same language as the source computer. Migration of users and settings between languages is not supported.

About migration templates

You specify the user information that you want to capture by setting up migration templates. When you set up a migration template, you specify the set of files, application settings, and registry keys that you want to capture from a computer.

Table 8-1 describes the components of a migration template.

Table 8-1 Components of a migration template

Component	Description
Application settings	The applications for which you want to capture user settings. The list contains all the applications that Symantec Ghost supports.
Specified user files and folders to include or exclude	A specified set of user files and folders to include or to exclude. Each set contains a directory path and file definition and may include variables and wildcard characters. You can specify whether to include or exclude particular sets of files. You can select files based on creation or modification dates and file size. You can specify a destination path and replacement options for the files that you want to include.
Specified registry keys to capture	The specified set of registry entries to capture. Each set contains a registry path and may include wildcard characters. You can specify a destination path and replacement options can be specified for registry keys that you want to include.

A default migration template is provided. The default template captures the Desktop, Document, Music, Pictures, and Video folders for all users. It also captures all supported (and installed) application settings. The default template is stored in the User Migration Templates folder.

About migration packages

A package contains data that is collected from a client computer. The package consists of application settings, user files and folders, and registry entries. A package is based on a migration template that is you create in the Console. You use the migration package after you update a user's computer to restore the user's application settings and personal data files.

Note: A package contains only the settings that are associated with a software application. It does not include the application.

How you set up a user migration task

The steps for creating a user migration task are as follows:

Create a User Migration: Capture task

The capture task captures the user settings and data folders that are specified in a selected template or templates and stores them in a migration package.

You must select a migration template or create one. A user migration template specifies the application settings and files, user files and folders, and custom registry entries that are captured and restored in a user migration task.

Create a User Migration: Restore task

The restore task restores application settings and files, user files and folders, and custom registry entries from a migration package to a destination computer.

If you installed an updated version of an application that Ghost supports, the restore task updates the user settings.

You can configure this task to run immediately or at another time.

You can create a user migration task that includes capture and restore steps. For example, you could set up one task that includes the following actions:

- Capture a user's settings and files and save them in a package on the Ghost Console Server or on the client computer.
  See "Capturing user data" on page 189.
- Restore the client computer from an image file to provision a computer with an operating system and applications.
  See "Setting Clone properties" on page 122.
- Restore the settings and files from the migration package that you created to the client computer.

See “Restoring user data” on page 195.

Creating user migration templates

You can create new migration templates at any time, and can modify existing templates to suit your requirements. You can create new templates directly in the Configuration Resources folder or as you set up a User Migration: Capture task. Each template must contain at least one item to include or exclude, or it must contain an application setting.

To create a migration template in the Configuration Resources folder

1. On the Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **User Migration Templates** folder, and then select the parent folder in which to place the new migration template.
3. In the folder, right-click, and then select **New Migration Template** to set the properties for the migration template.

To set properties for the migration template

1. In the Properties for New Migration Template window, on the Applications tab, in the Migration Template Name box, type a name for your new migration template.
2. In the Supported Applications list, select the applications for which you want to capture user settings and files.

   The list contains all the applications that Symantec User Migration supports. To select an application, click the checkbox next to the application name.

   If the application is not installed on the source computer, then no settings are captured.
3. If you want to include additional files and folders in the template, on the Files and Folders tab, under Included Files and Folders, click **Add**.

   See “Specifying the user files to include or exclude in the template” on page 179.
4. If you want to set options to exclude files and folders in the template, on the Files and Folders tab, under Excluded Files and Folders, click **Add**.
5. If you want to remove a restriction from the template, select the restriction, and then click **Delete**.
6. If you want to capture specific registry keys, on the Registry Keys tab, under Included Registry Keys, click **Add**.

   See “Specifying the registry entries to capture” on page 187.

7. If you want to exclude registry keys from the template, on the Registry Keys tab, under Excluded Registry Keys, click **Add**.
8. Click **OK** to save the migration template.

   The new migration template is added to the User Migration Templates folder and is available for inclusion in a capture task.

Specifying the user files to include or exclude in the template

You specify the user files that you want to capture in a template.

Table 8-2 describes the restrictions that you can apply to the files that you select.

Table 8-2 File restrictions

Component	Description
Source path	The source path specifies a folder, a group of files, or a particular file. You can specify an absolute path of a file or folder, or you can use a variable that specifies a system-defined path. **Note:** All paths must be specified without quotes. If you specify a folder path that includes spaces, you do not need to enclose the path in quotes. Ghost evaluates these variables to determine which path is used. For example, user files that are stored in one operating system might be stored elsewhere on another operating system. By using system-defined paths, the two paths are automatically associated, and the files from one path are upgraded to the other. You can use a variable as a complete path to collect all files and subfolders that are on that path. You can also use a variable as a partial path and append a subfolder. For example, to collect files from the C:\Documents and settings*user name*\My documents folder for each user, you can use the variable $MyDocuments$ to set the path. You can use wildcard characters to specify the group of files. For example, you can use * to select all files and subfolders or *.ext to select all files with the specified extension. **Note:** If you use an inclusion path that is not user-specific, you may capture files that do not belong to any of the users that you are migrating. For example, you may collect all document files on a local hard drive by specifying a path such as C:\*.doc. Ghost User Migration does not check that the files captured belong to one of the users that are being migrated. By default, if you do not specify a subset of files, then all files and folders are included.
Size restrictions	These settings are optional. You can select the files that are greater than or less than a specified size. For example, you might want to select all files smaller than 100 KB and ignore any larger files. If you want to select files between a minimum and maximum size, you must include all files less than the maximum size and exclude all files less than the minimum size.

Table 8-2 File restrictions *(continued)*

Component	Description
Date restrictions	These settings are optional. By default, all files that are specified in the directory path and file definition are selected. You can filter the selected files by creation date, modification date, or date last accessed. You can specify a particular date range to select all files in the range. You can select all files that are created, modified, or accessed during the previous days by specifying the number of days. For example, you might want to select just the files that have been accessed by the user in the previous month. Any other files are ignored.
Destination options	These options let you restore files to a path that is different from the source path. You can also choose how the existing files should be replaced. If you have not specified a system-defined path, then, by default, all data files and registry entries are restored to the location from which they were collected. If you want to restore the data files and registry entries to a different location on the destination computer, you must specify the appropriate paths to the directory. You can also select to save a backup copy of files that are replaced with files that are restored from the package. These options are available only when you include files in a capture task. **Note:** If the complete source path is not resolved, nothing is collected. If the target path does not exist, it is created as part of the restore process.

To specify the files to include or exclude in the template

1. In the File or Folder dialog box, in the Source Path drop-down list, do one of the following:

   - Type a path to a file or folder.
   - Select a system-defined path from the drop-down list.
     See "About user migration variables" on page 184.

   You can use a combination of a system-defined path and type a direct path.

2. If you want to include the subfolders of the specified path, check **Include Subfolders**.

   The specified file selection applies to all the subfolders.

3 If you want to include folders that have no files in them, check **Include Empty Folders**.

4 To set additional restrictions on the selected files, then select one or more of the following options:

Set date restrictions	See "To set date restrictions on files to include in the template" on page 182.
Set size restrictions	See "To set size restrictions on files to include in the template" on page 183.
Set destination options	See "To set a destination path" on page 183.

5 Click **OK**.

To set date restrictions on files to include in the template

1 In the File or Folder dialog box, under Date, check **Apply to files**.

2 In the drop-down list, select one of the following options:

Modified	Selects the files that were modified in the specified date range.
Created	Selects the files that were created in the specified date range.
Last Accessed	Selects the files that were last accessed in the specified date range.

3 Set the date criteria by selecting one of the following options:

Between	Set the start and end dates of the range by clicking each box and selecting the date from the calendar.
During the previous	Set the number of days by typing the appropriate number or by clicking the arrow buttons to change the current value. Days are counted from the current time to the same time on the appropriate day, not the complete day.

To set size restrictions on files to include in the template

1. In the File or Folder dialog box, under Size, if you want to include only those files that are less than a specified size, check **Less than**, and then in the KB box, specify the file size in kilobytes.

   You can specify the size by typing the appropriate number or by clicking the arrow buttons to change the current value.

2. If you want to include only those files that are greater than a specified size, check **Greater than**, and then in the KB box, specify the file size in kilobytes.

To set a destination path

1. In the Include Files or Folders dialog box, in the Replace drop-down list, select one of the following options:

Never	Existing files are not replaced.
Always	Existing files are always replaced.
Date is newer	Replace the existing file only if the one in the package is newer (for example, the date is more recent).
Version is newer	Replace the existing file only if the one in the package is a newer version (for example, the version number is higher). This option applies only to executable programs.
Date and version are newer	Replace the existing file only if the one in the package is both newer and a newer version. This option applies only to executable programs.

2. If you want to keep a backup of the replaced files, then check **Backup replaced files**.

   The backups are stored in the same location as the existing files.

3. If you want to restore the files to a path other than the source path, then check **Specify destination path**, and type the path to which you want the source files to be restored.

   You can type the entire path or use variables as building blocks where appropriate, in the same way that you set the source path.

   See “About user migration variables” on page 184.

About user migration variables

You can use variables as building blocks to specify part or all of the directory path. This use of variables lets you specify a directory that is set up by the operating system. For example, to collect files from the C:\Documents and Settings*user name*\My Documents folder for each user on Windows 2000 and XP computers, you can use the $MyDocuments$ variable.

Table 8-3 lists the variables that represent folder locations that the operating system determines.

You can only use the variables that are contained in the list. If you type any other variables, even though they are valid in the operating system, the directory path is not resolved.

Table 8-3 System-defined paths

Variable	Definition
$LocalDrives$	All local drives including removable media. This includes floppy drives, CD®) drives, and USB flash drives.
$LocalHardDrives$	All locally-mounted drives with non-removable media. For example, C:\
$NetworkDrives$	Mapped network drives.
$CommonDesktop$	File system directory that contains the files and folders that appear on the desktop for all users. Typically: \Documents and Settings\All Users\Desktop
$CommonDocuments$	File system directory that contains the documents that all users share. Typically: \Documents and Settings\All Users\Documents
$CommonStartMenu$	File system directory that contains the programs and folders that appear on the Start menu for all users. Typically: \Documents and Settings\All Users\Start Menu
$CommonStartup$	File system directory that contains the programs that appear in the Startup folder for all users. Typically: \Documents and Settings\All Users\Start Menu\Programs\Startup
$Fonts$	Virtual folder that contains fonts. Typically: \Windows\Fonts or \WINNT\Fonts

Table 8-3 System-defined paths *(continued)*

Variable	Definition
$MyDesktop$	File system directory that contains a specific user's desktop shortcuts and files. Typically: \Documents and Settings\User Name\Desktop
$MyDocuments$	$MyDocuments$ includes music, video, and picture files. You should use the $MyDocuments$ variable on client computers running Windows XP or earlier versions of Windows. If you use this variable on a Windows Vista computer, then Symantec Ghost displays a warning. File system directory that contains a specific user's personal files. Typically: \Documents and Settings\User Name\My Documents My Documents is the same as Personal.
$Documents$	You should use the $Documents$ variable on client computers running Windows Vista. The $Documents$ variable does not include a user's music, video, or picture files. To includes these files, you must use the $Music$, $Video$, and $Pictures$ variables. On Microsoft Vista computers, this directory is typically as follows: \Users\User Name\Documents\
$MyMusic$ $Music$	File system directory that contains a user's music files. On Windows XP computers, this is typically: \Documents and Settings\User Name\My Documents\My Music On Windows Vista computers, this is typically: \Users\User Name\Music
$MyPictures$ $Pictures$	File system directory that contains a user's graphics files. On Windows XP computers, this is typically: \Documents and Settings\User Name\My Documents\My Pictures On Windows Vista computers, this is typically: \Users\User Name\Pictures\

Table 8-3 System-defined paths *(continued)*

Variable	Definition
$MyVideo$ $Video$	File system directory that contains a user's video files. On Windows XP computers, this is typically: \Documents and Settings\User Name\My Documents\My Videos On Windows Vista computers, this is typically: \Users\User Name\Video\
$Profile$	File system directory that contains a specific user's documents and settings. Typically on Windows XP, this is: \Documents and Settings\User Name\ Typically on Windows Vista, this is: \Users\User Name\ This is provided to let users capture profile directories for which no variable is provided. For example, variables are provided for $Documents$ and $MyDesktop$, but not for non-standard paths such as "My eBooks". To capture a non-standard profile path such as My eBooks, you would specify $Profile$\My eBooks. When $Profile$ is used alone the migration engine attempts to capture all files in \Documents and Settings\[User], and may capture a lot of operating system/machine-specific data. This may have undesirable effects when restored on the target computer. **Note:** Including the entire profile when you also have specific applications selected in the template is not recommended. The migration engine transforms operating system/machine-specific data before it is restored to the target computer. Including $Profile$ without specifying a subdirectory has the potential to impact this process in various ways: for example, by migrating a machine or operating system-specific file which the defined application transformation has intentionally excluded.
$ProgramFiles$	File system directory that contains the program files. Typically: \Program Files
$StartMenu$	File system directory that contains Start menu items. Typically: \Documents and Settings\User Name\Start Menu or \WINNT\Profiles\User Name\Start Menu

Table 8-3 System-defined paths *(continued)*

Variable	Definition
$Startup$	File system directory that corresponds to the user's Startup program group. Typically: \Documents and Settings\User Name\Start Menu\Programs\Startup
$Windows$	Windows directory or SYSROOT. Typically: \WINDOWS or \WINNT

Specifying the registry entries to capture

You can capture and migrate registry entries. You do not need to use this feature to capture settings for applications that are supported by the migration template.

You specify the registry entries that you want to capture with a migration template.

You must determine whether the registry entries require destination paths. You must use a destination path when you want to move all entries and subkeys under a particular registry key to a different location (for example, for backup purposes).

To specify the registry entries to capture

1 In the Include Registry Keys dialog box, under Options, in the Path box, type the registry path and entry definition for the registry entries.

2 If you want to include the child keys in the capture, then check **Include Child Keys**.

3 In the Replace drop-down list, select one of the following:

Never	Existing entries are not replaced.
Always	Existing entries are always replaced.

4 If you want to restore the entries to another key or hive other than the source key, then check **Specify destination path**, and type the registry path and entry definition for the registry entries.

5 Click **OK**.

About managing migration templates

The Ghost Console provides a set of options that help you organize and manage your migration templates. These options let you set up the folder structure and move migration templates within them. You can also rename migration templates and delete any that you don't need.

See "Setting the resource folder view mode" on page 73.

See "Creating new folders" on page 73.

See "Moving Symantec Ghost Console resources" on page 74.

See "Renaming Symantec Ghost Console resources" on page 75.

See "Deleting Symantec Ghost Console resources" on page 75.

Viewing or modifying a migration template

You can open a migration template to view or modify. For example, you can view the contents of a migration template before you assign the template to a task.

Note: Any changes that you make to a migration template take effect immediately.

To view or modify a migration template

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **User Migration Templates** folder, and then select the parent folder of the migration template that you want to open.
3. Select the migration template, and then on the File menu, click **Properties**.
4. In the Properties for *Template name* window, view the options that are set in the migration template, and then make the appropriate changes.

   See "Creating user migration templates" on page 178.

Exporting a migration template

You can export a migration template as an XML file. You can use the exported XML file as a template in the Symantec User Migration Wizard.

For more information and additional template control options, see the *Symantec User Migration Guide*.

See "Symantec User Migration Wizard" on page 33.

To export a migration template

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **User Migration Templates** folder, and then select the parent folder of the migration template that you want to export.
3. Do one of the following:
   - Right-click the migration template, and then click **Export Migration Template**.
   - Select the migration template, and then on the File menu, click **Export Migration Template**.
4. In the Save As dialog box, select the location for the template, specify a suitable file name, and then click **Save**.

Importing a migration template

You can import a migration template from an XML file.

To import a migration template

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **User Migration Templates** folder, and then select the folder to which you want to import the migration template.
3. Do one of the following:
   - Right-click and then click **Import Migration Template**.
   - On the File menu, click **Import Migration Template**.
4. In the Open dialog box, select the appropriate XML file, and then click **Open**.
5. In the Properties for *Template Name* window, make any necessary changes.

   You may want to change the migration template name. The default name is the XML file name.
6. Click **OK**.

Capturing user data

You capture user data from a computer by setting up and running a User Migration: Capture task. This capture saves the user data in a user package. You can use the package to restore the user data to the same computer or to another computer by running a User Migration: Restore task. You can save all of the user packages on the Console server, or you can save each user package on the client computer from which it was collected.

You should save all user packages on the Console server when you want to move users from one computer to another. If the target of the task is a computer group, all packages are named automatically. If the target is a single computer, you can specify a name for the package or use the automatic naming option. You can set the location to which the user package files are saved on the Console server.

See "Setting the storage location for user packages" on page 201.

If you want to restore the user settings to the same computers from which they were collected, you may prefer to save each user package on the client computer. This option saves network bandwidth during the capture or restore process.

To capture user data

1. In the Symantec Ghost Console, in the left pane, expand the **Tasks** folder.
2. Select the parent folder in which to place the task.
3. On the File menu, click **New > Task**.
4. In the Properties for New Task window, in the Name box, type a name for the new task.
5. In the Task Steps list, check **User Migration: Capture** to activate the step.

   You can select other steps to perform, if required.
6. In the Target Machine Group/Machine box, click **Browse**, select the destination computer or computer group from the folder structure, and then click **OK**.
7. On the User Migration: Capture tab, under Package, select one of the following options to specify where to save the migration packages that are created by this task:

Save on the Ghost Console Server	All user packages are saved on the Console server. You must select this option when you move a user from one computer to another. The packages are saved to the location that is selected in the preferences for the Console. See "Setting the storage location for user packages" on page 201.
Save on the Client machine(s)	Each user package is saved on the computer from which it was collected.

8. In the User Package Naming box, specify a name for the user package and the location in which you want to save the package.

   See “Setting the name of the user package ” on page 194.

9. In the User Options box, in the Capture drop-down list, select one of the following options:

Domain user only	Migrates only the users that belong to a domain
Local machine only	Migrates only the user accounts that are stored locally
All users	Migrates all the users that are on the computer
Last logged in user	Migrates only the user who last logged in to this computer
DOMAIN\Username	Migrates the users that are specified in this box. You can use a wildcard character with a user name or a domain. For example, 2K3N* selects all users on the 2K3N domain, and *\Joe_* selects all users that start with Joe_ in any domain.

   Alternatively, you may specify one of the following by typing the appropriate text into the Capture box:

*My_User	Captures all users that are named My_User, both domain and local.
2K3N\My_User_1, 2K3N\My_User_3	Captures both specified users from 2K3N domain.

10. If you want to limit the number of users that you want to migrate to recent users, then check **Only Users Accessed Within**, and then in the Day box, scroll to the number of days.

    This setting limits the migration to those users who have logged in to the computer within the specified number of days. The maximum number of days that you can set is 365.

11. Under User Migration Templates, click **Browse**.

12. In the Select Migration Template dialog box, do one of the following:

- To use an existing template, expand User Migration Templates, and then select a template.
  The migration template specifies the migration that is captured in the task.
  To view the template properties, double-click it.
- To create a template, highlight **User Migration Templates**, and then click **New > New Item**.
  See "Specifying the user files to include or exclude in the template" on page 179.

13 Click **OK**.

14 In the Logging Level drop-down list, select one of the following event logging options:

Low	Logs errors and warnings only
Medium	Logs errors, warnings, and debugging information
Full	Logs errors, warnings, information, and debug details

15 In the Compression Level drop-down list, select the level to which the files are compressed when captured in a package as follows:

- None
- Low
- Medium
- Full

You can compress the file transmissions during create operations. The compression helps improve performance during the package creation and minimizes the storage requirements on the server.

16 If you want the task to stop if a warning is issued, then check **Abort on Warning**.

If multiple steps are included in the task, the task stops at the point of error. It does not attempt to run the rest of the steps. For example, if the task includes a capture step, clone step, and restore step, and the capture step returns a warning. The task fails without running the clone and restore steps.

17 If you want to migrate EFS encrypted files, check **Capture EFS Files Raw**.

See "About capturing EFS files raw" on page 193.

18 Do one of the following:

- To save the task, click **Save**.
- To run the task immediately, click **Execute**.

See “Executing tasks” on page 149.

When you run a User Migration: Create task, the user settings on each destination computer are stored in a user package. Each user package is an .ump file. It is saved on the Console server or on the client computer, according to the settings that you specified in the task. If the user package is saved on the Console server, the package definition is added to the User Packages folder.

About capturing EFS files raw

When EFS files are captured raw, the EFS-encrypted format is maintained during the migration process. The certificate which encrypted the files is required to allow the user to read the files after they have been restored to the target machine.

Prior to capturing EFS files in raw mode, you need to do the following:

- On the source computer, ask the end user to log on and export the certificate.
  To export a certificate using the command-line, execute: "cipher /x".
  The user will be asked to nominiate a password to protect the exported certificate.
  The certificate can also be exported using a graphical interface. To do this:
  Click Start > Run.
  Run **mmc certmgr.msc**.
  In the Microsoft Management Console, click Certificates > Current user > Personal > Certificates and then select the appropriate certificate.
  Click Action > All tasks > Export.
- On the target computer, ask the end user to logon and import the certificate.
  Ask the user to double click the certificate and follow the prompts to import it.
  The certificate can also be imported using a graphical interface. To do this:
  Click Start > Run.
  Run **mmc certmgr.msc**.
  In the Microsoft Management Console, click Certificates > Current user > Personal > Certificates and then select the appropriate certificate.
  Click Action > All tasks > Import.

Setting the name of the user package

The procedure for setting the name of the user package depends on whether you store the user packages on the Console server or on the client computers.

If the User Migration: Create task collects user packages from a group of computers, each user package is named automatically. The name uses the computer name and the creation date.

Note: The name that you specify for user packages that are stored on the Console server is used only in the Console. The actual file name on the server is always automatically set, and has the following format:

[*ComputerName*] [yyyy- mm-dd] [hh-mm-ss].ump

The space between items, and the space within the date field between the year and month is as shown above. For example: MyComputer 2008- 3-17 23-16-42.ump

The name that you specify for user packages that are stored on the client computers is the actual file name and location. You cannot view the package in the Ghost Console.

To set the name for user packages that are stored on the Console server

- Under Package, select one of the following options:

Automatically, using the Machine Name	The name format is: computername (yyyy-mm-dd hh:mm:ss).
Specified	If the User Migration: Create task collects a user package from a single computer, type the name of the user package. This option is available only if you select a single computer, not a group.

To set the name for user packages that are stored on the client computers

1. Under Package, click **Edit**.
2. In the Path to User Migration Package on Client window, under Volume Identifier, select one of the following:

Drive letter	Type the drive letter.
Volume label	Type the volume label.

3 In the Path box, type the appropriate path and file name.

4 Click **OK**.

Each user package is saved in the specified file on the client computer.

Restoring user data

You restore user data from a user package to a computer by setting up and running a User Migration: Restore task.

You can set up a User Migration: Restore task as a stand-alone task or as a step within a task.

Note: Client computers must be joined to the appropriate domain before you start restoring user data.

To create a User Migration: Restore task

1 In the Symantec Ghost Console, in the left pane, expand the **Tasks** folder.

2 Select the parent folder in which to place the task.

3 On the File menu, click **New > Task**.

4 In the Properties for New Task window, in the Name box, type a name for the new task.

5 In the Task Steps list, check **User Migration: Restore** to activate the step.

You can select other steps to perform, if required.

6 In the Target Machine Group/Machine box, click **Browse**, select the destination computer or computer group from the folder structure, and then click **OK**.

7 On the User Migration: Restore tab, under Package, select one of the following options to specify the location of the user packages to restore:

The package is located on the Ghost Console Server	All user packages are located on the Console server.
The package is located on the Client machine(s)	Each user package is located on the computer to which it will be restored.

8 Under Package, specify the name of the user package that you want to restore.

See “To select the package to restore ” on page 196.

9 In the Logging Level drop-down list, select one of the following event logging options:

Low	Logs errors and warnings only
Medium	Logs errors, warnings, and information
Full	Logs errors, warnings, information, and debugging information

10 Do one of the following:

- To save the task, click **Save**.
- To run the task immediately, click **Execute**.

See "Executing tasks" on page 149.

To select the package to restore

◆ Under User Package Naming, do one of the following:

- To select a package that has been named automatically, click **Select latest Package based on Package's Target Machine Name**.
  The name format is: machinename (yyyy-mm-dd hh:mm:ss).
  By default, the target computer name of a package is set to the source computer name.
  See "Viewing information about a user package" on page 202.
- To use the same naming convention that was selected in the capture step, click **As specified in the User Migration: Capture step**.
- To specify a package name and location if a package is stored on the Console, click **Specified**, and then click **Browse**.
  See "To select a package that is stored on the Console" on page 196.
- To specify a package name and location if a package is stored on the client computer, click **Specified**, and then click **Edit**.
  See "To select a package that is stored on the client computer" on page 197.

To select a package that is stored on the Console

1 In the Select User Package dialog box, expand **User Packages**.

2 Select the package that you want to restore, and then click **OK**.

To select a package that is stored on the client computer

1 In the Path to User Migration Package on Client dialog box, under Volume Identifier, select one of the following:

Drive letter	Type the drive letter.
Volume label	Type the volume label.

2 In the Path box, type the appropriate path and file name.

3 Click **OK**.

Creating local user accounts

If a local user is restored to a computer where their account does not already exist, a local account is created automatically and is assigned membership of the Users group. By default, all local account objects are created with the "User must change password at next logon" attribute enabled.

You can optionally create accounts with the "Account is disabled" attribute set. When migration is complete, the administrator may enable each account (as required) locally, or remotely using the MMC computer management snap in.

The local user account settings are contained in the following registry key:

HKLM\Software\Symantec\Symantec User Migration

To specify a password

- Set the LocalAccountPassword value.

  This value is of type String.

  The value data is the initial password for all local user accounts that are created. Each user will be prompted to change their password when they log on for the first time. If the value or data is not specified, an empty password is created.

  The initial password must comply with local security policy and password complexity rules.

  If the value specified for the password does not comply with local security policy, the account object will not be created.

Note: Windows security policy for local accounts is displayed in:

Control Panel > Administrative Tools > Local Security Settings > Account Policies > Password Policy.

For example, setting the LocalAccountPassword value to "My_Password99" passes the default password policy complexity checks for Windows 2000, 2003, and Vista domains.

To create local accounts in the 'Disabled' state

1. Set the CreateLocalAccountDisabled value.

   This value is of type DWord.

   The value data must be any non-zero value to set the "Account is disabled" attribute. When this attribute is set, the accounts must be enabled by an administrator before the users can log in.

2. To turn off this feature, set the value to 0.

Checking restored shortcuts

By default, all shortcuts are restored whether or not they are resolved. If you want to prevent unresolved shortcuts from being restored, you can enable the Shortcut Resolution Check feature. For Console-based migration, this also prevents network shortcuts from being restored.

To enable the Shortcut Resolution Check feature

◆ On each client computer for which you want to enable shortcut resolution checking, add the following registry key and set the appropriate value:

Key	HKLM\Software\Symantec\Symantec User Migration
Value	RestoreUnresolvedShortcuts
Type	DWord
Data	0 [Unresolved shortcuts will not be restored]
Data	1 [Unresolved shortcuts will be restored]

Managing user packages

The user packages that are saved on the Console server are displayed in the User Packages folder in Configuration Resources. You can organize and manage these user packages as you want, using a standard set of Console options. These options let you set up the folder structure and move user packages within them. You can also import and export user packages, rename user packages, and delete any that you don't need.

You can also use Symantec User Migration Package Explorer to view user packages. You can run Symantec User Migration Package Explorer from the Ghost Console or from the Start menu.

See "About Symantec User Migration Package Explorer" on page 203.

Note: User packages that are stored on client computers are not shown in the Console. When you save a user package on a client computer, you must specify a name for the user package file and a location in which to store it. When you set up the restore task, you must provide the full path, or volume label and directory and the file name of the user package to include.

See "Setting the resource folder view mode" on page 73.

See "Creating new folders" on page 73.

See "Moving Symantec Ghost Console resources" on page 74.

See "Renaming Symantec Ghost Console resources" on page 75.

See "Deleting Symantec Ghost Console resources" on page 75.

About User Migration reports

The User Migration report is generated for each capture and restore operation. It lists the users that were captured, and any users or files that were not captured, and the users that were restored, and any users and files that could not be restored. You can view the Migration Report in the Ghost Console, or in Symantec User Migration Package Explorer.

For capture operations the User Migration report is included in the package and can be viewed on the Logs tab of the User Migration Package Explorer. For restore operations, the User Migration report can be found on the client machine. For both capture and restore operations the User Migration report is also available in the task event log.

To open the User Migration report directly

1. Open the User Migration package in the User Migration Package Explorer.

   The migration options in effect at the time that the package was created can be viewed on the Logs tab.

2. Double-click `SCMMigrationReport.html`.

To open the User Migration report from the task event log

1. Right-click the task and then click **Event Log**.
2. Right-click the Make user migration package event, and then click **Error File**.

To view the migration options

- Double-click `MigrationOptions.xml`.

The User Migration report contains the following information:

Capture and Restore	User Migration Version
Capture	Users captured Users not captured Files that could not be captured
Restore	Restored users Users not restored Users which were remapped to other users Local user accounts created during the restore process Files which could not be restored Names of applications that were included in the package, but which are not present on the target machine.

Setting the storage location for user packages

You can specify the location on the Console server in which to store the user packages if they are not stored on the client computers. To ensure that there is enough available space for the packages you might need to change the storage location.

To set the storage location for user packages

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. On the Preferences tab, under User Migration, specify the location in which you want to store the user packages.

   You can type the full directory path, or click **Browse** to select it.
3. Click **Apply**.

Exporting a user package

You can export a user migration package as a .ump file.

To export a user package

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **User Migration Packages** folder, and then select the parent folder of the user package that you want to export.
3. Do one of the following:
   - Right-click the user package, and then click **Export Migration Package**.
   - Select the user package, and then on the File menu, click **Export Migration Package**.
4. In the Save As dialog box, select the location for the user package, specify a suitable file name, and then click **Save**.

Importing a user package

You can import a user migration package from a .ump file.

To import a user package

1. In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.
2. Expand the **User Migration Packages** folder, and then select the folder to which you want to import the user package.
3. Do one of the following:

- Right-click and then click **Import Migration Package**.
- On the File menu, click **Import Migration Package**.

4 In the Open dialog box, select the appropriate .ump file, and then click **Open**.

5 In the Property Sheet window, make any necessary changes.

You may want to change the user package name. The default name is the .ump file name.

6 Click **OK**.

Viewing information about a user package

You can view the following information about any user package that is stored on the Console server:

- User package name
- Name of the client computer from which the user package was collected
- Name of the user package file and its location on the Console server
- Date and time that the user package was created
- Target computer name
  The name of the client computer to which the package is restored if the Select latest Package based on Package's Target Machine Name is selected in a task. You can edit this setting.

You can also open the user package with Symantec User Migration Package Explorer. You can view the files, application settings, and logging information that is in a package. The features of Symantec User Migration Package Explorer are integrated into the Ghost Console.

To view information about a user package

1 In the Symantec Ghost Console, in the left pane, expand the **Configuration Resources** folder.

2 Expand the **User Migration Packages** folder, and then select the parent folder of the user package for which you want to view details.

3 Select the user package, and then on the File menu, click **Properties**.

4 If you want to view the user package, on the Property Sheet, click **Launch User Migration Explorer**.

5 Click **OK** to close the Property Sheet.

About Symantec User Migration Package Explorer

Symantec User Migration Package Explorer lets you manage all user migration packages. You can use Symantec User Migration Explorer to do the following:

- Open migration packages
- View the contents of a migration package
- Open user and application files in a migration package
- Save files from a migration package
- View user and application settings
- View or export User Migration: Capture reports
- View or export user migration options that were in effect during the capture operation
- View or export logs

Using Client Inventory

This chapter includes the following topics:

About the Client Inventory feature

The Symantec Ghost Client Inventory feature lets you obtain information from the Windows Management Instrumentation (WMI) repository on each Console client. You can choose the type of information that you want to collect and which computers to collect it from.

The information that you collect is stored in a database on the Console server and is updated on request. You can query this database to select the computers that have certain properties and can then use the selected computers as the target of a task. For example, you can select the computers that have available memory that is greater than a specified amount. You can view the property values for each computer. You can also produce reports that contain the property values for each computer in a group.

Client Inventory resources

You can access and maintain the Client Inventory via the Symantec Ghost Console. The Client Inventory resources are stored under the Inventory folder, and in the

Dynamic Machine Groups folder. You can also view Client Inventory information via the Machine Groups folder.

The Inventory folder contains the following subfolders:

Collected Data

Stores the collected data sets that define the type of information that you want to collect from other computers and store in the inventory database. You specify the WMI classes that you want to collect from the client computers. You can assign user-friendly names to the classes and properties. If you create a new class then all properties are collected. You can turn off any properties that you don't want to collect.

See "Managing collected data sets" on page 209.

Filter

Stores the filters that you use for querying the Inventory database. A filter contains a list of conditions, which may be linked by logical operators. Each condition specifies a single property and a corresponding restriction. When you apply a filter to a computer group, the result is a list of all the computers in the group that match the filter conditions.

See "Creating and maintaining filters" on page 223.

Report

Stores the reports that you use for retrieving detailed information for computers that match a specific filter. A report typically contains a filter and a view, and is applied to a particular computer group. The output of a report is the list of computers that match the filter conditions and, for each computer, the properties specified in the view. You can view reports on the screen, print them, and save them as text files.

See "Creating and running reports" on page 232.

View

Stores the views that you use for displaying property data. A view is the list of properties that is displayed when the view is applied to a computer group. Applying views is an efficient way of selecting and displaying the properties you are interested in. For example, you may want to set up views containing groups of related properties (such as software, hardware, or network) and apply them each time you want to view those properties for a computer group.

See "Viewing inventory information" on page 216.

The other folders that are used by the Client Inventory are as follows:

Machine Groups

Stores all the computers known to the Console, and the computer groups that you have set up. You can see inventory information for individual computers in the Properties window. You can also specify the views associated with each computer in a computer group.

See “Setting the common Inventory view for computer groups” on page 219.

See “Viewing inventory information for client computers” on page 221.

Dynamic Machine Groups

Stores the dynamic machine groups that you have set up. A dynamic machine group is the result of a filter applied to a computer group, and contains the computers in the target group that match the filter conditions. Each dynamic machine group is treated as a virtual computer group, and can be used as the target of a task.

See “Setting up dynamic machine groups” on page 237.

Using the Client Inventory

You need to set up and maintain the collected data sets, filters, and views that you want to use. You can use the available filters and views to create and run reports on particular computer groups, and view inventory information for client computers. You can also set up dynamic machine groups, and use them as the target of a task.

The Client Inventory relies on the data provided by Microsoft Windows Management Instrumentation (WMI). The accuracy of the data returned by WMI depends upon the version of the operating system, the service pack, and the version of WMI installed.

To use the Client Inventory

1. Set up the collected data sets to include all the WMI classes that you want to collect from the client computers.

   See “Setting up collected data sets” on page 210.

2. If necessary, set up the computer groups that you require.

   See “Setting up computer groups” on page 79.

3. Run a refresh inventory task to collect the appropriate WMI class instances from each of the computers in the target computer group.

   This task populates the inventory database, and produces the properties list for each collected data set.

   See “Populating the Inventory database” on page 212.

4 Set up the properties for each collected data set to suit your requirements.

When you add a new collected data set and get data for it, all the properties in the WMI class become available. You can then set the property display names, and specify which properties to include in the collected data set for subsequent database refreshes.

See "Setting up collected data set properties" on page 213.

5 Set up the views that you want to use.

A view is essentially a list of properties that you want to display. You can display the inventory information you are interested in by applying the appropriate views to client computers or computer groups.

See "Viewing inventory information" on page 216.

6 Set up the filters that you want to use.

A filter is essentially a query that you apply to a computer group. It searches the Inventory database and selects all the computers in the target group that match the filter conditions. You can set up filters to search for any combination of properties and property values that you want.

See "Creating and maintaining filters" on page 223.

7 Use the filters and views to create reports, set up dynamic machine groups, and show inventory information.

See "Creating and running reports" on page 232.

See "Setting up dynamic machine groups" on page 237.

See "Viewing inventory information for client computers" on page 221.

Managing Inventory resources

The Inventory folders show the resources that you have created and are available for you to use. The Symantec Ghost Console provides standard options to help you organize these resources as you wish. These options allow you to set up the folder structure, and move items within it as appropriate. You can also rename items, and delete any items that you don't need.

See "Setting the resource folder view mode" on page 73.

See "Creating new folders" on page 73.

See "Moving Symantec Ghost Console resources" on page 74.

See "Renaming Symantec Ghost Console resources" on page 75.

See "Deleting Symantec Ghost Console resources" on page 75.

Managing collected data sets

The Collected Data folder shows all the WMI classes defined in the inventory database. You need to set up the collected data sets to suit your requirements and to ensure that you collect data for all the WMI classes that you want. You can also choose to collect particular properties within a WMI class, and ignore the properties that you are not interested in.

Note: By default, the Collected Data folder is hidden in the Console. You must show it before you can create, view or modify any collected data sets.

See "Showing the Collected Data folder" on page 209.

About collected data sets

The collected data sets specify the WMI classes that are collected from client computers when you run a refresh inventory task. All instances of the specified classes found on client computers are copied and stored in the inventory database on the Console server. You can query the inventory database to obtain the information you want.

Groups of pre-defined collected data sets that contain commonly used WMI classes are provided. These include the basic Windows classes such as operating system, memory, and hard disk space.

Each WMI class has a number of properties, which represent the information gathered for the class. System properties are not displayed, and you cannot collect them.

If you need more information on these classes, or on WMI classes in general, refer to the documentation supplied by Microsoft. For more information see the article at the following URL:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wmi_classes.asp

You can add additional collected data sets to collect the information you require from the client computers. There is no restriction on the WMI classes you can use: they may be additional Microsoft WMI classes, or third-party vendor classes.

See "Setting up collected data sets" on page 210.

Showing the Collected Data folder

By default, the Collected Data folder is hidden in the Console. You can show it when you want to view the collected data sets, or make any changes.

To show the Collected Data folder

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. On the Inventory tab, check **Show Collected Data Sets in Inventory**.
3. Click **Apply**.

Setting up collected data sets

If you want to collect data for a WMI class that is not included in a collected data set, you need to create a new collected data set in the Console. You can then specify the WMI class and properties to collect. You can also modify existing collected data sets to change property names, or specify different properties to collect.

To set up collected data sets

1. Create the new collected data sets that you require.

   This defines the WMI namespace, WMI class name, and display name for each data set that you want to include.

   See "Creating a new collected data set" on page 210.
2. Run a refresh inventory task.

   The refresh inventory task reads the WMI repository on each client computer, and populates the inventory database with all the properties of all the new WMI classes that are found.

   See "Populating the Inventory database" on page 212.
3. Set up the WMI class properties for each collected data set.

   You can specify the display name of each property and whether or not to use it in data collection.

   See "Setting up collected data set properties" on page 213.

Creating a new collected data set

You create a new collected data set by defining the WMI namespace, WMI class name, and display name for the new collected data set in the Console.

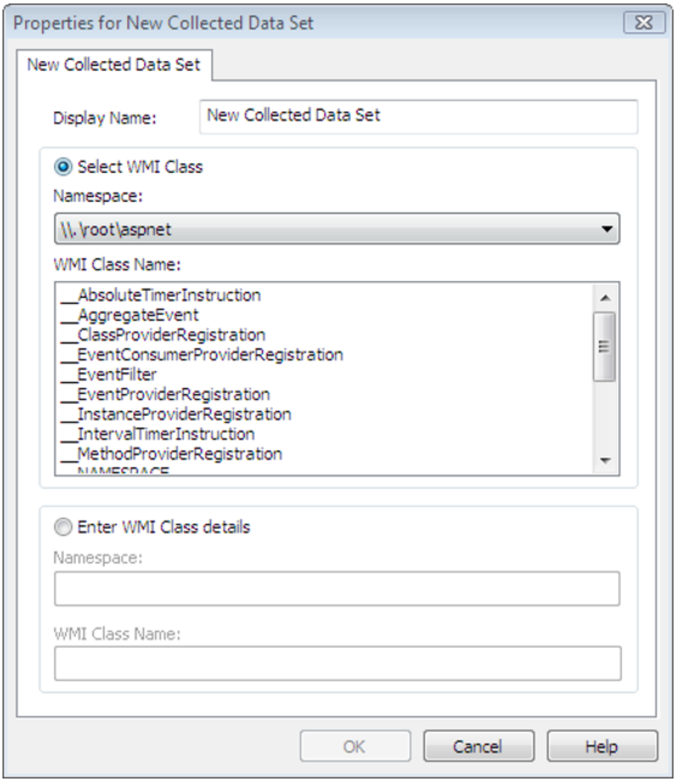
To create a new collected data set

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Expand the **Collected Data** folder, then expand the subfolder in which you want to create the new collected data set.
3. Do one of the following:

- In the Collected Data pane, right-click, then click **New Collected Data Set**.
- On the File menu, click **New > Collected Data Set**.

4 In the Properties for New Collected Data Set window, in the Display Name field, type a name for your new collected data set.

The name must be unique and may contain up to 50 alphanumeric characters. You should type a descriptive name that is easy to recognize when you are setting up filters and views.



Properties for New Collected Data Set

New Collected Data Set

Display Name: New Collected Data Set

● Select WMI Class

Namespace: \\.\root\aspnet

WMI Class Name:

__AbsoluteTimerInstruction
__AggregateEvent
__ClassProviderRegistration
__EventConsumerProviderRegistration
__EventFilter
__EventProviderRegistration
__InstanceProviderRegistration
__IntervalTimerInstruction
__MethodProviderRegistration
__NAMESPACE

○ Enter WMI Class details

Namespace:

WMI Class Name:

5 In the Namespace drop-down list, select the namespace of the WMI class that you want to collect, if it is listed.

The Namespace list contains all the WMI namespaces known to the Console. These are read from the WMI repository on the Console server. If the namespace of the class that you want to collect is not listed, go to step 7.

6 In the WMI Class Name list, select the class, if it is listed.

The WMI Class Name list contains all the WMI classes known to the Console in the selected namespace.

If you selected the WMI class that you want to collect from the list, go to step 10.

If the name of the WMI class that you want to collect is not listed, go to step 7.

7 Click **Enter WMI Class details**.

8 In the Namespace field, type the full namespace of the class that you want to collect.

The name may contain up to 255 alphanumeric characters.

9 In the WMI Class Name field, type the class name.

The name may contain up to 255 alphanumeric characters. The Console does not perform any validation on user-defined classes. If you make an error in typing the namespace or the class name, the Console is not able to find the class instance data on the client computers.

10 Click **OK**.

11 In the Properties dialog box, view the details of the new collected data set properties.

If the new collected data set is a user-defined WMI class, there are no properties displayed.

If the new collected data set is a WMI class already known to the Console, the Properties dialog box displays the class properties as they are currently defined. These are read from the WMI repository on the Console server, and are usually sufficient to work with. You can set up the properties as you want, or you may prefer to perform an Inventory task to update the Inventory database first.

12 Click **OK** to close the Properties dialog box.

The new class is added to the Collected Data view.

Populating the Inventory database

The properties for all WMI classes defined in the collected data sets are gathered when you run an Inventory task on the client computers. When you add a new collected data set, you need to run an Inventory task to collect the appropriate WMI class properties and add them to the Inventory database.

When you have populated the Inventory database, you need to proceed to the next step of the process, setting up the class properties for each collected data set.

See "Setting up collected data set properties" on page 213.

To populate the Inventory database

1. Set up an inventory refresh task, by selecting the Refresh Inventory step in the task definition.

   See "Setting up tasks" on page 119.

2. Run the inventory refresh task on the appropriate computer group.

   You may want to set up a computer group that contains all the Console client computers, to ensure that the Inventory database is complete and up-to-date.

   See "Executing a task from the Symantec Ghost Console" on page 150.

   If a WMI class has instances with different properties on different computers, the class properties are merged in the Inventory database.

   If no instances of a WMI class are found on any client computers, the class properties cannot be added to the database. If this occurs, you may want to check that you have specified the WMI namespace and class name correctly in the collected data set.

Setting up collected data set properties

You can set up the properties of each collected data set to suit your requirements. When you create a new collected data set, you need to set up the WMI class properties as part of the process. You can modify the property settings at any time.

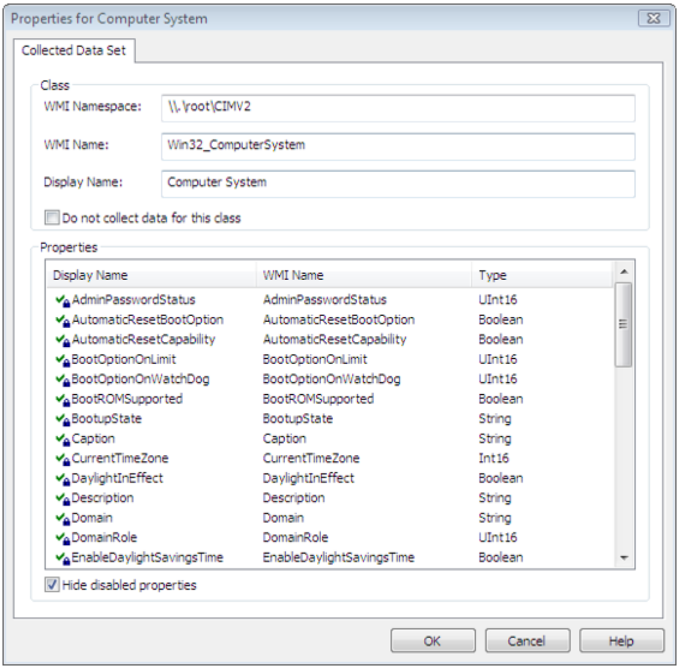
The default display name for each property is the WMI property name. You can change the property display names to make them more descriptive when showing inventory data. Descriptive property display names are also easier to use when you create filters and views.

You can specify the properties in each class that you want to collect from client computers. You can choose to collect particular properties within a class, and ignore the properties that you are not interested in. You may want to do this to make the inventory data collection process quicker and more efficient, and keep the size of the Inventory database to a minimum. By default, all properties of a class are enabled for collection, so they are included in the Inventory database.

To set up collected data set properties

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Expand the **Collected Data** folder, then expand the subfolder that contains the collected data set that you want to set up.
3. In the Collected Data pane, do one of the following:
   - Double-click the class.
   - Right-click the class, then click **Properties**.
   - Select the class, then, on the File menu, click **Properties**.
4. In the Properties for New Collected Data Set window, set up the collected data set properties to suit your requirements.

   You can sort the properties by display name, WMI name, or type, by clicking the appropriate column header to toggle the order.



Properties for Computer System

Collected Data Set

Class

WMI Namespace: \\.\root\CIMV2

WMI Name: Win32_ComputerSystem

Display Name: Computer System

□ Do not collect data for this class

Properties

Display Name	WMI Name	Type
✓ AdminPasswordStatus	AdminPasswordStatus	UInt16
✓ AutomaticResetBootOption	AutomaticResetBootOption	Boolean
✓ AutomaticResetCapability	AutomaticResetCapability	Boolean
✓ BootOptionOnLimit	BootOptionOnLimit	UInt16
✓ BootOptionOnWatchDog	BootOptionOnWatchDog	UInt16
✓ BootROMSupported	BootROMSupported	Boolean
✓ BootupState	BootupState	String
✓ Caption	Caption	String
✓ CurrentTimeZone	CurrentTimeZone	Int16
✓ DaylightInEffect	DaylightInEffect	Boolean
✓ Description	Description	String
✓ Domain	Domain	String
✓ DomainRole	DomainRole	UInt16
✓ EnableDaylightSavingsTime	EnableDaylightSavingsTime	Boolean

☑ Hide disabled properties

5 If you want to change the display name of a property, right-click the property name, then click **Rename**.

Type the new name, then press **Enter** or click anywhere in the window.

The name must be unique, and may contain up to 50 alphanumeric characters. You should choose a descriptive name that is easy to recognize when you are setting up filters and views.

6 To specify whether or not a property is collected from client computers and added to the Inventory database, right-click the property name, then click the one of the following options:

- Enable: To collect the property
- Disable: To ignore the property

The property status is indicated by the symbol beside the property display name. A green check mark means the property is enabled for data collection; an empty space means it is disabled.

You can also click directly on the space or green check mark to turn the status on and off.

A key symbol indicates a key property, and a padlock indicates a property that is currently used in a filter or view. These properties are always included in data collections, and you cannot disable them.

7 If you want to hide disabled properties, check **Hide disabled properties**.

8 If you want to ignore this collected data set when refreshing the Inventory database, check **Do not collect data for this class**.

This lets you temporarily disable all properties in the collected data set. You may want to do this to minimize the time that the refresh inventory task requires, by collecting only the data sets that you want.

9 When you have finished setting up the collected data set properties, click **OK**.

The refresh inventory task collects the enabled properties from the target computers. Any disabled properties are removed from the Inventory database.

Collected data sets that are ignored when refreshing the Inventory database are indicated in the Console by a small barred circle on the left side of the collected data set icon.

About managing collected data sets

You can organize the Collected Data folder as you want. The Console provides standard options that let you set up the folder structure, and move collected data sets within it as appropriate. You can also rename items, and delete any items that you don't need.

See "Setting the resource folder view mode" on page 73.

See "Creating new folders" on page 73.

See "Moving Symantec Ghost Console resources" on page 74.

See "Renaming Symantec Ghost Console resources" on page 75.

See "Deleting Symantec Ghost Console resources" on page 75.

Viewing inventory information

You can view the inventory information you want for client computers or computer groups by selecting pre-defined views. A view is essentially a collection of properties that you want to display.

You would typically set up a view as a group of related properties that you're interested in. For example, the Hardware view may include information such as the make and model of the client computer, its physical memory, processor speed and number and size of its hard drives. The Software view may include the operating system, versions of installed software, and any patches applied. The Networking view may include the IP and MAC addresses, Domain membership and the DNS server to which the computer is connected.

You can use views in reports, to obtain inventory information for the computers in a computer group. You can also use views to customize the information shown on the Inventory tab in the Properties window for client computers.

See "Creating reports" on page 233.

See "Setting the common Inventory view for computer groups" on page 219.

See "Setting the default Inventory views for new client computers" on page 221.

See "Viewing inventory information for client computers" on page 221.

Note: A set of pre-defined views is provided. These contain groups of properties that are commonly used. You can modify them to suit your requirements.

Creating views

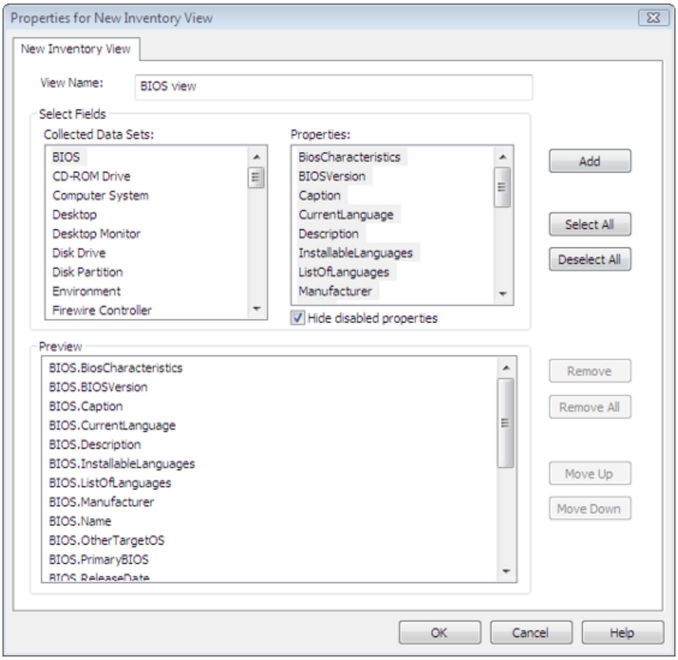
You can create new views and modify existing views at any time. When you create a view, you select the properties that you want to include.

Note: Disabled properties have no values when you use a view in a report or to display inventory information. If you want to see the values of these properties, enable the properties in the collected data set, and then perform a refresh inventory task to update the inventory database.

To create a view

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Expand the **View** folder, then select the subfolder in which you want to place the new view.
3. Do one of the following:
   - In the View pane, right-click, then click **New Inventory View**.
   - On the File menu, click **New > Inventory View**.
4. In the Properties for New Inventory View window, in the View Name box, type the name of the new view.

   The name must be unique, and may contain up to 50 alphanumeric characters. You should choose a descriptive name that indicates which properties are contained in the view.



Properties for New Inventory View

View Name: BIOS view

Collected Data Sets: BIOS, CD-ROM Drive, Computer System, Desktop, Desktop Monitor, Disk Drive, Disk Partition, Environment, Firewire Controller

Properties: BiosCharacteristics, BIOSVersion, Caption, CurrentLanguage, Description, InstallableLanguages, ListOfLanguages, Manufacturer

☑ Hide disabled properties

Preview:

BIOS.BiosCharacteristics
BIOS.BIOSVersion
BIOS.Caption
BIOS.CurrentLanguage
BIOS.Description
BIOS.InstallableLanguages
BIOS.ListOfLanguages
BIOS.Manufacturer
BIOS.Name
BIOS.OtherTargetOS
BIOS.PrimaryBIOS
BIOS.ReleaseDate

5 In the Collected Data Sets list, select the collected data set that contains properties that you want to add.

The Properties list shows the available properties for the selected data set. By default, the available properties are those that are enabled in the collected data set.

6 If you want to include disabled properties in the view, uncheck **Hide disabled properties**.

This option is checked by default. When you uncheck it, the Properties list is updated to show all properties of the selected data set, allowing you to select the properties that you want. Remember that the disabled properties are not collected from client computers until they have been enabled in the collected data set and a refresh task has been executed.

7 In the Properties list, select the properties you want to add.

If you want to select all the properties in the collected data set, click **Select All**.

If you want to clear your selection, click **Deselect All**.

8 Click **Add**.

The selected properties are added to the list in the Preview pane.

9 Repeat steps 5 through 8 for each collected data set that has properties that you want to include in the view.

10 In the Preview pane, arrange the list of properties in the order that you want them to appear when inventory information is displayed.

To move an item in the list, click it to select it, then click **Move Up** or **Move Down** as many times as necessary. Each click moves the item one place in the list.

If you want to remove an item from the list, click it to select it, then click **Remove**.

If you want to remove all items from the list, click **Remove All**.

11 When you have finished setting up the view, click **OK**.

The new view is added to the View folder.

Viewing or modifying views

You can view details of a view. You can modify a view by changing the properties to include. You may do this at any time.

To view or modify a view

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Expand the **View** folder, then select the subfolder that contains the view that you want to modify.
3. In the View pane, do one of the following:
   - Double-click the view that you want to modify.
   - Right-click the view that you want to modify, then click **Properties**.
   - Select the view that you want to modify, then, on the File menu, click **Properties**.
4. In the Properties for *View name* window, view the properties currently selected for the view, then make the appropriate changes.

   See “Creating views” on page 216.

About managing views

You can organize the View folder as you want. The Symantec Ghost Console provides standard options that let you set up the folder structure, and move views within it as appropriate. You can also rename views, and delete any views that you don’t need.

See “Setting the resource folder view mode” on page 73.

See “Creating new folders” on page 73.

See “Moving Symantec Ghost Console resources” on page 74.

See “Renaming Symantec Ghost Console resources” on page 75.

See “Deleting Symantec Ghost Console resources” on page 75.

Setting the common Inventory view for computer groups

You can set the common Inventory views for computer groups. These views are applied to all computers that are currently in the group. If a new computer is added to the group, it uses the default views set in the Console Option window.

See “Setting the default Inventory views for new client computers” on page 221.

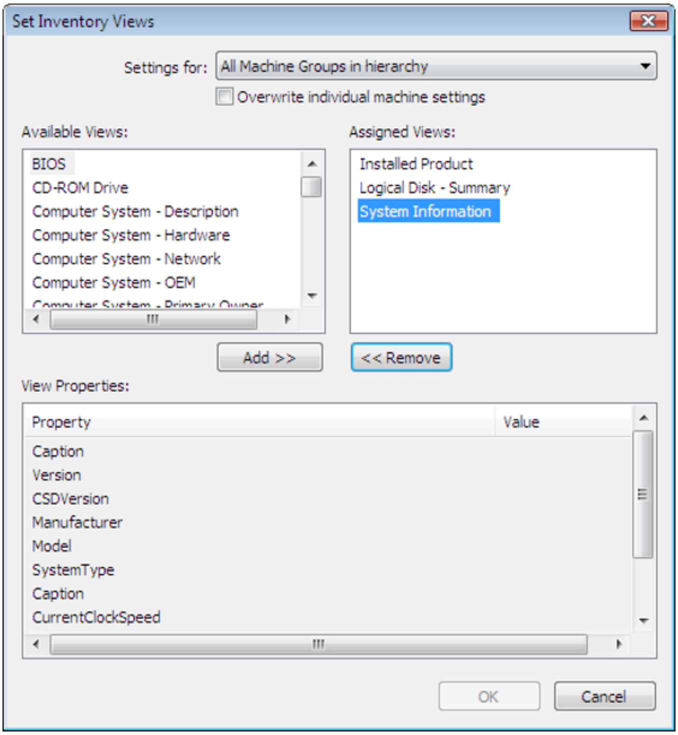
You will see the common views on the Inventory tab in the Properties window for each client computer. You can change the views for individual computers, for example, if you want to show more information for particular computers.

See “Viewing inventory information for client computers” on page 221.

To set the common Inventory view for a computer group

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. In the Machine Groups pane, right-click the computer group that you want to set up, then click **Set Inventory Views**.
3. In the Set Inventory Views window, in the Settings for box, select the appropriate option:

This Machine Group only	The view settings apply to this computer group only.
All Machine Groups in hierarchy	The view settings to apply to all computer groups in the same branch as this group.



Settings for: All Machine Groups in hierarchy

□ Overwrite individual machine settings

Available Views:

- BIOS
- CD-ROM Drive
- Computer System - Description
- Computer System - Hardware
- Computer System - Network
- Computer System - OEM
- Computer System - Primary Owner

Assigned Views:

- Installed Product
- Logical Disk - Summary
- System Information

View Properties:

Property	Value
Caption	
Version	
CSDVersion	
Manufacturer	
Model	
SystemType	
Caption	
CurrentClockSpeed	

4. If you want the computer group view settings to overwrite the individual settings for each computer in the group, check **Overwrite individual machine settings**.

5 To move the views that you want to use into the Assigned Views pane, do the following:

- To add views, select them in the Available Views pane, then click **Add**.
- To remove views, select them in the Assigned Views pane, then click **Remove**.

  The View Properties pane shows the properties (and their values if known) of the selected view. The properties are listed in the order in which they are set up in their respective views.

6 Click **OK**.

Setting the default Inventory views for new client computers

You can specify the views to use for a client computer when it is detected by the Symantec Ghost Console.

To set the default Inventory views for new client computers

1 In the Symantec Ghost Console, on the Tools menu, click **Options**.

2 On the Inventory tab, click **Modify**.

3 In the Set Inventory Views window, to move the views that you want to use into the Assigned Views pane, do the following:

- To add a view, select it in the Available Views pane, then click **Add**.
- To remove a view, select it in the Assigned Views pane, then click **Remove**.

  The View Properties pane shows the properties of the selected view.

  The properties are listed in the order in which they are set up in their respective views.

4 Click **OK**.

5 In the Options window, on the Inventory tab, click **Apply**.

Viewing inventory information for client computers

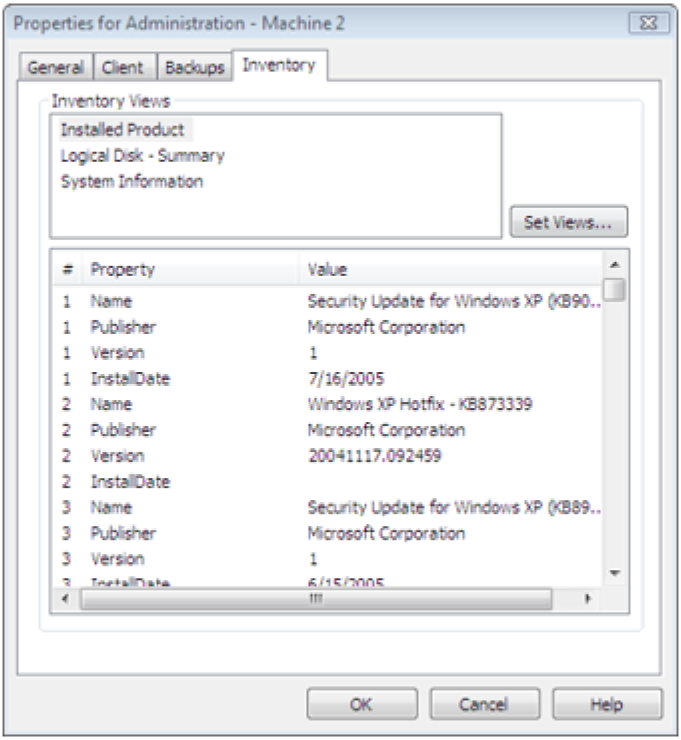
You can view inventory information for any client computer. The common views applied to the machine group folders are automatically applied to each computer. You can add views to individual computers to see more inventory information.

If you later change the common views for the computer group, the changes are merged with the views that are currently applied to individual computers in the group. The individual settings are updated to include any new views, but are not overwritten unless you choose to overwrite them.

To view inventory information for a client computer

1. In the Symantec Ghost Console, in the left pane, expand the **Machine Groups** folder.
2. Expand the computer group that contains the client computer that you want to view.
3. In the Machine Groups pane, do one of the following:
   - Double-click the computer for which you want to view inventory details.
   - Right-click the computer for which you want to view inventory details, then click **Properties**.
   - Select the computer for which you want to view inventory details, then, on the File menu, click **Properties**.
4. In the Properties for *Computer name* window, click the **Inventory** tab.

   This tab lists the views assigned to the computer. The default views are the common views currently applied to the computer groups folder.



Installed Product
Logical Disk - Summary
System Information

#	Property	Value
1	Name	Security Update for Windows XP (KB90...
1	Publisher	Microsoft Corporation
1	Version	1
1	InstallDate	7/16/2005
2	Name	Windows XP Hotfix - KB873339
2	Publisher	Microsoft Corporation
2	Version	20041117.092459
2	InstallDate	
3	Name	Security Update for Windows XP (KB89...
3	Publisher	Microsoft Corporation
3	Version	1
3	InstallDate	6/15/2005

5. In the Inventory Views list, select a view to display the instance number, name and value of each property that it contains.

6 If you want to change the views assigned to this computer, click **Set Views**.

7 In the Set Inventory Views window, to move the views that you want to use into the Assigned Views pane, do the following:

- To add a view, select it in the Available Views pane, then click **Add**.
- To remove a view, select it in the Assigned Views pane, then click **Remove**.

  The View Properties pane shows the properties of the selected view.

  If you remove a view that is one of the common views set for the computer group, it is automatically removed from the list of common views.

8 Click **OK** to close the Set Inventory Views window.

The Inventory Views pane on the Inventory tab shows the updated list of views.

9 If you want to save the changes you have made to the selected views, click **OK**.

If you want to remove the changes you have made and restore the previous selected views, click **Cancel**.

Creating and maintaining filters

A filter is a query that searches the Inventory database and returns all the records that match the specified property conditions. You can set up filters to search for the combination of properties you want. You can also set up filters to return all the records that do not match the filter conditions.

Note: You can only use properties that are enabled in the collected data sets. Disabled properties are not available. If you want to use any, you need to enable them in the collected data set first.

See "Setting up collected data set properties" on page 213.

The filters have been developed for US English client computers. As the data provided by WMI is dependent on the language of the client operating system, filters used with clients that are not US English may return an incorrect number of clients.

The Filter folder stores all the available filters. You can create new filters to suit your requirements, and can edit, copy or delete existing filters.

You can use filters in reports, to select the computers in a computer group that have particular property values. You can also use filters in dynamic machine groups, to set up virtual computer groups that contain the computers that match the filter conditions.

See “Creating reports” on page 233.

See “Creating dynamic machine groups” on page 238.

A set of pre-defined filters is provided. These are examples that illustrate the use of a filter. You can modify them to suit your requirements. The pre-defined filters include filters that are based upon the minimum requirements for Microsoft Vista as defined by Microsoft.

Creating filters

You can create new filters to suit your requirements. When you create a filter, you specify the filter conditions to use. Each filter condition is a restriction, such as a maximum or minimum value, placed on a single property. The conditions are linked by And, Or, And Not, or Or Not statements, which lets you group (nest) them as appropriate.

Before you create a filter, you should decide which filter conditions you need, and determine the grouping required. This lets you add the conditions in the correct order for the grouping you want to use. You cannot move a condition within the list.

To create a filter

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Click the **Filter** folder.
3. Do one of the following:
   - In the Filter pane, right-click, then click **New Inventory Filter**.
   - On the File menu, click **New > Inventory Filter**.

   If appropriate, you can copy an existing filter and rename it, and then modify it to suit your requirements. You may want to do this when you are creating a number of filters with the same components.
4. In the Properties for *Filter name* window, in the Filter Name box, type the new filter name.
5. Set up the filter conditions that you require.

   See “Setting up filter conditions” on page 225.

6. If you need to nest certain groups of conditions, or need two or more conditions to apply to the same instance of a class, create the appropriate groups.

   See “Grouping filter conditions” on page 228.

7. If you want to remove a condition, select it, then click **Delete**.

   The grouping, if any is applied to the condition, is automatically adjusted.

8. Specify whether you want to select the computers that match the filter conditions, or those that do not match the filter conditions, by clicking one of the following:

   - All machines from the Target group matching these filter conditions
   - All machines from the Target group that do not match these filter conditions

9. Click **OK** to save the filter.

   The new filter is added to the Filter pane, and is available for you to use in a report or dynamic machine group.

Setting up filter conditions

You can add or modify filter conditions as required.

To set up a filter condition

1. In the Properties for *Filter name* window, do one of the following:

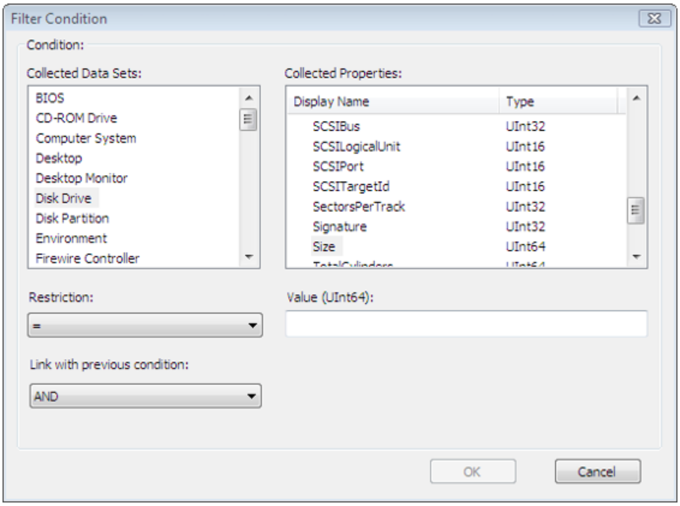
   - If you want to add a new condition, select the condition below that you want to add the new one, and then click **Add**.
     If you don’t select a condition, the new condition is added to the bottom of the list.

- If you want to modify a condition, select it and then click **Modify**.

2 In the Filter Condition window, in the Collected Data Sets pane, select the data set that contains the property for which you want to set a condition.

The Collected Properties pane lists all the available properties in the selected collected data set.

Available properties are those that are currently enabled for collection in the collected data sets. If a property is disabled in the collected data set, you cannot use it in a filter.



Collected Data Sets:

BIOS
CD-ROM Drive
Computer System
Desktop
Desktop Monitor
Disk Drive
Disk Partition
Environment
Firewire Controller

Collected Properties:

Display Name	Type
SCSIBus	UInt32
SCSILogicalUnit	UInt16
SCSIPort	UInt16
SCSITargetId	UInt16
SectorsPerTrack	UInt32
Signature	UInt32
Size	UInt64
TotalCylinders	UInt64

Restriction: =

Link with previous condition: AND

3 In the Collected Properties pane, select the property for which you want to set a condition.

4 In the Restriction box, from the drop-down list, select the operator that you want to use for the property.

The list contains all the operators that are relevant to the type of property selected.

The available comparison operators (conditions) and their limitations are described as follows:

=	Equal to	All except Array
< >	Not equal to	All except Array
<	Less than	All except Array and Boolean
<=	Less than or equal	All except Array and Boolean
>	Greater than	All except Array and Boolean
>=	Greater than or equal	All except Array and Boolean
Contains	Contains the specified string	String and Array only
Not Contains	Does not contain the specified string	String and Array only
Is Empty	Contains no characters	String and Array only
Is Not Empty	Contains characters	String and Array only
Is Null	Property does not exist; no instances collected	All property types
Is Not Null	Property exists; one or more instances collected	All property types

The numeric operators refer to the alphabetical order when applied to strings.

5 In the Value field, specify the value against which you want to compare the property as follows:

Boolean	Select the value from the drop-down list.
String, Array, UInt	Type the value.
DateTime	In the Value box, click to open a calendar, then select the date. If you want to specify a time as well, check **Time**, then type the time value or set it using the arrow buttons.

6 In the Link with previous/next condition drop-down list, select one of the following:

- AND
- OR
- AND NOT
- OR NOT

The default is AND. If you are adding a new condition, you can specify the link with the previous condition. If you are modifying a condition, you can specify the link with the next condition.

7 Click **OK**.

If you are creating a new condition, it is added to the list in the Properties for <Filter name> window.

Grouping filter conditions

By default, the filter conditions are evaluated in the order in which they are listed, and the links between them have the same priority. Each condition is evaluated independently of other conditions.

If you want to give higher priority to the links between particular conditions, or make two or more conditions apply to the same class instance, you need to group the filter conditions.

You can group filter conditions as follows:

Group	Evaluate the conditions as a single unit within the list of conditions. See “Grouping (nesting) filter conditions” on page 229.
Group on Instance	Evaluate the conditions on the same instance of a class. See “Grouping filter conditions on instance” on page 230.

Grouping (nesting) filter conditions

You can group two or more conditions as a single unit within the list of conditions. The grouped conditions are evaluated before the conditions outside the group.

A group may contain multiple nested levels of sub-groups, but each sub-group must be completely within its parent group. When a filter contains multiple levels of grouping, the innermost group is evaluated first.

For example, if you have a number of computers, with some running Windows XP and some running Windows 2000, you can apply the following filter:

```
OperatingSystem.Name       =   Windows XP      AND
 PhysicalMemory.Capacity    >   512 Mb     OR
 OperatingSystem.Name       =   Windows 2000    AND
 PhysicalMemory.Capacity    <   256 Mb
```

Without grouping, this filter returns only the Windows 2000 computers that have less than 256 MB of memory. The Windows XP computers that were selected with the first two conditions are not returned as they do not satisfy the fourth condition.

To make the filter return the Windows XP computers that have over 512 MB of memory and the Windows 2000 computers that have less than 256 MB of memory, you need to group each OperatingSystem condition with the corresponding PhysicalMemory condition. This grouping is shown below:

```
 (  OperatingSystem.Name      =    Windows XP         AND
    PhysicalMemory.Capacity   >    512 Mb    )   OR
 (  OperatingSystem.Name      =    Windows 2000       AND
    PhysicalMemory.Capacity   <    256 Mb    )
```

The grouping is indicated in the list of conditions as follows:

An opening parenthesis in the (... column	The first condition in the group.
A closing parenthesis in the ...) column	The last condition in the group.

When you delete conditions from a group, the grouping is automatically adjusted according to the remaining group start and end conditions. The grouping adjustment depends on whether the deleted conditions are at the start or end of the group, or in the middle as follows:

Conditions deleted from within a group, and no end-of-group conditions deleted.	Grouping is preserved on remaining conditions.

Condition deleted from start or end of a group.	Grouping is removed from remaining conditions. If a deleted condition is the start or end of two or more nested groups, all nested groups are ungrouped.

To group (nest) filter conditions

1. In the Properties for *Filter name* window, in the list of conditions, select the conditions that you want to group.

   You can select all the conditions, or just the first and last conditions. Any unselected conditions between the selected conditions are automatically included in the group.

2. Click **Group**.

   The grouping is indicated in the list of conditions.

3. If you need to undo any grouping, select all the conditions in the group, or the first or last condition of the group, then click **Ungroup**.

   If the selected condition is the first or last for two or more groups, the outermost group is ungrouped.

Grouping filter conditions on instance

If you need to apply two or more conditions to the same instance of a class, you can group the conditions on instance. When you do this, all the conditions in the group must be satisfied for properties of the same class instance. The same restrictions as for a nested group apply, but you cannot create any sub-groups on instance.

For example, you might have a computer with two logical disks as follows:

- Drive C: NTFS, 10 gigabytes
- Drive D: FAT, 30 gigabytes

You can apply the following filter:

```
LogicalDisk.FileSystem     =    NTFS         AND
LogicalDisk.Size           >    20 Gb
```

By default, the filter returns this computer because both conditions are met, one on each logical disk, even though the computer does not contain a disk that meets the filter criteria.

To make the filter exclude the computer unless it contains a logical disk that satisfies both the conditions, you need to group the conditions on instance:

```
 (   <* LogicalDisk.FileSystem   =   NTFS      AND
         *>LogicalDisk.Size          >     20 Gb    )
```

The grouping is indicated in the Property column, as follows:

<* preceding the class name	The first condition in the group on instance.
* preceding the class name	A condition (not the first or last) in the group on instance.
*> preceding the class name	The last condition in the group on instance.

A group on instance is automatically a nested group. This grouping is indicated by the (symbol in the (... column and the) symbol in the ...) column.

When you add conditions to the filter within a group on instance, you are restricted to properties for the same class as in the group.

To group filter conditions on instance

1. In the Properties for *Filter name* window, in the list of conditions, select the conditions that you want to group on instance.

   You can select all the conditions, or just the first and last conditions. Any unselected conditions between the selected conditions are automatically included in the group.

   All the conditions must relate to the same class in order to group them on instance.

2. Click **Group on Instance**.

   The grouping is indicated in the list of conditions, in the Property column.

3. If you need to undo the grouping on instance, select all the conditions in the group, or the first or last condition of the group, then click **Ungroup**.

Viewing or modifying filters

You can view details of a filter. You can modify a filter by changing the conditions it contains. You may do this at any time.

Note: If the filter is used in a dynamic machine group, any changes to the filter conditions affect the dynamic machine group.

To view or modify a filter

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Click the **Filter** folder.

3 In the Filter pane, do one of the following:

- Double-click the filter that you want to modify.
- Right-click the filter that you want to modify, then click **Properties**.
- Select the filter that you want to modify, then, on the File menu, click **Properties**.

4 In the Properties for *Filter name* window, view the conditions currently set for the filter, then make the appropriate changes.

If the filter is used in a dynamic machine group that is the target of a task, a warning message is shown. Click **Details** to view the list of tasks that are affected by changes to the filter.

See “Setting up filter conditions” on page 225.

5 Click **OK**.

About managing filters

You can organize the Filter folder as you want. The Symantec Ghost Console provides standard options that let you set up the folder structure, and move filters within it as appropriate. You can also rename filters, and delete any filters that you don’t need.

See “Setting the resource folder view mode” on page 73.

See “Creating new folders” on page 73.

See “Moving Symantec Ghost Console resources” on page 74.

See “Renaming Symantec Ghost Console resources” on page 75.

See “Deleting Symantec Ghost Console resources” on page 75.

Creating and running reports

A report is simply the association of one filter, one view, or one of each, and a target computer group. You cannot have two or more filters or views in the same report. If you run a report on a single computer, you must use a view; you cannot use a filter.

The output of a report depends on whether or not it includes a view. If the report has no view (just a filter), the output is the list of computers that satisfy the filter criteria. If the report contains a view, the output is the list of computers in the target computer group, and the values of the properties contained in the view.

You need to set up your filters and views before you can include them in a report. If necessary, you can create a new filter or view as you set up your new report.

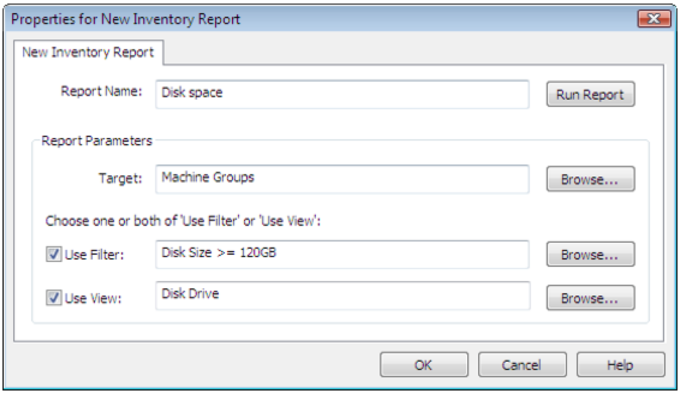
Creating reports

You can create a new report at any time, and can use any combination of filters and views. You can preview a report by running it immediately, or you can save it in the Reports folder and run it later.

To create a report

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Click the **Report** folder.
3. Do one of the following:
   - In the Report pane, right-click, then click **New Inventory Report**.
   - On the File menu, click **New > Inventory Report**.
4. In the Properties for New Inventory Report window, in the Report Name field, type the name of the new report.

   The name must be unique, and may contain up to 50 alphanumeric characters. You should choose a descriptive name that indicates what information is contained in the report.



Properties for New Inventory Report

New Inventory Report

Report Name: Disk space

Report Parameters

Target: Machine Groups

Choose one or both of 'Use Filter' or 'Use View':

☑ Use Filter: Disk Size >= 120GB

☑ Use View: Disk Drive

5. Next to the Target box, click **Browse** then, in the Select Target window, select the computer group that you want to use as the target of the report.
6. If you want to use a filter in the report, check **Use Filter**, then click **Browse**.

7 In the Select Inventory Filter window, select the filter that you want to use in the report.

If you need to create a new filter, in the Select Filter window, click **New** to open the Properties for New Filter window, then specify the appropriate details.

See “Creating filters” on page 224.

8 If you want to use a view in the report, check **Use View**, then click **Browse**.

9 In the Select Inventory View window, select the view that you want to use in the report.

If you need to create a new view, in the Select Inventory View window, click **New** to open the Properties for New View window, then specify the appropriate details.

See “Creating views” on page 216.

10 If you want to preview the report results before saving the report, click **Run Report**.

11 In the Inventory Report Results window, view the results, then click **Close**.

12 Click **OK** to save the report.

The new report is added to the Report folder.

Viewing or modifying reports

You can view details of a report, and can change the name, the filter, the view, or the target computer group if necessary.

To view or modify a report

1 In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.

2 Click the **Report** folder.

3 In the Report pane, do one of the following:

- Double-click the report you want to modify.
- Right-click the report that you want to modify, then click **Properties**.
- Select the report you want to modify, then, on the File menu, click **Properties**.

4 In the Properties for *Report name* window, view the report properties, then make the appropriate changes.

See “Creating reports” on page 233.

About managing reports

You can organize the Report folder as you want. The Symantec Ghost Console provides standard options that let you set up the folder structure, and move reports within it as appropriate. You can also rename reports, and delete any reports that you don't need.

See "Setting the resource folder view mode" on page 73.

See "Creating new folders" on page 73.

See "Moving Symantec Ghost Console resources" on page 74.

See "Renaming Symantec Ghost Console resources" on page 75.

See "Deleting Symantec Ghost Console resources" on page 75.

Running a report

You can run a report to obtain inventory information from the database. You should update the inventory database before running a report to ensure that the report results are up-to-date.

The following formats are for report results, depending on whether or not a view is included:

If the report contains a view	The output is a table listing computers and the values of the properties that were included in the view. You can set the sort order for each column by clicking the column headers. If the report contains a filter and a view, the table contains the computers that match the filter conditions. If the report does not contain a filter, the table contains all the computers in the target computer group.
If the report does not contain a view (just a filter)	The output is the list of computers in the target computer group that meet the filter criteria. For example, you may want to obtain a list of computers that have the prerequisites for a software rollout.

You can print the report results, or export the results to a formatted text file or a comma-separated file. You can also create a new dynamic machine group from the report.

See "Printing the report results" on page 236.

See "Exporting the report results to a file" on page 236.

See "Saving a report as a dynamic machine group" on page 237.

Note: You can also run a report directly from the Properties for <Report name> window, by clicking Run Report.

To run a report

1. In the Symantec Ghost Console, in the left pane, expand the **Inventory** folder.
2. Click the **Report** folder.
3. In the Report pane, do one of the following:
   - Right-click the report that you want to run, then click **Run Report**.
   - Select the report that you want to run, then, on the View menu, click **Run Report**.
4. In the Inventory Report Results window, view the report result.
5. If you want to preserve the report results, you can save the report as a dynamic machine group, export the results to a file, and print the results.
6. Click **OK** to close the Inventory Report Results window.

Printing the report results

You can print the report results on any printer that the Console can access.

To print the report results

1. In the Inventory Report Results window, click **Print**.
2. In the Print window, select the appropriate settings.
3. Click **OK**.

Exporting the report results to a file

You can export the report results to a formatted text file, or a comma-separated file. The file can be exported to any directory that the Console can access.

To export the report results to a file

1. In the Inventory Report Results window, click **Export**.
2. In the Export Inventory Report To window, browse to the location to which you want to export the results.
3. In the File Name field, type the file name.
4. In the Save as Type drop-down list, select one of the following:
   - Formatted Text File
   - Comma-separated File

- Comma-separated File (legacy format)

5 Click **OK**.

The file is saved in the specified location, and is automatically opened in Notepad.

6 View the file and make any appropriate changes or add extra information.

7 If necessary, save your changes, then close Notepad.

Saving a report as a dynamic machine group

You can save the filter and target computer group association in a report as a new dynamic machine group. The dynamic machine group contains only the computers in the target computer group that match the filter criteria. Computers may be added to, or removed from, a dynamic machine group as their property values change. Any view in the report is ignored, as a view always applies to all computers in the target group.

See "Setting up dynamic machine groups" on page 237.

To save a report as a dynamic machine group

1 In the Inventory Report Results window, click **Save**.

2 In the Properties for New Dynamic Machine Group window, type the name for the dynamic machine group.

3 Click **OK**.

The new dynamic machine group is added to the Dynamic Machine Groups folder.

Setting up dynamic machine groups

A dynamic machine group is similar to a report, but consists only of a filter applied to a target computer group. Dynamic machine groups are populated each time the inventory database is updated, and contain all the computers in the target computer group that currently match the filter conditions. The members of a dynamic machine group may change as their property values change.

Dynamic machine groups are stored as folders within the Dynamic Machine Groups folder. Each dynamic machine group can be used as the target of a task, in the same way as a computer group.

Note: You may want to refresh the inventory database before you use a dynamic machine group as the target of a task, to ensure the dynamic machine group contains the appropriate computers. The inventory database is not updated automatically.

Creating dynamic machine groups

You can create a new dynamic machine group at any time, and can use any filter and target computer group.

You can also create a dynamic machine group directly from the results of a report.

See "Saving a report as a dynamic machine group" on page 237.

To create a dynamic machine group

1. In the Symantec Ghost Console, in the left pane, expand the **Dynamic Machine Groups** folder.
2. Do one of the following:
   - In the Dynamic Machine Groups pane, right-click, then click **New Dynamic Machine Group**.
   - On the File menu, click **New > Dynamic Machine Group**.
3. In the Properties for New Dynamic Machine Group window, in the Dynamic Machine Group Name box, type the name of the new dynamic machine group.

   The name must be unique, and may contain up to 50 alphanumeric characters.
4. Next to the Target box, click **Browse**, then, in the Select Target window, select the computer group that you want to use as the target of the dynamic machine group.
5. Next to the Filter Name box, click **Browse**, then, in the Select Inventory Filter window, select the filter that you want to use in the dynamic machine group.

   If you need to create a new filter, in the Select Filter window, click **New** to open the Properties for New Filter window, then specify the appropriate details.

   See "Creating filters" on page 224.
6. Click **OK**.

   The new dynamic machine group is added to the Dynamic Machine Groups folder.

Viewing or modifying dynamic machine groups

You can view details of a dynamic machine group, and can change its name, the filter used, or the target computer group.

To view or modify a dynamic machine group

1. In the Dynamic Machine Groups pane, do one of the following:
   - Right-click the dynamic machine group that you want to view, then click **Properties**.
   - Select the dynamic machine group that you want to view, then, on the File menu, click **Properties**.
2. In the Properties for *Dynamic machine group name* window, view the details of the dynamic machine group, then make any appropriate changes.

   See "Creating dynamic machine groups" on page 238.

About managing dynamic machine groups

You can rename or delete dynamic machine groups. You cannot create folders inside the Dynamic Machine Groups folder, and you cannot copy or move dynamic machine groups.

See "Renaming Symantec Ghost Console resources" on page 75.

See "Deleting Symantec Ghost Console resources" on page 75.

Chapter 10

Additional Console options

This chapter includes the following topics:

- Monitoring Symantec Ghost Console activity
- Launching the Configuration Server
- Setting Symantec Ghost Console options
- Symantec Ghost Console security
- Changing the Symantec Ghost database account and password

Monitoring Symantec Ghost Console activity

Table 10-1 lists the logs and summaries with which you can review the history of a task or client computer.

Table 10-1 Logs and summaries

Logs/summaries	Description
Task Log	The history of execution for all tasks. See "To view the Task Log" on page 242.
Scheduler	A list of the tasks that are scheduled to run. See "To view or modify a list of scheduled tasks" on page 243.
Console Log	A log of all steps occurring during the execution of tasks from the command line or scheduler. See "To view the Console Log" on page 243.
Client Summary	A summary of all executions for a client computer. See "To view a Client Summary" on page 243.

Table 10-1 Logs and summaries *(continued)*

Logs/summaries	Description
Event Log	The history of all events for all computers for a task. See "To view the Event Log" on page 243.
User Migration report	This report is generated for each capture and restore operation. It lists the users that were captured, and any users or files that were not captured, and the users that were restored, and any users and files that could not be restored. This report can be opened from the Ghost Console or from Symantec User Migration Package Explorer. See "About User Migration reports" on page 200.
Ghost error file	The error file that is created on the client computer if an image create or image restore task fails. See "To view the Event Log" on page 243.
Event Details	The details for an item in the Client Summary or Event Log. See "To view Event Details" on page 244.
Active Tasks	The lower pane of the Console that shows details of tasks that are currently executing. See "To view Event Details" on page 244.

To view the Task Log

1. In the Symantec Ghost Console, on the View menu, click Task Log.
2. In the Task Log window, on the View menu, select a sort option:
   - Time: Time and date of execution
   - Name: Task title
   - User: User name from the logon window
   - Clients
   - Clients OK
   - Warnings

   Any task executed from the command line is logged under the user name command.

   When a task cannot be completed successfully, the Task Log contains diagnostic data if it is available.

To view or modify a list of scheduled tasks

1. In the Symantec Ghost Console, on the View menu, click **Scheduler**.
2. To view or modify the schedule properties, double-click the task.

To view the Console Log

1. In the Symantec Ghost Console, on the View menu, click **Task Log**.
2. In the Task Log window, on the View menu, click **Console Log**.

To view a Client Summary

1. In the Symantec Ghost Console, on the View menu, click **Task Log**.
2. In the Task Log window, select the task for which you want to view the log.
3. In the Task Log window, on the View menu, click **Client Summary**.
4. In the Client Summary window, double-click an item to open the Client Summary.

To view the Event Log

1. In the Symantec Ghost Console, on the View menu, click **Task Log**.
2. In the Task Log window, select the task for which you want to view the log.
3. In the Task Log window, on the View menu, click **Event Log**.
4. In the Event Log window, on the View menu, select a sort option:
   - Time: Time and date of execution
   - Step: Alphabetical sort of the steps in the task
   - Client: Computer name
5. In the Event Log window, on the View menu, click **View Ghost error file** to view the Ghost error log.

To view the Migration Report from the Ghost Console

1. In the Symantec Ghost Console, on the View menu, click **Task Log**.
2. In the Task Log window, select the task for which you want to view the log.
3. In the Task Log window, on the View menu, click **Event Log**.

   You can also open the Event Log by right-clicking the task in the bottom panel of the Ghost Console.
4. Highlight the step with a warning, then click **View Error file**.

To view Event Details

1. In the Symantec Ghost Console, on the View menu, click **Task Log**.
2. In the Task Log window, select the task for which you want to view the log.
3. In the Task Log window, on the View menu, click **Event Log**.
4. In the Event Log window, on the View menu, click **Event Details**.

To view Active Tasks

- In the Symantec Ghost Console, on the View menu, click **Active Task Pane**.

Launching the Configuration Server

The Configuration Server manages task executions and communication with clients. It usually runs in the background and does not require direct access.

However, you can manually launch the Configuration Server from the Symantec Ghost Console if you need to for any reason, for example, if you have closed down the Configuration Server by mistake.

To launch the Configuration Server

- In the Symantec Ghost Console, on the File menu, click **Launch Server**.

  This item is unavailable if the Configuration Server is already running.

Setting Symantec Ghost Console options

You can set the following user options in the Symantec Ghost Console:

Optional splash screen	If you select this option, a splash screen appears when the user opens the Console.
Turn off Ghost watermark	The Ghost watermark is the large, transparent icon in the lower-right of each folder.
Optional task start and stop messages	If you select this option, an message appears when you start a task and end a task.
Casual task warning	If you select this option, a warning message appears when you try to close a task without saving it.
Task log history	You can select the number of days that you want to retain a task log. You can also choose to clear the task log.

Number of minutes the Configuration Server waits for a client to respond after each step of a task	If the client fails to respond within the specified time, the task fails.
Folder in which to store baseline and incremental backups	See "Setting the location for backup images" on page 166.
Folder in which to store User Migration packages	See "Setting the storage location for user packages" on page 201.
Abort task warning	You can choose to warn users that you are about to run a task give them the option to cancel the task.
Frequency with which status reports are sent from Console client computers to the Console	This lets you reduce network traffic if required. This may be useful if computers are networked over a WAN. You can also set the client heartbeat for each subnet and for each client computer. If you set the client heartbeat to 0, then the status of the client computer is indicated as Unavailable on the Console. See "Setting the default client heartbeat interval" on page 82. See "Setting properties for a subnet" on page 84. See "Setting the client computer heartbeat interval" on page 88.
Set the default PreOS version for the virtual partition	You can select a default PreOS version that is installed when the virtual partition is created on a client. The client computer runs under the selected PreOS. You can select MS-DOS only if it is installed on your computer. See "Setting the Virtual Partition PreOS" on page 91.
Allow tasks to be initiated from a client computer	If a task is set up to run from a client, then you can initiate the execution of the task from the client computer. This lets end users execute tasks, or administrators execute tasks immediately from a client without having to return to the Console computer.

Control the amount of network bandwidth used	Symantec Ghost lets you control how much network bandwidth is used when transferring image files, data files, user packages or AI packages between the Console server and the client computers. By using this functionality, you can avoid overloading the network with GhostCasting traffic. See "Setting the default data transfer properties" on page 82.
Set the data transfer mode	You can set the data transfer mode depending on your network hardware setup. Used in conjunction with the network bandwidth limits, you can optimize the way in which image files, MTU user packages, and AI packages are transferred over your network. You can alter these settings globally, for a task, and for a single execution of a task. See "Setting the default data transfer properties" on page 82.
Set Inventory options	You can choose to show collected data sets in the Inventory folder and set default inventory views. See "Setting the default Inventory views for new client computers" on page 221. See "Showing the Collected Data folder" on page 209.

To display the splash screen

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. On the Preferences tab, check **Display Splash Screen on start**.
3. Click **Apply**.

To display the Ghost watermark in the Symantec Ghost Console

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. On the Preferences tab, check **Display Watermarks**.
3. Click **Apply**.

To display task start and finish messages

1. In the Symantec Ghost Console, on the Tools menu, click **Options**.
2. On the Preferences tab, check the following:
   - Display Task Start Message

- Display Task Finish Message

3 Click **Apply**.

To remind users to save a task

1 In the Symantec Ghost Console, on the Tools menu, click **Options**.

2 On the Preferences tab, check **Display Casual Task Warning**.

3 Click **Apply**.

To set the Task Log option

1 In the Symantec Ghost Console, on the Tools menu, click **Options**.

2 On the Preferences tab, under Task Log, type the number of days that you want to keep tasks in the log.

The maximum amount of time that you can keep tasks in the log is one year.

3 Click **Clear Log** to clear the Task Log immediately.

4 Click **Apply**.

To warn the client about a task

1 In the Symantec Ghost Console, on the Tools menu, click **Options**.

2 On the Client tab, in the Warn client field, type the number of seconds.

This causes a warning message to appear on the client computer a specified number of seconds before a task runs.

3 Click **User can abort an operation** to let the user abort the task.

4 Click **Proceed with operation if no user intervention** to let the task continue if the user does not respond to the warning message.

5 Click **Apply**.

To set the configuration server timeout option

1 In the Symantec Ghost Console, on the Tools menu, click **Options**.

2 On the Preferences tab, under Server Timeout, type the number of minutes that you want the configuration server to wait for clients.

3 Click **Apply**.

To allow client-initiated tasks

1 In the Symantec Ghost Console, on the Tools menu, click **Options**.

2 On the Client tab, click **Enable Client User Interface** to allow client computers to initiate execution of tasks.

3 Click **Apply**.

Symantec Ghost Console security

The Symantec Ghost Console Server and clients use public-key cryptography techniques to authenticate the server to the client. This ensures that only authorized servers remotely control, back up, restore, clone, and reconfigure client computers. During the Symantec Ghost Console Server installation, public and private certificate files are generated. These files are called Pubkey.crt and Privkey.crt.

These private certificates must be safeguarded. If an unauthorized user copies one, security is compromised. If you accidentally delete your private certificate and have no other copy, generate a new certificate pair and distribute the public certificate to all clients.

See "Generating new certificates" on page 248.

When a client communicates with the server, it uses a challenge-response protocol. The client must have the server's public certificate to perform this operation. Therefore, the server's public certificate must be distributed to all clients.

When the Console client is installed, it prompts for the Console computer name. This is the Windows computer name specified in Windows network settings. The client uses this name to communicate with the correct Console.

If the client computer is installed with a Ghost boot partition, you can generate a boot disk and a boot partition image file with the Ghost Boot Wizard. Use the wizard from the Console Server to ensure that the correct public certificate file is automatically included with all boot partition image files that include the Console client. If the client is installed with the virtual partition, this is done automatically.

Updating the client certificates

If you have more than one Symantec Ghost Console in your organization and you want to move a client from one to another, the public certificate must be updated on the client. You can do this manually by copying the Pubkey.crt file from the Console to which you want to move the client. You can also do this by performing a remote client install from the Console to which you want to move the client. This changes the Pubkey.crt on the client computer. After replacing Pubkey.crt restart the client service to ensure that the service uses the updated certificate.

Generating new certificates

If you lose your private certificate or if you think that security has been compromised, you should generate a new certificate pair and distribute the public certificate to all clients. You can distribute the certificate manually by copying the Pubkey.crt file to each client. You can also distribute the certificate to each client by performing a remote installation from the Console. The remote installation replaces the Pubkey.crt file on the client computer.

See “Updating the client certificates” on page 248.

To generate new certificates

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

2 Browse to the Symantec Ghost installation directory.

   The default directory is C:\Program Files\Symantec\Ghost.

3 Type **ngserver.exe -keygen**

Changing the Symantec Ghost database account and password

When you first install the Symantec Ghost Console, a user name and password are created for the Ghost database. This lets you access the database directly, for example, to run a script.

Warning: You should directly access the database only if you are an experienced user.

You can change the password to increase security on the database.

To change the database password

1 In the Symantec Ghost Console, on the Tools menu, click **Database Password**.

2 In the Database Credentials dialog box, in the Password field, type a new password.

3 Click **OK**.

Using a script file to manage your database credentials

You can retrieve the Ghost database account and password by using the scripting API for the Ghost Configuration Server service. You can use the script in one of the following ways:

With no arguments	Retrieves the user account name and password that are used by the Ghost Console to access the configuration database.
With one argument	Sets the password for the user account that is used by the Ghost Console to access the configuration database.

With two arguments, the first being the string dba	This lets you set a password for the built-in DBA user account for which you may have dependent code. This user account is turned off during installation for additional security. You can activate the account by running this script.

The script is as follows:

```
<job id="PasswordUtility">

<script language="VBScript"

' Access the Configuration Server service's root COM scripting object

set server = CreateObject("ConfigServer.Application")

' Get the database configuration object from the configuration server

set dbInfo = server.ConfigDatabase

'Obtain the current database username and password

user = dbInfo.Username

pass = dbInfo.Password

set args = WScript.Arguments

if args.Count = O then

WScript.Echo "User: " & user & vbCr & "Password: " & pass

elseif args.count = 2 and args.item(0) = "dba" then

pass = args.item(1)

call dbInfo.SetCredentials ("dba", pass)

end if

</script>

</job>
```

Section 3

Creating boot disks, exploring image files and Symantec Ghost support

Chapter 11

Creating boot packages with the Ghost Boot Wizard

This chapter includes the following topics:

- Specifying additional services
- Specifying the client to include
- Including additional files
- Setting up external storage support
- Setting up network client configuration
- Specifying the destination drive
- Selecting network drivers
- Specifying the network settings
- Specifying the Ghost Image details
- Specifying the TCP/IP Network Boot Image details
- Specifying the RIS menu details
- Creating a DOS boot disk manually
- Supporting regional keyboards and character sets

About the Symantec Ghost Boot Wizard

The Ghost Boot Wizard creates boot packages that let you complete various Ghost tasks. For any task, the Ghost Boot Wizard guides you through the steps for selecting the settings and drivers that you need to create the boot package.

About Ghost boot packages

A Ghost boot package lets you restart a computer from the package in DOS or Windows PE. If the package contains the Ghost executable, the computer starts Ghost.exe. You can then run Ghost.exe to back up, restore, and clone the computer from DOS or Windows PE without using the Console.

A Ghost boot package can be any of the following:

The Ghost executable, PreOS, and driver files that are loaded from a floppy disk set, VMware Virtual Floppy, or USB disk to let you run Ghost.exe on your computer

The PreOS must be DOS in order to create floppy disk sets or VMware virtual floppies. If you use Win PE as the PreOS to create a USB boot disk, you need at least 256 MB of free space on the USB drive.

Depending on the driver files that are included on your boot disk, the Ghost Boot Wizard usually requires three floppy disks to make a boot disk set. A Mapped Network Drive boot package may fit on one disk.

Symantec fully supports USB flash drives as removable devices; however other devices also work with these options.

Note: If you are using MS-DOS, when you format a USB drive using the Ghost Boot Wizard one partition is created with maximum size of 2 GB. You cannot create another partition in any remaining free space. For PC-DOS and WinPE, the partition is the size of the USB drive.

An image file

An image file that loads DOS and driver files from a network to let you run Ghost.exe on your computer without a boot disk

An ISO image

An ISO image that you can write to a CD or DVD to create a bootable CD or DVD that runs Ghost on your computer

Note: Multicard templates are not supported for ISO images.

A CD/DVD ROM Image

You can create a bootable CD or DVD by writing the image directly to a CD/DVD ROM.

Note: BluRay and HD DVD are not supported.

A One-Click Virtual Partition

A zip file, an executable, and a shortcut that runs the executable with the zip file as a parameter. You can store this on a network share and run it from the destination machine simply by clicking the shortcut.

Components of Ghost boot packages

The following files are required to run Ghost.exe and are included in a boot package:

Ghost.exe

The Ghost executable that is run from DOS or Windows PE.

Note: Mapped Network Drive packages might not include Ghost.exe.

DOS or Windows PE system files	PC-DOS and Windows PE are supplied for the purpose of creating Ghost boot packages. The appropriate PreOS files are installed automatically when you create the boot package using the Ghost Boot Wizard.
Any files and drivers required to access the selected hardware	This includes CD-R/RW drivers, network protocol files, or network interface card (NIC) drivers, or any other files for external storage access. **Note:** For best performance , you should use the latest version of the NIC driver. You might need to download the driver from the manufacturer.

Note: In versions previous to 8.0 of Symantec Ghost, MSCDEX was required to read an image from a CD. If you created a bootable CD using any version of Symantec Ghost you do not need to include MSCDEX in the boot package. If you created a bootable CD with another utility, MSCDEX must be included.

When to include a network card driver

If the boot package includes network support, the Universal Packet Driver (UNDI driver) enables detection of network cards in most computers without a specific network card driver. If the boot package does not work on a computer, then a new boot package must be created that uses the correct network card driver.

The UNDI driver can replace a specific driver in most of the following situations:

- If the computer has been manufactured within the last two or three years
- If the computer supports network booting using PXE (version 2.1)

Note: Symantec Ghost supports any version of PXE when booting a computer over a network from a PXE server.

The UNDI drivers support multiple network interface cards (NIC) in a computer. If you have more than one NIC in your computer, and you do not use the UNDI driver, then it is possible that Ghost might not select the correct card. If you do not want to use the UNDI driver, then you should edit the Protocol.ini file to select the correct card.

See “About Symantec Ghost support for multiple network interface cards ” on page 290.

The UNDI driver installation loads a driver from the option ROM of a network card. If any one of the following is disabled in the BIOS, you must enable the option in the BIOS before using the UNDI driver:

- Option ROM
- PXE
- UNDI

Symantec provides a Universal Packet Driver, but to create a mapped network boot package, you must provide a Universal NDIS Driver. When creating the mapped network boot package you are prompted for the location of the Universal NDIS Driver.

See "Downloading and installing a Universal NDIS driver" on page 257.

Downloading and installing a Universal NDIS driver

An NDIS Driver is required for windows networking support, which is required to map a drive. The Universal NDIS driver is supplied by 3Com.

The operation of the Universal NDIS Driver is largely dependent on a successful load of undi_drv.exe supplied with Ghost. Sometimes this driver may not load correctly on all computers. In that case, you should install and use a specific driver.

To download and install a Universal NDIS driver

1. Go to http://support.3com.com/infodeli/tools/nic/mba.htm and download the latest version of the 3Com MBA utilities.
2. Unzip the package.
3. When you are prompted for the location of the universal driver, select **MBAUtil\TCPIP**.

When to include MS-DOS in a boot package

Symantec Ghost supplies Windows PE and PC-DOS for you to include in a Ghost boot package. However, some computer models may not start from a Ghost boot package that contains either of these. If your computer does not start from a Ghost boot package, you should create a new Ghost boot package from the Ghost Boot Wizard and include Windows 95/98 MS-DOS.

Before you create an MS-DOS Ghost boot package, you must provide Windows 95/98 MS-DOS for the computer that is running the Ghost Boot Wizard.

See "Installing MS-DOS files" on page 262.

See "Installing MS-DOS Client files" on page 263.

Starting the Ghost Boot Wizard

After you start the Ghost Boot Wizard, you need to specify the PreOS that you want to use, and then select the type of boot package to create. The available types depend on the PreOS selection.

To start the Ghost Boot Wizard

1. On the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Boot Wizard**.
2. In the Symantec Ghost Boot Wizard, in the PreOS Version page, specify the PreOS version that you want to include in your boot package.

   See “Selecting the PreOS version to use” on page 258.

Selecting the PreOS version to use

You need to select the PreOS version to include in the boot package. PC-DOS, Windows PE (Win PE), and ThinStation (Linux) are supplied with Symantec Ghost. You can also use MS-DOS if you supply the appropriate files.

Note: The term "PreOS" is used here to mean the actual operating system, rather than the PreOS environment (which includes more than just the operating system). We define PreOS as follows:

An operating system that contains the code that is used to perform tasks on a client computer that cannot be performed while the client computer's operating system is running. Also used when the client computer has no operating system installed (a "bare metal" computer), for example, when restoring images.

Symantec Ghost uses Windows PE as the PreOS for Console tasks, and as the default for creating boot disks. You can also create boot disks using DOS, Linux, or your own customized Windows PE versions as the PreOS.

Two versions of Win PE are supplied with Symantec Ghost: WinPE, which is designed to run on 256 MB RAM computers, and WinPE-512, which is designed to run on 512 MB computers. Win PE-512 includes more drivers and packages.

You need to select the version that you want to use as the default Win PE. You do this in the Windows PE Editor window.

See “Setting up different versions of Windows PE” on page 259.

To select the PreOS version to use

1. In the PreOS Version page, in the Type list, select the PreOS that you want to include in the boot package:

- PC-DOS
- MS-DOS
- Windows PE (default)
- Linux

2 If you are using Win PE as the PreOS, and want to include all the drivers from the Ghost Deploy Anywhere driver database on the boot disk, check **Include Deploy Anywhere Driver Database with the image**.

3 Click **Next**.

Setting up different versions of Windows PE

You can set up multiple versions of Windows PE on your system, and choose the version that you want to use in the Ghost Boot Wizard.

To set up different versions of Windows PE

1 In the PreOS Version page, in the Type list, select **Windows PE**.

2 Click **Edit**.

3 In the Windows PE Editor window, set up the Win PE versions that you want to make available to the Ghost Boot Wizard.

The list pane displays all the available Win PE versions and their locations. You can do any of the following:

Create a new version of Windows PE

Select the version of Win PE that you want to copy, and then click **Copy**.

See “Creating and modifying Win PE versions” on page 260.

Modify the selected Win PE version

Select the version of Win PE that you want to modify, and then click **Edit**.

See “Creating and modifying Win PE versions” on page 260.

Refresh the selected Win PE version.

Select the version of Win PE that you want to refresh, and then click **Refresh**.

This refreshes the selected Win PE version to include the latest files in the WIM. You may need to do this to ensure that you have the most recent version of the Ghost executable files.

Remove the selected Win PE version.

Select the version of Win PE that you want to remove, and then click **Remove**.

You can remove any version except the default Win PE that is supplied with Ghost.

4 Click **OK**.

To select the default Win PE version

1 In the Windows PE Editor window, select the Win PE version that you want to use as the default PreOS in the Ghost Boot Wizard.

2 Click **OK**.

Creating and modifying Win PE versions

You can create and modify new versions of Win PE by copying an existing image and adding or removing drivers as appropriate. You can also add new drivers to the Ghost Deploy Anywhere driver database, and then include the new drivers in your Win PE versions.

To create or modify a Win PE version

1. In the Windows PE Editor window, select the version of Win PE that you want to copy or modify, and then click **Copy** or **Edit**, whichever is appropriate.
2. If you creating a new Win PE version, in the Windows PE Drivers window, in the Name box, type a suitable name for the new version.
3. On the Network Drivers and Storage Drivers tabs, select the drivers that you want to include in the Win PE version by checking the appropriate check boxes.

   The current drivers are checked by default. If you want to remove a driver, uncheck the appropriate check box.

   If you want to include or remove all drivers on the current tab, click **Add All** or **Remove All**, whichever is appropriate.
4. If you want to add a new driver to the Ghost Deploy Anywhere driver database, click **Add New Driver**.

   See “Adding new drivers to the Ghost Deploy Anywhere driver database” on page 261.

Adding new drivers to the Ghost Deploy Anywhere driver database

You can add new drivers to the Ghost Deploy Anywhere driver database. The drivers in the Ghost Deploy Anywhere driver database are available for use by the Deploy Anywhere feature when retargetting a client computer, and by the Ghost Boot Wizard when modifying a Win PE version.

To add a new driver to the Ghost Deploy Anywhere driver database

1. In the Windows PE Drivers window, click **Add New Driver**.
2. In the New Windows Driver window, select the driver that you want to add and specify the appropriate driver details:

Location	The folder in which the driver is located. Type the folder path, or click **Browse** and select it.
Friendly Name	A suitable name for the driver. This is used in the Ghost Deploy Anywhere driver database and displayed in the Windows PE Drivers window.
Applicable OS	Specify the operating systems that the driver supports by checking the appropriate check boxes.

3. Click **OK**.

Installing MS-DOS files

In some case, a boot package that includes PC-DOS might not start all of your computers. To work around this, you can include MS-DOS instead of PC-DOS in your boot package.

If you want to use MS-DOS as the PreOS in your boot disk, you need to supply the appropriate files. Using an MS-DOS system disk that was formatted on a Windows 95/98 computer, you can install the MS-DOS files during the creation of the boot package.

See “Installing MS-DOS Client files” on page 263.

To create an MS-DOS system disk on a Windows 95/98 computer

1. Insert a blank floppy disk into drive A of a Windows 95/98 computer.
2. On the Windows taskbar, click **Start > Program Files > Windows Explorer**.
3. Right-click drive A.

   Warning: Do not right-click drive C.

4. Click **Format**.
5. Check **Copy System Files**.
6. Click **Start** to format the disk.

To install MS-DOS files

1. In the PreOS Version page, in the Type list, select **MS-DOS**.
2. Click **Get Files**.
3. In the Get MS-DOS dialog box, do one of the following:

To get MS-DOS from a floppy disk.	Click **From Floppy Disk**, and select a floppy drive.
To get MS-DOS from a folder.	Click **From Directory**.

4. Click **OK**.
5. If you are getting MS-DOS from a folder, in the Browse for Folder dialog, select the appropriate folder.

To remove MS-DOS from your computer

1. In the PreOS Version page, select the files that you want to remove and then click **Remove**.
2. In the confirmation pop-up, click **OK**.

Installing MS-DOS Client files

If you are using the mapped network drive functionality and MS-DOS, you must include the Microsoft DOS Client files. You must install the files on the computer before you can include them on the boot package.

The following files are required:

EMSBFR.EXE
LMHOSTS
NEMM.DOS
NET.EXE
NET.MSG
NETBIND.COM
NETH.MSG
NETWORKS
NMTSR.EXE
PROTMAN.DOS
PROTMAN.EXE
PROTOCOL
TCPDRV.DOS
TCPTSR.EXE
TCPUTILS.INI
TINYRFC.EXE
UMB.COM
IFSHLP.SYS
EMM386.EXE
HIMEM.SYS
WFWSYS.CFG

To install the Microsoft DOS Client files

1. In the PreOS Version page, click **Get MS Client**.

   This option is available only when the MS-DOS system files are installed.
2. In the Browse for Folder dialog, select the MS-DOS LAN Client files.

Selecting the boot package type

You can include any of the following features in a boot package:

- Support for CD-R/RW, DVD, LPT, USB, and FireWire

- Network support for TCP/IP peer-to-peer connections and GhostCasting
- Support for reading and writing an image to and from CD/DVD
- Support for mapping network drives
- An image of the Console Boot Partition.
- RIS boot packages that support Microsoft Remote Installation Service (RIS) with Symantec Ghost
- TCP/IP network boot images that use 3Com DynamicAccess Boot Services to allow access to Symantec Ghost without a boot disk

Table 11-1 provides information about the types of boot packages that you can make and how they can be used.

Table 11-1 Boot package types

Intended use	Ghost Boot Wizard options
Local use of Ghost.exe: ■ Disk-to-disk ■ Partition-to-partition ■ Disk or partition to and from local JAZ or ZIP drive	You can use either of the following options: ■ Standard Ghost Boot Package ■ Network Boot Package
Clone, back up, or restore over peer-to-peer connection between two computers using LPT, FireWire, or USB cable.	Standard Ghost Boot Package
Clone, back up, or restore over TCP/IP peer-to-peer connection with network support between two computers.	You can use either of the following options: ■ Network Boot Package ■ Drive Mapping Boot Package **Note:** A Drive Mapping Boot Package supports NDIS drivers but does not support using packet drivers. To use Ghost.exe with network support using packet drivers, you should create a Network Boot Package.
Back up or restore a computer onto an image file on a CD/DVD that is on a CD/DVD writer supported by Symantec Ghost.	Standard Ghost Boot Package

Table 11-1 Boot package types *(continued)*

Intended use	Ghost Boot Wizard options
■ Restore a computer from a Ghost image file on a CD that is on a CD-R/RW drive not supported by Symantec Ghost. The image file was not stored on the CD using Symantec Ghost. Contains generic CD drivers. ■ Access files other than a Ghost image file on a CD.	CD/DVD Startup Boot Package with Ghost
Map a drive on a workstation to a shared resource on a server and use Symantec Ghost to clone, back up, or restore.	Drive Mapping Boot Package
Install the Console boot partition on a client computer.	Console Boot Partition
Start Ghost.exe on a client computer from the network (without a boot disk).	TCP/IP Network Boot Image
Start a client computer from the network to connect to the Symantec Ghost Console.	TCP/IP Network Ghost Client Boot Image
Create an entry in the RIS menu on a client computer to start the computer from the network.	Microsoft RIS Boot Option

To select the boot package type

1 In the Image Type page, select the appropriate boot package type:

Standard Ghost Boot Package	See "Creating a standard Ghost boot package" on page 266.
Console Boot Partition	See "Creating a boot image that contains a Console boot partition" on page 268.
TCP/IP Network Boot Image	See "Creating a TCP/IP Network Boot Image" on page 269.
TCP/IP Network Ghost Client Boot Image	See "Creating a TCP/IP Network Ghost Client Boot Image" on page 271.
Network Boot Package	See "Creating a Network Boot Package" on page 272.
Drive Mapping Boot Package	See "Creating a Drive Mapping Boot Package" on page 273.
CD/DVD Startup Boot Package with Ghost	See "Creating boot packages with CD and DVD support" on page 274.
Microsoft RIS Boot Option	See "Creating a boot package that supports RIS" on page 275.

The available types depend on your choice of PreOS.

2 Click **Next**.

Creating a standard Ghost boot package

The standard boot package that Ghost Boot Wizard creates is one that does the following:

- Runs Ghost.exe for local operations.
- Writes Ghost images directly to media on a CD/DVD writer supported by Symantec Ghost. The media must be supported by the CD/DVD writer.
- Runs Ghost.exe on two computers that are connected by either an LPT or USB cable.
- Runs Ghost.exe to back up to or restore from an external device that is connected by USB or FireWire.

To create a standard Ghost boot package

1 In the Introduction page, click **Standard Ghost Boot Package**.

2 Click **Next**.

3 Complete the following pages:

Additional Services	Applies to PC-DOS only. See "Specifying additional services" on page 276.
Client Type	Applies to both PC-DOS and Win PE. See "Specifying the client to include" on page 278.
Additional Files	Applies to both PC-DOS and Win PE. See "Including additional files" on page 281.
External Storage Support	Applies to PC-DOS only. See "Setting up external storage support" on page 282.
Network Client Configuration	Applies to Win PE only. See "Setting up network client configuration" on page 283.
Destination Drive	Applies to both PC-DOS and Win PE. See "Specifying the destination drive" on page 284.

4 In the Review page, verify that the settings are correct.

If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.

5 Click **Next** to start creating the boot package.

6 In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Creating a boot image that contains a Console boot partition

You can create an image that contains the Console boot partition. Install this image on client computers to allow remote control by the Console.

See "Installing the Console client" on page 51.

To create a boot image that contains a Console boot partition

1. In the Introduction page, click **Console Boot Partition**.
2. Complete the following pages:

Network Interface Card	Applies to PC-DOS only. See "Selecting network drivers" on page 288.
Client Type	Applies to both PC-DOS and Win PE. See "Specifying the client to include" on page 278.
Additional Files	Applies to both PC-DOS and Win PE. See "Including additional files" on page 281.
Network Settings	Applies to PC-DOS only. See "Specifying the network settings" on page 296.
Network Client Configuration	Applies to Win PE only. See "Setting up network client configuration" on page 283.
Ghost Image Details	Applies to both PC-DOS and Win PE. See "Specifying the Ghost Image details" on page 299.

3. In the Review page, verify that the settings are correct.

   If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.

4 Click **Next** to start creating the boot package.

5 In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Creating a TCP/IP Network Boot Image

You can create an image file that lets you start client computers in Ghost.exe, from the network, using 3Com DynamicAccess Boot Services software.

To create a TCP/IP Network Boot Image

1. In the Introduction page, click **TCP/IP Network Boot Image**.
2. Complete the following pages:

Network Interface Card	Applies to PC-DOS only. See “Selecting network drivers” on page 288.
Client Type	Applies to both PC-DOS and Win PE. See “Specifying the client to include” on page 278.
Additional Files	Applies to both PC-DOS and Win PE. See “Including additional files” on page 281.
External Storage Support	Applies to PC-DOS only. See “Setting up external storage support” on page 282.
Network Settings	Applies to PC-DOS only. See “Specifying the network settings” on page 296.
Network Client Configuration	Applies to Win PE only. See “Setting up network client configuration” on page 283.
TCP/IP Network Boot Image	Applies to both PC-DOS and Win PE. See “Specifying the TCP/IP Network Boot Image details” on page 299.

3. In the Review page, verify that the settings are correct.

   If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.
4. Click **Next** to start creating the boot package.
5. In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Creating a TCP/IP Network Ghost Client Boot Image

You can create an image file that lets you start client computers from the network and connect to the Symantec Ghost Console, using 3Com DynamicAccess Boot Services software.

To create a TCP/IP Network Ghost Client Boot Image

1 In the Introduction page, click **TCP/IP Network Ghost Client Boot Image**.

2 Complete the following pages:

Network Interface Card	Applies to PC-DOS only. See “Selecting network drivers” on page 288.
Client Type	Applies to both PC-DOS and Win PE. See “Specifying the client to include” on page 278.
Additional Files	Applies to both PC-DOS and Win PE. See “Including additional files” on page 281.
Network Settings	Applies to PC-DOS only. See “Specifying the network settings” on page 296.
Network Client Configuration	Applies to Win PE only. See “Setting up network client configuration” on page 283.
TCP/IP Network Boot Image	Applies to both PC-DOS and Win PE. See “Specifying the TCP/IP Network Boot Image details” on page 299.

3 In the Review page, verify that the settings are correct.

If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.

4 Click **Next** to start creating the boot package.

5 In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Creating a Network Boot Package

The Ghost Boot Wizard helps you create boot packages that provide network support for GhostCasting and TCP/IP peer-to-peer connections.

This option is available only for PC-DOS.

To create a Network Boot Package

1 In the Introduction page, click **Network Boot Package**.

2 Complete the following pages:

Network Interface Card	See “Selecting network drivers” on page 288.
Client Type	See “Specifying the client to include” on page 278.
Additional Files	See “Including additional files” on page 281.
External Storage Support	See “Setting up external storage support” on page 282.
Network Settings	See “Specifying the network settings” on page 296.
Destination Drive	See “Specifying the destination drive” on page 284.

3 In the Review page, verify that the settings are correct.

If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.

4 Click **Next** to start creating the boot package.

5 In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Creating a Drive Mapping Boot Package

You can use the Ghost Boot Wizard to create boot packages that map a drive letter to a shared resource on a network server. This drive mapping lets you access a network drive from Ghost.exe.

You can choose to include Ghost.exe in the boot package. If you do not include Ghost.exe, you must run Ghost from the network drive. If you include Ghost.exe in the boot package, you cannot create a boot package on a floppy disk set. You can save the package to any other destination, such as a USB drive, a CD ROM image or ISO image.

Note: A Drive Mapping Boot Package supports NDIS drivers but does not support using packet drivers. If you want to run Ghost.exe with network support and you want to use packet drivers, you should create a Network Boot Package.

Note: If you do not run Ghost.exe from the A drive, then you must reset the environment variable WATTCP to provide the location of the Wattcp.cfg file.

See "To reset the environment variable to the correct location of Wattcp.cfg" on page 336.

This option is available only for PC-DOS.

To create a Drive Mapping Boot Package

1 In the Introduction page, click **Drive Mapping Boot Package**.

2 Complete the following pages:

Network Interface Card	See "Selecting network drivers" on page 288.
Client Type	See "Specifying the client to include" on page 278.
Additional Files	See "Including additional files" on page 281.
External Storage Support	See "Setting up external storage support" on page 282.
Network Client Configuration	See "Setting up network client configuration" on page 283.
Network Client Address	See "Specifying the network settings" on page 296.
Destination Drive	See "Specifying the destination drive" on page 284.

3 In the Review page, verify that the settings are correct.

If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.

4 Click **Next** to start creating the boot package.

5 In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Creating boot packages with CD and DVD support

A boot package with CD/DVD support lets you access images and other files stored on CD-R/RW and DVD drives that are not supported by Symantec Ghost.

This kind of package also contains the DOS system files and Ghost.exe.

To create a boot package with CD-ROM and DVD support

1. In the Introduction page, click **CD/DVD Startup Package with Ghost**.
2. Complete the following pages:

Client Type	See "Specifying the client to include" on page 278.
Additional Files	See "Including additional files" on page 281.
External Storage Support	See "Setting up external storage support" on page 282.
Destination Drive	See "Specifying the destination drive" on page 284.

3. In the Review page, verify that the settings are correct.

   If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.
4. Click **Next** to start creating the boot package.
5. In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Creating a boot package that supports RIS

Ghost Boot Wizard Remote Installation Service (RIS) leverages the Preboot Execution Environment (PXE) feature of PC-98 specified computers to provide a remote installation service for Windows 2000. Symantec Ghost provides a cloning solution suitable for deployment or migration of any computer operating system with specific support for Microsoft Windows. Symantec Ghost also works with Windows systems prepared with the Microsoft SysPrep tool.

You can create a RIS boot package in the Symantec Ghost Boot Wizard only when running on a Windows 2000/2003/XP server with RIS installed. An entry for the boot package appears in the RIS menu.

Note: This option only appears if Microsoft Remote Installation Service is installed on your computer.

To create a boot package that supports RIS

1. In the Introduction page, click **Microsoft RIS Boot Option**.
2. Complete the following pages:

Network Interface Card	See "Selecting network drivers" on page 288.
Client Type	See "Specifying the client to include" on page 278.
Additional Files	See "Including additional files" on page 281.
External Storage Support	See "Setting up external storage support" on page 282.
Network Client Configuration	See "Setting up network client configuration" on page 283.
Network Client Address	See "Specifying the network settings" on page 296.
RIS Boot Menu	See "Specifying the RIS menu details" on page 300.

3. In the Review page, verify that the settings are correct.

   If you want to edit the configuration files, click **Start Editing**, and then make the appropriate changes. When you have finished, click **Stop Editing** to save the new details.
4. Click **Next** to start creating the boot package.
5. In the Finished page, click one of the following:

Start Again	Restart the Ghost Boot Wizard to create another boot package.
Finish	Close the Ghost Boot Wizard.

Specifying additional services

You can select which storage, peer-to-peer, and SCSI CD/DVD options you want the boot package to support.

To specify the additional services

1. In the Additional Services page, select the services that you want by checking the appropriate check boxes:

USB support	Adds support for USB peer-to-peer to the boot package.
LPT support	Adds support for LPT peer-to-peer to the boot package.
Include Adaptec ASPI drivers	Adds Adaptec ASPI drivers to the boot package. These drivers are required to write an image directly to a SCSI CD-R that is supported by Symantec Ghost.

2. If you want to set the USB peer-to-peer drivers, click **Advanced**.

   See “Selecting the USB peer-to-peer drivers” on page 277.

3. If you want to change the LPT mode or port, click **Advanced**.

   See “Setting the LPT port or mode” on page 277.

4. Click **Next**.

Selecting the USB peer-to-peer drivers

You can select USB peer-to-peer drivers to include in the boot package. In most cases, you do not need to change the default driver setting. If you have problems connecting using peer-to-peer, then select another option and try again.

To set USB peer-to-peer drivers

1. In the USB Advanced Settings dialog box, select one of the following:

All drivers	Includes all USB peer-to-peer drivers in the boot package
UHCI driver	Includes only UHCI drivers in the boot package
OHCI driver	Includes only OHCI drivers in the boot package

2. Click **OK**.

Setting the LPT port or mode

The default mode for an LPT connection is ECP/EPP. If you are having problems with your LPT connection, set the mode to Bidirectional 8bit or Bidirectional 4bit. The next time that you create a boot package, the mode is reset to the default, ECP/EPP High Speed.

If you have multiple parallel ports and want to connect using a port other than the default LPT1, use the LPT port option to specify the port into which your cable is plugged.

To set the LPT port or mode

1. In the LPT configuration dialog box, under Mode, select one of the following:
   - ECP/EPP High Speed
   - Bidirectional 8bit
   - Bidirectional 4bit
2. Under Port, select one of the following:
   - Default
   - LPT1
   - LPT2
   - LPT3
3. Click **OK**.

Specifying the client to include

You need to specify the Symantec Ghost software that you want to run when starting computers with the finished boot package. Usually the Ghost Boot Wizard provides a default location in which the required files can be found. However, if the files have been moved or you need to use a different version of the clients, you need to specify the new location.

Note: Not all of the steps in the following procedure are relevant to every boot package. The Client Type page shows only the settings that are appropriate to the type of boot package that you are creating.

To specify the client to include

1 In the Client Type page, select the appropriate one of the following:

Do not include any Ghost executables

Excludes Ghost.exe from the boot package. This option is available only if you are creating a Drive Mapping Boot Package.

If you do not include Ghost.exe in the package then you must execute Ghost from a network drive. If you do not include Ghost.exe in the package then all other Client Type boxes are unavailable.

Symantec Ghost

Includes the Ghost executable in the boot package. The boot package lets you connect to a running GhostCast Server to transfer image files to and from the client.

Symantec Ghost Console Client

Includes the Symantec Ghost Console Client in the boot package. The Symantec Ghost Console Client interacts directly with the Symantec Ghost Console to provide remote configuration capabilities. If this option is selected, both the Console client and the GhostCast client are added to the resulting boot package, as the Console client relies on Ghost.exe for disk cloning.

2 If necessary, under Program Location(s), specify the location of the client executable files:

- Ghost.exe: The Ghost executable
- Ngctdos.exe: The Symantec Ghost Console client
- Ghstwalk.exe: Ghost Walker

To change any of these values, click **Browse** and then select the appropriate executable file.

3 If necessary, in the Parameters box, specify the command-line parameters to use.

See “About adding command-line parameters to a boot package” on page 280.

4 If necessary, in the Machine Group box,, type the name of the computer group folder.

When a Console Client is first discovered on the network, the Console creates an icon for it in the Machine Group section of the Default folder. When DOS Console Client computers are discovered, they are identified by Adapter Address only. Specifying a group folder makes identification of the computer easier.

5 If necessary, in the Config Folder box, specify the configuration folder that you want to use.

The default configuration folder in which computers started from this boot package appear when viewed from the Console. This option is useful if the client does not have the Windows Ghost client installed. It allows similar client computers to automatically appear in a separate folder of your choosing.

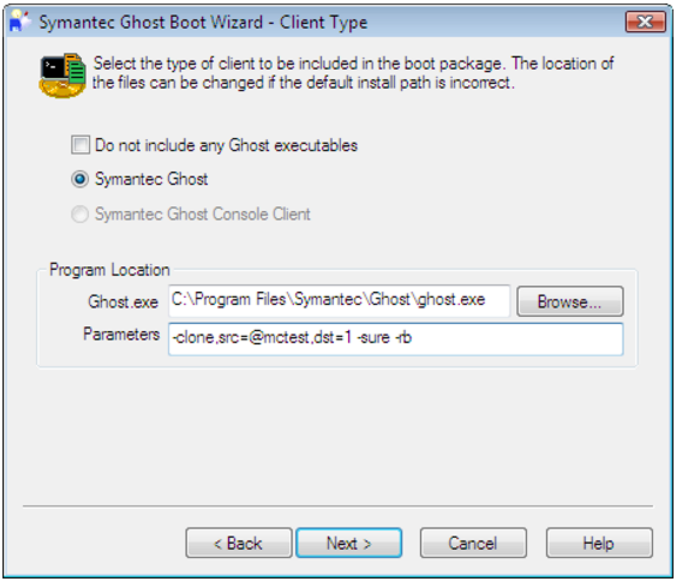
6 Click **Next**.

About adding command-line parameters to a boot package

You can add command-line parameters to a boot package to instruct Symantec Ghost to perform certain actions.

Command-line parameters can be added while creating a Standard Boot Package, Network Boot Package, Drive Mapping Boot Package, CD/DVD Startup Package with Ghost, or a TCP/IP Network Boot Image.

In the following example, the parameters instruct Symantec Ghost to connect to the GhostCast session called test and restore the disk image to the first drive:



Symantec Ghost Boot Wizard - Client Type

Select the type of client to be included in the boot package. The location of the files can be changed if the default install path is incorrect.

□ Do not include any Ghost executables

● Symantec Ghost

○ Symantec Ghost Console Client

Program Location

Ghost.exe: C:\Program Files\Symantec\Ghost\ghost.exe

Parameters: -clone,src=@mctest,dst=1 -sure -rb

Table 11-2 Command parameters

Switch	Description
-sure	Removes the need to confirm the specified details.

Table 11-2 Command parameters *(continued)*

Switch	Description
-rb	Causes a restart immediately after the cloning operation.
-clone	Used with the parameter src=@mctest and dst=1. @mc indicates the GhostCast session name. In this case, the session name is test. The session name must match on the client and server. dst=1 refers to the destination being fixed disk 1.

In the following example, the parameters instruct Symantec Ghost to back up your main disk to an image on another drive:

```
-clone,mode=create,src=1,dst=D:\backups\maindrv.gho
```

Table 11-3 Command parameters

Clone parameters	Description
mode=create	Creates an image file
src=1	Specifies drive 1 as the source drive
dst=D:\Backups\Maindrv.gho	Saves the image to the file D:\Backups\Maindrv.gho

See “About Symantec Ghost switches” on page 521.

Including additional files

You can select any additional files that you want to include in the boot package, and specify their locations in the boot package.

To include additional files

1 In the Additional Files page, specify any additional files that you want to include in the boot package:

To add files to the list	Click **Add**, and then in the Additional Files dialog, select the files that you want to add to the list. In the Destination Folder on media box, specify the folder in which to place the selected additional files. If you want to place additional files in a number of different locations, you need to repeat this procedure for each destination folder, and add the appropriate files.
To remove files from the list	Select the files that you want to remove, and then click **Delete**.

The list pane displays details of the additional files: the full path and file name, size, and destination folder.

2 Click **Next**.

Setting up external storage support

If necessary, you can override BIOS USB control.

To set up external storage support

1 In the External Storage Support page, specify the options that you want by checking the appropriate check boxes:

Override BIOS USB control	Moves control of USB devices from the BIOS to Ghost. This option is unavailable if you have previously included USB support in the boot package. **Note:** Do not select this option if you are creating a bootable USB device.
Override BIOS FireWire control	Moves control of FireWire devices from the BIOS to Ghost.

2 Click **Next**.

Setting up network client configuration

You can let a boot package connect to your network by specifying the appropriate network client configuration parameters.

To set up network client configuration

1 In the Network Client Configuration page, specify the information that is required to connect to your server:

Client Computer Name

The name of the computer after starting from the floppy package.

This name does not have to be the same as the name given to the computer in Windows. If you are creating more than one package, a number is appended to the computer name parameter for subsequent packages to ensure that it is always unique.

User Name

The user name with which the boot package logs on to the network.

The specified user must exist on the network and have sufficient access rights to the files and directories required.

User Password

The password for the user specified above.

Domain or Workgroup

The domain or workgroup to which the user belongs.

Drive Letter

The drive letter on which the network share appears.

Ensure that you select a drive letter greater than any existing drive letter.

DOS or Win PE accesses the network share through the mapped drive, which appears as though it is a hard drive connected to your computer.

If you want to prevent the boot package from mapping a drive at startup, select <None>. In this case, you need to map a drive yourself from the DOS prompt after the computer has started.

Maps To

The Universal Naming Convention (UNC) path to the network share.

UNC paths take the form \\server\share name\subdirectory. For example, if a folder that you want to access is shared as Ghost on a computer named Boss, the UNC path would be \\Boss\Ghost.

2 Click **Next**.

Specifying the destination drive

You can select the destination on which to create the boot package.

Warning: The selected device is automatically formatted before use. Any existing data on the device is deleted.

Table 11-4 describes the destination drive options. Some options may not be available for all types of boot packages.

Table 11-4 Destination drive options

Option	Description
Floppy Disk set	Saves the boot package to a set of floppy disks. This option is unavailable if you are creating a Drive Mapping Boot Package and you do not include Ghost.exe in the package. See "To create a Floppy Disk Set" on page 286.
VMware Virtual Floppy	Saves the boot package to a VMware virtual floppy disk. See "To create a VMware Virtual Floppy" on page 286.
USB Disk	Saves the boot package to a removable or unremovable device or disk. Symantec fully supports USB flash drives as a removable device; however, other devices also work with this option. The target computer must support being started from the device, and must be configured correctly. For example, the BIOS must support the option to start from the device. If you are using WinPE as the preOS, you need at least 256 MB of free space on your USB device. All information on the selected device is deleted. The device is automatically formatted before use. **Note:** If you are using MS-DOS, a 2GB partition is created on the device and any remaining space on the device is unavailable. The device is reformatted and any existing data is overwritten. For PC-DOS and WinPE, the partition is the size of the USB drive. See "To create a USB Disk" on page 286.
Create ISO image	Saves the boot package to an ISO image. Using third-party software, you can write the ISO image to a CD or DVD. This option is unavailable if you use a Multicard template. See "To create an ISO image" on page 287.

Table 11-4 Destination drive options *(continued)*

Option	Description
CD/DVD ROM Image	Saves the boot package to a CD/DVD ROM. **Note:** BluRay and HD DVD are not supported. See "To create a CD/DVD ROM Image" on page 287.
One-Click Virtual Partition	Saves the boot package to a one-click virtual partition. This comprises a zip file, an executable, and a shortcut that runs the executable with the zip file as a parameter. You can store this on a network share and run it from the destination machine simply by clicking the shortcut. See "To create a One-Click Virtual Partition" on page 288.

To create a Floppy Disk Set

1. In the Destination Drive page, click **Floppy Disk Set**.
2. Specify the appropriate parameters in the following fields:

Floppy Disk Drive	Select the drive letter of the floppy disk drive that you want to use to create the boot disk.
Number of disks to create	Specify the number of boot disks that you want to create. This option is useful for creating a batch of identical boot disks for use in multiple clients. If you have selected a static IP address in the Network Settings dialog box or the Network Client Settings dialog box, a unique IP address is generated for each disk. The IP address is incremented by one for each subsequent disk.
Format disk(s) first	Ensure that this option is checked to format the disks before copying the files needed to start your client computer. Formatting the disk ensures that any existing files are removed, and that there is enough space for the boot files on the disk. If this option is unchecked, any files that exist on the disk remain.
Quick Format	Ensure that this option is checked to erase the floppy disk but keep the existing disk format if the disk has already been formatted as a 1.44 MB floppy disk. If this option is not checked, the Ghost Boot Wizard completely formats the disk, which takes significantly longer.

3. Click **Next**.

To create a VMware Virtual Floppy

1. In the Destination Drive page, click **VMware Virtual Floppy**.
2. Under Filename, click **Browse** and then select the location and file name of the VMware virtual floppy disk.
3. Click **Next**.

To create a USB Disk

1. In the Destination Drive page, click **USB Disk**.
2. If you are using Windows PE, in the adjacent drop-down list, select the file system that you want to use:

- FAT
- NTFS

3 Specify the appropriate parameters in the following fields:

Available Devices	Click the down arrow to view and select a device on which to create the boot package. The device is formatted before the boot package is created, so all existing data on this device is deleted.
Show only removable devices	By default, Available Devices lists only those devices that Windows sees as removable. To see all devices, including hard disks, uncheck this option.
Support for creating bootable CDs/DVDs	Select this option if you want to create bootable CDs or DVDs. This option adds an image of a bootable floppy disk to the boot package. If you are using Ghost to write an image directly to a CD or DVD, this option adds support for making the CD or DVD bootable.

4 Click **Next**.

To create an ISO image

1 In the Destination Drive page, click **Create ISO image**.

2 Under Filename, either type the full path and file name for the ISO image, or click **Browse** to select an existing ISO file.

3 If you want to create bootable CDs or DVDs, check **Support for creating bootable CDs/DVDs**.

This option adds an image of a bootable floppy disk to the boot package. If you are using Ghost to write an image directly to a CD or DVD, this option adds support for making the CD or DVD bootable.

4 Click **Next**.

To create a CD/DVD ROM Image

1 In the Destination Drive page, click **CD/DVD ROM Image**.

2 In the drop-down list, select the CD/DVD R/W drive to which to write the boot package image.

3 Click **Next**.

To create a One-Click Virtual Partition

1. In the Destination Drive page, click **One-Click Virtual Partition**.
2. Under Folder, either type the full path to the folder in which you want to store the virtual partition, or click **Browse** to select the appropriate folder.
3. Click **Next**.

Selecting network drivers

You need to select the network driver that is appropriate for the make and model of the network card that is installed on the client computers.

If the Universal Network Driver cannot access the network interface card installed in the target computer then you must select the appropriate driver. If the driver that you require is not in the list, you need to add the driver to the Ghost Boot Wizard before you can continue. You must create a boot package for each network card, unless you use the multicard template.

You can use multicard templates to create a boot package containing several NDIS2 drivers. When the computer starts from the boot package, a special multicard driver checks the computer's hardware to see if any of the NDIS2 drivers can be used to access the installed network card.

Multicard templates are useful because several makes and models of network cards are often used in a single LAN. You can create a single boot package for use with all of your computers without modification.

Note: Multicard templates are not supported for ISO images.

Refer to the Software License Agreement for use restrictions.

See "About selecting a network driver template" on page 289.

See "Maintaining the list of available network drivers" on page 291.

To select network drivers

1. In the Network Interface Card page, select the appropriate network driver.

   If necessary, click **Show all drivers** to see all the available drivers.

   If you want to include two or more drivers in the same boot package, select Multicard Template.
2. Click **Next**.

3 If you selected Multicard Template, in the Multicard Drivers page, select the appropriate NDIS2 drivers.

  If you want to create a floppy disk set, you should select no more than four or five drivers. The space is limited on a floppy disk.

4 Click **Next**.

About selecting a network driver template

For the boot package to work correctly, it is important that you select the correct network driver template. When you create a boot package for client computers, the template that you select must be suitable for the network cards installed in the computers that are to start from the package.

See "Determining the required NIC type" on page 289.

The name of the network interface card as shown in Windows may not exactly match the name of the correct template in the Ghost Boot Wizard. For example, Windows might list the card as 3Com Fast EtherLink XL 10/100Mb TX Ethernet NIC (3C905B-TX). In this case, 3C905B-TX is the model number of the card. Therefore, you can use the Ghost Boot Wizard template that is named 3COM 3C90X. This template works for all 3C90- cards.

In some cases, you might have a choice between an NDIS2 driver and a packet driver version of the same template. Both templates should work, but you might find that one gives better performance. You can experiment to determine which one works better.

It is possible that there is no existing template in the Ghost Boot Wizard that is suitable for the network interface card installed in your computer. In this case, obtain the DOS drivers for the network interface card either from the disk supplied with the card or from the manufacturer's Web site, and add a new template to the Ghost Boot Wizard.

See "Adding a network driver template" on page 292.

If you have different network interface cards installed in client computers, then you may be able to use the multicard template to create a single boot package that works on each of your computers without modification.

Determining the required NIC type

You can use the Ghost Console to check the client computer's network interface card in the Ghost Console. If the client computer is not installed with the Console client, then you can find the name of the driver from Network Properties within Windows. This must be done on the client computer for which you are preparing the boot package.

See “Viewing Symantec Ghost Console resource properties” on page 76.

To determine which network interface card is installed on a Windows 2000 computer

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. Double-click **System**.
3. On the Hardware tab, click **Device Manager**.
4. Expand **Network adapters**.

   The make and model of the installed network interface card are listed.

To determine which network interface card is installed on a Windows XP computer

1. On the Windows taskbar, click **Start > Control Panel > System**.
2. On the Hardware tab, click **Device Manager**.
3. Expand **Network adapters**.

   The make and model of the installed network interface card are listed.

About Symantec Ghost support for multiple network interface cards

The UNDI drivers support multiple network interface cards in a computer. If you have more than one NIC in your computer, and you do not use the UNDI driver, then it is possible that Ghost might not select the correct card. If you do not want to use the UNDI driver, then you should edit the Protocol.ini file to select the correct card.

If Ghost does not select the correct card, you can edit the Protocol.ini file to specify the correct settings to bind the network driver to the correct network card. You must specify the physical location of the network card in the computer. The information that you must include in the Protocol.ini file is specific to the driver and to the network.

Note: The network driver must be a PCI network card.

Before you edit the `Protocol.ini` file, you need the following information:

PCI Location Bus, Slot, and Function keywords	You can obtain this information from the manufacturer of your NIC. The manufacturer might also require you to include additional information in the `Protocol.ini` file. For example, the manufacturer might require you to place the keyword information in a specific section of the file. **Note:** Some manufacturers use the term "device" instead of "slot".

PCI bus number, slot number, and function number	You can obtain this information by checking the client computer properties in the Ghost Console. See "To view Symantec Ghost Console client computer properties" on page 87. Symantec Ghost displays the PCI information in decimal format. A manufacturer might require that you use this hexadecimal format in the `Protocol.ini` file.

When you have the PCI information, you can edit the `Protocol.ini` file.

For example, a manufacturer provides the following keywords:

- SLOT
- BUSNO
- FUNCTNO

The Symantec Ghost client dialog properties lists the following properties:

B:0 S:17 F:0

In this case, you would edit the Protocol.ini file as follows:

- SLOT=17
- BUSNO=0
- FUNCTNO=0

Maintaining the list of available network drivers

You can create new driver templates from scratch, or by copying an existing template and making the necessary modifications. You can also delete any driver templates that you no longer require.

To maintain the list of available network drivers

- In the Network Interface Card page, set up the network drivers that you want to make available in the Ghost Boot Wizard.

  The list pane displays all the available drivers. You can do any of the following:

Add a new driver template	Click **Add**. See "Adding a network driver template" on page 292.
Modify an existing driver template	Select the driver template that you want to modify, and then click **Modify**.
Copy an existing driver template	Select the driver template that you want to copy, and then click **Copy**. The new (copied) driver template is added to the list.
Rename a driver template	Select the driver template that you want to rename, and then click **Rename**. In the list, type the new driver template name.
Delete driver templates	Select the driver templates that you want to delete, and then click **Delete**. In the confirmation pop-up, click **Yes**.

Adding a network driver template

The Ghost Boot Wizard includes drivers for over 130 network interface cards. If your driver is not in the list, you can add it to the wizard so that it is set up the next time that you need it. There are two types of drivers that a Ghost client can use, a packet driver or an NDIS2 driver. Both types of drivers are usually supplied with network cards so that you have the choice of which driver to use. Some network card manufacturers do not supply packet drivers with their hardware.

To add a network driver template

1 In the Network Interface Card page, click **Add**.

2 In the Template Type dialog box, select the appropriate template type:

Packet Driver	Packet drivers are usually DOS executables (with .com or .exe file extensions) that load from the Autoexec.bat file before Symantec Ghost loads. Symantec Ghost communicates directly with the packet driver to use the services provided by the network card. See "Customizing a network driver template" on page 295.
NDIS2 Driver	NDIS2 drivers work with the Microsoft Network Client. Symantec Ghost also uses them for GhostCasting. NDIS2 drivers are DOS drivers that load from the DOS Config.sys file. Symantec Ghost does not communicate with NDIS2 directly, but uses a shim (supplied by the Ghost Boot Wizard) to access the network card. See "Customizing a network driver template" on page 295.

3 Click **OK**.

4 In the Template Properties window, specify the appropriate settings.

Setting the packet driver template properties

You can set or modify the packet driver template properties at any time. You need to specify the driver executable, and can optionally set command-line parameters and the multicasting mode.

Command-line parameters vary from driver to driver and are usually optional with plug-and-play network cards. If you think that your selected driver may require command-line parameters to work correctly on your network, then consult the documentation that came with your network card. This is often in the form of a `Readme.txt` file in the same directory as the driver itself.

Most network interface cards support different methods of receiving multicasts from the network. Symantec Ghost can usually determine the best method to use based on information in the driver. However, some drivers misrepresent their capabilities. In these cases you must explicitly set the multicasting mode.

To set the packet driver template properties

1 In the Template Properties window, on the Packet Driver tab, specify the appropriate settings:

Driver Executable

The name and location of the packet driver executable file. Click **Browse** and then select the file from your file system.

If you are installing the packet driver from the original disks that came with your network interface card, the packet driver is probably inside a directory called PACKET or PKTDRV.

Parameters

Type any command-line parameters that you need to use.

A preview of the line that appears in the Autoexec.bat of the finished Ghost boot package appears at the bottom of the dialog box.

Mode

Specify the appropriate multicasting mode:

- Select Automatically
  This is the default. Symantec Ghost selects the best mode to use based on the information in the driver.
- Receive Mode 5
  This may be less efficient than letting Ghost select the mode automatically but it is supported by most cards. Use this mode if the default option does not work.
- Receive Mode 6
  Less efficient than mode 5. Use this mode if Receive Mode 5 does not work.

2 Click **OK**.

Setting the NDIS2 driver template properties

You can set or modify the NDIS2 driver template properties at any time. You need to specify the driver executable and the driver name, and can set the Protocol.ini configuration file parameters and the multicasting mode.

See "Customizing a network driver template" on page 295.

To set the NDIS2 driver template properties

1 In the Template Properties window, on the NDIS Driver tab, click **Setup**.

2 In the Browse for Folder dialog, select the appropriate NDIS2 driver.

In many cases Ghost can automatically determine the other parameters for your network. When locating the directory that contains the driver, look for a folder named Ndis or Ndis2. If you have a choice between DOS and OS2 folders, select DOS. The driver date lets you check that you have the latest driver.

3 If the setup fails to complete the driver properties, you can specify the appropriate settings manually:

Filename

Specify the DOS file name and location of the NDIS2 driver executable file. Click **Browse** and then select the file from your file system.

Driver Name

Type the internal name of the driver.

The internal name of the driver is used when generating the Protocol.ini configuration file and must always end with a $ character. Read the sample Protocol.ini file in the same directory as the driver itself to find the internal driver name.

The internal name of the driver is often the DOS file name with the file name extension replaced with a $. For example, the internal name of Mydriver.dos is Mydriver$.

Parameters

Type the parameters for the Protocol.ini configuration file.

If you use Setup to automatically fill in this page, you will see the parameters that you need to adjust. For the majority of plug-and-play cards, all of the parameters are optional, so you can either accept the defaults or leave this field empty.

Mode

Specify the appropriate multicasting mode:

- Select Automatically
  This is the default. Symantec Ghost selects the best mode to use based on the information in the driver.
- Receive Mode 5
  This may be less efficient than letting Ghost select the mode automatically but it is supported by most cards. Use this mode if the default option does not work.
- Receive Mode 6
  Less efficient than mode 5. Use this mode if Receive Mode 5 does not work.

4 Click **OK**.

Customizing a network driver template

You may require additional drivers and programs in order to use the network device attached to your computer. For example, many USB network devices must load an extra driver for the USB port before the driver for the network device.

You can add files to the network driver template and customize the `Autoexec.bat` and `Config.sys` files of the resulting boot package. Usually these are either DOS drivers or executable programs, but you can add any type of file.

Note: If you are creating a floppy disk set and you edit `Autoexec.bat`, you should ensure that the same changes are made to `Autoexec.bat` on both disks in the floppy disk set.

If this template is used as a multicard template, then any additional files or modifications are overridden by its settings.

To customize a network driver template

1. In the Template Properties window, on the Advanced tab, do any of the following:

Add a file to the template	Click **New** and, in the Browse for File dialog, select the appropriate file.
Remove a file from the template	In the additional files list, select the file that you want to remove and then click **Delete**.
Add `Autoexec.bat` entries	In the Autoexec.bat Additions pane, type any additional Autoexec.bat entries for the driver. The entries appear before any network-related commands, such as Netbind.com or the packet driver executable.
Add `Config.sys` entries	In the Config.sys Additions pane, type any additional Config.sys entries for the driver. The entries appear before any driver-related devices to ensure that the enabling drivers load before the main network device drivers specified on the network driver page.

2. Click **OK**.

Specifying the network settings

You need to specify the network settings for the client that is to be booted from this boot package. This enables the client software to communicate with the server using a built-in TCP/IP protocol stack.

Each computer on a TCP/IP network needs a unique IP address so that the network can identify it. An IP address takes the form of four numbers separated by periods (for example, 192.168.0.1). Ghost uses these addresses to specify which computers receive information.

Ghost can obtain IP addresses in the following ways:

DHCP — Dynamic Host Configuration Protocol (DHCP) simplifies the task of configuring Ghost clients. Using DHCP, a Ghost client can automatically determine its IP address by contacting a DHCP server running on the network. DHCP also provides both the subnet mask and gateway address parameters.

Static IP addressing — If you select Static IP addressing, the IP address of the Ghost client is stored in the Wattcp.cfg configuration file. This is the only option on networks that do not include DHCP servers. Because the IP addresses are managed manually, ensure that the Ghost client is not given the same address as an existing computer on the network.

Network parameters such as IP address and subnet mask for Symantec Ghost and Dosghsrv.exe are stored in the text file `Wattcp.cfg`. This file is created by the Ghost Boot Wizard but can be edited on the boot package manually.

To specify the network settings

1 In the Network Settings page, or the Network Client Address page (whichever is appropriate), specify the appropriate settings:

DHCP will assign the IP settings

Select this option to use DHCP to obtain network parameters automatically.

The IP settings will be statically defined

Select this option to statically assign network parameters.

The IP address, subnet mask, and gateway addresses must be specified. This is only necessary on networks that do not contain DHCP servers.

First IP address

Specify the IP address in the standard dotted-decimal notation.

If you are using the Ghost Boot Wizard to generate a batch of boot packages, the last number in the IP address is incremented for each package, ensuring that the address is different on each package.

Subnet Mask

Specify the range of IP addresses that are directly accessible from the current IP address.

Each of these locally accessible computers becomes a member of the local subnet. A computer is on a different subnet if the IP address is outside of this range of addresses. To communicate with a computer on another subnet, a gateway is used.

Gateway

Specify the address of the gateway computer in the dotted-decimal notation.

The gateway computer acts as a link between two subnets. This value is used by the client to forward packets to computers that are not connected to the same subnet as the client computer. All information that passes between the subnets is forwarded by way of the gateway computer.

DNS Address

Specify the address of the Domain Name Server.

Router Hops

Specify how many routers the client searches across when attempting to find the GhostCast Server.

The default value of 16 lets Ghost find the server as long as it is not more than 16 router hops away. This is sufficient for most networks.

2 Click **Next**.

Specifying the Ghost Image details

You need to specify the name and location of the Ghost image file to which the boot package is to be saved.

To specify the Ghost Image details

1 In the Ghost Image Details page, in the Image File box, specify the full file name of the image file to be created.

   You can type the full path and name, or click **Browse** and select the appropriate image file.

2 In the Description box, type a short description of the image file.

   This description is used in other Ghost applications, providing relevant information about the image file to users.

3 Click **Next**.

Specifying the TCP/IP Network Boot Image details

You need to specify the name of the image file to be created for use with a network boot server.

Although the Ghost Boot Wizard creates the image file, it does not attempt to add the file to the list of boot options provided by the network boot server. Before using the image you must manually configure your network boot server to use the image. For more information, see the documentation for your particular server software.

Note: For WinPE PXE images, the Ghost Boot Wizard updates the TFTP server to boot the new WinPE. This is different from DOS environments where you need to configure the 3COM PXE separately.

To specify the TCP/IP Network Boot Image details

1 In the TCP/IP Network Boot Image page, specify the appropriate settings:

TFTP Root Directory	Applies to Win PE only. The TFTP server root directory. Type the appropriate path, or click **Browse** and select it from your file system.
Name	Applies to Win PE only. The name of the Win PE Image (WIM) file to be created.
Image File	Applies to PC DOS only. The name of the image file to be created.

2 Click **Next**.

Specifying the RIS menu details

You need to specify the details that are used on the RIS Boot Menu.

To specify the RIS menu details

1 In the RIS Boot Menu page, specify the appropriate settings:

RIS Boot Menu Name	The name that appears on the RIS Boot Menu. When you select this name from the menu, your client computer starts from the network card.
RIS Boot Menu Description	The help message to display when the menu option is selected on the RIS Boot Menu. You can use this field to add a descriptive comment about the files included in the boot package.
RIS Boot Directory	The name of the directory under the main RIS tree in which the boot package is installed. The Ghost Boot Wizard automatically generates the contents of this field from the text you type for the RIS menu name. You should not change the text in this field from the default.
Language	Select the language to use.

2 Click **Next**.

Creating a DOS boot disk manually

There may be times when you want to create boot disks manually. For example, you may wish to create a NetWare boot disk, add custom programs, or add batch files.

To create a DOS boot disk manually

1 If the operating system is DOS/Win 98, insert a blank, formatted floppy disk into drive A.

2 Type the following:

```
C:\> sys c: a:
```

3 Set up the packet driver interface.

For example, type the following command to copy the network interface card packet driver file:

```
C:\> copy 3c5x9pd.com a:\
```

See “Setting up packet drivers” on page 302.

4 To copy `Ghost.exe` and `Wattcp.cfg` to the floppy disk, type the following:

```
C:\> copy progra~1\Symantec\ghost\ghost.exe a:\
```

```
C:\> copy progra~1\Symantec\ghost\wattcp.cfg a:\
```

5. Edit the `Wattcp.cfg` file.

   For example:

   IP = 192.168.100.44

   NETMASK = 255.255.255.0

   The `Wattcp.cfg` file stores the TCP/IP stack configuration details and specifies the IP address and subnet mask of the computer.

   See your system administrator for IP and netmask values.

6. Edit the `Autoexec.bat` startup file.

   For example:

   ```
   3c5x9pd.com 0x60
   ```

   ```
   ghost.exe
   ```

   Add the command line for the packet driver to the `Autoexec.bat` file.

   For more information, see the packet driver documentation.

   Ensure that the same changes are made to `Autoexec.bat` on both disks in the floppy disk set.

   You can add additional command-line switches to the Ghost.exe command to automate the cloning process.

   See "About Symantec Ghost switches" on page 521.

Setting up packet drivers

There are several packet driver interface options as follows:

- Network interface card-dependent packet driver.
  See "To set up a network interface card-dependent packet driver" on page 303.
- NDIS version 2.01 driver with packet driver shim supplied by Symantec Ghost. NDIS version 3 or later drivers do not work with the Ghost client.
  See "To set up an NDIS 2.01 network adapter driver with supplied packet driver shim" on page 303.
- Third-party network adapter driver and packet driver shim.
  These have not been tested or documented with the GhostCasting feature. This includes ODI-based packet driver shims such as Odipkt.com.

Packet drivers are easy to set up and require minimal configuration. The NDIS driver setup is more complex. The selection of NDIS 2.01 and shim, or a network interface card-specific packet driver depends on factors such as availability, reliability, ease of use, and speed. By running a system test, you can choose the best alternative for your network interface card (that is, the specific packet driver or the NDIS 2.01 driver and shim).

Note: Do not use the Microsoft Network Client Installation program to create a GhostCast boot package as they are not compatible.

To set up a network interface card-dependent packet driver

1. Locate the packet driver for your network interface card.

   Packet drivers are usually supplied on the installation disk included with a network interface card or may be available on the manufacturer’s Web site.

2. Load the packet driver onto the computer using the appropriate command-line argument, as follows:

   - 3COM590 PCI network interface card packet driver:

     ```
     A:\> 3c59xpd.com
     ```

   - 3COM509 ISA network interface card packet driver:

     ```
     A:\> 3c5x9pd.com 0x60
     ```

   - NE2000 compatible using software interrupt 0x60 at IRQ10 and IObase 0x280:

     ```
     A:\> ne2000pd.com 0x60 10 0x280
     ```

     The syntax for the NE2000pd command is a typical example of an ISA driver command line. You can find the IRQ and IO base address values using the setup program included with the network interface card. The software interrupt can be between 0x60–0x7f.

To set up an NDIS 2.01 network adapter driver with supplied packet driver shim

1. Locate the NDIS 2.01 driver for the network interface card.

   NDIS (version 2.01) drivers are usually supplied on the installation disk included with a network interface card and have a .dos file extension. Alternatively, NDIS (version 2.01) drivers may be available on the network interface card manufacturer’s Web site.

2. Copy and modify `Protocol.ini`, `Config.sys`, and `Autoexec.bat`.

   Base configuration files ready for editing are included in the GhostCasting installation files. Extract these configuration files and edit as shown. If you are creating a floppy disk set and you edit Autoexec.bat, you should ensure that the same changes are made to Autoexec.bat on both disks in the floppy disk set.

3. In the Ghost directory, copy the following files from the \ndis directory:

- Protman.dos
- Protman.exe
- Netbind.com
- Dis_pkt.dos

4 Restart the computer.

The packet driver interface should now be ready for Symantec Ghost to use.

About the files that are required in your boot disk set

Table 11-5 lists the files that your directory or floppy package should contain when you create a boot disk set manually.

Table 11-5 Required files

System files	Configuration files	NDIS files
Command.com	Config.sys	Dis_pkt.dos
Msdos.sys (hidden)	Autoexec.bat	Netbind.com
Io.sys (hidden)	Protocol.ini	Protman.dos
		Protman.exe
		*.dos

Note the following:

- Protman.exe is used during the NETBIND and is not needed in Autoexec.bat.
- *.dos is the network interface card specific driver (for example, ELNK3.DOS).

Following is a sample Protocol.ini file:

```
[PROTMAN]
drivername = PROTMAN$
[PKTDRV]
drivername = PKTDRV$
bindings = PC_CARD
intvec = 0x60
chainvec = 0x66
[PC_CARD]
drivername = PNPND$
```

Change the [PC_CARD] module driver name to correspond to the NDIS driver in use for your network interface card. For example, if you use a 3COM509 card then change the driver name to:

drivername = ELNK3$

Type any additional required options for the network interface card configuration in the [PC_CARD] module. Refer to the documentation or the sample Protocol.ini for the network interface card in use, if required. For example, the 3COM509 card lets you optionally specify the IO Base address:

[PC_CARD]

drivername = ELNK3$

IOADDRESS = 0x300

Following is a sample `Config.sys` file:

```
device=protman.dos /I:\
device=dis_pkt.dos
device=pnpnd.dos
```

The /I: in the first line indicates the location of the Protocol.ini file and must be present. For example, /I:\ specifies the root directory and /I:A:\NET specifies A:\NET.

The last line refers to the driver for the network interface card. For example, if you use a 3COM509, the last line of Config.sys should be replaced with:

device=ELNK3.DOS

Following is a sample `Autoexec.bat` file:

```
prompt $p$g
netbind
```

NETBIND binds the NDIS drivers together and installs the packet driver interface.

Supporting regional keyboards and character sets

You can customize boot disks and packages to support regional keyboards and character sets by editing the `Local.cfg` file. The `Local.cfg` file does not support languages that use double-byte character sets.

The `Local.cfg` file is one of the files that is required to support the Ghost Boot Wizard. It is stored in one of the following locations:

Windows Vista	\Users\Public\AppData\Symantec\Ghost\Template\Common

Windows XP	\Documents and Settings\All Users\Application Data\Symantec\Ghost\Template\Common
Windows 2000	\Documents and Settings\All Users\Application Data\Symantec\Ghost\Template\Common

The `Local.cfg` file includes instructions for editing the file.

Chapter 12

Backing up with CD-R/RW and DVD-R/RW

This chapter includes the following topics:

Image files and CD/DVD writers

This section applies only to DOS/Windows Ghost. The Linux version of Ghost does not support direct writing to CD/DVD.

Symantec Ghost support of SCSI, IDE, FireWire, and USB CD and DVD writers allows the storage of a single image file onto one or more CD-R/RW or DVD-R/RW.

Note: Ghost can read image files that were written to CD/DVD by third-party device, provided the image file is in the root folder and complies with the Ghost naming convention (for example, `cdr00001.gho`).

When you use CD/DVD writers with Ghost.exe, you can select a writer as the destination device in the File Locator window. Each writer is shown as @CD-Rx, where x is a number starting at one and increasing incrementally for each writer present.

For Symantec Ghost to access SCSI CD/DVD writers, a DOS ASPI driver must be installed. Also, when you create a Ghost boot package from the Ghost Boot Wizard, you must include the Adaptec ASPI drivers.

See “Creating a standard Ghost boot package” on page 266.

Symantec Ghost works with most SCSI and IDE writers produced in 2000 and later. It may or may not work with older models. Use the latest firmware available for your CD/DVD writer. An IDE CD/DVD writer performs best if it is mounted on the secondary IDE controller.

A list of CD/DVD writers with which Symantec Ghost has been tested is available on the Symantec Service and Support Web site:

http://www.symantec.com/techsupp/cddvddriver

Table 12-1 lists the media that you should use with CD and DVD writers and the action, if any, that Symantec Ghost takes.

Table 12-1 CD and DVD media

Type of drive	Media
CD-R	Blank
CD-RW	Prompts you to erase existing data before writing new data
DVD-R	Blank
DVD-RW	Prompts you to erase existing data before writing new data
DVD+R	Blank
DVD+RW	Prompts you to overwrite existing data

When you create an image on a CD/DVD, you can make the CD/DVD bootable. To make the CD/DVD bootable you must have a Windows boot disk that loads the CD/DVD drivers and assigns the drive letters to the CD/DVD drives. You must have the Windows boot disk available when you create the image using Ghost.exe. When you use the bootable CD/DVD to restore the image file, you must run Ghost.exe from the mounted drive. If you make the CD/DVD bootable, you must have the DOS drivers that let you view the contents of the CD/DVD.

Saving an image file directly to a CD/DVD drive

This section applies only to DOS/Windows Ghost. The Linux version of Ghost does not support direct writing to CD/DVD.

You can save an image file directly to a CD or DVD. You can also make the CD/DVD bootable.

When writing an image file directly to a CD-R/RW or DVD-R/RW, note the following:

- The CD/DVD drive must be compatible with Symantec Ghost.
- Symantec Ghost automatically spans CD-R/RW disks if necessary. You do not need to use a spanning switch.
  See "Image files and volume spanning" on page 316.
  If Symantec Ghost does not support your CD-R/RW drive and the image file is too large to fit on one CD, you can still save the image file to CD.
  See "Saving an image file to an unsupported CD/DVD drive" on page 310.
- If the CD-RW/DVD-RW contains data, Symantec Ghost prompts you to confirm that you want the data erased.

Saving a bootable image file to a supported CD/DVD

This section applies only to DOS/Windows Ghost. The Linux version of Ghost does not support direct writing to CD/DVD.

Saving an image file to a supported CD/DVD and making it bootable is a process with several phases as follows:

- Create a Ghost boot package.
- Start your computer.
- Create and save the image file.

When writing an image file directly to a CD/DVD, note the following:

- The CD/DVD drive must be compatible with Symantec Ghost.
- Symantec Ghost automatically spans CD/DVDs if necessary. You do not need to use a spanning switch.

Note: When creating the bootable CD/DVD ensure that the floppy disk that you use to make the CD or DVD bootable has mouse.ini on it already, or does not load mouse.com. If you do not then the mouse driver tries to write mouse.ini to the CD/DVD and hangs while attempting to do this.

Create the Ghost boot disks

To write an image file directly to a CD/DVD, you must have a boot package that includes the appropriate drivers to start the computer. You can use the Ghost

Boot Wizard to create a boot package, using the CD/DVD Startup Disk with Ghost option. This option creates a boot package that contains the Ghost executable, DOS system files, and the CD/DVD driver files.

See "Creating boot packages with CD and DVD support" on page 274.

Create and save the image file

Restart your computer using the boot package and create an image of the computer, choosing the CD/DVD drive as the destination drive.

See "Creating a backup image file" on page 339.

Symantec Ghost lets you make the CD bootable during the creation of the image file. To make the CD bootable, follow the on-screen instructions. If you are using a floppy disk set, when prompted for the required files, insert the first boot disk into the computer's floppy disk drive. When asked if you want to copy Symantec Ghost to the CD/DVD, insert the second boot disk and follow the on-screen instructions.

Saving an image file to an unsupported CD/DVD drive

Not all CD/DVD drives are supported by Symantec Ghost. If your drive is unsupported, you can create an image file and then write it to CD/DVD using third-party software.

If your drive is unsupported, and the image file is too large to fit onto one disk, you can still save the image file to CD/DVD.

There is more than one way to save an image file to an unsupported CD/DVD drive as follows:

- Splitting the image file during a backup
  See "Splitting an image file during a backup" on page 311.
- Splitting the image file after it has been created
  See "About image file spans" on page 327.

The image file is initially saved to another partition or hard disk and then copied to a CD/DVD using your CD/DVD recording software.

To save an image file onto a CD, you must split the image file into files that fit on a CD. Split the image into files that are not larger than 620 MB. This leaves room on a CD for any additional files that you might need or any difference in the capacity of the CD.

Note: Some CD/DVD writers let you write directly to the CD/DVD as if to a drive letter. Symantec Ghost does not support the ability to write data directly to a CD/DVD.

Splitting an image file during a backup

To split an image file as it is created, run Symantec Ghost from the command line in DOS, using the -split and -auto switches.

To split an image file during a backup

1. Start Ghost.exe using the -split and -auto switches.

   For example:

   ```
   a:\ghost.exe -split=600 -auto
   ```

2. Create and save the image file.

The -split switch in this example limits the image size to a maximum of 600 megabytes for any one segment. The -auto switch names each of the segments numerically.

See “Creating a backup image file” on page 339.

Chapter 13

Symantec Ghost support for image files and disks

This chapter includes the following topics:

About Symantec Ghost image files

You can create image files by using the Symantec Ghost executable, the GhostCast Server, or the Symantec Ghost Console.

Symantec Ghost supports VMWare Disk images (.vmdk files) for both creating and restoring images. Note that .vmdk files do not have a Description field, and cannot be used in Ghost Explorer. Symantec Ghost supports Backup Exec System Recovery (.v2i, .iv2i) and DeployCenter Library (.pqi) images for restoring a computer only.

The image files created with Symantec Ghost have a .gho or .ghs extension by default. They contain the entire disk or partitions of the disk. Image files support the following:

- Various levels of compression
- CRC32 data integrity checking
- Splitting of media files
- Spanning across volumes

Symantec Ghost images contain only the actual data on a disk. If you have a 9 GB drive with only 600 MB of data, the Symantec Ghost image is approximately 600 MB, or is smaller if you use compression.

You can use Ghost Explorer to selectively recover individual files from an image file without restoring the complete disk or partition. You can also use Ghost Explorer to edit Ghost images.

Image files and compression

Image files created in Symantec Ghost support several levels of data compression. When Symantec Ghost is in interactive mode, three compression options are available: none, fast, and high. The Symantec Ghost command-line switch -z provides access to nine levels of compression.

See “About Symantec Ghost switches” on page 521.

As a rule, the more compression you use, the slower Symantec Ghost operates. However, compression can improve speed when there is a data transfer bottleneck. There is a big difference in speed between high compression and no compression when creating an image file on a local disk. Over a network connection, fast compression is often as fast as, or faster than, no compression. Over a parallel cable, high compression is often faster than no compression because fewer bytes are sent over the cable. Decompression of high-compressed images is much faster than the original compression. The level of compression that you select depends on your individual requirements.

The compression option is not available when you take an image of a drive that uses BitLocker Drive Encryption.

Performance on a network

One advantage of Symantec Ghost is speed. It takes minutes to install an operating system such as Windows XP, onto 10 or 100 computers. Many factors affect performance.

When you use Symantec Ghost across a network, use the fast compression option. If disk space is at a premium, you can use higher compression, but it can affect speed. The fastest performance over a network is usually achieved with GhostCasting.

Using a 10 MB/second Ethernet network, a 25-60 MB/minute server speed is common.

The following factors influence this range:

- Using up-to-date drivers
- LAN traffic
- Choice of network hubs or switches, including brand and model
- Compression

On a 100 MB/second Ethernet network, it is possible to achieve 80-300 MB/minute under ideal conditions. This speed is influenced by computer hardware and LAN performance. Greater performance is achieved with faster computers, NICs, and hard disks.

Image files and CRC32

Cyclic Redundancy Checking (CRC) is a data error checking technique. CRC ensures that the original data written to the image file is the same as the data on the disk. CRC32 is a CRC technique that uses a 32-bit value to store error checking information.

When an image file is created, CRC32 details are embedded into the file to ensure that image file corruption is detected when the image is restored to disk. CRC32 is currently included on a file-by-file basis with FAT partitions and on a volume basis for NTFS partitions.

In addition to image file error detection, the CRC values are used to verify that image files and partitions or disks are identical. This offers an additional method to detect bad sector writes and other drive anomalies that may be missed during normal imaging checks.

You can generate a text file that contains CRC values and associated file attributes using the -CRC32 command-line switch.

See “Using the -CRC32 switch” on page 548.

Image files and volume spanning

You can capture an image in a single file or span an image across a number of files.

Standard image files consist of a single file that contains the contents of the complete disk or required partitions. This type of image file is used for storing system configurations on server network drives for later restoration, or on other hard drives and tape drives where the volume is large enough to hold the complete image file.

Limitations on the image file size

The maximum file size is determined by the file system. If Ghost is writing an image onto a FAT32-formatted disk, the maximum file size is 4 GB. If the image is written to an NTFS-formatted disk, there is no maximum file size. Ghost writes to an image file until a write failure occurs. If the write failure occurs because the maximum file size is reached or because there is no more space left on the disk, then Ghost spans the image and creates a new image-file segment.

Size-limited image files

There are situations in which it is not practical to have a standard image file. Symantec Ghost can split an image file into segments (known as spans) that are limited to a user-specified size. For example, you may want to keep files created on your network drive limited to 100 MB so that you can transfer them easily in the future. This option is most commonly used to limit span sizes to 620 MB for later transfer to a CD.

If you access a large image file over a mapped network drive verify that the file is no bigger than 2 GB. The DOS drivers cannot successfully access large files over a mapped network drive. By splitting the file into spans, you enable Ghost to access a large image file.

See “About image file spans” on page 327.

Spanned image files

Spanned image files are similar to size-limited image files. The difference is that each segment file (or span) of the image file is limited by the actual volume size of the media to which the image is being saved. This lets you specify a drive and file name and lets Symantec Ghost determine when to request another volume or location for the remaining data. This is very useful when using ZIP, JAZ, LS120 Superdisk, and other drive types.

Spanning must be executed locally. If you try to span over a peer-to-peer connection (LPT, USB, TCP/IP, or GhostCasting), a disk full error message appears. However, splitting can be used in all situations.

Symantec Ghost also allows size limiting of spans when spanning volumes to ensure that no span exceeds the maximum size.

See "Spanning across multiple volumes and limiting span sizes" on page 317.

With all image files, the only constraint on the selection of the destination volume is that it must not be part of the source selection. For example, it cannot be on a source disk or partition if that disk or partition is to be included in the image.

The spanned files are named according to Microsoft application guidelines.

For example, as follows:

- First file: Filename.gho
- Second file: Filen001.ghs
- Third file: Filen002.ghs

You can use the -cns switch for an alternative naming standard.

For example, as follows:

- First file: Filename.gho
- Second file: Filename.001
- Third file: Filename.002

See "About Symantec Ghost switches" on page 521.

Spanning across multiple volumes and limiting span sizes

When you create an image file from a disk or partition, the destination drive might have insufficient space to store the image file. If Symantec Ghost determines that this is the case, it alerts you and asks whether to enable spanning. Symantec Ghost assumes that compression reduces the size of the image by one-third when it determines whether the image will fit. Alternatively, you can use the -span and -split command-line switches to configure Symantec Ghost to use image file size limiting.

See "Command-line switches" on page 522.

Before it saves the disk contents to the image file, Symantec Ghost shows the source and destination details and offers a chance to cancel. The default is to cancel.

Once the process starts, the image file creation continues until the destination volume is full.

If you started spanning onto a JAZ disk and want to span a 3.0 GB drive onto JAZ disks, you can choose to continue on JAZ disks. If you want to span across different forms of media, you can select a different type once the first portion of the span has completed. You cannot mix CD/DVD media with other types of media, such as JAZ or hard disk.

Note: You must record where the span segments are saved and the segment file names. Symantec Ghost does not record the locations and file names you selected.

Information about the partitions is stored at the start of the image file. This is updated at the end of the Ghost process, which might require you to reinsert the first disk in the span set. Symantec Ghost prompts you for the first disk in the span set and for subsequent volumes when restoring from an image.

Restoring from a spanned image

The process when restoring a disk or partition from a spanned image file is the same as restoring from an unspanned image file. However, during the restoration of the spanned image file, you are prompted for the locations of the image file spans. You must know the span segment locations and file names.

You can continue on the same form of media. For example, if you originally spanned onto a JAZ disk and want to restore a 3.0 GB drive from JAZ disks, you can replace the disk and continue from JAZ disks. Alternatively, you can restore from different media types.

Symantec Ghost automatically restores spanned images without prompting if it can find the next span.

Image files and tape drives

This section applies only to DOS/Windows Ghost. The Linux version of Ghost does not support direct writing to tape drives.

Ghost support of tape drives allows the storage of a single image file on a tape. When the image is written to the tape, Ghost.exe uses no associated file system, which means that you cannot access the tape from a drive letter as if it were another storage drive. Ghost does not support spanning to multiple tapes.

When you use tape drives with Ghost.exe, you can select the tape drive as the source or destination device in the File Locator window. Each tape device is shown as MTx, where x is a number starting at 0 and increasing incrementally for each drive present.

For Ghost.exe to access SCSI tape drives, a DOS ASPI driver must be installed prior to use.

See “Creating a standard Ghost boot package” on page 266.

Ghost.exe in its default mode performs well with most tape devices. In some situations with older tape devices and possibly with unreliable tapes, Ghost.exe may need to be configured to slow down or alter the way it uses the tape device.

See “Command-line switches” on page 522.

Note: Ghost Explorer cannot access an image stored on tape.

Drives with BitLocker Drive Encryption

The compression option is not available when you take an image of a disk that uses BitLocker Drive Encryption. Ghost performs a sector-by-sector copy of the entire disk.

You must verify that the disk on which the image is to be restored is identical to the source disk in every way. You should take a copy of a disk that uses BitLocker Drive Encryption only as a backup. If you restore an image onto a drive that has a different geometry, Windows Vista cannot interpret the disk.

Dynamic disks in Windows Vista/XP/2003/2000

Symantec Ghost supports backing up, restoring, and cloning simple or mirrored volumes on dynamic disks. Spanned, striped, and RAID-5 volumes are not supported by Symantec Ghost. You can back up an image of a partition on a disk in a dynamic disk set to an image file. If you back up a disk, then all of the partitions that Ghost supports on the disk, and only those partitions, are backed up to an image file.

Operations that support dynamic disks are as follows:

- Partition-to-partition
- Partition-to-image
- Disk-to-disk
- Disk-to-image
- Check image
- Check disk
- CRC32

- CRC32 verify

You can restore an image of a dynamic disk only to a basic disk, not to a dynamic disk. After you have restored the image file to a basic disk, you can then use Windows 2000 Disk Manager to convert the disk to a dynamic disk.

To delete a dynamic disk, use GDisk. Use the switch gdisk /mbr /wipe to delete all partitions from the disk. This method destroys all data on the disk.

See “About GDisk” on page 471.

See “Command-line switches” on page 522.

You can also take a disk image of a dynamic disk if you use the image all (-ia) switch. The -ia switch performs a sector-by-sector copy of the entire disk. The disk on which the image is to be restored must be identical to the source disk in every way. This function is only useful for creating a backup. If you restore an image created using -ia onto a drive with different geometry, Windows cannot interpret the dynamic disk.

If you restore an -ia disk image of a dynamic disk onto a SCSI hard drive and you receive a Destination drive too small message, you must load the ASPI driver for the SCSI card. Without an ASPI driver, Symantec Ghost does not always detect the correct size of the SCSI drive and cannot determine whether the drive is large enough to hold the image.

Note: Use the -ia switch with caution because it is slow and the image file would be very large.

Support for Disk Drive Overlays (DDO)

Symantec Ghost supports DDO as follows:

- Backing up or cloning a disk with a DDO creates an image file that does not include the DDO.
- Restoring an image onto a disk with a DDO leaves the DDO intact.
- Use the -ib switch to include the DDO in the backup or clone.
- Restoring the image file created replaces the existing DDO with the DDO included in the image.
- A GDisk disk wipe overwrites a DDO.
  See “Deleting and wiping your disk” on page 482.

Hibernation and swap files

When Symantec Ghost creates image files or clones, it does not include hibernation and swap files. These files are valid only for one Windows session, and when they are included in an image file, they make it significantly larger.

Symantec Ghost implements file skipping differently for each of the following file systems:

- FAT file systems: Files are not included on the image file or destination disk.
- NTFS file systems: A file with the same name is created on the image file or destination disk, but the contents of the file are not copied.

The following files are skipped on all file systems:

- 386Spart.par
- Amizvsus.pmf
- Dos data.sf
- Ghost.dta
- Hiberfil.sys
- Hibrn8.dat
- Hybern8
- Navsysl.dat
- Navsysr.dat
- Pagefile.sys
- Pm_hiber.bin
- Save2dsk.bin
- Saveto.dsk
- Spart.par
- Swapper.dat
- Toshiber.dat
- Virtpart.dat
- Win386.swp

Backing up or migrating a server

You can use Symantec Ghost to back up or migrate a server. However, it is not recommended that you use Symantec Ghost to roll out an image of a server to multiple computers.

If you are rolling out an image of a server you must resolve Security Identifier (SID) and configuration issues.

Resolving SID and configuration issues

If you are backing up a server then you do not need to change the SID and the operation should be successful if the computer's hardware is not changed after the backup has been made. If the hardware is changed then the computer might not start after the backup is restored.

If you are migrating a server then you do not need to change the SID and the operation should be successful if the hardware is identical on the source and destination hard drives or computers.

You can clone a server if the source and destination servers log on to two totally different networks and the two servers cannot see each other on the network. The source and destination computers must have identical hardware. In addition to SID considerations, Windows maintains many configuration settings that are unique to each server. For example, the choice of Domain Name Service (DNS) or Dynamic Host Configuration Protocol (DHCP) might affect whether a server can start, or if that computer can log on to a particular network or be recognized on the network. Symantec Ghost does not automatically configure such settings. These configuration settings must be manually changed.

For more information, consult your Windows and networking documentation.

Modifying image file contents with Ghost Explorer

This chapter includes the following topics:

Using Ghost Explorer

The Ghost Explorer utility lets you view, alter, add, and extract files from a Ghost image (.gho) file.

Note: You cannot open VMWare Disk image (.vmdk) files with Ghost Explorer.

Using Ghost Explorer, you can do the following:

- View image file contents and save a list of files within an image file.
- Extract files or directories from an image file.
- Add, move, copy, delete, and launch files from and within an image file.
- Use drag-and-drop or cut-and-paste functionality to add files and directories from Windows Explorer to the image file.
- Set span sizes.
- Add a description to an image file.
- Compile an image file to improve restore performance.

Ghost Explorer supports the following partition types:

- FAT12
- FAT16
- FAT32
- NTFS
- Linux Ext2/3

To open Ghost Explorer

◆ On the Windows taskbar, click **Start > All Programs > Symantec Ghost > Ghost Explorer**.

To access a list of file commands

◆ Right-click a file or directory in Ghost Explorer to access a list of file commands.

Viewing image files and their properties

You can view the contents of an image file, including details of the partitions, directories, and files. You can also view the image file properties.

If the image file contains NTFS partitions that are stored on a CD you might receive frequent prompts to swap CDs when you try to view the image file. To avoid this problem, copy the spans from the CD onto a hard disk and then view the image file on the hard disk.

To view an image file and the properties

1 Open Ghost Explorer.

See "To open Ghost Explorer" on page 324.

2 On the File menu, click **Open**.

3 Select an image file.

4 Click **Open**.

5 On the File menu, click **Properties** to view the image file properties.

Launching a file

Ghost Explorer restores a file to a temporary directory and attempts to open it. If the file is an executable program, it is run. If it is a data file and there is an application installed and associated with this file type, the application opens with the data file.

If you try to launch an application that depends on other files within the image file, it will probably fail. Ghost Explorer does not determine what dependencies exist. Extract the required files and then run the application file.

To launch a file

1 In Ghost Explorer, in the right pane, select a file.

2 On the File menu, click **Launch**.

Extracting a file or directory from an image file

You can extract a file or directory directly from an image file using Ghost Explorer. This does not delete the original file, but copies it to a new location.

Note: You can also use a drag-and-drop operation to move a file from Ghost Explorer to Windows Explorer to extract it.

To extract a file or directory from an image file

1 In Ghost Explorer, open the image file.

2 Select the file or directory to be extracted.

3 On the File menu, click **Extract**.

4 In the Extract To dialog box, select the location to which you want to extract the file or directory.

5 Click **Extract** to save the file or directory to the chosen location.

Modifying image files

Whether you can add, delete, or view an image file, or move files within an image file, depends on the version of Symantec Ghost that was used to create the image file. You can check the version of Symantec Ghost used to create your image file in the image file properties. Ghost Explorer cannot open a file created with a version of Symantec Ghost earlier than 3.0.

You can use Ghost Explorer to add files or directories from Windows Explorer to any image file that was created in Symantec Ghost version 6.0 or later. You can also delete files from any image file that was created in Symantec Ghost 5.1d or later. If you add a file or directory to an image file the original span split is preserved.

See “Viewing image files and their properties” on page 324.

Ghost Explorer supports Windows cut-and-paste operations within image files. For example, you can copy, paste, move, delete, and add files to images. You can also use a drag-and-drop operation to move files from Windows Explorer to Ghost Explorer.

To avoid problems, you should avoid making the following types of changes to an image file:

- Ghost Explorer prevents you from adding files to the root folder of Linux Ext2/3 partitions. If you add files, the new files are not visible when you restore the image, and the e2fsck tool reports errors.
- Do not add files to the root folder of a Ghost boot-partition image that contains PC DOS. A computer that is cloned from this image does not start.

Warning: If you use Ghost Explorer to add files to an image file, there may be some performance degradation when you restore the file using GhostCasting. Ghost Explorer calculates whether compilation is recommended. If it is, you can compile the file to improve performance.

See “Compiling an image file” on page 328.

Listing the contents of an image file

You can create a text file that contains a list of the directories and their details (and, optionally, files) that are in the current image file. You can store this file with the image file to keep an easily accessible list of the image file contents.

To list the contents of an image file

1. In Ghost Explorer, open the image file.
2. On the File menu, click **List Contents**.
3. Click one of the following:

Directories Only	List the directories only
Include Files	List the directories and the files
Include Details	List directories, files, and file details

4. Select a directory to which to save the text file.
5. Type a file name.
6. Click **Save**.

About image file spans

You can split an existing image file into smaller spans. This function is useful if, for example, you need to split a file into two or more files that can then be saved onto a CD/DVD drive that is unsupported by Symantec Ghost. After you split an image file you must compile it.

See “Compiling an image file” on page 328.

Note: If the CD/DVD drive is supported by Symantec Ghost, then as you create the image file you can save the image file directly to the CD/DVD.

Setting the default split options

Once this option is set, it becomes the default for all regenerated files.

To set the default split options

1. In Ghost Explorer, on the View menu, click **Options**.
2. In the Options dialog box, check **Span Image**.

3 In the Split point (MB) box, type the required size.

If you are splitting the file to save onto CD, then set the size to 600 MB.

4 If you want Ghost Explorer to choose a default name for additional span files that it creates, click **Autoname Spans**.

5 Click **OK**.

Compiling an image file

If you add or delete files from an image file, the image file becomes fragmented. Symantec Ghost takes longer to restore a fragmented image than a compiled file. You can improve the performance of a restore by compiling a file before you restore it. When you compile a file, the file is defragmented. If you want to split an existing image, then you must compile it to span the image file.

You can check the properties of the image file to determine whether compilation is recommended.

To compile an image file

1. On the File menu, click **Compile**.
2. If you want to span the image file, in the Save As dialog box, check **Span Image**, and then in the Split point (MB) box, type the required size.

   If you are splitting the file to save it on a CD, then set the size to 600 MB.
3. If you want Ghost Explorer to choose a default name for any additional span files that it creates, click **Autoname Spans**.
4. In the File name box, type a name and a location for the first new file.

   If you are splitting a file, all of the new files that are created are saved in the same location. You should use a different name than the original image file to avoid confusion.
5. Click **Save**.
6. If you are splitting the file, click **OK** each time that you are prompted to create a new span segment.

Using Ghost Explorer from the command line

You can start Ghost Explorer from a command prompt by typing its path and file name.

To start Ghost Explorer from a command prompt

1 On the Windows taskbar, click **Start > Programs > Accessories > Command Prompt**.

2 Type:

c:\Program Files\Symantec\Ghost\Ghostexp

This is the default path to Ghost Explorer.

3 Press **Enter**.

Ghost Explorer has a batch mode in which it carries out a single command and then exits. In this version, batch mode supports the saving of the contents to a text file only.

Table 14-1 specifies the switches to use the batch mode.

Table 14-1 Batch mode switches

Switch	Description
-t	Saves the list of directories in the dump file to a file with the same name as the image file but with an extension of .txt
-tf=filename	Saves a list of directories and files to filename
-tv	Saves a verbose listing of directories and files
-tv=filename	Saves a verbose list of directories and files to the file specified

See "Listing the contents of an image file" on page 327.

If Ghost Explorer reports that a spanned or split image is corrupt without prompting for the second part of the image, it may not recognize that the image is split. Starting with the -split argument forces Ghost Explorer to treat an image as a split image.

Using Ghost Explorer with long file names

The image index created by versions of Symantec Ghost prior to 5.1c did not handle long file names containing double-byte characters correctly, such as file names in Asian or Eastern European languages. Ghost Explorer may be able to show these names properly by reading them directly from the image file instead of from the index. However, the restoring of the image is much slower. Use the switch -ignoreindex to force this behavior. You must have the correct char set loaded.

To set the correct char set

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. Double-click **Regional Options**.
3. Select the required language option, and then click **OK**.

Section 4

Using Symantec Ghost locally

Chapter 15

Using Symantec Ghost as a stand-alone program

This chapter includes the following topics:

About Ghost.exe

Ghost.exe is a stand-alone program run within DOS that lets you copy disks or partitions from one computer to another. You can use Ghost to create image files and restore them.

Note: For Ghost32, VMDK images are supported for all normal operations, and PQI and V2I images are supported as a source (but not as a destination) in all cloning operations. You must have `v2DiskLib.dll` in the same directory as Ghost32.exe.

The information about Ghost.exe is also true for Ghost for Linux, with the following limitations:

- Direct writing to CD or tape is not supported.
- Peer to peer connections over printer cable or USB cable are not supported.

Using Ghost.exe on a stand-alone computer

The following is an overview of how to start and run Ghost.exe.

Note: Ghost.exe does not fit on a single floppy disk. Ghost.exe is concatenated on a RAM drive in DOS and executed from the RAM drive. The concatenation is transparent.

To use Ghost.exe on a stand-alone computer

1. Start Ghost.exe.

   See "Starting Ghost.exe" on page 335.

   Add command-line switches, if necessary.

   See "About Symantec Ghost switches" on page 521.

2. If necessary, establish a peer-to-peer connection.

   See "Establishing a peer-to-peer connection with Ghost.exe" on page 337.

3. Select the Ghost.exe operation:

   - Disk or partition to image file
   - Disk or partition from image file
   - Disk to disk
   - Partition to partition
   - Check image or disk

4. Do one of the following:

   - Select the source hard disk or partitions.
   - Select the image file.

5 Do one of the following for operations other than checking an image:

- Select the destination hard disk or partition.
- Select the image file.

Warning: Make sure that you select the correct destination. The destination disk is completely overwritten with no chance of recovering any data.

---

6 Complete the Ghost.exe operation.

Starting Ghost.exe

Ghost.exe is a DOS-based application that runs in DOS mode outside of Windows. You cannot run Ghost.exe within Windows Vista/XP/2000, Linux, OS/2, or other non-DOS operating systems. You can run Ghost.exe on a non-DOS operating system by using a Ghost boot package. The Ghost boot package lets you start the computer in DOS.

See "About Ghost boot packages" on page 254.

To start Ghost.exe

◆ Do one of the following:

Start the computer in DOS mode.	At the DOS prompt, type the following command: **progra~1\symantec \ghost\ghost.exe**
Use a DOS boot disk to start the computer.	After the first DOS boot disk loads you are prompted to insert the second Ghost boot disk. Ghost starts automatically. You can create a DOS boot disk on a computer that is running Windows or DOS. Additional DOS drivers might be required to runGhost.exe. If you cannot access some hardware or network resources, such as a CD-R/RW drive, you can use the Ghost Boot Wizard to create a boot disk that contains the necessary drivers. See "About Ghost boot packages" on page 254.
Use a DOS boot package to start the computer.	When the computer starts Ghost starts automatically. You can use the Ghost Boot Wizard to create a DOS boot package. See "About Ghost boot packages" on page 254.

Using Ghost.exe with a mapped network drive

When you access a mapped network drive you must be aware of the following:

- You must use a mapped network boot package created from the Ghost Boot Wizard.
  See "Creating a Drive Mapping Boot Package" on page 273.
- If the boot package contains Ghost.exe then you cannot save the package to a floppy disk set. You can save the package to a USB flash drive or an ISO image.
- If you run Ghost.exe from any location other than A: then you must reset the environment variable to the correct location of Wattcp.cfg before you start Ghost.
  See "About the Wattcp.cfg configuration file" on page 559.
- DOS drivers cannot handle large files over a mapped network drive. Therefore, Ghost sets a 2 GB split limit when writing to a mapped network drive. Before you access a large image file over a mapped network drive you should split the image file into spans that are no greater than 2 GB.
  See "About image file spans" on page 327.

If you have restarted the computer with a boot package that does not contain Ghost. exe then the computer restarts to a command prompt, for example D:\. You must reset the Wattcp environment variable to D:\net\wattcp.cfg. You can then start Ghost.exe from the mapped network drive.

If you have restarted the computer with a boot package that contains Ghost.exe then Ghost starts after the computer has restarted. If GhostCasting or peer-to-peer services are not available from the menu then ensure that Ghost is reading a Wattcp.cfg that has SHARE_MODE=1. Exit Ghost and then at the command prompt, reset the Wattcp environment variable. For example, if you are at the command prompt D:\, then reset the Wattcp environment variable to D:\net\wattcp.cfg, ensuring that D:\net\wattcp.cfg has SHARE_MODE=1. You can then restart Ghost from either D:\ or from a mapped network drive.

To reset the environment variable to the correct location of Wattcp.cfg

1. On the command line, type the following:

   set wattcp=<drive>\net\wattcp.cfg

2. Press **Enter**.

Establishing a peer-to-peer connection with Ghost.exe

Note: The Linux version of Ghost supports peer to peer connections over TCP only. It does not support LPT or USB connections.

If you are using an LPT, USB, or TCP peer-to-peer connection, then you must set up the connection between computers before a clone, backup, or restore operation.

The computers must be physically connected using one of the following:

LPT	A parallel connection cable
USB	A USB 1.1 cable See "Parallel Technologies cables" on page 557.
TCP peer-to-peer	A network connection See "TCP/IP connections" on page 552.

In a peer-to-peer operation, one computer is designated the master computer, and the other is designated the slave computer.

Table 15-1 describes the possible Ghost.exe processes and the master/slave relationships that exist within these processes.

Table 15-1 Master and slave computers

Action	Master	Slave
Disk-to-disk clone	Computer containing source disk	Computer containing destination disk
Back up disk to image file	Computer containing source disk	Computer receiving destination image file
Restore disk from image file	Computer containing destination disk	Computer containing source image file
Partition-to-partition clone	Computer containing source partition	Computer containing destination partition
Back up partition to image file	Computer containing source partition	Computer receiving destination image file
Restore partition from image file	Computer containing destination partition	Computer containing source image file

Select which computer is the master (the computer from which you control the connection) and which is the slave (the other computer participating in the connection). All operator input must occur on the master computer.

You must have two Ghost boot packages with which to start both the master and slave computers. You can create the boot packages using the Ghost Boot Wizard.

See "About Ghost boot packages" on page 254.

Note: You must create both boot packages in the same version of Symantec Ghost. You cannot use one boot disk that was created in Symantec Ghost 8.0 and one boot disk that was created in Symantec Ghost 11.5 in the same task.

To establish a peer-to-peer connection with Ghost.exe

1. Do one of the following:

   - On the master computer, insert the first Ghost boot disk into the floppy disk drive, and then restart the computer.
     Repeat this step on the slave computer.
   - Restart the master computer and the slave computer by using the Ghost boot package.

2. If you are using a floppy disk set, then, when prompted, insert the second Ghost boot disk into the floppy disk drives of the master computer and the slave computer.

   Ghost.exe starts automatically.

3 On the slave computer, on the main menu, do one of the following:

USB connection	Click **Peer to peer > USB > Slave** to start the computer as the slave computer.
LPT connection	Click **Peer to peer > LPT > Slave** to start the computer as the slave computer.
TCP/IP connection	Click **Peer to peer > TCP/IP > Slave** to start the computer as the slave computer. Make note of the IP address that is displayed in the Slave Connect dialog box.

4 On the master computer, on the main menu, do one of the following:

USB connection	Click **Peer to peer > USB > Master** to start the computer as the master computer.
LPT connection	Click **Peer to peer > LPT > Master** to start the computer as the master computer.
TCP/IP connection	Click **Peer to peer > TCP/IP > Master** to start the computer as the master computer. Type the IP address that is displayed on the slave computer.

About splitting images in a peer-to-peer operation

When you perform a peer-to-peer operation, an image is split when it reaches 2 GB in size unless you have set the split size to another value using the -split command switch. If this switch is explicitly set to 0, the image does not split.

See "About Symantec Ghost switches" on page 521.

Creating a backup image file

You can create a backup of a hard disk or one or more partitions.

The backup is saved as an image file, which you can store on the following:

- Second hard disk
- Second partition on your hard disk (partition backup only)
- LS120 Superdisk, JAZ, or ZIP disk

- CD-R/RW or DVD-R/RW/+R/+RW
  See “Saving an image file directly to a CD/DVD drive” on page 308.
- FireWire hard disk
- USB 1.1/2.0 hard disk
- Tape
- Locally mapped network file server
- Another computer using a peer-to-peer connection

Compression may affect the speed of your operation. When you select a compression level, Ghost.exe estimates the amount of space available for the destination image file. If there is insufficient space, Ghost.exe prompts you to enable spanning of image files.

Backing up a hard disk to an image file

When you back up a hard disk, a copy of the entire disk is saved as an image file.

To back up a disk to an image file

1 On the Ghost.exe main menu, do one of the following:

Local	Click **Local > Disk > To Image**.
Peer-to-peer connection	Click **Disk > To Image**.

2 In the Source Drive dialog box, select the source disk.

The Source Drive dialog box shows details of every disk that Ghost.exe finds on the local computer.

3 In the File Locator dialog box, type the image file destination and name.

4 In the Image file description dialog box, type a description of the image file.

You can modify this description on the Console or in Ghost Explorer.

5 Click **Save**.

6 When you are prompted to select the compression level, select one of the following:

No	For no compression
Fast	For low compression
High	For high compression

See "Image files and compression" on page 314.

7 In the Compress Image dialog box, select a compression option.

8 If Ghost detects that there is not enough space for the image file, you are prompted to enable spanning.

9 Check the details and ensure that the correct options are selected.

10 Do one of the following:

To proceed with the image file creation	Click **Yes**. The system performs an integrity check of the file structure on the source disk. The source disk is then copied to the destination image file. If you need to cancel the process, press **Ctrl+C**, but be aware that this action leaves the destination image file in an unknown state.
To return to the menu	Click **No**.

11 If spanning is required, do one of the following:

- Insert the next media, then click **OK**.
- Click **Browse**, then select the location of the next span of the image file.

See "Image files and volume spanning" on page 316.

12 Verify the integrity of the image file.

See "Verifying integrity" on page 351.

Backing up a partition to an image file

You can create an image file from one or more partitions to use as a backup or to clone onto another partition or disk.

To back up a partition to an image file

1. On the main menu, do one of the following:

Local	Click **Local > Partition > To Image**.
Peer-to-peer connection	Click **Partition > To Image**.

2. In the Source Drive dialog box, select the source drive.

   The Source Drive dialog box contains the details of every disk that Ghost.exe finds on the local computer.

3. In the Source Partition dialog box, select the source partitions to include in the destination image file.

   The Source Partition dialog box contains the details of all the partitions on the selected source disk. You can select multiple partitions.

4. Click **OK**.
5. In the File Locator dialog box, select the image file destination and name.
6. In the Image file description box, type a description of the image file.
7. Click **Save**.
8. When you are prompted to select the compression level, select one of the following:

No	For no compression.
Fast	For low compression.
High	For high compression.

   See "Image files and compression" on page 314.

9. In the Compress Image dialog box, select a compression option.
10. If Ghost detects that there is not enough space for the image file, you are prompted to enable spanning.

11 In the Proceed with partition image creation? dialog box, do one of the following:

To proceed with the image file creation	Click **Yes**. The system performs an integrity check of the file structure on the source partitions. The source partitions are then copied to the destination image file. If you need to cancel the process, press Ctrl+C, but be aware that this action leaves the destination image file in an unknown state.
To return to the menu	Click **No**.

12 If spanning is required, do one of the following:

- Insert the next media, then click **OK**.
- Click **Browse**, then select the location of the next span of the image file.

See "Image files and volume spanning" on page 316.

13 Verify the integrity of the image file when it has been created.

See "Verifying integrity" on page 351.

Restoring from an image file

You can restore a hard disk or a partition.

The restore is made from a previously created image file that is stored on one of the following:

- Second hard disk
- Second partition on your hard disk
- LS120 Superdisk, JAZ, or ZIP disk
- CD-R/RW or DVD-R/RW/+R/+RW
  See "Saving an image file directly to a CD/DVD drive" on page 308.
- FireWire hard disk
- USB 1.1/2.0 hard disk
- Tape
- Mapped network drive

- Drive on another computer (peer-to-peer)
- Drive or partition being restored

Restoring a hard disk from an image file

When you restore a hard disk, it is overwritten by the contents of the image file.

To restore a disk from an image file

1 On the main menu, do one of the following:

Local	Click **Local > Disk > From Image**.
Peer-to-peer connection	Click **Disk > From Image**.

2 In the File Locator dialog box, do one of the following:

- Type the path and file name of the image file.
- Click **Browse** to locate the image file.
  Specify the drive or device and select the full path name. The image file may reside on a local drive or on a locally mapped network file server. When using a peer-to-peer connection, the image file is located on the slave computer.

3 Press **Enter**.

4 In the Destination Drive dialog box, select the destination disk.

Choose carefully as this is the disk that will be overwritten.

The Destination Drive dialog box shows the details of every drive that Ghost.exe finds on the local computer.

5 In the Destination Drive Details dialog box, confirm or change the destination disk partition layout.

The Destination Drive Details dialog box shows a suggested partition layout for the destination disk. By default, Ghost.exe tries to maintain the same size ratio between new disk partitions.

You can change the size of any target FAT, NTFS, or Linux Ext2/3 partition by entering the new size in megabytes.

You cannot enter a value that exceeds the available space, is beyond the file system's limitations, or is not large enough to contain the data held in the source image.

Warning: The Destination Drive Details dialog box shows a suggested partition layout for the destination drive once the cloning process is completed. This partition layout may mirror the source drive layout. Therefore, the destination drive details appear similar to the source drive.

6 Click **OK**.

7 Do one of the following:

To proceed with the disk cloning.	Click **Yes**. Ghost.exe creates the destination disk using the source image file disk details. If you need to abort the process, press **Ctrl+C**, but be aware that this leaves the destination disk in an unknown state.
To return to the menu.	Click **No**.

Warning: Only click Yes if you are sure that you want to proceed. The destination disk is completely overwritten with no chance of recovering any data.

8 If prompted to insert an image span, when prompted, do one of the following:

- Insert the next media, then click **OK** to continue.
- Click **Browse** to restore from a different location, then type the location and file name of the image file span.

9 Restart the computer when the disk image restore is complete.

10 Verify the integrity of the destination disk.

See "Verifying integrity" on page 351.

You can also run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination disk.

Restoring a partition from an image file

When you restore a partition, it is overwritten by the data from an image file.

To restore a partition from an image file

1 On the main menu, do one of the following:

Local	Click **Local > Partition > From Image**.
Peer-to-peer connection	Click **Partition > From Image**.

2 In the File Locator dialog box, do one of the following:

- Type the path and file name of the image file.
- Click **Browse** to locate the image file.
  Specify the drive or device and select the full path name. The image file may reside on a local drive or on a locally mapped network file server. When using a peer-to-peer connection, the image file is located on the slave computer.

3 Press **Enter**.

4 In the Source Partition dialog box, select the source partition from the image file.

The Source Partition dialog box contains the details of all of the partitions in the image file.

5 In the Destination Drive dialog box, select the destination disk.

The Destination Drive dialog box contains the details of every disk that Ghost.exe finds on the local computer.

6 In the Destination Partition dialog box, select the destination partition.

Select an existing partition carefully as this is the partition that will be overwritten.

The Destination Partition dialog box contains the details of all of the partitions on the selected destination disk. You can create a new partition if space is available. If you create a new partition, it can be resized during the cloning operation.

7 In the Proceed with partition restore? dialog box, do one of the following:

To proceed with the partition cloning.	Click **Yes**. Ghost.exe overwrites the destination partition using the partition details contained in the image file. If you need to abort the process, press **Ctrl+C**, but be aware that this leaves the destination partition in an unknown state.
To return to the menu.	Click **No**.

Warning: Only click Yes if you are sure that you want to proceed. The destination partition is completely overwritten with no chance of recovering any data.

8 If prompted to insert an image span, when prompted, do one of the following:

- Insert the next media, then click **OK** to continue.
- Click **Browse** to restore from a different location, then type the location and file name of the image file span.

9 Restart the destination computer when the partition copy is complete.

10 Verify the integrity of the destination partition.

See "Verifying integrity" on page 351.

You can also run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination partition.

Cloning disks and partitions

By default, Ghost.exe tries to maintain the same size ratio between new disk partitions. However, you should note the following:

- You can change the size of any destination FAT, NTFS, or Linux Ext2/3 partition by entering the new size in megabytes.
- You cannot enter a value that exceeds the available space, is beyond the file system's limitations, or that is not large enough to contain the data held in the source partition.

Cloning disk to disk

When you clone disk to disk, Ghost.exe copies the contents of one hard disk onto another.

To clone disk to disk

1 On the Ghost.exe main menu, do one of the following:

Local	Click **Local > Disk > To Disk**.
Peer-to-peer connection	Click **Disk > To Disk**.

2 In the Source Drive dialog box, select the source disk.

The Source Drive dialog box shows the details of every disk that Ghost.exe finds on the local computer.

3 In the Destination Drive dialog box, select the destination disk.

Choose carefully as this is the disk that will be overwritten.

If a peer-to-peer connection method is used, the destination disk can be any of the slave computer's disks. However, if this is a local disk-to-disk copy, then the source disk is unavailable for selection.

4 Confirm the destination disk layout.

Warning: The Destination Drive Details dialog box shows a suggested partition layout for the destination drive once the cloning process is completed. This partition layout may mirror the source drive layout. Therefore, the destination drive details appear similar to the source drive.

5 Click **OK**.

6 When the "Proceed with disk clone?" prompt appears, do one of the following:

To proceed with the disk cloning.	Click **Yes**. The system performs an integrity check of the file structure on the source disk, and then copies the source disk to the destination. If you need to abort the process, press **Ctrl+C**, but be aware that this leaves the destination disk in an unknown state.
To return to the menu.	Click **No**.

Warning: Only click Yes if you are sure that you want to proceed. The destination disk is overwritten with no chance of recovering any data.

7 Restart the computer.

Warning: You should remove one of the hard disks before you restart your computer. If you leave two hard disks in the computer, damage can occur to both of the bootable operating systems.

8 Verify the integrity of the destination disk.

See "Verifying integrity" on page 351.

You can also run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination disk.

Cloning partition to partition

When you clone partition to partition, Ghost.exe copies the contents of one partition onto another.

To clone from partition to partition

1 On the main menu, do one of the following:

Local	Click **Local > Partition > To Partition**.
Peer-to-peer connection	Click **Partition >To Partition**.

2 In the Source Drive dialog box, select the source disk.

The Source Drive dialog box shows details of every disk that Ghost.exe finds on the local computer.

3 In the Source Partition dialog box, select the source partition.

The Source Partition dialog box shows the details of all of the partitions on the selected source disk.

4 In the Destination Drive dialog box, select the destination disk.

The Destination Drive dialog box shows the details of every disk that Ghost.exe finds on the destination computer. For peer-to-peer connections, the slave computer is the destination.

5 In the Destination Partition dialog box, select the destination partition.

Select an existing partition carefully as this is the partition that is overwritten.

The Destination Partition dialog box shows the details of all of the partitions on the selected destination disk. If this is a local partition-to-partition copy, then the source partition is unavailable for selection. However, you can create a new partition if space is available. If you create a new partition, it can be resized during the cloning operation.

6 Click **OK**.

7 When the final Proceed with Partition Copy? prompt appears, do one of the following:

To proceed with the partition copy.	Click **Yes**. If you need to abort the process, press **Ctrl+C**, but be aware that this leaves the destination disk in an unknown state.
To return to the menu.	Click **No**.

Warning: Only click Yes if you are sure that you want to proceed. The destination partition is completely overwritten with no chance of recovering any data. This is the last chance to back out.

8 Restart the destination computer when the partition copy is complete.

9 Verify the integrity of the destination partition.

See “Verifying integrity” on page 351.

You can also run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination partition.

Verifying integrity

After a backup, restore, or clone operation, check the integrity of the partition, hard disk, or image file.

To verify the integrity of an image file

- On the computer on which the image file is saved, on the main menu, do one of the following:

Local	Click **Local > Check > Image File**
Peer-to-peer connection	Click **Check > Image File**.

To verify the integrity of a disk

1. On the main menu, do one of the following:

Local	Click **Local > Check > Disk**.
Peer-to-peer connection	Click **Check > Disk**.

2. Select the source disk to verify.
3. Click **OK**.
4. Click **Yes** to start the disk check.

Adding switches to your Ghost.exe operation

You can include a number of options (or switches) that can also be entered using the command line. These switches are set in the Ghost.exe user interface as follows:

To add switches to your Ghost.exe operation

1. On the main menu, click **Options**.
2. Select from the following the options to include in your current cloning task.

Span/CRC	-span, -auto, -cns, -crcignore, -fcr
FAT 32/64	-f32,-f64, -fatlimit
Misc	-sure, -fro, -rb, -fx
Image/Tape	-ia, -ib, -id -tapeeject, -tapesafe, -tapeunbuffered, -tapebuffered
Security	-pwd, -locktype=type

   See “About Symantec Ghost switches” on page 521.

3. On the Save Settings tab, click **Save Settings** to confirm the list of active switches listed.
4. Click **Accept** to include the settings in the current task.

Running Ghost32.exe in Windows

Ghost32.exe is a Win32 version of Ghost.exe. It is designed to run on Microsoft Windows Vista/XP/2000. You can use Ghost32.exe to perform most Ghost operations on hard drives that are accessible from these operating systems. The hard drives must be able to communicate with the GhostCast Server.

If you run Ghost32.exe in Windows, note the following information:

- The partition on which Windows is installed cannot be overwritten.
- In Windows 2000, if you are overwriting a disk, you must restart the computer. In Windows XP/2003 Server, you should not have to restart the computer.
- Hard-disk sizes might appear smaller than their actual sizes. Ghost32.exe can only access the shown destination size. The remaining space is not used.
- Ghost32.exe does not support mount-point volumes on Windows Vista/XP/2000 computers.
- Hot imaging, which is the ability to capture an image of a computer without leaving Windows, is supported for Windows XP and Vista. The captured image is based on volume snapshots.
  You can use the forcevolumesnapshot switch to force an attempt to use volume SNAPSHOT on volumes in preference to standard volume locking.

Before executing Ghost32 on Windows 9x-based computers, ensure that the following files are in the same directory as Ghost32.exe:

- Int86_32.dll
- Int86_16.dll

You can find these files in the Symantec Ghost Solution Suite folder.

To run Ghost32 in Microsoft Vista, you must run the command prompt as an administrator.

To run the command prompt as an administrator

1. On the taskbar, click **Start > All Programs > Accessories**, right-click **Command Prompt** and click **Run as administrator**.
2. In the User Account Control dialog box, type the administrator credentials.
3. Click **OK**.

Compatibility with Ghost.exe

Ghost32.exe shares the following functions with Ghost.exe:

- Both Ghost.exe and Ghost32.exe can be a master or slave in a TCP/IP peer-to-peer operation.
- Image files that are created with Ghost.exe and Ghost32.exe are interchangeable.

Ghost32.exe differs from Ghost.exe in the following ways:

- You can run Ghost32.exe in Microsoft Windows Vista/XP/2000.
- LPT peer-to-peer is not supported.
- USB peer-to-peer is not supported.
- You cannot use Ghost32.exe with a disk or partition that has files open during the operation.
  For example, the system partition.
- When writing to CD/DVD, Ghost32.exe is not copied onto the CD/DVD.

Chapter 16

Performing post-clone configuration from the command-line

This chapter includes the following topics:

About performing applying post-clone configuration changes from the command-line

GhConfig is a executable program that lets you create configuration data files. You can use the configuration data files to apply configuration settings to a cloned computer. You can apply the configuration settings from the command-line without using the Console.

The versions of GhConfig are as follows:

- GhConfig.exe: Runs in DOS
- ghconfig: Runs in Linux
- GhConfig32.exe: Runs in Windows

The differences between the GhConfig tool and the post-clone configuration features that are available from the Ghost Console are as follows:

- The GhConfig tool lets you add Microsoft Windows Vista/XP/2000 computers to a domain. However, you must create the computer account in the domain before adding the computer to the domain. For the computer account to work, you must first add the security permissions for the Windows 2000/XP native mode, domain controllers in active directory.

- You can configure GhConfig to run one time. This option is available on stand-alone computer installations only. It prevents GhConfig from running on that computer after it runs the first time. To use GhConfig again on that computer, you must uninstall and reinstall GhConfig.

Applying a post-clone configuration from the command-line

Applying a post-clone configuration from the command-line involves the following steps:

- If you want to add the computer to a domain, then install the Configuration client on the computer.
  The Configuration client installation installs the GhConfig executable program and a simplified version of the Console client on the computer.
  See "Installing the Configuration Client Stand-alone" on page 55.
- Create a configuration data file, which contains a set of configuration settings..
- Run GhConfig to apply the configuration data files to the target computer.
- Restart the computer.

Creating a configuration data file

You can create a configuration data file using the GhConfig keywords. You can also export a configuration data file from the Ghost Console for a client computer.

See "Creating a new configuration set" on page 97.

The configuration data file that you create must meet the following requirements:

- It must follow a pre-defined format, which consists of a command keyword that is followed by a value, repeated.
- Each configuration data file must begin with the keyword CONFIG_COMMANDS and end with the keyword END_CONFIG_COMMANDS.
- The data files must be named either Ghregupd.reg or Gvpcfg.bin.

The following text provides an example of the contents of a configuration data file:

```
CONFIG_COMMANDS
COMPUTERNAME = "MY_COMPUTER" "MY_COMPUTER"
COMPUTERDESCRIPTION = "This is my demonstration computer" "This is my demon
WORKGROUP = "DEMONSTRATION" "DEMONSTRATION"
END_CONFIG_COMMANDS
```

Table 16-1 lists the command keywords that you can use to build the configuration data file.

Table 16-1 Configuration data file keyword commands

Keyword	Description
COMPUTERNAME	The name of the computer
COMPUTERDESCRIPTION	A description of the computer
DOMAINNAME	The name of the domain to which the computer belongs
DOMAINLOGIN	For Windows 98 computers, a number value that defines whether the computer should log on to the domain. The DOMAINLOGIN values are as follows: ■ 1: Yes ■ 0: No
DNSHOST	The name of the DNS host
DNSDOMAIN	The name of the DNS domain
DNSSERVER	The IP address of the DNS server
DEFAULTUSER	The default user name
DEFAULTGATEWAY	The IP address of the default gateway
IPADDRESS	The IP address of the computer
SUBNETMASK	The subnet mask
WORKGROUP	The workgroup to which the computer belongs
WINSSERVER	The IP address WINS server
NOVELLUSERNAME	The Novell user name
NOVELLTREE	The NetWare tree
NOVELLCONTEXT	The NetWare context

Table 16-1 Configuration data file keyword commands *(continued)*

Keyword	Description
NOVELLPREFERREDSERVER	The name of the Novell NetWare preferred server

Applying the configuration data file

You can apply the settings defined in the configuration data file by running the GhConfig executable program. Before you run GhConfig, you should verify that the operating system that you want to configure is not running If you want to join a computer to a domain, then the stand-alone client must be installed after you start Windows.

Table 16-2 lists the modes that are available with GhConfig and Ghconfig32.

Table 16-2 GhConfig switches

Switch	Description
-ad=image file name -addDisk=image file name	Mounts the specified vmdk, pqi, v2i, or iv2i image file ("add" the image as a disk). Once added, the disk can be used in all normal operations.
windows	Displays information about the Windows installations that are available. You can use this information with the /w switch. **Note:** The windows switch is not available on GhConfig32 when running on Vista.
[nics]	Displays information about the network cards that are available in the specified Windows installation.
[/w=windows_dir] [/c=config_dir]	Applies a configuration file to a Windows installation as follows: ■ windows_dir is the path to the Windows folder. If you do not specify a path, then GhConfig attempts to locate the active Windows installation and requests confirmation of the installation. ■ config_dir is the folder in which the configuration file is stored.

Table 16-2 GhConfig switches *(continued)*

Switch	Description
/translate	This switch is for GhConfig32 and applies only to Windows (not DOS or Linux). It attempts to translate between the dotted numeric notation that many of the Ghost tools use and drive letter notation used by Windows. You need to provide the translation parameter. For example: `/translate=1.1:` or `/translate=c:` If the translation can be made, the program shows the translation: '1.1: => C': or 'C: => 1.1:'. GhConfig32 also writes the translation to a file, `drvTrans.txt` in the working directory. If you need to translate between these formats in a script, the results can be parsed and used. This feature is especially useful when the mapping between the Ghost and Windows drive identifiers is not known until run time.
help	Lists the commands that are available.

Any errors that are generated are logged to ghconfer.txt, which is stored in the same folder as GhConfig.exe.

To apply the configuration data file

1. Start the computer in the appropriate operating system (DOS, Windows PE, or Linux).
2. Verify that the configuration data files and GhConfig are available on the target computer and that they are in the same folder.

   For example, you can place the files on a floppy disk or on a shared network drive.
3. Restore the computer.

   See "Restoring from an image file" on page 343.
4. Before you restart your computer, run the appropriate executable (GhConfig.exe, GhConfig32.exe, or ghconfig).

Section 5

GhostCasting image files

Chapter 17

Using GhostCasting to create and restore images

This chapter includes the following topics:

- About GhostCasting
- Preparing for GhostCasting
- Creating a GhostCast Server
- Starting a GhostCast session
- Creating an image file
- Restoring an image file onto client computers
- Controlling the GhostCast session from the server
- Setting Auto Start parameters
- Setting the data transfer mode
- Controlling the amount of network bandwidth used
- Viewing and changing GhostCast Server session options
- Running Ghost.exe on a client computer

About GhostCasting

GhostCasting lets multiple computers running Symantec Ghost receive the same information over a computer network simultaneously. The GhostCast Server works with Ghost.exe to create an image file of a model computer or restore an image file onto a number of client computers.

Symantec Ghost supports VMWare Disk images (.vmdk files) for both creating and restoring images. Symantec Ghost supports Backup Exec System Recovery (.v2i, .iv2i) and DeployCenter Library (.pqi) images for restoring a computer only.

The GhostCast Server supports the following forms of data transfer for transferring files:

- Unicasting
- Direct Broadcasting
- Multicasting

GhostCasting makes workstation migration and rollouts more efficient and may eliminate replicated network traffic. You can use it through the Windows interface, command-line switches, batch files, or a combination of all methods.

The following applications are used in GhostCasting:

- The GhostCast Server on the network server restores image files to multiple clients or creates an image file from a single connected client.
- On a client workstation, Ghost.exe receives and writes the image file to the local disk.

GhostCasting supports the following:

- Ethernet networks
- Token ring networks
- Image file creation
- Multicast-enabled routers
- Automatic IP address selection using BOOTP or DHCP
- Session start scheduling
- Partition-only GhostCasting
- Multiple, simultaneous sessions, or one session per server

Splitting images in a GhostCast operation

When you perform a GhostCast operation, an image is split when it reaches 2 GB in size unless you have set the split size to another value with the -split command switch. If this switch is explicitly set to 0, the image does not split.

See “About Symantec Ghost switches” on page 521.

Preparing for GhostCasting

Before GhostCasting, you must set up the required software and hardware.

To prepare for GhostCasting

1. Set up the network hardware.
   - Install the network adapter.
   - Connect cabling.
   - Set up the network adapter using the manufacturer's installation program.
   - Run the network adapter test program to check the network adapter and cabling.
2. Determine the IP and networking settings.
   - BOOTP/DHCP vs. manual configuration
   - Network adapter drivers
   - Other overall requirements

   See "About IP addresses for GhostCasting" on page 385.

About creating the model computer

Create a model computer to serve as a template for client computers. This is the first step in creating a Symantec Ghost image. Set up a computer with Windows and all of its drivers installed and configured as you want all of your computers configured.

You may need to create a model computer for each unique hardware setup. For example, if you have some computers with SCSI disks and some with IDE disks, you need to have separate images for them. However, on Windows 2000/XP computers, Microsoft Sysprep can help you create a generic template image for different hardware setups.

Note: Before you take an image of a Windows Vista/XP/2000 computer, you should verify that the computer is not a member of a domain .

Creating a GhostCast Server

The GhostCast Server creates or distributes a copy of an image file to Symantec Ghost clients in a session composed of one server, a single image file, and one or more similar clients. The session name acts as a key. The session name identifies the session and is used by clients to indicate the session that they are to join.

To create a GhostCast Server

1. Install GhostCast Server (Ghostsrv.exe).

   See “Installing Symantec Ghost Standard Tools” on page 56.

2. Create a boot package that contains Ghost.exe for the client computers.

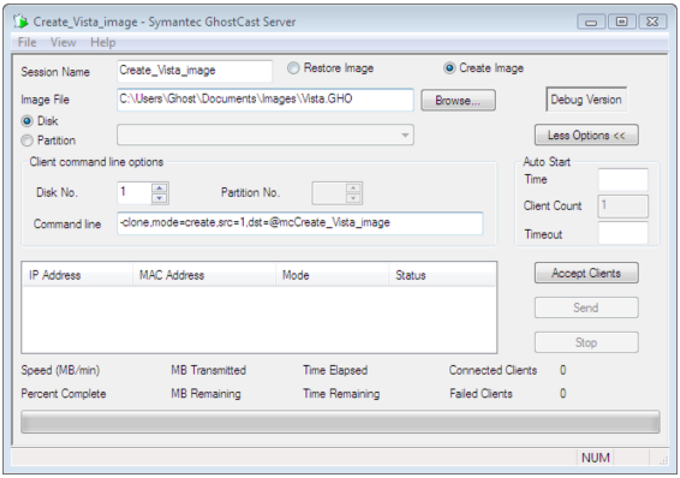
   See “Creating a Network Boot Package” on page 272.

Starting a GhostCast session

After setting up the server and preparing the boot package for the client computers, you can run a GhostCast session.

To start a GhostCast session

1. On the GhostCast Server computer, on the Windows taskbar, click **Start > Programs > Symantec Ghost > GhostCast Server**.



Create_Vista_image - Symantec GhostCast Server

Session Name: Create_Vista_image ○ Restore Image ● Create Image

Image File: C:\Users\Ghost\Documents\Images\Vista.GHO

● Disk
○ Partition

Client command line options

Disk No. 1 Partition No.

Command line: -clone,mode=create,src=1,dst=@mcCreate_Vista_image

Auto Start
Time
Client Count 1
Timeout

Connected Clients 0
Failed Clients 0

2. In the GhostCast Server window, in the Session Name box, type a session name.

   A GhostCast session name can be any alphanumeric sequence of characters and must be unique on your network. You can use spaces on the GUI but not with command-line switches. Session names are not case-sensitive.

Creating an image file

To create an image file, you must first start a GhostCast session from the GhostCast Server. Once you create a session on the server, join the GhostCast session from the source computer.

To create an image file using the GhostCast Server

1. In the GhostCast Server window, click **Create Image**.
2. Do one of the following:
   - In the Image File box, type the name and full path of the image file that you are creating.
   - Click **Browse** to find the location.

   You can overwrite existing files.
3. Do one of the following:
   - To create an image of an entire disk, click **Disk**.
   - To create an image of a selected partition, click **Partition**.
4. Click **Accept Clients** to accept the client computer into the session.

   The Accept Clients button becomes active when all boxes are filled in.
5. Start Ghost.exe on the destination client computers and begin a GhostCast session.

   See "To connect a source computer to a GhostCast session" on page 367.

Connecting a computer to a session

Once the GhostCast session is started on the server, you can start the client computer from a boot disk and have it join the session.

To connect a source computer to a GhostCast session

1. Create a GhostCast session on the GhostCast Server.

   See "To create an image file using the GhostCast Server" on page 367.
2. Using the Ghost network boot package, start Ghost.exe on the client computer.

3 On the Ghost.exe menu, click **GhostCasting**, then select one of the following:

Multicast	Connect to the session using Multicasting
Direct Broadcast	Connect to the session using direct broadcasting
Unicasting	Connect to the session using Unicasting

4 In the GhostCast Session Name to Join dialog box, type the session name.

5 Click **OK**.

6 Select the disk from which to take an image.

7 Click **OK**.

8 Select the partition from which to take an image, if required.

9 Click **OK**.

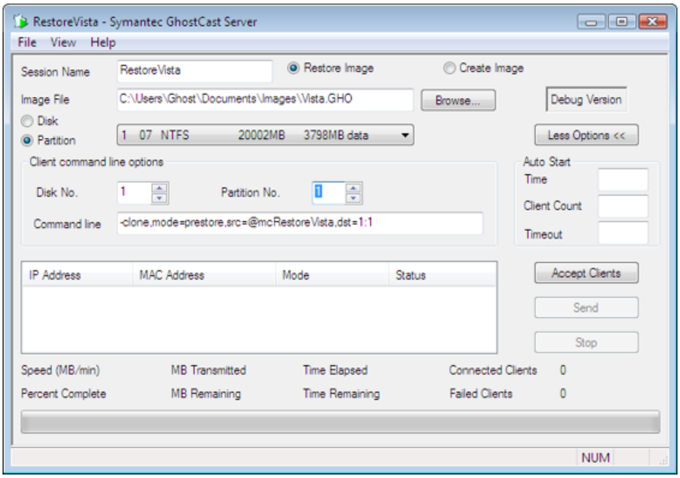
10 Select the level of compression that you require.

11 Click **Yes** to begin.

See "Running Ghost.exe on a client computer" on page 377.

Restoring an image file onto client computers

To restore an image file, you must first start a GhostCast session on the GhostCast Server. Once you create a session, connect the client computers to the GhostCast session.



Session Name RestoreVista
● Restore Image ○ Create Image
Image File C:\Users\Ghost\Documents\Images\Vista.GHO
○ Disk
● Partition 1 07 NTFS 20002MB 3798MB data
Client command line options
Disk No. 1 Partition No. 1
Command line -clone,mode=prestore,src=@mcRestoreVista,dst=1:1
Auto Start
Time
Client Count
Timeout
Speed (MB/min) MB Transmitted Time Elapsed Connected Clients 0
Percent Complete MB Remaining Time Remaining Failed Clients 0

To restore an image onto client computers using the GhostCast Server

1. Click **Restore Image** to send an image file to all connecting clients.
2. Do one of the following:
   - In the Image File box, type the name and full path of the image file containing the image.
   - Click **Browse** to find the location.
3. On the File menu, click **Image Description** to view or modify a description of the image file.

   The disk or partition settings must be selected. If the file selected is not a valid image file, an error message appears.
4. Do one of the following:
   - To restore an image of an entire disk, click **Disk**.
   - To restore an image of a partition and select the partition from the image file, click **Partition**.
5. Click **Accept Clients** to accept the client computer into the session.

   The Accept Clients button becomes active when all required boxes are filled out.
6. Join the client computers to the GhostCast session.

   See "To join a GhostCast session to restore an image file to client computers" on page 370.
7. Click **Send** to start the image restore and the GhostCast session when all of the required clients have joined the session.

The progress indicator shows the status of the GhostCast session as it proceeds, along with other image file and transfer details. The statistics shown are based on the image file size and reflect the sizes after compression. The speed shows the actual amount of data being sent over the network in megabytes-per-minute from the image file. The client status changes to In Progress.

If you close the GhostCast Server or turn off the computer once a GhostCast session has started, the GhostCast session stops and a warning message appears.

You must start Ghost.exe on the client computer and join the clients to the GhostCast session.

To join a GhostCast session to restore an image file to client computers

1. On the client computers, use the Ghost Boot Disk to start Ghost.exe.
2. On the Ghost.exe menu, click **GhostCasting**, then select one of the following:

Multicast	Connect to the session using Multicasting
Direct Broadcast	Connect to the session using Direct Broadcasting
Unicasting	Connect to the session using Unicasting

3. In the GhostCast Session Name to Join dialog box, type the session name.
4. Click **OK**.
5. Select the disk to restore.
6. Click **OK**.
7. Select the partition to restore, if required.
8. Click **OK**.
9. Click **Yes** to indicate that the computer is ready for the image restore to begin.

   See "Running Ghost.exe on a client computer" on page 377.

   The IP and MAC addresses of the client computers that are connected and waiting for the GhostCast session to start appear in the Connected Clients list along with their status.

Controlling the GhostCast session from the server

In the GhostCast session, you can specify the client disk or partition to restore from the server. You can also define command-line options to execute on the client computer as part of the cloning task.

To create an image file using the GhostCast Server and command-line options

1. On the GhostCast Server, start a GhostCast session to create an image file.

   See "To create an image file using the GhostCast Server" on page 367.
2. Click **More Options**.
3. In the Disk No. box, type the disk number.
4. In the Partition No. box, type the partition number if you are creating an image of a partition.

   The client clone command appears in the Command line box.

5 Add other switches to the command line to execute specific command-line options on the client computer, if required.

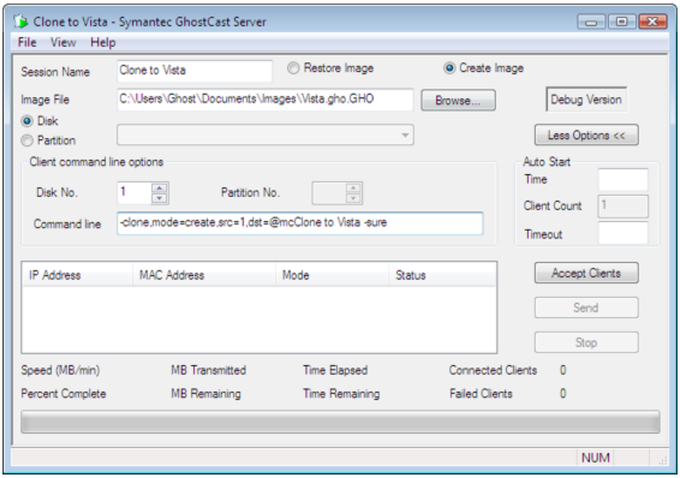
For example, if the initial command is:

-clone,mode=pcreate,src=2,dst=@mcSessionNm

Add the following switches to avoid prompts and restart the client computer after the image has been extracted:

-clone,mode=pcreate,src=2,dst=@mcSessionNm -sure -rb

Only use the -sure switch when you are certain that you are writing from the intended disk or partition.



Clone to Vista - Symantec GhostCast Server

Session Name: Clone to Vista
○ Restore Image ● Create Image
Image File: C:\Users\Ghost\Documents\Images\Vista.gho.GHO
● Disk
○ Partition
Client command line options
Disk No.: 1
Partition No.:
Command line: -clone,mode=create,src=1,dst=@mcClone to Vista -sure
Auto Start
Time:
Client Count: 1
Timeout:

IP Address	MAC Address	Mode	Status

Speed (MB/min) MB Transmitted Time Elapsed Connected Clients 0
Percent Complete MB Remaining Time Remaining Failed Clients 0

6 Click **Accept Clients** to accept the client computer into the session.

7 Start the client computers in DOS.

8 Run Ghost.exe using the -ja switch to log on to the GhostCast session from the command line:

```
ghost.exe -ja=SessionNm
```

9 Confirm your choices on the client computers if the -sure switch was not used.

See “Running Ghost.exe on a client computer” on page 377.

To restore an image onto client computers using the GhostCast Server

1 Create a GhostCast session to restore an image from the GhostCast Server.

2 Click **More Options**.

3 In the Disk No. box, type the disk number.

4 In the Partition No. box, type the partition number, if required.

5 In the Command line box, type the client clone command.

Add other switches to the command line to execute specific commands on the client computer.

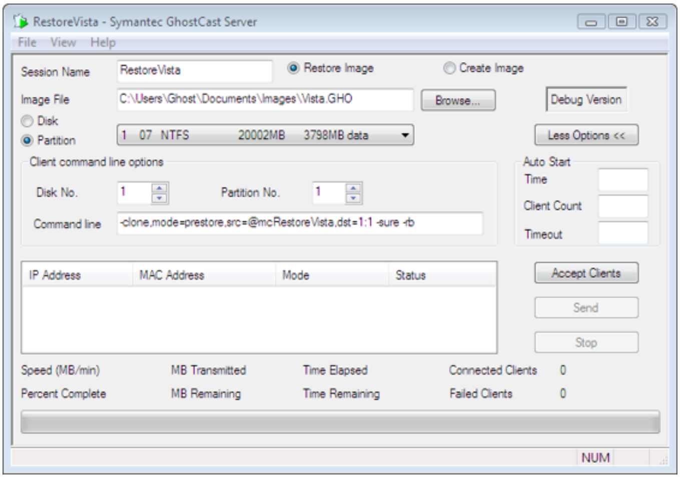
For example, if the initial command is:

-clone,mode=prestore,src=@mcSessionNm,dst=1:1

Add the following switches to avoid prompts and restart the client computer after the image has restored:

-clone,mode=prestore,src=@mcSessionNm,dst=1.1 -sure -rb

Only use the -sure switch when you are sure that you are writing to the intended disk or partition.



RestoreVista - Symantec GhostCast Server

Session Name: RestoreVista

● Restore Image ○ Create Image

Image File: C:\Users\Ghost\Documents\Images\Vista.GHO

○ Disk
● Partition: 1 07 NTFS 20002MB 3798MB data

Client command line options

Disk No.: 1
Partition No.: 1

Command line: -clone,mode=prestore,src=@mcRestoreVista,dst=1:1 -sure -rb

Connected Clients: 0
Failed Clients: 0

6 Click **Accept Clients** to accept the client computer into the session.

7 Start the client computers in DOS.

8 Run Ghost.exe using the -ja switch to log on to the GhostCast session from the command line:

ghost.exe -ja=SessionNm

9 Confirm your choices on the client computers if the -sure switch was not used.

See “Running Ghost.exe on a client computer” on page 377.

Setting Auto Start parameters

When your GhostCast session includes restoring an image file to client computers, you can set the server to start the session automatically. The start time can be based on a single parameter or a combination of parameters.

If you specify more than one Auto Start parameter, the session starts when one of the conditions is fulfilled.

To set Auto Start parameters

1 In the GhostCast Server window, click **More Options**.

2 Do one or more of the following:

To use the time parameter:	Type a specified time using a 24-hour clock and within the next 24-hour time period. For example, 5:30 AM would be 05:30, and 5:30 PM would be 17:30.
To use the number of clients parameter:	Type the number of clients that are connected to the session. For example, if the threshold is set to 10, then the server waits and accepts clients until the tenth client. Once the tenth and final client is accepted, the server stops accepting clients and starts sending out to the connected client computers.
To use the timeout parameter:	Type a number of minutes after the last client joined. For example, if the timeout is set to 15, the server waits indefinitely until the first client is accepted. After the first client joins, the 15 minute countdown starts. If no more clients join, the session starts 15 minutes later. If another client joins before the 15 minutes timeout, the timeout counter resets to 15 minutes and starts counting down again.

Setting the data transfer mode

You can set the data transfer mode to optimize the use of your network hardware setup. Used in conjunction with network bandwidth limits, you can optimize the way data files are transferred over your network.

Table 17-1 lists the transfer options.

Table 17-1 Transfer options

Mode	Description	Use if
Unicast	Each packet is addressed to one computer. One stream of data is sent for each client.	You are transferring a data packet to one or two computers only.
Directed broadcast	Data is sent to all computers on a specified subnet. If clients are on more than one subnet, one stream is sent to each subnet.	Your network hardware does not support Multicasting.
Multicast	Data is sent to all computers on the network that have requested the data. Only one stream of data is sent.	Unicast or subnet targeted broadcasting are not appropriate.

Multicasting is usually the most efficient option for the following reasons:

- Only one stream of data is sent out for all clients.
- Multicasting sends packets only to client computers that have requested data from the GhostCast Server.

This requires the support of appropriately configured routers and switches. You can alter settings globally or for a GhostCast session.

Symantec Ghost attempts to use Multicasting by default. If you have set the data transfer mode to Unicast or Directed broadcast, then Symantec Ghost uses that method. If Directed broadcast or Multicasting fails, then Symantec Ghost attempts to use Unicast.

See “Setting the default data transfer properties” on page 82.

To set the data transfer mode

1. In the Symantec GhostCast Server window, on the File menu, click **Options**.
2. Click **Force Mode**.
3. Select one of the following:
   - Multicast
   - Directed Broadcast
   - Unicast
4. Click **OK**.

Controlling the amount of network bandwidth used

Symantec Ghost lets you control how much network bandwidth is used when GhostCasting. By using this functionality, you can avoid overloading the network with GhostCasting traffic.

You can enter a value for restoring an image, creating an image, or both. The values are saved and loaded the next time that you run the GhostCast Server. However, if you run a GhostCast session from the command line, the limits that are set on the command line are used for that session only.

See "GhostCast Server command-line options" on page 380.

Limiting network bandwidth is useful in some circumstances. Consider the following:

- By limiting network bandwidth, you can increase performance on the network for users who are not the intended recipients of image files.
- If your network hardware does not support multicasting, then limiting bandwidth is helpful in many situations.

Table 17-2 provides a guide to network hardware setups and when you may or may not want to limit network bandwidth.

Table 17-2 Limiting network bandwidth

Limit network bandwidth for	Hub only	Layer 2 switch	Layer 3 switch or multicasting compatible router and layer 2 switch
Unicast	Yes	No	No
Subnet targeted broadcast	Yes	Yes	Yes
Multicast	Yes	Yes	No

In situations where you would not limit network bandwidth, the hardware directs the traffic to intended recipients only, and all other users should be unaffected.

To set a limit for network bandwidth

1. In the Symantec GhostCast Server window, on the File menu, click **Options**.
2. In the Options dialog box, check **Limit data throughput for**.

   If this option is not enabled, then no limit is set.

3. In the Restoring box, type the maximum MB per minute to set a limit for restoring an image.
4. In the Creating box, type the maximum MB per minute to set a limit for creating an image.

   The ideal maximum usage to expect is as follows:

100 BaseT	300 MB per minute
10 BaseT	60 MB per minute

Viewing and changing GhostCast Server session options

In the Options dialog box you can specify session parameters.

You can specify a range of multicast addresses. Addresses in the following range are valid: 224.0.2.0-239.255.255.255. To specify an exact address, set the end address to the same as the start address. By setting a wide range of addresses, you can limit the chance of conflict if you run two or more GhostCast operations simultaneously. This option should be used by advanced users only.

To view or record GhostCast Server options

1. On the File menu, click **Options**.
2. If you want to use a specified multicast address range, click **Use Specified Multicast Address Range**, then type the multicast From and To addresses.
3. Click **Multicast Scope TTL** to set the time to live.

   This limits how far the data passes through a network. Time to live is decremented by every router through which the data packet passes.
4. Select one of the following:

Restart On Completion	Restart the GhostCast Server, accepting clients and using the same Auto Start parameters.
Close GhostCast Server On Completion	Close Symantec GhostCast Server once the session is complete.

5 Click **Log clients** to create a log that lists GhostCasting session details, including when a session took place, the computers involved, and whether the session was successful.

The log is saved to the path specified.

6 In the Log Level box, select a log level to set a level of diagnostic GhostCast logging.

7 In the Log File box, type a destination log file location.

Running Ghost.exe on a client computer

When using GhostCasting, the client executable, Ghost.exe, restores a GhostCast copy of an image file onto the client computer or creates an image file onto the GhostCast Server.

Ghost.exe runs under DOS and uses a packet driver interface to the network card. The TCP/IP settings are stored in a configuration file Wattcp.cfg that is located in the same directory as Ghost.exe.

As with all Symantec Ghost applications, DHCP, BOOTP, and manually set IP addresses are supported.

Use the Symantec Ghost GhostCast client command-line switches to run Ghost.exe from the command line or in the GhostCast session.

For a GhostCasting session, the selection of the partition or drive to write to, or read from, on the client is specified either on the client or in the command-line option on the server. Use the -ja switch on the client to run the operation from the server.

For any GhostCasting session, the session name on the entry screen of the client should match the GhostCast Server session name.

GhostCasting from the command line

This chapter includes the following topics:

About running GhostCast Server from the command line

You can run the Symantec GhostCast Server from the command line by including switches with ghostsrv.

You can run GhostCast Server from the command line. Use a batch file or third-party scheduler application to start the server.

The syntax for running GhostCast Server is as follows:

```
ghostsrv filename session [options]
```

Where:

filename	Specifies the path and file name of a disk image file.
session	Specifies the session name.

See “GhostCast Server command-line options” on page 380.

Starting the GhostCast session

Once you have created a GhostCast session and the client computers have appeared on-screen, you can start the transmission.

To start the session transmission

- When all clients have connected, click **Start**.

GhostCast Server command-line options

Table 18-1 lists the GhostCast Server command-line switches.

Table 18-1 GhostCast Server switches

Switch	Description
-Ncount	Starts the GhostCast transmission after count clients have joined the session.
-Ttime	Starts sending to a session automatically after a specified time (24-hour hh:mm format) with a maximum of 24 hours.
-Ominutes	Starts transmission minutes after the last client connection.
-Llevel	Creates a log file specifying log level E, S, W, I, or A. The log level x can be E (errors), S (statistics), W (warnings), I (information), or A (all) in increasing order of logging detail.
-Ffilename	Specifies log file name for the -L option and is by default, Ghostlog.txt.
-C	Closes ghostsrv application after GhostCast session completion.
-D	Uses create from client mode. Restore to client is the default.
-R	Restarts the GhostCast session on completion and waits for client connections again after GhostCasting is complete.
-P	Specifies partition mode operation. If restoring to clients, the partition number must be given. If creating an image from client, no partition number is required.
-U	Forces the multicast mode, as follows: ■ -UM (Multicast) ■ -UU (Unicast) ■ -UD (Directed Broadcast)

Table 18-1 GhostCast Server switches *(continued)*

Switch	Description
-Mxxx.xxx.xxx.xxx	Sets the multicast address to xxx.xxx.xxx.xxx. Addresses between 224.0.2.0—239.255.255.255 are valid.
-Mxxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx	Specifies a range of multicast addresses. The address is chosen from within this range. Addresses between 224.0.2.0—239.255.255.255 are valid.
-DISKnumber	Specifies the client disk number to which to restore or create the image file.
-PARTnumber	Specifies the client partition number to which to restore or create the image file.
-Gswitch	Specifies switches to include in the command line and those used by the Ghost application.
-HLxxx	Sets the maximum amount of bandwidth consumed while restoring an image, where xxx is the number of megabytes per minute.
-HDxxx	Sets the maximum amount of bandwidth consumed while creating an image, where xxx is the number of megabytes per minute.
-TTLxxx	Sets the multicasting time to live.

Command-line option examples using GhostCast Server

Table 18-2 lists some examples of using GhostCast Server.

Table 18-2 GhostCast Server command-line examples

Summary	Syntax	Description
Creating an image file of a complete disk from a client computer and saving to image file c:\test123.gho using the session name labmodel	ghostsrv c:\test123.gho labmodel -d	Starts a GhostCast session called labmodel and creates or overwrites the image file c:\test123.gho. The first connecting client's IP address appears on-screen, and the session starts automatically. The client computer indicates the source drive to use for the image file creation.

Table 18-2 GhostCast Server command-line examples *(continued)*

Summary	Syntax	Description
Creating an image file of a partition from a client computer to an image file	ghostsrv c:\test123.gho TestSession -d -p	Starts a GhostCast session called TestSession and creates or overwrites the image file c:\test123.gho. The first connecting client's IP address appears on-screen, and the session starts automatically. The client computer indicates the source drive and partitions to include in the image created.
Restoring a disk image file onto client computers	ghostsrv.exe c:\test123.gho TestSession	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. Start the session transmission. See "Starting a GhostCast session" on page 366.
Restoring a specific partition from an image file onto client computers	ghostsrv c:\test123.gho TestSession -p2	Starts a GhostCast session called TestSession and uses the second partition in the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen.
GhostCasting a specific partition from an image file to a specific partition on a destination drive	ghostsrv c:\test123.gho TestSession -p1 -DISK1-PART2	Starts a GhostCast session called TestSession, uses the first partition in the image file c:\test123.gho, and places it in the second partition of the clients' first disk. The connecting clients' IP addresses appear on-screen. Start the GhostCast transmission. See "Starting a GhostCast session" on page 366.

Table 18-2 GhostCast Server command-line examples *(continued)*

Summary	Syntax	Description
Specifying the number of clients to Auto Start	ghostsrv c:\test123.gho TestSession -n10	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. Once 10 clients have connected, the session transmission starts automatically.
Specifying a time for Auto Start	ghostsrv c:\test123.gho TestSession -t13:30	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. At half past one in the afternoon (1:30 PM), the session transmission starts automatically.
Specifying time-based and client-count Auto Start and automatic closing	ghostsrv c:\test123.gho TestSession -t13:30 -n10 -c	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. At either half past one in the afternoon (1:30 PM) or after 10 clients join the session, transmission starts automatically. Ghostsrv does not wait for both conditions to be met. When the GhostCast session is completed, ghostsrv closes down as requested.
Isolating problems	ghostsrv c:\test123.gho TestSession -la -ferrlog.txt-n10	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. Once 10 clients connect, the session transmission starts automatically and a log file, Errlog.txt, is created for debugging. Creating a log file reduces the performance of the GhostCast transmission.

GhostCasting and IP addresses

This chapter includes the following topics:

About IP addresses for GhostCasting

An IP network using locally specified addresses requires each manually setup computer to have the following:

- A unique IP address
- The correct subnet mask
- The default gateway (optional)

Specify the TCP/IP configuration parameters using one of the following methods:

- Locally on a computer in a configuration file
- Automatically using a BOOTP or DHCP server

Locally specified IP addresses

The GhostCast Server receives its locally specified IP addresses, subnet masks, and default gateways from the TCP/IP parameters in the Network option of the Windows Control Panel.

Examples of Wattcp.cfg client configuration files

The following example displays the IP details on a computer and the details in the Wattcp.cfg file:

IP details:

- IP address: 192.168.100.3
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.100.1

Wattcp.cfg:

- IP = 192.168.100.3
- Netmask = 255.255.255.0
- Gateway = 192.168.100.1

If the server and client are within the same subnet, a default gateway is not required. If they are on a separate subnet, a default gateway must be supplied.

About using BOOTP/DHCP to assign IP addresses

If a BOOTP or DHCP server is installed on the network, you may take advantage of DHCP or BOOTP for IP address assignment. A DHCP server is included in Windows NT Server release 4.0 and Windows 2000. Other DHCP and BOOTP applications are available for various operating systems and can be used with GhostCasting.

If you are GhostCasting to many clients, not having to edit a unique Wattcp.cfg file on every client may be advantageous. Balanced against this is the additional complexity of the DHCP setup.

BOOTP/DHCP automatically defined IP address

Specifying a local configuration for every computer on an IP network can be inconvenient or impractical. GhostCasting supports BOOTP and DHCP servers.

You must run the BOOTP or DHCP server to specify a computer's IP address. The BOOTP/DHCP server listens on the network for computers requesting an IP address and replies with the address that the BOOTP/DHCP server is configured to provide. The BOOTP/DHCP server must be configured to provide the IP address, subnet mask, and (optionally) the default gateway.

Section 6

Creating executables to roll out applications

Chapter 20

Using AutoInstall

This chapter includes the following topics:

About AutoInstall executables

An AutoInstall executable contains all the changes that are made to files and registry keys when an application is installed and configured on a model computer. When you deploy an AutoInstall executable to a computer, the executable installs and configures the application by making the same changes to files and registry keys.

Note: AutoInstall executables are designed to be deployed to computers that have the same hardware and same operating system as the model computer.

How Ghost AutoInstall works

Ghost AutoInstall lets you create and customize AutoInstall executables.

Note: On x64 platforms, you can only capture 32-bit applications. AutoInstall does not support 64-bit applications.

Ghost AutoInstall comprises two main components:

- AutoInstall Snapshot takes snapshots of the model computer.
  Each snapshot records the current state of all the files and registry keys on the model computer, and stores the information in an .aic file. It then uses the snapshot files to create an installation script that specifies the changes that were made to the model computer.
- AutoInstall Builder uses the installation script to build the AutoInstall executable.
  AutoInstall Builder lets you customize the AutoInstall executable by editing the installation script.

The process of creating an AutoInstall executable is outlined below.

To create an AutoInstall executable

1. Set up your model computer.

   The model computer should be a clean computer, with just the operating system and Ghost AutoInstall installed.

2. Take a pre-installation snapshot of the model computer.

   This records the current state of the model system, and is used as the baseline for building the AutoInstall executable. You can reuse this baseline snapshot if necessary. For example, after building and testing an AutoInstall executable, you may want to change the configuration settings for the installed applications.

3. On the model computer, install and configure the applications that you want to include in the package.

   You can install one or more applications, and configure them to suit your requirements. Any changes to files or settings that you make on the model computer will be included in the AutoInstall executable.

4. Take a post-installation snapshot of the model computer.

   This records the new state of the model system. AutoInstall Snapshot compares this snapshot with the pre- installation snapshot to determine the changes that were made to the model computer. It then creates an installation script (an .aic file) that defines the files and settings that were changed.

5 If you want to customize your executable, edit the installation script in AutoInstall Builder to make the appropriate changes.

You may want to do this for setting up attended installations.

6 Build the AutoInstall executable on the model computer.

AutoInstall Builder builds the AutoInstall executable by capturing all the settings and files referred to by the installation script. You can test the AutoInstall executable by running it directly from AutoInstall Builder on another computer (not the model computer on which the AutoInstall executable was built).

If you need to make changes to the AutoInstall executable, you can open it in AutoInstall Builder, edit the installation script, and then rebuild it on the model computer.

Installing Ghost AutoInstall on the model computer

Before you can create an AutoInstall executable, you must set up the model computer and then install Ghost AutoInstall on it.

The model computer should have the same operating system and service packs as those that will receive the AutoInstall executable. Ideally, this computer should have only the operating system installed and have network support to connect to the Ghost Console.

To install Ghost AutoInstall on the model computer

1 Insert the Symantec Ghost Solution Suite CD into the CD-ROM drive.

2 In the Symantec Ghost Solution Suite installation window, click **Install Tools and Utilities**.

3 Click **Install AutoInstall**.

4 In the Symantec Ghost AI Snapshot window, click **Next**.

5 Accept the terms of the license agreement, then click **Next**.

6 If you want to specify a custom location for the installed files, click **Change** and select the appropriate location.

If you want to use the default location, ignore this step.

7 Click **Next**.

8 In the Custom Setup window, click **Next**.

9 Click **Install**.

10 When the installation has completed, click **Finish**.

About setting up target computers

The AutoInstall client program is installed as part of the Symantec Ghost client software.

See "Installing the Console client" on page 51.

Once installed, the client program runs in the background on client computers, ready to launch AutoInstall deployment tasks when they are deployed from the server.

Installing Microsoft products using AutoInstall executables

There are some issues that you may need to consider when using AutoInstall executables to deploy Microsoft software to computers.

- AutoInstall executables are not suitable for deploying Microsoft service packs.
  Symantec does not recommend using Ghost AutoInstall to install Microsoft service packs.
  To install service packs, use the Transfer Files and Execute Commands tasks from the Console.
- Do not let the model computer restart before building the AutoInstall executable.
  If you are installing non-Microsoft software, you can allow restarts before performing the post-installation snapshot and building the AutoInstall executable.
- You cannot add an uninstall command to the AutoInstall executable.
  You can add an AutoInstall uninstall command to an AutoInstall executable if you are deploying non-Microsoft software. This feature does not work with Microsoft products because you must build the AutoInstall executable before any restarts.

Creating an AutoInstall executable to deploy Office XP

Due to the Product Activation feature in Microsoft Office XP, you must stop Office XP from locking to the model computer before you create the AutoInstall executable. You can use MSI commands to prevent the hardware detection and activation process from occurring until Office XP is deployed to the managed computers and launched for the first time.

Before you install Office XP on your model computer and build the AutoInstall executable, you must have the following:

- The Microsoft patch for enterprise deployments specified in the Microsoft Knowledge Base article number Q304226.
  You can find the article at:
  http://support.microsoft.com/support/kb/articles/Q304/2/26.ASP
- A Volume License Key from Microsoft. This is the product ID number that you specify when you launch the Office XP installation.

Table 20-1 describes the parameters used in the Office XP installation from the command line.

Table 20-1 Command line parameters

Parameter	Description
Setup.exe	The setup file for MSI. If MSI is already installed, the Office XP MSI file (PROPLUS.MSI) can be called instead.
ENTERPRISE_IMAGE [boolean] = 1	This parameter is set to 1 to prevent Setup.exe from creating a digital license identification based on the hardware components of the model computer. This setting lets Setup generate a unique digital license identification on each managed computer when the package is deployed.
NOUSERNAME [boolean] = 1	This parameter is set to 1 to make Office XP prompt for the user name the first time the user runs any Office XP application.
PIDKEY [string] = ["Product_ID_KEY"]	This parameter is the volume license key supplied by Microsoft. Do not include dashes when entering the Product ID number on the command line.

To create an AutoInstall executable to deploy Office XP

1. On the model computer, perform the pre-installation scan.
2. Launch Office XP installation via the following command line:

   ```
   "Office XP_path\Setup.exe" ENTERPRISE_IMAGE="1" NOUSERNAME="1"
   PIDKEY="{Product_ID_KEY}"
   ```

   See Table 20-1 on page 393.
3. When the Office XP installation has finished, apply the Microsoft patch for enterprise deployments.
4. Before allowing the model computer to restart, perform the post-installation scan and build the AutoInstall executable.

   You must not let the computer restart before performing the second scan and building the AutoInstall executable.

Creating the installation script

The installation script is a text file that lists the files and registry values to include in the AutoInstall executable, and defines how the installation is performed. The installation script is read by AutoInstall Builder when it builds the AutoInstall executable on the model computer.

You create the installation script by running AutoInstall Snapshot on the model computer, and installing and configuring the software that you want to include in the AutoInstall executable.

To create the installation script

1. Prepare the model computer.

   The model computer should be a clean computer, with just the operating system and Ghost AutoInstall installed.

   See “Preparing the model computer” on page 395.

2. If necessary, set up the custom exclusion list.

   If you want to exclude particular files or folders from the snapshot, you can specify them in the model computer registry.

   See “Setting up file and folder exclusions” on page 395.

3. Take a pre-installation snapshot of the model computer.

   You can reuse an existing snapshot if appropriate. You may want to do this if you need to modify the installed applications, install or remove components, or make other configuration changes, without having to start again from a clean computer.

   See “Taking the pre-installation snapshot” on page 396.

4. On the model computer, install and configure the applications that you want to include in the executable.

   See “Installing the software on the model computer” on page 398.

5. Take a post-installation snapshot of the model computer.

   AutoInstall Builder compares the before and after snapshots, and creates an installation script that defines the differences between them. AutoInstall Builder uses this script to build the AutoInstall executable.

   See “Taking the post-installation snapshot” on page 399.

Preparing the model computer

The model computer should be a clean computer, with just the operating system and Ghost AutoInstall installed. Any other applications or services running on the model computer may affect the changes that are made by the installation that you want to capture, and could corrupt the executable.

If you are modifying an existing AutoInstall executable, the model computer must be in the same state as it was when you created the AutoInstall executable. Any changes that have been made to the model computer after the pre-installation scan will be included in the modified AutoInstall executable.

The model computer should have the same operating system and similar hardware as the computers to which the executable is to be deployed.

To prepare the model computer

1. Disable any programs that are running in the background.

   Many computers have applications, for example an antivirus application, running in the background. These may modify files and settings during the installation process. These changes are recorded by AutoInstall Snapshot and are therefore included in the installation script.

2. If the installation process includes restarting the computer, disable any applications or services on the Startup menu that execute during the restarting process.

   When you have prepared the model computer, you can start AutoInstall Snapshot and take the pre-installation snapshot.

Setting up file and folder exclusions

You can exclude particular files and folders from the snapshot, and hence from the installation script. You specify the list of exclusions in the model computer registry.

To set up file and folder exclusions

1. On the model computer, open the Registry Editor.
2. Open the following registry value:

   HKLM/SOFTWARE/Symantec/Symantec Ghost/AutoInstall/SnapshotExclude

   If necessary, create the value as a new Multi-String Value (type REG_MULTI_SZ).

3. Edit the registry value to specify the custom exclusion list as the registry value data.

   You can specify as many files and folders as you want.

The following conditions apply:

- The path strings can specify either files or folders to exclude from the AI Snapshot scan. Folders must have a trailing backslash (\ ).
- You can use environment variables in the path string, for example %SYSTEM%. These are expanded by AI Snapshot.
- If the aitrace.log file exists, it logs the list of files and folders that are specified in this registry key. If environment variables are used, the expanded path string is logged.

Taking the pre-installation snapshot

The pre-installation snapshot is the baseline against which all system changes are monitored. Any installation and configuration changes that you make on the model computer before taking the pre-installation snapshot are not included in the package.

If you are taking a new snapshot, you can specify the disks and folders to monitor for both the pre-installation and post-installation snapshots. You need to monitor the disks and folders that are affected by the installation in order to record all the changes to files and settings on the model computer. However, the snapshot process runs faster and more efficiently if you exclude any disks and folders that are not used by the installation.

If you are reusing the existing pre-installation snapshot, the disks and folders that are monitored are specified for the existing snapshot, and you cannot change them. AutoInstall Snapshot reads the existing snapshot and then skips directly to the installation phase.

You would reuse the existing pre-installation snapshot if you want to modify the installation script by adding or removing applications or files, or making configuration changes. For example, after building and testing a package you may want to make some minor changes to the installed applications. You would reuse the existing snapshot and then make the changes to the model computer. The alternative, taking a new pre-installation snapshot, means you would have to clean everything off the model computer and start the installation process over again.

You can specify the default working directory for Ghost AutoInstall. AutoInstall Snapshot stores all snapshots, temporary working files, and scripts in subfolders under this directory. If you build an AutoInstall executable directly from AutoInstall Snapshot, the executable is also stored here.

AutoInstall Snapshot automatically purges the working directory at regular intervals, clearing everything except for the resulting AutoInstall executables.

See “Starting AutoInstall Snapshot” on page 397.

See “Setting the AutoInstall Snapshot default settings” on page 397.

Starting AutoInstall Snapshot

You can start AutoInstall Snapshot from the Start menu.

To start AutoInstall Snapshot on the model computer

1. On the model computer, on the Windows taskbar, click **Start > All Programs > Symantec Ghost > AI Snapshot**.
2. If necessary, set the AutoInstall Snapshot default settings to suit your requirements. You can specify the following:
   - The disks and directories that you want to monitor
   - The default working directory
   - Whether to create a new pre-installation scan or use the existing one.

   See “Setting the AutoInstall Snapshot default settings” on page 397.
3. Click **Next**.

   AutoInstall Snapshot displays progress as it scans the model computer. When it has finished, the Start Your Installation window appears.

   See “Installing the software on the model computer” on page 398.

Setting the AutoInstall Snapshot default settings

You can set the AutoInstall Snapshot default settings to suit your requirements. You can specify the disks and directories that you want to monitor, the default working directory, and whether to create a new pre-installation scan or use the existing one.

To set the AutoInstall Snapshot default settings

1. In the Ghost AutoInstall Snapshot window, click **Options**.
2. In the Default Settings dialog, under Search Path, specify the disks and folders that you want to monitor.
   - To add a disk or folder, click **Add**. In the Browse for Folder dialog, select the appropriate disk or folder, and then click **OK**.
   - To remove a disk or folder, select it in the list, and then click **Remove**.
3. Under Working Directory, specify the working folder for AutoInstall Snapshot.

   Click **Browse**, and then in the Browse for Folder dialog, select the appropriate folder, and then click **OK**.

4 Specify whether you want to create a new pre-installation scan or use the existing pre-installation scan, by choosing the appropriate option:

- Put a new system scan in working directory
- Reuse an existing system scan in working directory

If you reuse the existing pre-installation scan, the search path is set to whatever was used to create the scan, and you cannot change it.

5 Click **OK**.

Installing the software on the model computer

When you have taken the pre-installation snapshot of the model computer, you can install and configure the software that you want to include in the AutoInstall package. You can install the software from the network, or from a CD.

Warning: If you are installing Microsoft software, do not let the model computer restart before building the AutoInstall executable. You must cancel all restart prompts. This lets AutoInstall Snapshot perform a complete scan of the model computer.

To install the software to be packaged

1 In the Start Your Installation window, do one of the following:

- If you are installing from an autorun CD, click **Next**, then insert the CD and install the software.
- If you are installing from a local folder or network location, specify the software installation file name (usually Setup.exe). You can type the path or click **Browse** and select it from the Select Install Program dialog. To continue, click **Monitor**.

- If you are adding or removing files, or making configuration changes to installed software, click **Next**.

2 Install and configure the software that you want to include in the package.

If you are installing Microsoft software, cancel any computer restart by clicking **No** or pressing **Ctrl-Esc**. For all other software vendors, restart the computer if the installation requires it.

Some installation programs launch slowly and have long pauses between screens. Ensure the installation is complete before you continue.

3 When the software installation is complete, in the Is Software Installation Complete? window, in the Install Package Name box, type a name for the installation package.

This name is used for the installation script, and is the default name for the AutoInstall executable.

Taking the post-installation snapshot

When you have installed and configured the software that you want to include in the AutoInstall package, you can take the post-installation snapshot of the model computer.

AutoInstall Snapshot compares the post-installation snapshot with the pre-installation snapshot that you created before installation. It places references to the differences, such as new files and directories, groups and icons, and modifications to the system registry, in an installation script. The installation script (an .aic file) is stored in the Configs folder under the default working directory.

To take the post-installation snapshot of the model computer

1 In the Is Software Installation Complete? window, click **Compare**.

AutoInstall Snapshot displays progress as it scans the model computer.

2 When the comparison has finished, a message appears displaying the installation script name and location. Click **OK** to close the message pop-up.

3 In the Ready to Build window, do one of the following:

- If you want to create the AutoInstall executable from the installation script, click **Build**.
  A pop-up displays progress as AutoInstall Builder creates the AutoInstall executable.
- If you want to customize the installation script or add an uninstall command, click **Modify**.

See "Customizing AutoInstall executables" on page 400.

If you want to modify the installation script, you need to maintain the model computer in the post-installation state until after you have built the AutoInstall executable. If you make any further changes to the model computer before building the AutoInstall executable, the installation script may not function correctly, and the resulting AutoInstall executable may be corrupt.

4 When the AutoInstall executable has been built, the name and location are displayed in the Congratulations window. Click **Finish** to close AutoInstall Snapshot.

Customizing AutoInstall executables

The installation script that you created by using AutoInstall Snapshot defines the AutoInstall executable that you can deploy when you run an AutoInstall task from the Console. You can customize an AutoInstall executable by editing the script in AutoInstall Builder before you build the executable. For example, you may want to make a lengthy installation process run automatically without user interaction, or you may want to add your own graphics and splash screens to set up an attended installation.

See "Modifying the AutoInstall executable" on page 400.

See "An example of variables and commands in AutoInstall" on page 401.

See "Modifying installation scripts in AutoInstall Builder" on page 402.

Modifying the AutoInstall executable

AutoInstall Builder uses the installation script to build the AutoInstall executable. AutoInstall Builder runs on the model computer, and captures all the settings and files referred to by the installation script.

You can modify an AutoInstall executable at any time by opening it in AutoInstall Builder and editing the installation script. AutoInstall Builder automatically rebuilds the AutoInstall executable as necessary.

If you edit a script or modify an AutoInstall executable, you must maintain the model computer in the same state as the post-installation snapshot until after you have built the customized AutoInstall executable. Any changes that you make to the model computer between taking the post-installation snapshot and building the AutoInstall executable may corrupt the executable.

AutoInstall Builder will not build an AutoInstall executable if it will exceed 2 GB.

AutoInstall Builder lets you edit the installation script to integrate graphics, sound, and animation into your AutoInstall executable. You can also include messages and questions, and can edit .ini files and registry settings. You can use If statements to adapt to individual configurations or test for CPU, RAM, and video configurations. AutoInstall Builder creates a wizard interface for the AutoInstall executable that can be run on the target computer as an attended installation.

When editing an installation script, note that extra spaces and carriage returns may cause syntax errors, so should not be added. Extra lines are ignored, so you can add them for readability. For documenting the script, you can use the REM command to add remarks to any line. The text on a REM line is ignored by AutoInstall Builder even if it is a valid command.

AutoInstall Snapshot does not automatically add an uninstall function to an AutoInstall executable. If you want to include this option, you can do so by adding an Uninstall command to the installation script in AutoInstall Builder.

See “Adding an uninstall command to an installation script” on page 405.

An example of variables and commands in AutoInstall

You can customize your package for attended installations by adding commands and variables to the installation script. These let you ask for and receive user input, run commands, and customize the screens and messages that are displayed during installation.

The following example script gives the user a choice of three options, and then installs the appropriate files.

The options are:

- To install templates for administration personnel
- To install templates for customer service personnel
- To cancel the installation without installing any files

The sample script is shown below:

```
UNINSTALL: yes, packagename="Distribute Files Package"
BEGINFIRSTSCREEN title="Installing template files"
This program lets you install template files to your hard drive.
ENDFIRSTSCREEN
BEGINGROUP EXCLUSIVE, caption="Installing template files"
Select one of the following options to install the correct template files.
01 [x] Administration
Install Administrative templates
02 [ ] Customer Service
Install Customer Service templates
```

```
03 [ ] Cancel
ENDGROUP
POPMESSAGE 0, fontsize=23
Installing administration templates
EndPop
POPMESSAGE 01
Installing customer service templates
EndPop
IF GROUP = 01
FILE: "Admin.000", overwrite=ask, popid=00,
From="C:\Documents and Settings\Administrator\Admin.dot"
SHORTCUT: "$ALLUSERSDIR$", "Administration"
ENDIF
IF GROUP = 02
FILE: "CUST_S~1.000", overwrite=ask, popid=01,
From="C:\Documents and Settings\Administrator\Cust_service.dot"
SHORTCUT: "$ALLUSERSDIR$", "Customer Service"
ENDIF
IF GROUP = 01
BEGINLASTSCREEN title="Files Install", caption="Files Install"
The file has been successfully installed onto your computer.
ENDLASTSCREEN
ENDIF
IF GROUP = 02
BEGINLASTSCREEN title="Files Install", caption="Files Install"
The file has been successfully installed on your computer.
ENDLASTSCREEN
ENDIF
```

Modifying installation scripts in AutoInstall Builder

You can modify an installation script at any time. When you create a new AutoInstall executable, you have the option to modify the script before building the executable. You can also modify the installation script for an existing AutoInstall executable, by opening the executable in AutoInstall Builder and making the necessary changes to the script. AutoInstall Builder rebuilds the AutoInstall executable as necessary.

The installation script is displayed in the top right pane. The left pane lists the available commands grouped by type. When you select a line in the script or a command in the left pane, details of the command parameters are shown in the bottom right pane.

See “AutoInstall Builder command types” on page 403.

See “Opening an installation script for editing” on page 404.

See “Modifying an installation script” on page 404.

See “Adding an uninstall command to an installation script” on page 405.

AutoInstall Builder command types

Table 20-2 outlines the command types that are available in AutoInstall Builder.

Table 20-2 AutoInstall Builder command types

Command type	Description
Base Installation	Defines how the installation begins. For example, WindowsItem lets you add, remove, or replace items within a program group.
Appearance	Defines how the installation appears to the user. For example, IntroScreen lets you display a graphic when the installation begins.
Messages & Inputs	Adds messages that require user input. For example, Prompts lets you change the messages that display during the installation.
System Changes	Makes changes to Windows during the installation. For example, Registry lets you insert or delete items in the Windows registry.
If Conditions	Lets you include If statements for unattended installations. For example, IfMemory() checks for a specified memory value during the installation.
Defaults & Calls	Set up defaults and include calls to external programs. For example, RunAtExit lets you run an external program at the end of the installation.

The AutoInstall Builder command types are fully described in the AutoInstall Builder installation script reference section.

See “AutoInstall Builder commands” on page 409.

Opening an installation script for editing

You can open an installation script directly from AutoInstall Snapshot before you build the AutoInstall executable, or from AutoInstall Builder to modify an existing AutoInstall executable.

To open an installation script from AutoInstall Snapshot

- ◆ If you have just created an installation script in AutoInstall Snapshot, click **Modify**.

  AutoInstall Builder starts with the script opened for editing.

To open an installation script from AutoInstall Builder

1. Start AutoInstall Builder.
2. In AutoInstall Builder, on the File menu, click **Open**.
3. In the Open dialog, do one of the following:
   - If you want to open a script directly, select the appropriate .aic file.
     These are stored in the Configs folder under the default working directory.
   - If you want to open the script from an AutoInstall executable, select the appropriate AutoInstall executable.
     These are usually stored in the default working directory.
4. Click **Open**.

   The installation script opens in AutoInstall Builder.

Modifying an installation script

You can modify an installation script to create an AutoInstall executable that suits your requirements. For attended installations, you can add custom screens and messages, as well as graphics and sound files. For unattended installations, you can add If conditions to check client compatibility before the installation proceeds.

To modify an installation script

1 In AutoInstall Builder, in the upper right pane, edit the script to suit your requirements by adding, removing and modifying commands:

To modify a command	Select the appropriate line, change the parameters in the lower right pane, then click **Modify**.
To add a new command	Select the line above the location at which you want to add the new command. In the left pane, select the command that you want to add, set the parameters in the lower right pane, then click **Add**.
To delete a command	Select the appropriate line, then press **Delete** or right-click and click **Cut**.
To move a command	Select the appropriate line, then right-click and click **Cut**. Select the line above the location at which you want to place the command, then right-click and click **Paste**.
To comment out a command	Select the appropriate line, then right-click and click **Rem**.

The AutoInstall Builder command types are fully described in the AutoInstall Builder installation script reference section.

See “AutoInstall Builder commands” on page 409.

2 When you have finished making changes to the script, on the File menu, click **Save**.

You can now build and test the customized AutoInstall executable.

See “Building and testing AutoInstall executables” on page 406.

Adding an uninstall command to an installation script

If you want to make an AutoInstall executable removable from a computer, you need to include an uninstall command in the installation script before you build the executable.

Note: If the AutoInstall package is deploying Microsoft software, you cannot add an uninstall command. This command works only for packages that are deploying non-Microsoft software.

When an AutoInstall executable that has the uninstall feature enabled is deployed to a computer, the AutoInstall executable records all the changes that it makes during installation. These changes are stored in hidden files under the working directory. When the uninstall option is activated, the AutoInstall executable refers to these files and undoes all the changes that it has made to the managed computer.

The uninstall executable name is added to the list of programs in the Add/Remove Programs list on the Windows Control Panel. The computer user can use this facility to remove whatever was installed by the AutoInstall executable in the same way as they remove unwanted programs.

Note: Use the option to remove groups during uninstall cautiously. Some computer users might select an existing group for the installation, or add files to the group after installation.

To add an uninstall command to an installation script

1. In AutoInstall Builder, in the upper right pane, select the script line below which you want to add the uninstall command.
2. In the left pane, expand BASE INSTALLATION and then click **UnInstall**.
3. In the lower right pane, check **Remove Groups During Uninstall** to remove any program groups that were created during the installation.
4. In the Package Name box, type the name of the uninstall executable.

   This name is added to the list of programs in the Add/Remove Programs list on the Windows Control Panel. The default is the name of the AutoInstall executable.
5. Click **Add** to add the uninstall command line to the script.

Building and testing AutoInstall executables

When you have finished making changes to your installation script, you can build the AutoInstall executable on the model computer. AutoInstall Builder builds the AutoInstall executable by capturing all the settings and files referred to by the script. The AutoInstall executable is a single .exe file, with a maximum size of 2 GB.

You can test the AutoInstall executable by running it directly from AutoInstall Builder. This lets you validate the installation and make any necessary changes to the installation script.

See “Building an AutoInstall executable” on page 407.

See “Testing an AutoInstall executable” on page 408.

Building an AutoInstall executable

There are two ways that you can build an AutoInstall executable with the AutoInstall Packager:

- Directly from AutoInstall Snapshot when you create the installation script.

  You may want to do this if you do not need to view or modify the installation script. AutoInstall Builder runs in the background to build the AutoInstall executable, and places it in the AutoInstall Snapshot default working directory.
- From AutoInstall Builder after viewing or modifying the installation script.

  You would do this when you customize your installation script, or modify an existing AutoInstall executable. AutoInstall Builder places the AutoInstall executable in the directory that you specify in the Build Install dialog.

Note: The two methods may place the AutoInstall executable in different locations. The build locations for AutoInstall Snapshot and AutoInstall Builder are the same when the AutoInstall Packager is first installed on the model computer, but the two settings may be changed independently.

To build an AutoInstall executable directly from AutoInstall Snapshot

1. In AutoInstall Snapshot, after performing the post-installation scan, click **Build**.

   A pop-up displays progress as AutoInstall Builder creates the AutoInstall executable.
2. When the AutoInstall executable has been built, the name and location are displayed in the Congratulations window. Click **Finish** to close AutoInstall Snapshot.

To build an AutoInstall executable from AutoInstall Builder

1. In AutoInstall Builder, after viewing or modifying the installation script, on the Build menu, click **Build**.
2. In the Build Install dialog, specify the folder to which you want to save the AutoInstall executable file.

   The default is the working folder
3. Click **Build**.

   A pop-up displays progress as AutoInstall Builder creates the AutoInstall executable.

4 If you are rebuilding an existing AutoInstall executable after modifying the installation script, and are saving it to the same location, you are prompted to confirm that you want to overwrite the original version. Click **OK**.

5 When the build has completed, a message appears displaying the AutoInstall executable file location. Click **OK** to close the message pop-up.

Testing an AutoInstall executable

When you have generated an AutoInstall executable, you may want to verify that it is complete and does what you want. You can test an AutoInstall executable by running it from AutoInstall Builder on another computer. Do not run the AutoInstall executable on the same model computer on which it was built.

To test an AutoInstall executable

1 Set up a suitable test computer with the same operating system and similar hardware to the model computer.

2 On the test computer, install AutoInstall Builder.

3 Start AutoInstall Builder and open the AutoInstall executable.

4 In AutoInstall Builder, on the Build menu, click **Run**.

5 As the AutoInstall executable runs, you can verify that it does what you expect. When the installation has finished, you can check that the software is installed and configured correctly.

Chapter 21

AutoInstall Builder installation script reference

This chapter includes the following topics:

- AutoInstall Builder commands

AutoInstall Builder commands

You can customize your AutoInstall packages by adding and modifying the AutoInstall Builder commands in the installation script (the .aic file). For attended installations, you can add custom screens and messages, as well as graphics and sound files. For unattended installations, you can add IF conditions to check the managed computer compatibility before the installation proceeds.

You can modify an AutoInstall Builder installation script via the AutoInstall Builder.

See "Customizing AutoInstall executables" on page 400.

The available commands are listed in the left pane of the AutoInstall Builder window, and are grouped by type. For more information, see the following sections:

Base Installation commands

Appearance commands

Messages and Inputs commands

System Changes commands

Defaults and Calls commands

IF conditions

Some of the commands support using variables.

See "Using variables in commands" on page 438.

Base Installation commands

The base installation commands include the following:

- Title
- FirstScreen
- Directory
- File
- WindowsItem
- LastScreen
- UnInstall

Title

Sets up a title that appears at the top left of the screen when the user receives an installation. You can specify a title or subtitle in each command. You can also customize the text size, color, and font to suit your requirements.

FirstScreen

Sets up a message that appears at the beginning of the installation, providing additional installation information to the user.

You can specify the following:

- Screen title and caption wording.
- Message text. Use carriage returns for line breaks. AutoInstall Builder sizes the width of the message box automatically.
- A bitmap to appear on the left side of the message box. The bitmap should be 125 pixels wide and 275 pixels high. It can have up to 256 colors.

FirstScreen can be used many times.

Directory

Specifies the installation path options. The Directory options include:

- Installing the program in the default directory, as well as an alternate directory. To create a subdirectory in the default directory, use the File command. To create a subdirectory relative to the default directory, use the $DEFAULTDIR$ variable.

- Prompting the user to type an installation path, suggest a path, or prevent the user from changing the installation drive or directory.
- Specifying the minimum disk space required for the installation. The user will be prompted if their system has less than the minimum disk space.
- Displaying additional messages or bitmaps to the user.

File

Select the files to include in the AutoInstall package, and specify the directories into which the files are copied on the managed computer.

Each file or directory of files in the installation set needs a File command associated with it. You can create an individual File command for each file, or use wildcards to combine File commands. The order of the File commands determines the order in which files are copied.

The File options include:

- Including individual files or directories of files.
- Specifying where the installation files are located on the distribution source media. If no value is specified, files are installed from where the installation program was executed. The source function is commonly used to install from a CD-ROM or network drive, or to backup files on the user's system.
- Specifying where to install files. This is not the same as the default directory. The most common use for the Destination box is to create a subdirectory in the default directory.
  To install files in the Windows directory or other special directory, enter a variable in the Destination box, such as $WINDIR$, $WINSYSDIR$, $WINTEMPDIR$, $PROGFILESDIR$, $DIRn$, $SOURCEDIR$, $LOCATEDIR$, or $ASKn$. Alternatively, click System Variable to display a list of variable names and select the one that you want.
  You can also specify a directory path in the Destination box. For example, c:\ installs the files to the root directory on the C drive. Use \ to install the files on the root of the default directory. Use .. to install files to the directory above the default directory. Only use a path you are sure already exists on the user's system.
- Specifying whether or not to overwrite a file if it already exists on the user's system. The options are:
  - Yes to overwrite existing files.
  - No to leave existing files intact.
  - Ask to prompt the user whether to overwrite existing files.

  - New to overwrite only if the existing file is older (based on time/date stamp) than the file in the installation set.

    If the file is a .vbs, .dll, .exe, or .ocx file, the age is based on the internal version number instead of the time/date stamp.

- Selecting the file's DOS attribute after installation: read only, archive, hidden, or system. If you do not select an attribute, the default is to Normal, which allows read/write access.
- Installing a file only if the user selects certain parameters, such as the Group ID.
- Displaying a pop-up message as files are copied. This message remains on the screen until the next file with a Pop ID is specified or until the end of file copying.
- Displaying a bitmap on the left, middle side of the background screen. You can also specify an audio file.

The advanced settings are set in the following checkboxes:

No shrink
Removes the file compression. This is common when the installation files are on a CD-ROM and you want the files to be accessible to the user without using the installation program.

No bind
Prevents combining the specified file with the .exe file, leaving them as independent files that are accessible outside the installation program. If unchecked, the installation program combines all files into a single file and binds it to the installation executable.

No uninstall
Leaves the specified file on the user's system when the user runs the uninstall program.

Shared
Adds a ShareDLL specification to the file. On installation it registers this file as a shared dll in the registry key, HKLM\Software\Microsoft\Windows\CurrentVersion\Shared DLLs. Uninstalling this package deregisters this file.

Temp
Specifies that the file is copied to the Windows temp directory for use during installation. It is removed after installation.

Self-register
Registers the file in the Windows registry during the installation. The file must be an autoregistering file, such as a .dll, .ocx, or .vbx file. If the file does not autoregister, use the Registry command to manually specify the registration parameters.

Font
Installs the file to the font directory and registers it in Windows. This automatically sets up the new font.

WindowsItem

Add a shortcut to the user's desktop by selecting the Windows program group and associated icon.

You can specify the following parameters:

- The Windows program group.
- Whether you are adding, removing or replacing items within the program group. If you add an item that already exists, the Add command keeps the original item, as well as the new item. If you replace an item, only the new one exists. The remove command isn't generally used for installations. You can create a separate configuration file that removes a program group or program group icon. You must specify both the program group and item to remove an item.
- The command-line that executes the program when the user clicks the program icon on the desktop, and the associated working directory.
- The icon for the shortcut, either by file name or index number. If the icon is embedded in a program file, and there are multiple icons in the file, the index number specifies the icon that appears. For example, 1 means the first icon embedded in the program file.

LastScreen

Sets up a message that appears at the end of the installation, providing additional installation information to the user.

You can specify the following:

- Screen title and caption wording.
- Message text. Use carriage returns for line breaks. AutoInstall Builder sizes the width of the message box automatically.
- A bitmap to appear on the left side of the message box. The bitmap should be 125 pixels wide and 275 pixels high. It can have up to 256 colors.

UnInstall

Specify whether an uninstall program is created for the user. You can optionally delete any program groups that were created during the installation. Use this option cautiously as some users might select an existing group for the installation or add files to the group after installation.

Each AutoInstall package has a post-remove script that will uninstall the package from the managed computer if the uninstall feature is enabled. The post-remove script calls the same AutoInstall executable and adds the switch /All to the command line.

When an AutoInstall package that has the uninstall feature enabled is deployed to a managed computer, the AutoInstall executable records all the changes that it makes during installation. These changes are stored in hidden files under the working directory. When the package is uninstalled, the AutoInstall executable refers to these files and undoes all the changes that it has made to the managed computer.

The uninstall package name is added to the list of programs in the Add/Remove Programs list on the Windows Control Panel. The managed computer user can use this facility to uninstall the package in the same way as they remove unwanted programs.

Appearance commands

The appearance commands include the following:

- Animation
- IntroScreen
- IntroSound
- ScreenColor
- ScreenGraphic

Animation

Display still or animated pictures during the file copy or search process. The files appear sequentially so that they produce an animated effect.

The bitmaps should be 55 pixels wide by 55 pixels high. They can have up to 256 colors.

IntroScreen

Display a graphic as the installation begins.

You can specify the following parameters:

- The bitmap that is displayed.
- Whether or not to enlarge the graphic to cover the full screen.
- The length of time that the bitmap appears on-screen. The user can clear the bitmap by touching a key.

IntroSound

Specify a sound file to play as installation begins.

ScreenColor

Select the background color for the installation screen. You can select a color for the entire screen, or choose a top and bottom color for a gradient effect.

ScreenGraphic

Display a graphic during installation. You can set the bitmap that appears and its location on the screen. The ScreenGraphic command is generally used to display company logos.

AutoInstall Builder automatically makes the bitmap background transparent. It does this by checking the top-left pixel to determine the background color, and makes that color transparent. If you do not want to use a transparent bitmap, change the upper-left pixel to a color that is not used anywhere else in the bitmap.

Messages and Inputs commands

The messages and inputs commands include the following:

- Ask
- Group
- InsertDisk
- PopMessage
- Prompts
- SetVariable
- ShowReadme

Ask

Prompt the user for input and store it in the $ASKn$ variable. The user can type information or answer a Yes/No question. You can have up to nine $ASKn$ variables in your installation script, numbered from 1 to 9.

You can specify the following parameters:

- Ask ID: the value of n in the $Askn$ variable name.
  For example, if you select 3, the variable is $Ask3$. Once you collect input from the user, you can use the $ASKn$ variable with the WinItem, IniFile, AddText, Config., Autoexec, RunAtExit, File, and other commands.

- Caption: the title that appears on the top border of the dialog box.
- Prompt: the message that the user sees. Use the Text box to type a more detailed description of the question.
- User Entry and Yes/No Buttons: specify whether the user enters information or answers a Yes/No question.
- A suggested value for user entry. This information appears in the entry box on the dialog box.
- Yes Prompt and No Prompt: specify the words that appear on the Yes and No button. Yes and No are the defaults, but you can use Agree and Disagree or a combination you choose.
- Text File Name: a text file name to display a message during installation. This is useful for displaying a copyright file or license agreement.
- A bitmap to appear on the left side of the message box. The bitmap should be 125 pixels wide by 275 pixels high. It can have up to 256 colors.

Group

Provide the user with installation options, such as which files are copied during installation. This command defines the file groups and creates a dialog box detailing the user's choices. It is generally used to provide different installation options, such as adding the program documentation to the complete installation, instead of including only the program files for a light installation.

You can specify the following parameters:

- Caption: The dialog box title.
- Prompt: The message that instructs the user to select one or more items in the dialog box.
- Selecting whether the options use check boxes or radio buttons. Check boxes let the user select one or more items. They are displayed in a scrollable list. Radio buttons let the user select only one item. You can create up to 24 check boxes and radio buttons, but only the first eight buttons appear in the dialog box. If you have a lot of options, you can divide them into subgroups of the original group.
- Selecting a bitmap to display on the left side of the message box. The bitmap should be 125 pixels wide and 275 pixels high. It can have up to 256 colors.
- Entering the name of the selectable item in the Item name box and assign it an identification number. This number is used by the File command to determine which files are installed. It can also be used in an IF statement. You

can also set the item to be selected by default. The user can select it or deselect it during installation.

- Text: A more detailed description of the item.
- Item name, Selected, and Text: Repeated so that you can enter multiple items at once.

InsertDisk

Prompts the user to insert a specified disk. You need to supply the disk number and label. This is used to prompt the user, and to verify that the correct disk has been inserted.

PopMessage

Displays a message to the user when the installation is copying files. Each message is linked to a particular File command, and appears when that command is being executed.

You can specify the following parameters:

- The Pop ID of the File command to which the message relates.
- The message text.
- The size and font of the message text.

Prompts

You can modify the messages and prompts that may be used in the installation. These are displayed when appropriate. Select the prompts that you want to use and edit the text as appropriate.

AutoexecPrompt	Asks the user for permission to change the Autoexec.bat file.
BackPrompt	Defines the word that appears on the Back button. The underline character, when pressed in conjunction with the Alt key, creates a shortcut to the button.
BadDrivePrompt	Appears when the user specifies a drive that is not available. The prompt for drive name is based on the DefaultDir, Dir2, and Dir3 commands.
BrowseButtonPrompt	Defines the word that appears on the Browse button.
BrowseCaptionPrompt	Defines what appears in the title bar of the Browse dialog box.

BrowseDrivePrompt and BrowseDirPrompt	Defines the drive and directory that appear by default in the Browse dialog box.
CancelPrompt	Defines the word that appears on the Cancel button.
ConfigPrompt	Appears when the Config. command is used. It asks the user for permission to change the Config.sys file.
CopyFilePrompt	Defines the message that appears while files are being copied to the managed computer.
CopyTitlePrompt	Defines the title that appears while files are being copied to the managed computer.
DetailPrompt	Defines the word that appears on the Detail button.
FileExistPrompt	Appears when the overwrite=ask parameter is used with the File command.
FileNotFoundPrompt	Appears when a file name specified in the installation script is not found on the installation disk. This usually occurs when the user inserts the wrong disk in the drive.
FinishPrompt	Defines the word that appears on the Finish button.
IniFilePrompt	Appears when the INIFILE command asks the user for permission to modify an .ini file.
InsertDiskCaption	The caption that appears when the user is prompted for a disk.
InsertDiskPrompt	Appears when the user is prompted to insert the next disk.
InstallToPrompt	Appears when the user is prompted to specify the installation location.
LocatePrompt	Appears when AutoInstall Builder is scanning for files on the user's system. It is associated with the Locate command.
NextPrompt	Defines the word that appears on the Next button.
NoAll Prompt	Defaults all answers to No.
NoGroupPrompt	Appears when the BeginGroup command is used and the user has not selected at least one program group.
NoPrompt	Defines the word that appears on the No button.
NoSpacePrompt	Appears when there is not enough disk space on the user's system. It is used in conjunction with the MinDiskSpace command.
OKPrompt	Defines the word that appears on the OK button.

QuitPrompt	Appears when the user clicks Cancel during an installation.
RebootPrompt	Appears when the Reboot command is used. It asks the user for permission to restart the system.
RecoverPrompt	Message that is displayed when an AutoInstall package fails to deploy. The message is shown on a message-box with Yes/No buttons. Clicking Yes continues package deployment from the point of failure, clicking No starts package deployment from the beginning.
ReplaceFileCaption	Message that is presented to the user to request confirmation of file replacement.
ReplaceLockFilePrompt	Appears when the user's computer needs to be restarted in order to replace files that are open and locked by the system.
UninstallBeginPrompt	Appears when the user runs the uninstall program.
UninstallEndPrompt	Appears when the uninstall program finishes.
UninstallTitlePrompt	Defines the title that appears at the top of the uninstall screen.
WarningCaption	Defines the caption for warning messages.
YesAllPrompt	Defaults all answers to Yes.
YesPrompt	Defines the word that appears on the Yes button.

SetVariable

Create a custom variable name and assign a string value to it. If the value contains all numbers, it is tested as a number instead of a string. The value can be a constant, a system value, or from previous user input. The value is not case sensitive.

This command is commonly used for easier readability, or to give a label to a constant.

ShowReadme

Display a text “Readme" file at the conclusion of the installation process. You need to specify the name of the text file.

System Changes commands

The system changes commands include the following:

- AddText

- Autoexec
- Backup
- Config
- Copy
- Delete
- IniFile
- Reboot
- Registry
- Regserver
- Rename
- Shortcut
- NTService
- WinGroup

AddText

Create or edit a text file to include in the installation.

You can specify the following parameters:

Name	The name of the text file. If the file exists, it is modified. If the file does not exist, it is created.
Text	The text to add to the file.

Position

The position at which to add the specified text. The position can be defined by a line number or text string.

If you enter a positive number, the text is placed the specified number of lines from the top of the text file. Negative entries count up from the bottom of the text file. The text is inserted in the file unless you click Replace.

If you enter a string, the installation program finds the string in the text file and inserts the specified text below the string or replaces it. You can use a wildcard as the last character.

For example,

FILES=*

Installation searches for a text line that starts with the string to the left of the asterisk and either adds a line after it or replaces it, depending on the options you select.

Autoexec

Modify the user's Autoexe.bat file. You can use this command multiple times in the same package.

Your options include:

- Adding the default installation path to the user's Autoexec.bat file.
- Adding an additional path to the user's Autoexec.bat file.
- Adding a line to the end of the user's Autoexec.bat file.
- Adding a SHARE command to the file.
  The /F parameter is the minimum part of the SHARE command. This allocates the specified bytes of memory to hold file sharing information. The /L parameter specifies the minimum number of simultaneous file-region locks.
  Refer to your operating system documentation for more information.
- Displaying a dialog box to ask the user for permission to make the specified changes.

Backup

Create a backup subdirectory under the default installation directory, $DEFAULTDIR$, and backup any file that will be overwritten during installation. All overwritten files are copied to the backup directory whether or not they were in the same directory originally.

Config

Specify changes to the user's Config.sys file. It is sometimes used to add a device driver that is required by the newly installed software. If AutoInstall Builder makes a change to the user's Config.sys file, it creates a backup of the original named Config.bak. This command can be used multiple times in the installation script.

Your options include:

- Setting the minimum value for the Buffers command in the user's Config.sys file.
- Setting the minimum files value for the Files command in the user's Config.sys file.
- Adding a line to the user's Config.sys file.
- Displaying a dialog box to ask the user for permission to make the specified changes.

Copy

Copy a file from one location to another. This command is often used to make copies of files from one directory on the user's system to another directory.

You can specify the following parameters:

- The name and path of the file to be copied.
- The destination name and path.
  If the destination file already exists, it is overwritten if it is older than the source file.

Delete

Lets you delete a file during the installation. The file can be on the managed computer or a part of the installation set.

IniFile

Create or modify an .ini file on the managed computer.

You can specify the following parameters:

File Name	The name of the .ini file that you want to create or modify.
Section	The section of the file in which the new line will be placed. If the section doesn't already exist, AutoInstall Builder creates it.

Entry

The ini file parameter.

String

The value of the ini parameter.

For example, if the line is HOSTDIR=c:\temp, then HOSTDIR is the Entry parameter and c:\temp is the String parameter.

Add

Check this to add a line to the .ini file even if a line with the same entry value exists in the section. If Add is unchecked, AutoInstall Builder replaces a line with the same entry value with the new line.

Ask

Prompt the user for permission to modify the .ini file.

Reboot

Restart the user's system after the installation. Your options are:

System

Restart the operating system.

In Windows 2000/XP, this is equivalent to restarting Windows.

Windows

Restart Windows.

In Windows 2000/XP, this is equivalent to stopping all programs and logging off of Windows.

Registry

Insert, delete, or modify items in the Windows registry. There can be multiple Registry commands in a single installation script.

Options include entering the name of the registry key that you want to insert, delete, or modify. Then, entering the action you want to perform:

Delete

Removes the key from the registry.

New

Adds a key to the registry.

Query

Specifies where in the structure the key and associated values should be stored.

To create a new key or modify the existing key organization, use the new or delete commands.

To add information to the registry, use the New and Query functions. Use the Key command followed by one or more Value statements. Single Key commands and all Value statements begin with BeginRegistry command and end with EndRegistry.

Regserver

Register a self-registering component, for example, an .ocx or .dll file.

Rename

Rename a file on the user's system or on the installation disks. You specify the existing file name and associated path, and the new file name and path.

Shortcut

Create a shortcut on the user's system.

You can specify the following parameters:

- The command-line executable the shortcut invokes, any additional command-line parameters, and the working directory for the command-line arguments.
- The shortcut name that appears to the user.
- Whether the shortcut is visible by all users or just the user currently logged on to the Windows operating system.
- An icon for the shortcut, which you can specify either by file name or index number.
  If the icon is embedded in a program file, and there are multiple icons in the file, the index number specifies the icon that appears. For example, 1 means the first icon embedded in the program file.
- The size of the window in which the specified executable runs.

NTService

Start or stop a service on a Windows NT system.

You can specify the following parameters:

Service name	The name of the service
Start service	Check this to start the service. Leave it unchecked to stop the service. If you stop a service, it stops at the beginning of the installation, before any files are installed. If you start a service, it occurs after all of the file commands are executed, so that the service file is in the correct location to be executed.

WinGroup

Let the user choose an existing program group or create a new one. The WinGroup command appears the current Windows program groups so that the user can select from the list or create a new one.

You can specify the following parameters:

- The default program group name.
- The prompt, caption, and text of the message that prompts the user for a Windows group name.

Defaults and Calls commands

The defaults and calls commands include the following:

- BlankLine
- FontName
- OverWriteFile
- ProgressBar
- Rem
- RunAtStart
- RunAtMiddle
- RunAtExit

BlankLine

Insert a blank line in the installation script. You would do this for formatting and readability only, and has no effect on the execution of the file.

FontName

Specify the font to use as the default font in dialog boxes. This is used when no font has been specified for the individual dialog boxes.

OverWriteFile

Defines what happens when a file in the installation set already exists on the user's system. This is the default setting, and is used when no entry was made in the File command.

The options are:

No	Leaves existing files intact.
Ask	Asks the user whether to overwrite existing files.
New	Overwrites if the existing file is older (based on time/date stamp) than the file in the installation set. If the file is a .vbs, .dll, .exe, or .ocx file, the age is based on the internal version number instead of the time/date stamp.
Yes	Overwrites files.

ProgressBar

You specify the total file size so that the progress bar moves smoothly. If you let AutoInstall Builder collect files, compress them, and build the installation, AutoInstall Builder automatically calculates this value.

You only need this command if you build AutoInstall executables manually.

Rem

Add a remark to the installation script. The script compiler ignores remark lines.

RunAtStart

Run an external program at the beginning of the installation.

You can specify the following parameters:

- The command line to start the executable. The executable may be an .exe, .com, .bat, .pif, or .dll file.
- For executable files, any necessary command-line parameters.
- For DLLs, the function that is run from the .dll library, and an optional input variable that is necessary to run the .dll.
  The $DLLRETURN$ variable uses an integer, unless you add str after the variable. For example, 128, str is an acceptable variable name.
  You can also specify whether the .dll returns a value. The default return type is an integer. If your .dll returns a string, check the Function Returns a String option. The string is saved in the $DLLReturnStr$ variable.

RunAtMiddle

Run an external program during the installation.

You can specify the following parameters:

- The command line to start the executable. The executable may be an .exe, .com, .bat, .pif, or .dll file.
- For executable files, any necessary command-line parameters.
- For DLLs, the function that is run from the .dll library, and an optional input variable that is necessary to run the .dll.
  The $DLLRETURN$ variable uses an integer, unless you add str after the variable. For example, 128, str is an acceptable variable name.
  You can also specify whether the .dll returns a value. The default return type is an integer. If your .dll returns a string, check the Function Returns a String option. The string is saved in the $DLLReturnStr$ variable.

RunAtExit

Run an external program at the end of the installation.

You can specify the following parameters:

- The command line to start the executable. The executable may be an .exe, .com, .bat, .pif, or .dll file.
- For executable files, any necessary command-line parameters.
- For DLLs, the function that is run from the .dll library, and an optional input variable that is necessary to run the .dll.
  The $DLLRETURN$ variable uses an integer, unless you add str after the variable. For example, 128, str is an acceptable variable name.
  You can also specify whether the .dll returns a value. The default return type is an integer. If your .dll returns a string, check the Function Returns a String option. The string is saved in the $DLLReturnStr$ variable.
- Whether or not to wait before starting the executable.

IF conditions

You can add conditional sections to your installation script by defining the IF statement that controls the conditional section. When you add an IF statement to your script, the Else and Endif lines are added automatically. You can then edit the script to add the appropriate statements to the conditional section.

You use the following operators in conditional statements: =, <, >, <=, >=, <>. Most conditional statements let you compare two values with these operators. Some conditional statements also let you compare a value with a range of values. If the conditional statement is true, the conditional section is executed.

You can include the following IF statements in an installation script:

- IF $ASKn$

- IF $SYSn$
- IF $variable$
- IF CPU()
- IF DiskSpace()
- IF DOSVer()
- IF FileVer()
- IF CDROM()
- IF Group
- IF IsFile()
- IF Locate()
- IF Memory()
- IF Search()
- IF SoundCard()
- IF Video()
- IF WinVer()

You can also add the following commands to your conditional sections:

- Else
- EndIf
- ExitMessage

IF $ASKn$

$ASKn$ values are assigned by collecting user input in response to an Ask command. There are nine variables, $ASK1$ through $ASK9$.

IF $ASKn$ compares the variable value with the value that you specify in the conditional statement. The values stored in the $ASKn$ variables are strings and are compared alphabetically. For example, 99 is considered larger than 100 because the first character 9 is larger than the first character 1.

In the following example, the user is prompted to enter a serial number and the response is stored in the variable $ASK3$. The IF statement compares the user's value to 1B456Q9. If it isn't the same, the exit message appears and the installation ends.

```
ASK3: "", prompt="Enter your serial number:"
```

```
IF $ASK3$ <> "1B456Q9"

EXITMESSAGE

Invalid serial number - installation terminated

EXIT

ENDIF
```

See “ExitMessage” on page 438.

IF $SYSn$

$SYSTEM$, $SYS2$, and $SYS3$ values are assigned by collecting input that the user enters on the command line during the package deployment. You need to type a dash (-) in front of the value to assign it to a variable.

For example:

If the user enters install -update, the $System$ variable value is set to update.

If the user enters setup -d:\network -c:\local -update, the $System$ variable value is set to d:\network, $Sys2$ is set to c:\local, and $Sys3$ is set to update.

IF $SYSn$ compares the value of a particular variable with the value that you specify in the conditional statement.

This example expects the user to enter a password on the command line, such as open_sesame, and checks the entry. If it does not match, package deployment is aborted.

```
IF $SYSTEM$ <> open_sesame

EXITMESSAGE

Incorrect password - installation terminated.

EXIT

ENDIF
```

IF $variable$

The $variable$ gets its input from the SetVariable command.

IF $variable$ compares the $variable$ value with the value (a constant or system variable) that you specify in the conditional statement.

A text value corresponding to the day of the week had been set earlier in the script with the SetVariable command, as shown. If the day of the week is correct, a short message appears. Otherwise, installation is aborted.

```
ASK1: "", prompt="What day of the week is today?"

SET $day_of_week$ = "$ASK1$"

IF $day_of_week$ = "Tuesday"

BEGINFIRSTSCREEN

Today is Tuesday. Your installation may proceed.

ENDFIRSTSCREEN

ELSE

EXITMESSAGE

Today is not Tuesday. This installation should be run only on a Tuesday.

EXIT

ENDIF
```

A numeric value can also be checked. If the text value contains all digits, it is assumed to be a number.

Thus

```
SET $A$ = "6"

IF $A$ < "1234"
```

is true, because the number 6 is less than the number 1234, but

```
SET $A$ = "6a"

IF $A$ < "1234"
```

is false, because 6 alphabetizes higher than 1.

IF CPU()

CPU() returns the CPU value of the managed computer.

IF CPU() compares the detected CPU value with the value specified in the conditional statement.

IF DiskSpace()

DiskSpace( ) returns the free space on each available drive.

IF DiskSpace( ) compares the detected disk space value for a specified disk with the value specified in the conditional statement.

Note: AutoInstall Builder automatically detects available disk space for installing files, so you do not usually need to use the IF DiskSpace( ) command in your scripts. You can also specify the required space in the DefaultDir/Dirn command.

IF DOSVer()

DOSVer() returns the version number of the DOS operating system.

IF DOSVer() compares the detected version number with the value or range specified in the conditional statement.

The following example checks for DOS 5.0 or greater on the managed computer:

```
IF DOSVer() >= 5

ELSE

EXITMESSAGE

Not compatible with your DOS version - install ended.

EXIT

ENDIF
```

The following example checks for at least DOS version 3.1 but less than version 5.0 on the managed computer:

```
IF DOSVer() = range(3.1,4.9)

ELSE

EXITMESSAGE

Not compatible with your DOS version - install ended.

EXIT

ENDIF
```

IF FileVer()

FileVer() returns the time stamp (date) and internal version number of a specified file on the managed computer.

IF FileVer() compares the time stamp or version number (whichever you specify) with the value specified in the conditional statement.

This command is generally used to determine whether certain files need be installed, or to determine the version of an application that is currently installed on the managed computer.

IF CDROM()

CDROM() returns true when the managed computer has a CD-ROM drive.

IF CDROM() evaluates the value of CDROM(). The conditional statement requires no further values or operators.

IF Group

Group is the value of the file group that the user has selected for installation on the managed computer.

See "Group" on page 416.

IF Group compares the value of the file group with the values specified in the conditional statement. You can specify one or more values in a string list, with each value separated by a comma. Valid values for groups are integers between 0 and 99.

In the example below, if the user selects group 10 or 20 (as defined by the Group command), the appropriate program group and program item is installed on the managed computer:

```
IF GROUP = 10, 20

WINITEM: "Zip Finder", "$defaultdir$\zip.exe", "ZIPman"

ENDIF
```

If the user selects multiple groups, all group values are compared in the conditional statement. Any match satisfies the conditional statement.

IF IsFile()

IsFile() returns true if a specified file is found in a specified directory on the managed computer.

IF IsFile() evaluates the value of IsFile(). You need to specify the file name and directory path. You can use variables to specify the path (for example, $WINDIR$, $SYSTEM$, $SOURCEDIR$, $LOCATEDIR$, and so on).

In the following example, an existing file, Myprog.ini, is renamed to Myprog.inx, if it exists in the Windows directory on the managed computer.

```
IF ISFILE("$WINDIR$\myprog.ini")

RENAME: "$windir$\myprog.ini" "$windir$\myprog.inx"

ENDIF
```

IF Locate()

Locate() returns true if a specified file is found on the managed computer.

IF Locate() evaluates the value of Locate(). You need to specify the file name, and may include a directory path. If you specify a path, you can use variables (for example, $WINDIR$, $SYSTEM$, $SOURCEDIR$, $LOCATEDIR$, and so on). You can also choose to search all drives, or just the local or network drives on the managed computer.

Note: CD-ROM drives are treated as local or network drives and are searched, which may be a slow process.

The following example searches the C drive on the user's system for the file zipcode.exe:

```
IF LOCATE("zipcode.exe", c)

DEFAULTDIR: "$LOCATEDIR$"

ELSE

DEFAULTDIR: "c:\zipcode"

ENDIF
```

If the file is found, the suggested installation directory is set to the directory that contains zipcode.exe. If the file isn't found, the suggested installation directory is set to C:\zipcode.

IF Memory()

Memory() returns the total memory of the managed computer.

IF Memory() compares the detected value with the value specified in the conditional statement.

The following example checks whether the managed computer has at least 2 MB of RAM.

```
IF MEMORY() < 2000K

EXITMESSAGE

Not enough memory.

ENDIF
```

If the computer has less than this amount, a message is displayed and the package deployment stops.

IF Search()

Search() searches a text file for the occurrence of a specific text string. You can refine the search by choosing to ignore all lines that start with a specific string, and you can specify strings that must be found before or after the search string.

If the search is successful, this function returns true and assigns the variable $SEARCH$ with the numeric value of the line number in which the string was found. It also assigns values to $LEFT$ and $RIGHT$ variables. These two variables contain the text that appears to the left and the right of the search string on the same line.

IF Search() evaluates the value of Search(). This function is commonly used in conjunction with the AddText command to edit a line in an existing text file.

The example below searches for the string zipcode.exe in the text file C:\Autoexec.bat. If the string is found, the parameter -USA is inserted into the line immediately after zipcode.exe. Any other text in that line, either in front of or following zipcode.exe is maintained.

```
IF Search("zipcode.exe","c:\Autoexec.bat")

ADDTEXT: "$LEFT$zipcode.exe -USA$RIGHT$", "c:\Autoexec.bat",

"$SEARCH$", replace

ENDIF
```

This example prompts the user for a name and assigns the value to $ASK1$. The Search function searches for the string Sir in the file Readme.txt that is on the source drive. The line number in which Sir appears in this text file is assigned to the variable $SEARCH$. The AddText command locates that line and replaces it with the user's name (as stored in $ASK1$). It restores the text before and after Sir by using the variables $LEFT$ and $RIGHT$.

```
ASK1: "your name", prompt="Please enter your name:"

IF Search("Sir","$sourcedir$\readme.txt")

ADDTEXT: "$LEFT$$ASK1$$RIGHT$", "$defaultdir$\readme.txt",

"$SEARCH$", replace

ENDIF
```

This example replaces a line in a specific section in an .ini file. The function searches in the section labeled Network for the string Drive= and substitutes the string Drive1=.

```
IF SEARCH("Drive=","$windir$\pcloan.ini", ";", begin="[Network]",

 end="[end]")

ADDTEXT: "$LEFT$Drive1=$RIGHT$", "$windir$\pcloan.ini",

"$SEARCH$", replace

ENDIF
```

Note that this example skips any line starting with a semicolon (;).

IF SoundCard()

SoundCard() returns true when the managed computer has a soundcard on one of its serial ports.

IF SoundCard() evaluates the value of SoundCard(). The conditional statement requires no further values or operators.

In the following example, if a soundcard is detected, the file sound.drv is installed. Otherwise, the file nosound.drv is installed.

```
IF SOUNDCARD()

FILE: "sound.000", FROM="c:\sound\sound.drv"

ELSE

FILE: "nosound.000", FROM="c:\sound\nosound.drv"

ENDIF
```

IF Video()

Video() returns three values describing the video display capability of the managed computer: number of colors supported, horizontal resolution, and vertical resolution.

IF Video() compares the detected values with the values that you specify in the conditional statement. You can compare either the number of colors or the resolution, or both as an And/Or condition. If you compare both values in the same conditional statement, the same operator (greater than or less than) is used.

The following example installs a file based on the video capability of the managed computer. If it is greater than 640 horizontal resolution by 480 vertical resolution, and 3 colors, then color.drv is installed. Otherwise, bw.drv is installed.

```
IF VIDEO() > 3,640,480

FILE: "color.000", FROM="c:\video\color.drv"

ELSE

FILE: "bw.000", FROM="c:\video\bw.drv"

ENDIF
```

The following example checks only the number of colors, and then installs the appropriate file.

```
IF VIDEO() > 3

FILE: "color.000", FROM="c:\video\color.drv"

ELSE

FILE: "bw.000", FROM="c:\video\bw.drv"

ENDIF
```

The following example checks only the resolution, and then installs the appropriate file.

```
IF VIDEO() > 640,480

FILE: "color.000", FROM="c:\video\color.drv"

ELSE

FILE: "bw.000", FROM="c:\video\bw.drv"

ENDIF
```

IF WinVer()

WinVer() returns the version number of the Windows operating system.

IF WinVer() compares the detected version number with the value or range specified in the conditional statement.

The value of a Windows version is the value defined by Microsoft:

3.1	Windows 3.1
3.11	Windows for Workgroups
3.5	Windows NT 3.5
3.51	Windows NT 3.51
3.95	Windows 95
4.0	Windows NT 4.0
4.1	Windows 98
4.9	Windows Me
5.0	Windows 2000
5.1	Windows XP
6.0	Windows Vista

The following example checks whether the managed computer has Windows 98 or later installed.

```
IF WINVER() >= 4.1

ELSE

EXITMESSAGE

Not compatible with your Windows version - install ended.

EXIT

ENDIF
```

The following example checks that the managed computer has at least Windows 98 but less than Windows XP.

```
IF WINVER() = range(4.1,5.0)

ELSE
```

```
EXITMESSAGE

Not compatible with your Windows version - install ended.

EXIT

ENDIF
```

Else

Create an Else condition within the script section under the IF statement.

EndIf

The EndIf statement is required to end an IF condition.

ExitMessage

ExitMessage is used to exit the installation script (which terminates package deployment) within an IF statement.

You can specify the message title and text to display to the user of the managed computer when the package deployment is being cancelled. You can use carriage returns for line breaks. The message box width is resized automatically.

The following example checks for a previously installed copy of zipcode.exe. If the file is not found, a message is displayed and the package deployment halts immediately:

```
IF LOCATE("zipcode.exe")

DEFAULTDIR: "$LOCATEDIR$"

ELSE

EXITMESSAGE

A previous version of the software was not found.

You may not install this upgrade.

EXIT

ENDIF
```

Using variables in commands

Many AutoInstall Builder commands support using variables. Variables are assigned values based on the user's unique system or input. For example, the

$WINSYSDIR$ variable can be used as part of the directory path in several commands. This variable is assigned the value of the Windows system directory. When used with the File command, it lets you install files into the Windows system directory, even when the location of this directory may be different for each managed computer.

You can use the following variables in commands:

- $ALLUSERSDIR$
- $ASKn$
- $CURUSERDIR$
- $DEFAULTDIR$
- $DEFAULTDRIVE$
- $DIRn$
- $DLLRETURN$ and $DLLRETURNSTR$
- $LOCATEDIR$
- $LOCATEDRIVE$
- $MACHINENAME$
- $MODEMCOM$
- $PROGFILESDIR$
- $SEARCH$, $LEFT$, and $RIGHT$
- $SOURCEDIR$
- $SOURCEDRIVE$
- $SYSTEM$, $SYS2$, and $SYS3$
- $Variable$
- $WINDIR$, $WINDRIVE$, $WINSYSDIR$, and $WINTEMPDIR$
- $WINHELPDIR$
- $WINGROUP$

$ALLUSERSDIR$

$ALLUSERSDIR$ is assigned the Common Programs (WinNT) or Programs (Win9x) subdirectory of the All Users directory. The All Users directory is given by the following registry key:

WinNT	Common Programs entry in HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Win9x	Programs entry in HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

$ASKn$

$ASK1$ through $ASK9$ are assigned values if the ASK1 through ASK9 commands are used, respectively. Each is assigned a value after the user has been prompted for information.

See “IF $ASKn$” on page 428.

Common uses include:

- A request for user information (such as the user's name and company) to personalize the installed software.
- A request for a serial number to verify that installation is authorized.

$CURUSERDIR$

$CURUSERDIR$ is assigned the value of $SystemDir$\Profiles\Username for the currently logged on user. This variable is supported in the Windows NT environment only.

It is most commonly used to assign desktop shortcuts, Send To or Start Menu settings, and other entries in the user profile for the currently logged on user only, instead of to the Default User or All Users. This value includes both the disk drive and the directory path. When an install occurs, the value is read from the destination computer's system.

$DEFAULTDIR$

$DEFAULTDIR$ is assigned the value of the primary directory in which the installation occurs. This value includes both the disk drive and the directory path.

You would typically use the DefaultDir command to display a suggested value and give the user the option of changing it. The variable value is assigned after the user has had a chance to change it, so that the variable value accurately reflects where to install the files.

See “Directory” on page 410.

Common uses include:

- Adding the installation directory to the user's PATH.
- Adding a device driver to the Config.sys file.
- Providing the installation directory path to an external executable.

$DEFAULTDRIVE$

$DEFAULTDRIVE$ is assigned the value of the default installation drive, for example, C. This variable is similar to $DEFAULTDIR$, but it contains the drive value (one letter) only and not the directory value. It is assigned the value after the user enters information in response to the DEFAULTDIR prompt.

$DIRn$

$DIR2$ through $DIR9$ are assigned values if the DIR2 through DIR9 commands are used, respectively. Each is assigned a value after the user is prompted for a path.

See "Directory" on page 410.

Common uses include:

- Adding the installation directory to the user's PATH.
- Adding a device driver to the Config.sys file.
- Providing the installation directory path to an external executable.

$DLLRETURN$ and $DLLRETURNSTR$

$DLLRETURN$ and $DLLRETURNSTR$ are assigned values when a .dll is executed using the RunAtStart, RunAtMiddle, and RunAtExit commands and the executed .dll function generates a return value. Many .dlls do not generate return values. If the return value from the .dll is a string instead of a number, the returned string is stored in variable $DLLRETURNSTR$.

$LOCATEDIR$

$LOCATEDIR$ is assigned a value by the Locate() function, which searches the user's system for a particular file. If the file is found, the variable is assigned the value of the directory path (including the disk drive letter) in which the file was located.

See "IF Locate()" on page 433.

Common uses include:

- Setting the installation directory to the directory in which a previous version of the software is found.

For example, if you are upgrading and you want to install in the directory in which the user installed the last version of the software.

- Installing a file in another application's directory.

  For example, you supply a script file for a database program and you want this script to reside in the database program's directory rather than the directory in which your software is being installed.

$LOCATEDRIVE$

$LOCATEDRIVE$ is assigned a value by the Locate() function, which searches the user's system for a particular file. If the file is found, the variable is assigned the value of the drive in which the file was located.

This variable is similar to $LOCATEDIR$. However, it contains the drive value (one letter) only and not the directory value.

See "IF Locate()" on page 433.

$MACHINENAME$

$MACHINENAME$ is assigned a value corresponding to the NetBIOS name stored in the managed computer. This variable is useful for a silent installation customization.

$MODEMCOM$

$MODEMCOM$ is assigned a value corresponding to the COM port in which the modem was found. Values are 1, 2, 3, and so on. This variable is assigned its value when the FindModem() function is used.

$PROGFILESDIR$

$PROGFILESDIR$ assigns the value of the Program Files directory for a managed computer. This value includes both the disk drive and the directory path. When an install occurs, the value is read from the destination computer's system.

$SEARCH$, $LEFT$, and $RIGHT$

$SEARCH$, $LEFT$, and $RIGHT$ are assigned values using the Search() function. The Search() function is used within an IF statement to search the user's text file for a specified string. If the string is found, the variable $SEARCH$ is assigned the numeric value of the line number in which the string was first found. $LEFT$ is assigned the string value of whatever is on the same line to the left of the searched for string. $RIGHT$ is assigned the string value of whatever is on the same line to the right of the searched for string.

For example, the tenth line in the user's text file is:

```
c:\dos\share /l:500
```

If you search for share, the Search() function locates it, and assigns the three variables the following values:

```
$SEARCH$ = 10
```

```
$LEFT$ = c:\dos\
```

```
$RIGHT$ = /l:500
```

These variables (along with the IF function and AddText function) can be used to edit specific lines in text files. Common uses of these variables are:

- Adding parameters to commands currently in Autoexec.bat or Config.sys files without removing existing parameters.
- Editing a line in a database or network control text file.

$SOURCEDIR$

$SOURCEDIR$ is assigned the value of the drive and the directory on which the installation occurs. This is usually the root directory of the disk drive that contains your installation disk. This value includes both the disk drive and the directory path.

Common uses include:

- Passing the location of the original installation disk to an external program invoked with the RunAtExit command.
- Using variable to remove a file from the installation disk (using the DELETE command) to prevent a second installation.

$SOURCEDRIVE$

$SOURCEDRIVE$ is assigned the value of the drive on which the installation occurs and is usually the disk drive that contains your installation disk. This variable is similar to $SOURCEDIR$. However, it contains the drive value (one letter) only and not the directory value.

For example, using a variable to define a device driver for a CD-ROM drive in a .ini file using the INIFILE command or Config.sys file using the CONFIG command.

$SYSTEM$, $SYS2$, and $SYS3$

$SYSTEM$, $SYS2$, and $SYS3$ are text variables that are assigned the value that the user types on the command line when running the installation program.

For example, if the user types install -update -c:\data -15236, $SYSTEM$ is assigned the value update, $SYS2$ is assigned the value c:\data, and $SYS3$ is assigned the value 15236. If the user types setup -d:\network, $SYSTEM$ is assigned the value d:\network. The dash (-) must precede the text that the user types on the command line. If the dash is omitted, the parameter is interpreted as the installation script (.aic file) name.

Common uses include:

- Allowing variables to be passed from one installation to a second installation.
- Providing a user-supplied variable for testing with an IF statement.

$Variable$

$Variable$ is a custom-named text variable that is equal to a constant or one of the other variables listed. The variable name (between the $ symbols) may be up to 20 characters long. Spaces are not allowed, but you can use the underscore (_) and dash (-) as separators.

The text value is not case sensitive. If the value of $variable$ contains all digits, the value is evaluated as a number and not text. For example, Tuesday, TUESDAY, and Tuesday are all equivalent text values. The variable 6 would be evaluated as less than 1234, but 6a would be evaluated as greater than 1234zzz.

Common uses include:

- Allowing variables meaningful names.
- Providing a user-named variable for testing with an IF statement.

$WINDIR$, $WINDRIVE$, $WINSYSDIR$, and $WINTEMPDIR$

$WINDIR$, $WINDRIVE$, $WINSYSDIR$, and $WINTEMPDIR$ are assigned the directory path of the Windows directory, the drive letter on which Windows is located, the Windows system directory, and the Windows temporary directory, respectively.

Common uses with the File command include:

- Installing fonts or drivers into the Windows system directory.
- Copying or updating .ini files in the Windows directory.

$WINHELPDIR$

$WINHELPDIR$ is supported in the Windows 95/NT environment only. This variable is assigned the directory path of the Windows Help directory.

For example, copying application Help files with the FILE command into the Windows 95/NT Help directory.

$WINGROUP$

$WINGROUP$ is assigned a value only if the WinGroup command is used. It is assigned a value after the user has been prompted for the name of a Windows program group into which to install the software.

See “WinGroup” on page 425.

It takes on the value of whatever the user has entered.

For example, installing icons into the specified program group using the WinItem command.

See “WindowsItem” on page 413.

Section 7

Updating Security Identifiers (SIDs) and computer names

Chapter 22

Updating Security Identifiers (SIDs) and computer names

This chapter includes the following topics:

About making SID changes with Sysprep and Ghost Walker on NT-based clients

Client computers must be uniquely identified to operate on a network. This is achieved using the Security Identifier (SID) and the computer name. When you restore an image onto a number of client computers, you must assign unique identifiers as part of the task.

Note: If an image file of a Windows Vista/XP/2000 computer contains encrypted files and you perform a SID change, then these files become inaccessible. Before you create the image file, you should decrypt any encrypted files.

Symantec Ghost supports the following SID-changing tools:

- Microsoft application Sysprep

- Symantec utility Ghost Walker

Symantec Ghost Walker capabilities

The following versions of Ghost Walker are included with Symantec Ghost:

Ghstwalk.exe	Runs in DOS
GhWalk32.exe	Runs from the command line in a Windows operating system

Ghost Walker has the following capabilities:

- Lets you change the SID after a clone operation without having to restart the computer.
- Alters the computer SID to a unique and randomly generated value.
- Alters the SIDs of all local workstation users present on the operating system installation.
- Alters all local workstation user SIDs in Access Control Lists (ACLs) for file and registry objects. Local users retain user profiles and access rights.
- Alters the computer names for Windows Vista/XP/2000 operating systems. The computer name does not change in the Symantec Ghost Console.

Symantec Ghost Walker limitations

Ghost Walker has the following limitations:

- Computer name change functionality is limited. A new name must contain the same number of characters as the original.
- It is not officially endorsed by Microsoft.
- If you run GhWalk32.exe in Windows, then you cannot change the computer name or SID of the boot volume.

Microsoft Sysprep capabilities

Due to Microsoft policies, Sysprep is the recommended tool for Windows XP.

Microsoft Sysprep has the following capabilities:

- Invokes the Windows Setup Wizard (normally only seen during installation) so that users can enter new user, license, and identification details.
- Can be configured to trigger a driver database rebuild, letting Windows use plug-and-play to detect all device drivers required for the new hardware

environment and to discard any unused drivers. Use of this option is not supported by Symantec Ghost.

- Allows alternate mass storage controller drivers to be installed during the initial post-clone boot. The newly cloned operating system can then start in the new hardware environment to the point when plug-and-play detection can be safely invoked.
- Supports almost all of the unattended installation parameters set, including computer name, domain, network settings, and more. This provides a comprehensive set of tools for reconfiguring the newly cloned computer and also allows a fully automated process to be conducted.
- Optionally alters the identity of the operating system installation by changing the SID.

Microsoft Sysprep limitations

Microsoft Sysprep has the following limitations:

- Does not change the SID of a local workstation user and, therefore, does not have to alter SIDs located in file or registry Access Control Lists (ACLs).
- Requires an additional restart.

SID changing limitations

SID changing is an approximate technology, as you can only change SIDs in known locations.

Problems arise because of the following factors:

- A growing number of third-party and Microsoft applications are taking their own private or derived copies of the computer name and SID and storing them in proprietary formats in registry and file locations, making them inaccessible to SID changes.
- Microsoft technologies such as Windows NTFS File Encryption, Windows NT, and Windows Protected Storage make use of SIDs as unique tokens. They use local workstation user SIDs as part of the encryption key that controls access to encrypted information. If the SID is changed, it renders encrypted data unreadable.

Warning: For these reasons, you are strongly advised to test computer environments and the applications on them before mass rollouts or upgrades.

About losing access to external data objects

Changing the SID of a workstation or a clone of a workstation that has been in use for some time may be more problematic than changing the SID of a newly installed workstation or a clone of a newly installed workstation. When a workstation user, as opposed to a domain user, creates data objects on computers that are participating in a workgroup or a peer-to-peer environment, security information is created for those data objects that are based on the user's SID (which is based on the workstation SID).

When Ghost Walker updates the SID, it not only changes the computer SID, but also all of the workstation user and group SIDs. This is done because user and group SIDs are assumed to be based on the workstation's computer SID (which is now updated). This may mean that the security information on external computers no longer matches the new SIDs of the workstation users, which may result in a loss of access to those data objects.

About identifying user names and passwords across workstations

If there are two workstations in a domain that have two users with the same user name and password, the domain gives each of them access to the other's resources even if their SIDs are different. This is a fairly common situation following cloning.

Updating the SID on a workstation does not stop this situation from occurring. You must change the password of one of the users.

Using Ghost Walker

Ghost Walker lets you alter the identification details of Windows Vista/XP/2000 computers after a clone operation. You can assign a unique computer name and a computer Security Identifier (SID) to each Windows Vista/XP/2000 computer.

When you update the SID using Ghost Walker, all existing workstation users and their passwords, permissions, and registry settings are maintained.

Ghost Walker can be operated from the GUI or from the command line. Ghost Walker does not run from Windows 2000 DOS shell.

The Ghost Walker window lists all bootable Windows Vista/XP/2000 systems on the computer. Ghost Walker determines that there is an installed operating system if a full set of registry hive files and the operating system kernel executable are located in their normal locations.

Ghost Walker lists the following operating system details:

- Logical ID (system ID generated by Ghost Walker)
- Drive number
- Partition number
- Volume label (partition name)
- Partition file system type
- Computer name
- Operating system type, version, or build

To alter identification details for a client computer using Ghost Walker

1. Remove any Windows Vista/XP/2000 workstations that are members of a server domain.

   After you complete the update, you must add each workstation to the domain with the new SID and computer name.

2. Do one of the following:

   - Start DOS, and then, at the command line, type **Ghstwalk.exe**, and then press **Enter**.
   - Start the computer in WinPE, and then run GhWalk32.exe.

     Ghost Walker lists all of the interpretable volumes on the computer as follows:

     - If there is one operating system on the computer, the details of this operating system appear in the top pane, and all volumes appear in the bottom pane.
     - If there is more than one operating system on the computer, the details of all of the operating systems appear in the top pane.

3. If there is more than one operating system on the computer, in the Select a System ID box, type an ID to select an operating system. Then, click **V -Change Additional Vols** to add or remove non-bootable volumes to be updated.

   Warning: You must include any non-bootable volumes that might have security information or shortcuts that contain the computer name of the bootable operating system embedded in them. Failure to do so results in mismatched data and a loss of security access.

4 To change the computer name, type **N**, and then press **Enter**.

The new name must be the same length as the previous name. The box that you type the name into is the correct length of the name.

The name cannot contain any of the following characters:

/\[]“:;|<>+=,?*

5 Press **Enter** to start the update.

The screen displays the new name. For Windows 2000 computers, a new SID is included.

The computer name and SID updates occur in the following locations:

- The registry of the selected operating system
- The file system on which the operating system resides
- Any additional volumes that are included in the update

6 If you removed a Windows 2000 computer from a server domain, add the computer back to the domain.

Running Ghost Walker from the command line

You can run Ghost Walker from the command line in DOS or WinPE.

The command-line syntax is as follows:

```
GHSTWALK[/CN=
<new_computer_name>|“<random_computer_name_format>”]
[/BV=<drv>:<part>[/AV=ALL|/AV=<drv>:<part> ... ]]
[/SURE][/DIAG][/IGNORE_DOMAIN][/IGNORE_ENCRYPTFILES]
[/REBOOT][/REPORT[=<report filename>]][/#E=<license file>]
[SID=<replacement SID][/FNI][/FNS][/FNX]
[/MNUPD=<registry path>][@<argumentfile>]
[LOGGING][SAFE_LOGGING][/H|/HELP|/?]
```

Table 22-1 describes the command-line options.

Table 22-1 Command-line options

Switch	Description
/CN= <new_computer_name>	Specifies a new computer name. The new name must be the same length as the original name and cannot contain any of the following characters: /\[]”:;|<>+=,?* To include spaces in the computer name, enclose the computer name in quotes. For example, /CN="EW PC 123"
/CN= "<random_computer_name_format>"	Replaces the original computer name with a randomly generated name using the <random_computer_name_format> template. The <random_computer_name_format> template specifies which sections of the new name are randomly generated and the type of random value to place in that location. Only one instance of the following keywords is permitted in a template: `<RANDOM_NUMERIC>` - Generate random numbers `<RANDOM_ALPHA>`- Generate random letters `<RANDOM_HEX>` - Generate random hex digits (0-9, A-F) Examples: `/CN="PC<RANDOM_NUMERIC>"` replaces the computer name with a name that starts with PC, followed by a series of random digits between 0 and 9. `/CN="ID<RANDOM_ALPHA>X"` replaces the computer name with a name that starts with ID, followed by a series of random letters, ending with the character X. `/CN="<RANDOM_ALPHA>"` replaces the computer name with a name that is randomly generated using letters. The random output fills out the format string to produce a new computer name of the same length as the original name. Ensure that the format string allows enough room to embed at least one random character without exceeding the length of the original name.

Table 22-1 Command-line options *(continued)*

Switch	Description
/BV=<drv:part>	Specifies the drive number and partition number of the bootable operating system installation to update. If there is more than one operating system, then this switch must be included in the command.
/AV=<drv:part>	Specifies the drive number and partition number of an additional volume containing a file system to update. More than one volume may be specified by repeating the argument for each additional volume. This switch cannot be combined with /AV=ALL.
/AV=ALL	Specifies that all other volumes are to be included as additional volumes. /AV=ALL cannot be combined with the /AV=<drv>:<part> switch.
/SURE	Specifies that the update should start without user confirmation.
/BATCH	Specifies that the update should start without user confirmation, and operation during error situations requires no user input.
/DIAG	Specifies that the utility can only generate diagnostic dumps and log files (not update the computer name or SID).
/IGNORE_DOMAIN	Specifies that Ghost Walker should not check Windows NT or 2000 installations for domain membership.
/REBOOT	Restarts the computer after a successful update.
/REPORT[=<filespec>]	Generates a report containing details of the update to \UPDATE.RPT. An alternate report file can be specified.
/LOGGING	Specifies that diagnostic logging is generated to the Gwalklog.txt file. Recommended for Technical Support use only.
/SAFE_LOGGING	Ensures that all diagnostic logging gets flushed to disk by closing and reopening the Gwalklog.txt file after every log statement. This results in very slow execution. Recommended for Technical Support use only.

Table 22-1 Command-line options *(continued)*

Switch	Description
/#E=<license file>	Specifies a Ghost license file to activate Ghost Walker.
/H|/HELP|/?	Shows command-line syntax Help.
/SID=<replacement SID>	Specifies a replacement SID to be used instead of a randomly generated one. The replacement SID must be in the format S-1-5-21-xxx-xxx-xxx and have the same number of characters as the original SID.
/IGNORE_ENCRYPTFILES	Disables the warning generated by Ghost Walker when it encounters Windows 2000/XP NTFS encrypted files during its initial disk scan. Changing the SID of a Windows 2000 installation results in indecipherable NTFS encrypted files.
/MNUPD=<registry path>	Specifies a registry location that you want Ghost Walker to search for instances of the computer name to update them. This registry key and its subkeys are searched for matched instances of the computer name (of the same length). If any are found, they are updated to the new computer name. Multiple registry locations may be specified with multiple instances of this switch.
@<argumentfile>	Specifies a file containing command-line switches that Ghost Walker should open and read in addition to those specified in the command line. The argument file should only contain one argument on each line. Do not include “” in the file.
/FNI	Disables the direct IDE drive access method.
/FNS	Disables the direct SCSI drive access method.
/FNX	Disables the Extended Int0x13 drive access method.

Following is an example of command-line use:

```
GHSTWALK /BV=1:2 /AV=1:1 /AV=2:1
/CN="WS4-<RANDOM_HEX>-443"/SURE /REBOOT
```

The above command line does the following:

- Updates the Windows Vista/XP/2000 installation that is located on the second partition of the first disk.
- Updates file systems on additional volumes on the first partition of the first and second disks.
- Changes the computer name to one starting with WS4- and ending with -443, placing random hexadecimal values in the remaining spaces until the new name is the same length as the old one. For example, WS4-53ADF76-443.
- Does not prompt the user for final confirmation.
- Reboots after the computer name is changed.

Using Symantec Ghost with Sysprep

This chapter includes the following topics:

About Sysprep

Sysprep is a Microsoft utility that helps prepare Microsoft Windows computers for cloning and customizes the configuration settings when a computer is cloned. It is available on the Microsoft Web site, or it may be on your Microsoft Windows installation CD. Sysprep changes the settings on source and target computers to make cloning among computers with different hardware setups possible.

Sysprep uses unattended files that you can edit to provide computer-specific information before and after you complete a cloning task. Depending on your operating system, the unattended file is named follows:

Windows 2000/XP/2003	Sysprep.inf
Windows Vista	Unattend.xml

Sysprep uses the unattended files in the following ways:

- As a source of information that is usually provided to the user through prompts.

- To alter configuration settings that are not provided for in the Sysprep user interface.
- To specify defaults that the Mini-Setup Wizard uses to configure the destination computers after receiving the image.

If the source or target computers are running Microsoft Windows XP Home, then Sysprep uses the Windows Welcome to request computer-specific information from user input.

Some data from the unattended files is used to prepare the source computer for duplication and customization before creating the image. Some of the settings specified in the unattended files are applied by Sysprep after you restore the image back onto the destination computers. The unattended files are not included with the Sysprep download from Microsoft. You must create the unattended files according to Microsoft guidelines or with the tools provided by Microsoft.

Sysprep also ensures that the Security Identifiers (SID) on the destination computers are unique.

It is recommended that you read the documents listed in Table 23-1, even if you are familiar with Sysprep.

Table 23-1 Sysprep documentation

Get information on	From
How to deploy Microsoft Windows 2000 using Sysprep	The following documents on the Microsoft Windows 2000 Professional CD: ■ Support\Tools\Deploy.cab\Deptool.chm ■ Support\Tools\Deploy.cab\Unattend.doc
How to deploy Microsoft Windows XP through Sysprep	The following documents are available on the Microsoft Windows XP Professional CD: ■ Support\Tools\Deploy.cab\Deploy.chm ■ Support\Tools\Deploy.cab\Ref.chm
How to deploy Microsoft Windows Vista using Sysprep	The following documents on the Microsoft Windows Automated Installation Kit DVD: ■ Docs\Chms\Waik.chm ■ Docs\Chms\Unattend.chm

Note: Do not use Sysprep and a configuration task to set the same configuration settings in case of conflict between the settings. For example, do not instruct Sysprep to add a computer to a domain and set this in a configuration task.

Setting up Sysprep

Use the Symantec Ghost Console to automatically install and configure Sysprep on the Console client computers.

Symantec Ghost supports Sysprep version 1.1 for Windows 2000 and Sysprep version 2.0 for Windows XP. The version that is included with Windows 2000 is Sysprep version 1.0, which has reduced functionality.

Sysprep for Windows Vista is included in the Vista installation.

The Sysprep files are available for a specific operating system as follows:

Windows 2000	Download Sysprep version 1.1 from the Microsoft Web site: http://www.microsoft.com/windows2000/downloads/tools/sysprep/default.asp
Windows XP	Copy Sysprep version 2.0 from the following directory on the Windows XP installation CD: Support\Tools\Deploy.cab
Windows Vista	Sysprep for Vista is included in the Vista installation. It is installed in <Windows>\system32\sysprep.

Managing Sysprep versions

Symantec Ghost has predefined Sysprep versions for Windows 2000, XP, and XP (64-bit), but does not supply the corresponding Sysprep executables. You need to obtain these and use them to update the predefined Sysprep versions before you can make use of them.

Sysprep.exe and Setupcl.exe must be present in the Sysprep folder for Sysprep to install the files. All files in the Sysprep folder and subfolders are installed in the Console local data area (except for the empty ones). Before you create a Sysprep image, all folders and files from that location are copied to the Console client computer.

You can update the predefined versions with the latest Sysprep executables as they become available, and you can create your own custom Sysprep versions that use particular versions of the executables. For example, you may want to have a Sysprep version for a particular OS service pack. You can remove your own Sysprep versions when necessary, but you cannot remove the predefined versions.

To add or update a Sysprep version

1 In the Ghost Console, on the Tools menu, click **Supported Sysprep Versions**.

2 In the Supported Sysprep Versions window, do one of the following:

To add a new version	Click **New**. In the New Sysprep Executables window, in the Name box, type a suitable name for the new version.
To update an existing version	Select the version that you want to update, and then click **Update**.

3 In the New Sysprep Executables window, click **Browse**.

4 Select the folder that contains the new Sysprep executables, and then click **OK**.

5 Click **OK**.

The appropriate executable files are copied into the Console local data area, and the new or updated version is shown in the Supported Sysprep Versions window.

To remove a Sysprep version

1 In the Ghost Console, on the Tools menu, click **Supported Sysprep Versions**

2 In the Supported Sysprep Versions window, select the version that you want to remove, and then click **Remove**.

The executable files are removed from the Console local data area, and the corresponding version is removed from the Supported Sysprep Versions window.

Adding or updating a Sysprep configuration

Once you have copied the Sysprep files on to your computer and set up the appropriate Sysprep versions, you can create and modify Sysprep configurations. A Sysprep configuration includes an answer file and, optionally, additional files such as required drivers. It also includes a reference to the Sysprep version on which it is based, but does not copy or modify the executable files. You can modify a Sysprep configuration at any time.

To add a Sysprep configuration

1 In the Ghost Console, do one of the following:

- On the File menu, click **New > Sysprep Configuration**.

- In the Properties for *Task Name* window, on the Sysprep tab, click **Browse**.
  In the Select Sysprep Configuration window, click **New > New Item**.
- In the left pane, expand the Configuration Resources folder, and then select the Sysprep Configurations folder.
  In the right pane, right-click and then click **New Sysprep Configuration**.

If you do not install the Sysprep files, your Sysprep tasks fail to execute.

2 In the Sysprep Configuration dialog, in the Name box, type a suitable name for the Sysprep configuration.

3 Under Version, click **Browse** and then, in the Select the required Sysprep version window, select the appropriate version.

4 Under Sysprep Answer File, do one of the following:

To create a new answer file	Click **Create**.
To import an existing answer file	Click **Import** and then select the answer file that you want. If you want to change any settings in the answer file, click **Modify**.

5 In the Create Sysprep answer file for Windows 2000/XP/Vista window, specify the settings that you want to use.

If you want to edit the file manually, click **Edit File**, and then make the necessary changes.

6 Click **OK**.

7 Under Additional Files, specify any additional files and folders that you want to include in the Sysprep configuration:

To add files	Click **Add Files** and then select the appropriate files.
To add a folder	Click **Add Folder** and then select the appropriate folder.
To remove an item	Select the files or folder that you want to remove and then click **Remove**.

For example, you may want to include some drivers that are required on your target computers.

8 Click **OK**.

The specified answer file is created, and the additional files are copied to the Console local data area. The new configuration is added to the Sysprep Configuration folder.

Deleting a Sysprep configuration

If you delete a Sysprep configuration, the corresponding answer file and any additional files are removed from the Console local data area. The Sysprep version on which the configuration is based is not affected.

You cannot delete a Sysprep configuration if it is attached to a task.

To delete a Sysprep configuration

1 In the left pane, expand the Configuration Resources folder, and then select the Sysprep Configurations folder.

In the right pane, right-click on the Sysprep configuration that you want to delete, and then click **Delete**.

2 In the confirmation dialog, click **Yes**.

The answer file, and any additional files that were included in the configuration, are deleted from the Console local data area. The Sysprep configuration is removed from the Sysprep Configuration folder.

How Sysprep works with cloning and the Console post-configuration process

During the cloning and the Console post-configuration process, Sysprep and the Console client interact as described below.

During a create image file task, Sysprep does the following:

- Sysprep sets up the model computer before you create an image.
- It then restarts the computer and the image create task executes.
- After the image is created, the client remains in the PreOS and does not process the Mini-Setup Wizard or Windows Welcome.

During a restore task, Sysprep does the following:

- The image file is restored onto the Console client computers and the computers start.
- The Ghost post-clone configuration checks whether Sysprep is configured to run. If Sysprep is configured to run then Ghost updates the unattended files (`Sysprep.inf` or `unattend.xml`) with the details from the Sysprep configuration.
  If the Sysprep configuration uses the default settings, then the Ghost post-configuration process applies the default computer name or workgroup settings. Any custom settings that you included in the Sysprep.inf or unattend.xml file are overwritten. If you do not want your Sysprep answer file settings to be overwritten, verify that the configuration step is not included in the task.
- The Sysprep process starts.
- Sysprep uses either the Mini-Setup Wizard along with information specified in Sysprep.inf, or the Windows Welcome, to gather configuration parameters and then complete its post-cloning configuration.

  Note: If mandatory configuration settings are not defined in Sysprep.inf, the user is prompted for them in the Mini-Setup Wizard.

- If Sysprep has been enabled to change the SID, it changes it once the Console client computer has been configured.
- The Console client completes the remainder of its post-configuration tasks after Sysprep has restarted a second time. Depending on the post-configuration tasks that the Console client has completed, it may restart the computer a third time.

Creating an image with Sysprep

Include Sysprep in an image restore task by including an image file that was created in an image create task using Sysprep.

To create an image with Sysprep

1. In the Ghost Console, on the File menu, click **New > Image Create Task**.
2. In the Properties for New Task window, complete the Network and the General image create details.

   See “Setting general image create task properties” on page 115.

   See “Setting network properties” on page 117.
3. On the Sysprep tab, click **Run Microsoft Sysprep on this machine before creating the image**.
4. Under Sysprep Configuration, click Browse and then select the Sysprep configuration that you want to use.

   You can also add a Sysprep configuration now.

   See “Adding or updating a Sysprep configuration” on page 462.
5. If you want to execute commands that are not automatically generated by Symantec Ghost, under Advanced Settings, in the Extra Sysprep Command Line Arguments box, type the appropriate Sysprep switches.

   See “About using Sysprep switches” on page 467.
6. If the Sysprep configuration is Windows 20000/XP, then click **Tell Sysprep to perform a SID change when restoring this image to a destination machine** for Sysprep to change the SID on the destination computer.

   If this option is selected, then do not use Ghost Walker to perform a SID change when restoring an image onto client computers.
7. If the Sysprep configuration is Windows Vista, then click **Run Sysprep with generalize switch to remove machine-specific information** to add the generalize switch.

   The generalize switch adds SID-change functionality and removes and hardware-specific information.
8. If necessary, check **Run the MiniSetup wizard which processes the sysprep.inf file**.

   This lets Sysprep run the Mini-Setup Wizard when cloning Microsoft Windows XP Professional.

   If this option is not selected, then the Windows Welcome appears instead of the Mini-Setup Wizard the next time the computer is started.

About using Sysprep switches

If you are using other Sysprep switches, consult the Sysprep documentation and ensure that they do not conflict with Ghost operation.

Table 23-2 lists the Sysprep switches are generated automatically by Symantec Ghost or are set in the Console.

Table 23-2 Sysprep switches

Operating System	Switches set by Ghost	Optional switches
Windows 2000	The following switches are set by Ghost: ■ -quiet ■ -nosidgen You can set this option on the Ghost Console Sysprep task window. ■ -reboot	The following switch is optional: ■ -pnp
Windows XP	The following switches are set by Ghost: ■ -quiet ■ -nosidgen You can set this option on the Ghost Console Sysprep task window. ■ -reboot ■ -reseal ■ -mini You can set this option on the Ghost Console Sysprep task window.	The following switches are optional ■ -pnp ■ -activated
Windows Vista	The following switches are set by Ghost: ■ -oobe ■ -reboot ■ -quiet ■ -generalize You can set this option on the Ghost Console Sysprep task window.	

Section 8

Symantec Ghost utilities

Chapter 24

Managing partitions using GDisk

This chapter includes the following topics:

About GDisk

GDisk is a utility that lets you create partitions, reinitialize master boot records, delete data, and wipe your disks in many different ways.

The following versions of GDisk are included with Symantec Ghost:

GDisk.exe	Runs in DOS
gdisk	Runs in Linux
GDisk32.exe	Runs from the command line in a Windows operating system
GDisk64.exe	Runs from the command line in a 64-bit Windows operating system

GDisk is a complete replacement for the Fdisk and Format utilities and offers the following features:

- On-the-fly formatting
- Extensive partition reporting
- High-security disk wiping
- The ability to hide a partition or make a hidden partition visible
- Compliance with the U.S. Department of Defense requirements for securely wiping disks

Unlike Fdisk, which uses interactive menus and prompts, GDisk is command-line driven. This offers quicker configuration of a disk's partitions and the ability to define GDisk operations in a batch file.

Running GDisk

GDisk.exe must be run in DOS mode. GDisk32.exe can be run from within Windows. gdisk for Linux runs only under Linux.

Note: To run GDisk32 or GDisk64 in Microsoft Vista, you must run the command prompt as an administrator. To run gdisk for Linux, you must run as root.

To run GDisk.exe

1. Start your computer in DOS mode.
2. At the DOS prompt, type **Progra~1\Symantec\Ghost\GDisk** followed by the required disk and switches.

To run the command prompt as an administrator

1. On the taskbar, click **Start > All Programs > Accessories**, right-click **Command Prompt** and click **Run as administrator**.
2. In the User Account Control dialog box, type the administrator credentials.
3. Click **OK**.

To run GDisk32.exe

1. On the Windows taskbar, open a command window.
2. At the command prompt, type **Program Files\Symantec \Ghost\GDisk32** followed by the required disk and switches.

To run GDisk64.exe

1. On the Windows taskbar, open a command window.
2. At the command prompt, type **Program Files\Symantec \Ghost\GDisk64** followed by the required disk and switches.

To run gdisk for Linux

- At the command prompt, type the appropriate path (the location to which you extracted the Linux tools) and executable name (gdisk), followed by the required disk and switches.

Overview of the main command-line switches

GDisk has 11 main modes of operation. The first four correspond to the menu options on the FDisk main menu.

Some command-line switches work only with the DOS version of GDisk or only with the Windows 32 version of GDisk.

Table 24-1 describes the switches that set the mode in which GDisk operates.

Table 24-1 GDisk main commands

Mode	Switch	Explanation
Create	/cre	Creates primary DOS partitions and extended DOS partitions.
Delete	/del	Deletes partitions of any type, including non-DOS partitions.
Status (default)	/status	Lists information on the specified fixed disk and its partitions.
Activate	/act /-act	Activates and deactivates a partition (specifying it as the bootable partition).
Hide	/hide /-hide	Hides or unhides an existing partition.
Reinitialize MBR	/mbr	Reinitializes the Master Boot Record.

Table 24-1 GDisk main commands *(continued)*

Mode	Switch	Explanation
Reinitialize GPT	/gpt	Reinitializes a GPT disk.
Batch	/batch	Uses batch-mode command execution.
Disk wipe	/diskwipe	Wipes the contents of the whole disk.
Boot.ini	/bootini	Makes a modification to the Windows 2000/XP boot menu (Windows only).
View	/view	Lets you view the contents of a disk to confirm an overwrite pattern after a disk wipe.

Online Help for command-line switches

You can get an overview of the nine modes of operation and their switches by using the Help switch. The syntax for displaying help in GDisk is as follows:

Note: An additional switch not shown is the /VERSION switch. This switch shows the version information for the GDisk and GDisk32 executable.

More detailed Help is available by qualifying the Help command with the switch for one of the nine main modes of operation.

For example, to view the detailed Help file for Hide, type one of the following command lines:

GDisk.exe	C:\progra~1\symantec\ghost\gdisk /hide /?
GDisk32.exe	C:\progra~1\symantec\ghost\gdisk32 /hide /?

Switches common to all GDisk commands

Table 24-2 describes the switches for any of the main GDisk operations.

Table 24-2 Switches common to all GDisk commands

Switch	Explanation
/ad=image file name /addDisk=image file name	Mounts the specified vmdk, pqi, v2i, or iv2i image file ("add" the image as a disk). Once added, the disk can be used in all normal operations.

Table 24-2 Switches common to all GDisk commands *(continued)*

Switch	Explanation
/x	Prevents GDisk from using extended disk access support. This may result in GDisk not being aware of the full capacity of the disk.
/i	Prevents GDisk from using direct IDE disk access support. This may result in GDisk not being aware of the full capacity of the disk.
/s	Prevents GDisk from using direct SCSI disk access support. This may result in GDisk not being aware of the full capacity of the disk.
/y	Suppresses prompting to confirm the operation. If you do not use this switch, you are not necessarily prompted before a partition is deleted or another possibly destructive operation is executed.
/sure	Suppresses prompting to confirm the operation and has the same functionality as /y.
/r	Causes GDisk to restart the computer if the operation is successful.
/u	Turns off Ultra Direct Memory Access (UDMA). This switch works in DOS only.
/forceusb	Forces USB support to start, even when the USB controller is being run by something else. The forceusb attempts to take over the USB Host Controller and then attempts to return it to the previous state once the Ghost operation is complete. This works for controllers as follows: ■ EHCI controllers with BIOS support are taken over and then returned to the BIOS. ■ UHCI controllers with BIOS support are taken over and then returned to the BIOS. For example, the keyboard is returned after the Ghost operation is finished. ■ OHCI controllers with BIOS support are taken over but not returned to the BIOS. Note the following: ■ Use this switch with caution. ■ Avoid using the forceusb switch to take over a USB controller from a driver, for example, Iomega USB drivers. You may encounter problems if you do this. This switch works in DOS only.

Table 24-2 Switches common to all GDisk commands *(continued)*

Switch	Explanation
/nousb	Disables USB support. This switch works in DOS only.
/ force1394	Forces FireWire support to start, even when the FireWire controller is being run by something else. The force1394 switch attempts to take over the FireWire Host Controller. To enable native BIOS support, you must restart the computer. Note the following: ■ Use this switch with caution. ■ Avoid using the force1394 switch to take over a FireWire controller from a driver, for example, Iomega FireWire drivers. You may encounter problems if you do this. This switch works in DOS only.
/no1394	Disables FireWire support. This switch works in DOS only.

Creating a partition

The create command lets you create a partition and specify the parameters of the partition. The command uses the largest block of unused disk space to create the partition. You can specify the partition type and the partition size. You can use the /for switch with the create command to format the partition. Otherwise, the partition is not formatted. You cannot create a dynamic disk partition.

Note: When GDisk creates a FAT32 partition, it aligns the first data sector to a 4 KB boundary from the start of the partition.

The create command uses the following syntax:

GDisk

```
gdisk disk /cre {/pri| /ext| /log}[/sz: {MB|pcent{p|%}}]
[/end] [/for [/q] [/ntfs[:vista|xp|2000]]
[/align[:chs|1mb]] [/v[:label]]] [/-32] [/ntfat16]
```

GDisk32

```
gdisk32 disk /cre{/pri|/ext|/log} [/sz:{MB|pcent{p|%}}]
[/end][/for [/q][/ntfs[:vista|xp|2000]]
[/align[:chs|1mb]][/v[:label]]] [/-32] [/ntfat16]
```

For example, to create a FAT32 formatted partition that uses the entire disk, you can use the following command:

```
gdisk 1 /cre /pri /for /q
```

Table 24-3 describes the switches that you can use with the create command.

Table 24-3 Create switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128.
/cre	Creates a partition or a logical drive.
/pri	Creates a primary partition for an MBR or a GPT disk.
/ext	Creates an extended partition. This is supported for MBR only.
/ext2	Formats an ext2 partition. For example: `gdisk /cre /pri /for /ext2`
/log	Creates a logical drive in the extended partition. This is supported for MBR only.
/sz:MB	Specifies the size of the partition in megabytes (MB). This is rounded up to the nearest cylinder.
/sz:pcent{p|%}	Specifies the size of the partition as a percentage of the total disk size, not the available disk space.
/end	Creates the partition at the end of the free space. If this switch is not used, then the partition is created at the beginning of the free space. If the command line specifies that all of the available space is to be used to create the partition, then the /end switch is ignored.
/for	Formats the new partition once it has been created. Unless the /ntfat16 or /-32 switches are used, the partition type is determined by the following: ■ If the partition is less than 16MB: FAT12 ■ If the partition is between 16MB and 512MB: FAT16 ■ If the partition is greater than 512MB: FAT32
/ntfs[:vista|xp|2000]	Formats the new partition as NTFS. You can use the /for switch with this command to format the NTFS partition with the required volume type.

Table 24-3 Create switches *(continued)*

Switch	Explanation
/align[:CHS|1MB]	Aligns the partition with a boundary as follows: ■ CHS: Aligns the partition to a track or cylinder boundary. This setting is the default. ■ 1MB: Aligns the partition with a boundary of 1 MB. You can use the lba switch to view the partition alignment. **Note:** The 1MB alignment option supports Windows Vista.
/q	Performs a quick format if used in combination with the /for switch. If you do not use this switch, then GDisk performs a surface scan of the partition and marks any bad sectors.
/v[:label]	Gives the new formatted partition the specified label when used in combination with the /for switch.
/-32	Indicates that the partition is not formatted as FAT32. Limits primary and logical partitions to 2048 MB. Partitions over 16 MB are formatted as FAT16. This switch is useful if the operating system does not support FAT32, such as Windows NT 4.
/ntfat16	Lets you create a FAT16 primary or logical partition, up to 4097 MB. The cluster size is 64 KB. Partitions over 16 MB are formatted as FAT16. DOS systems may be unable to access partitions that are created with this switch and are over 2048 MB.

Reinitializing the Master Boot Record

You can use the /mbr command to rewrite the boot code in the master boot record (MBR). For example, you can use the /mbr command to reinitialize the MBR to eliminate a boot-sector virus. You can also use the /mbr command with the /wipe option in DOS to delete a dynamic disk.

Note: You must use the /mbr command when you delete Linux partitions if LILO or Grub resides in the MBR.

The syntax for this command is as follows:

GDisk.exe	`gdisk disk /mbr [/wipe] [/p] [/z]`
gdisk	`gdisk disk /mbr [/wipe] [/p] [/z]`

GDisk32.exe	`gdisk32 disk /mbr {/p /z}`
GDisk64.exe	`gdisk64 disk /mbr {/p /z}`

Table 24-4 lists the mbr switches.

Table 24-4 /mbr switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128.
/mbr	Reinitializes the boot code in the Master Boot Record.
/wipe	Deletes the partition on the disk (DOS and Linux only).
/p	Preserves the disk signature.
/replace: [filename]	Replace the Master Boot Record with the specified mbr file.
/z	Clears the disk signature and sets it to 0.

If you clear the disk signature on a Windows computer then the disk must be initialized by Windows before it can be used. This is performed automatically when a computer is started. You can use the Disk Manager feature in Windows to initialize the disk manually. Microsoft Vista does not support automatic initialization.

Reinitializing GPT disks

You can use the /gpt command with /wipe to reformat a GPT disk. You can also use the /gpt switch with the /wipe switch in DOS to delete a dynamic disk.

The syntax for this command is as follows:

```
gdisk disk /gpt /wipe
```

Table 24-5 lists the gpt switches.

Table 24-5 /gpt switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128
/gpt /wipe	Reformats a GPT disk (DOS only)

Showing information about disks

The status switch shows information about the fixed disks and partitions on a disk, including the model of the disk. You must specify the disk number to get information about the partitions on a disk.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

GDisk.exe	gdisk [disk] [/status] [/raw|lba] [/ser]
GDisk32.exe	gdisk32 [disk] [/status] [/raw|lba] [/ser]

Table 24-6 lists the status switches.

Table 24-6 /status switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128.
/raw	Shows the contents of the partition table in CHS or GPT form if used with the disk switch.
/lba	Shows the contents of the partition table in logical block form if used with the disk switch.
/ser	Shows the serial number of the disk.

Performing multiple GDisk operations using batch mode

Use the batch mode switch, /batch, to perform multiple GDisk operations with a single command. Using the /batch switch lets you avoid loading GDisk from the boot disk each time. Batch commands can either be supplied interactively at a prompt or in a previously prepared text file.

If the name of a text file is supplied along with the batch mode switch, GDisk opens the file and executes the commands within it until all commands have been executed or one of the commands encounters an error.

For example:

```
C:\> gdisk /batch:cmds.txt
```

If the batch mode switch is supplied without a file name, GDisk prompts you for the commands to execute.

Note: To use GDisk32.exe in the example commands, replace gdisk with gdisk32.

Command-line arguments that apply to all of the batch commands can be specified on the original command line along with the batch mode switch. The lines found in the batch file (or typed at the prompt) are appended to the already partially formed command line.

Following is a sample batch command file called Two-new.txt. Blank lines and lines starting with the number (hash) symbol are considered comments. These lines are ignored. In the following example, the commands do not specify the fixed disk on which to operate:

```
# delete all partitions
/del /all
# create formatted FAT16 primary DOS partition and then create
 an extended # partition
/cre /pri /-32 /for /q
/cre /ext
# create formatted FAT16 logical DOS partition
/cre /log /-32 /for /q
```

The following command deletes all partitions and creates two new ones on the second fixed disk with confirmation prompting turned off:

```
gdisk 2 /y /batch:two-new.txt
```

The following four commands to be executed are a combination of the original command plus the commands from the batch file:

gdisk 2 /y /del /all

gdisk 2 /y /cre /pri /-32 /for /q

gdisk 2 /y /cre /ext

gdisk 2 /y /cre /log /-32 /for /q

Batch files may be nested recursively. For example, a second file called Std_init.txt contains the following lines:

1 /batch:two-new.txt

2 /batch:two-new.txt

As a result, the following command performs the actions of two-new.txt on both fixed disks:

gdisk /batch:std-init.txt

Deleting and wiping your disk

GDisk lets you delete data and partitions on your disk or wipe your entire disk. You cannot delete a dynamic disk partition with the /del switch.

The switch /del /all deletes all partitions that are on the disk. Any other space that has not been used for creating a partition is not deleted. Deleting an extended partition also deletes any logical partition within it.

The /diskwipe switch wipes the entire disk, partitions, partition table, MBR, and all used and unused space.

See "About GDisk disk-wipe specifications" on page 567.

Depending on the version of GDisk that you require, the syntax for the delete command is one of the following:

GDisk

```
gdisk disk /del {/pri[:nth]|/ext[:nth]|/log:nth|
/p:partn-no|/all}
[/qwipe|/dodwipe|/customwipe:n][/[-]hpa]
```

GDisk32

```
gdisk32 disk /del {/p:partn-no|/all} [/qwipe|/dodwipe
|/customwipe:n]
```

Table 24-7 lists the delete command switches.

Table 24-7 /del switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128.
/del	Deletes a partition or a logical drive.
/pri[:nth]	Deletes the nth primary partition on an MBR or a GPT disk. The default setting is 1.
/ext[:nth]	Deletes the nth extended partition as well as any logical partitions in the extended partition. This switch is supported on MBR disks only. The default setting is 1.
/log:nth	Deletes the nth logical drive from the extended partition. This switch is supported on MBR disks only.
/p:partn-no	Indicates which partition to delete on an MBR or a GPT disk. You should use the partition number that is reported by GDisk in standard display mode for partn-no. Do not use the /lba or the /raw switches to find the partition number.

Table 24-7 /del switches *(continued)*

Switch	Explanation
/all	Deletes all partitions.
/qwipe	Overwrites the partition's data area before deleting the partition. Makes 1 pass of deleting the data on the disk.
/dodwipe	Overwrites the partition's data area before deleting the partition. Makes 6 passes of deleting the data on the disk.
/customwipe:n	Overwrites the partition's data area n times before deleting the partition. You can set n from 1 to 100. The /customwipe:6 switch is equivalent to a sanitize /dodwipe operation.

Depending on the version of GDisk that you require, the syntax for the diskwipe switch is as follows:

GDisk.exe	gdisk disk /diskwipe [dodwipe| /customwipe:n][/[-]hpa]
GDisk32.exe	gdisk32 disk /diskwipe [dodwipe| /customwipe:n]

Note: You must restart the computer after a disk wipe operation.

Table 24-8 lists the diskwipe switches.

Table 24-8 /diskwipe switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128. n - The disk number
/disk:	One of the following: ■ ALL - All attached disks ■ SYSTEM - The disk containing the bootable OS.
/diskwipe	Wipes the contents of the entire disk. Using this switch on its own wipes all partitions.
/dodwipe	Overwrites the disk including all partitions. Makes six passes of deleting the data on the disk.

Table 24-8 /diskwipe switches *(continued)*

Switch	Explanation
/customwipe:n	Overwrites the disk's data area n times and deletes partitions. You can set n from 1 to 100. The /customwipe:6 switch is equivalent to a sanitize /dodwipe operation.
/hpa	Wipes any HPA/PARTIES area found on the disk. (DOS only - does not apply to GDisk32)
/-hpa	Ignores any HPA/PARTIES area found on the disk. (DOS only - does not apply to GDisk32)
/keepghostboot	Preserve the Ghost partition that was used to boot.

Following are examples of the delete and wipe switches:

- gdisk 1 /del /all /qwipe completes one pass to delete all partitions and data on disk 1.
- gdisk 1 /del /p:2 /qwipe wipes partition 2 on disk 1 with one pass.
- gdisk 1 /diskwipe /customwipe:15 wipes the entire disk with 15 passes.

Wiping Host Protected Areas (HPA)/PARTIES

During execution of a DoD disk wipe, GDisk attempts to detect an HPA/PARTIES area on the disk.

Note: This functionality operates with GDisk.exe only. It does not apply to GDisk32.exe.

The sequence of the wipe is as follows:

- If GDisk detects such an area, then it shall notify the user that it was found and ask the user whether this area should be unlocked so that it can be erased.
- If the user requests that the area be unlocked, then GDisk will attempt to unlock the area. Otherwise, GDisk continues, ignoring the HPA area.
- If the area is not password-protected and is successfully unlocked, then GDisk notifies the user and erases the entire disk, including the HPA/PARTIES area.
- If the area is password-protected and cannot be unlocked, then it notifies the user that the unlock failed and asks if the users wants to continue. The user is also informed that the HPA/PARTIES area could possibly be unlocked using the BIOS.

- If the user wants to continue, then GDisk continues to erase the disk, ignoring the HPA/PARTIES area.

There are optional command-line switches as follows:

/-hpa

GDisk does not look for an HPA on the disk.

For example:

gdisk 1 /diskwipe /dodwipe /-hpa performs a DoD disk wipe without checking for an HPA on the disk. If an HPA area is present, it is not wiped.

/hpa

GDisk detects and attempts to unlock the HPA on the disk. If the area cannot be unlocked, then GDisk exits.

For example:

gdisk 1 /diskwipe /dodwipe /hpa performs a DoD disk wipe attempting to unlock any HPA on the disk.

Confirming a disk wipe

The view:n command-line switch lets you view the overwrite pattern on the disk to confirm the overwrite has occurred. This lets you display one or more sectors, starting at sector n, of a physical disk on screen (by default, 1 sector shall be displayed). Sector numbers start at 0.

The optional arguments are as follows:

num:m

m sectors are displayed starting at the sector indicated in the view command.

If num:m is not specified, then GDisk defaults to displaying only one sector as indicated by view:n.

page

GDisk waits for you to press a key after each page of sector content is displayed. You can press q to exit.

If page is not specified, then GDisk defaults to continuously outputting the contents of the sectors specified until finished.

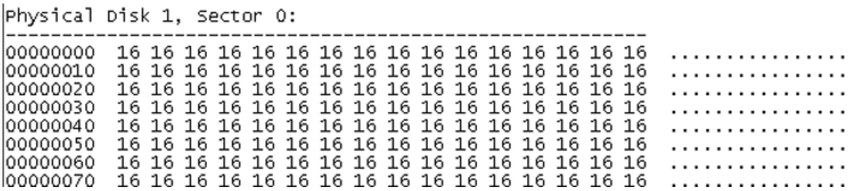
Each sector is displayed as a table with 16 columns containing the sector offset, then hex bytes, and lastly 16 ASCII characters representing each byte. The table has n rows where n depends on the sector size. This is usually 32 rows (sector size of 512 bytes).

For example, displays sectors 0, 1, and 2 on screen:

```
gdisk 1 /view:0 /num:3
```

Figure 24-1 shows the output display.

Figure 24-1 Viewing disk wipe output



```
Physical Disk 1, Sector 0:
----------------------------------------------------------
00000000  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000010  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000020  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000030  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000040  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000050  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000060  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000070  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
```

Activating or deactivating a partition

A computer starts in an active partition. Using the /act or /-act switches, you can choose the partition to which the computer starts.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

GDisk.exe	gdisk disk /[-]act /p:partn-no
GDisk32.exe	gdisk32 disk /[-]act /p:partn-no

Table 24-9 lists the act switches.

Table 24-9 /act switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128.
/act	Activates a partition.
/-act	Deactivates a partition.
/p:partn-no	Indicates the partition to activate or deactivate. Only primary partitions can be activated. Use the number reported by GDisk in standard display mode (not using /lba or /raw) for partn-no.

Hiding or unhiding a partition

You can hide a partition so that a user cannot see it.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

GDisk.exe	gdisk disk /[-]hide /p:partn-no
GDisk32.exe	gdisk32 disk /[-]hide /p:partn-no

Table 24-10 lists the hide switches.

Table 24-10 /hide switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 128.
/hide	Hides a partition.
/-hide	Unhides a partition.
/p:partn-no	Indicates the partition to hide or unhide. Use the number reported by GDisk in standard display mode (not using /lba or /raw) for partn-no.

Modifying the Windows 2000/XP boot menu

The /bootini switch lets you make a modification to a Windows 2000/XP boot menu. The following modifications are supported:

- Displaying a list of current boot entries
- Adding an entry to boot.ini
- Removing an entry from boot.ini
- Setting the default boot option and timeout

This switch functions with GDisk32.exe and GDisk64.exe only.

When GDisk32 or GDisk64 changes the state of boot.ini, a copy of the current boot.ini is created.

Table 24-11 lists the boot.ini copy names.

Table 24-11 Original and copy names

Original boot.ini filename	Boot.ini copy name
Named boot.ini	boot_GDISK32_copy.ini
Not named boot.ini and with a period. For example: my.ini	my_GDISK32_copy.ini

Table 24-11 Original and copy names *(continued)*

Original boot.ini filename	Boot.ini copy name
Not named boot.ini and without a period. For example: myBootFile	_GDISK32_copy is appended to the end of the file name: myBootFile_GDISK32_copy

Specifying the boot.ini path and file name

The /inifile switch is common to all operations performed with the /bootini switch.

The /inifile switch lets you specify the full path and file name of the current Windows 2000/XP boot.ini file. This lets you locate boot.ini if it is not on drive C.

The default value for this switch is C:\boot.ini.

Displaying the list of current boot entries

Use the /bootini switch to display the existing boot menu for the current Windows 2000/XP operating system.

The syntax for this command is as follows:

```
gdisk32 /bootini [/inifile:filename]
```

Adding an entry to boot.ini

You can add the following functions to a boot.ini file:

- Starting another installation of Windows 2000/XP that resides on a different partition.
- Starting a non-Windows 2000/XP operating system that resides on a different partition.

GDisk does not add an entry to boot.ini in the following cases:

- An entry with the description already exists in Boot.ini (case insensitive).
- The referenced partition is of type Extended.
- The referenced partition is hidden.

Table 24-12 describes the function of each switch for both types of entries.

Table 24-12 Boot.ini switches

Switch	Explanation
/bootini	Modifies boot.ini.
/add	Creates a new entry in boot.ini.
/d:diskno	Represents the physical fixed disk, from 1 to 128.
/p:partno	Indicates the partition from which to boot.
/desc:description	Specifies the description to appear in the NT boot loader menu.
/inifile:filename	Specifies the full path and file name for boot.ini. The default value is C:\boot.ini.
/bsectfile:filename	Specifies the boot-sector file to create. For example, C:\bsect.dat.
/winnt	Adds an entry to start a Windows 2000/XP operating system.
/sysfolder:folder	Specifies the system folder on the Windows 2000/XP operating system from which to start. The default value is Winnt.
/r	Restarts after the execution of the command.

Adding an entry to start Windows 2000/XP

The syntax for this command is as follows:

```
gdisk32 /bootini /add /d:disknumber/p:partno /desc:description /winnt
[/sysfolder:folder] [/inifile:filename] [/r]
```

This entry uses the Advanced RISC Computing (ARC) style path to describe the relative disk location for the entry. The entry has the following format:

```
<ARC style path>\<system folder>="description”
```

For example:

```
multi(0)disk(0)rdisk(0)partition(1)\winnt="Boot NT System”
```

For more information, see the Microsoft Knowledge Base article Q102873 - “BOOT.INI and ARC Path Naming Conventions and Usage.”

Note the following:

- GDisk uses only Multi(X) syntax when describing ARC style paths, as opposed to SCSI(X).
- GDisk always uses multi(0)disk(0) as the beginning of the ARC style path.

- /winnt instructs GDisk32 to create an ARC style entry and must be used if the target operating system is Windows 2000/XP. If this switch is not used, then GDisk32 creates an entry as if the target operating system is not Windows 2000/XP.
- /sysfolder lets you specify the Windows system folder on the target operating system. The system folder is usually Winnt. If the system folder is not Winnt, then provide the path to this folder, but do not include the root directory.
  For example, use /sysfolder:"2k\WinNt", not /sysfolder:"f:\2k\WinNt".

Adding an entry to start a non-Windows 2000/XP operating system

The syntax for this command is as follows:

```
gdisk32 /bootini /add /d:diskno/p:partno /desc:description
[/inifile:filename] [/bsectfile:filename] [/r]
```

This entry to boot.ini references a boot-sector file used to continue the boot process.

The entry has the following format:

full path to boot sector file\boot sector file="description"

For example:

C:\bootos2s.dat="Boot OS/2 System"

When adding this entry, GDisk does the following:

- Reads the first sector of the targeted partition (boot sector).
- Writes out the contents of that sector to a boot-sector file.
- Adds a reference to that boot-sector file to boot.ini.

The /bsectfile switch is optional. It is used if you want the created bootsect.dat file to be saved somewhere other than the default location.

You must specify the full path and file name for the boot-sector file that is created when you use the /bsectfile switch.

GDisk32 does the following by default:

- Builds the file name from the entry descriptions, omitting any invalid characters under DOS rules for 8.3 file name format.
- Creates the boot-sector file in the root directory of the C drive and gives it a .dat file extension.
  For example:

  ```
  gdisk32 /add /d:1 /p:2 /desc:"*** Boot OS/2 ***"
  ```

This produces a boot-sector file C:\bootos2.dat.

Removing an entry from boot.ini

The syntax to remove an entry from boot.ini is as follows:

```
gdisk32 /bootini /remove /entry:number [/inifile:filename] [/r]
```

Table 24-13 lists the remove switches.

Table 24-13 /remove switches

Switch	Explanation
/remove	Removes the entry from boot.ini.
/entry:number	Removes the ID of the entry from boot.ini.

If the entry to be removed is the default boot option, then GDisk removes the entry and sets the first entry in the remaining list as the default boot entry.

GDisk does not remove the entry if it is the only entry in boot.ini.

Setting the default boot option and timeout

Use the /default switch to set the default boot option and timeout.

The syntax for this command is as follows:

```
gdisk32 /bootini /default [/entry:number] [/timeout:sec]
[/inifile:filename] [/r]
```

Table 24-14 lists the default boot option and timeout switches.

Table 24-14 Default boot option and timeout switches

Switch	Explanation
/default	Sets the default boot option and timeout.
/entry:number	Sets the ID of the entry as the default boot option.
/timeout:sec	Sets the number of seconds before the default boot option is selected.

Support for large hard-disks

GDisk supports all operations on disks up to 2 TB, and can also wipe disks larger than 2 TB.

GDisk includes large disk-drive support for IDE and SCSI hard drives (disks that exceed the 1024 cylinder BIOS limitation, which translates to a capacity greater than 7.8 GB). GDisk can directly access hard disks through the IDE controller or ASPI interface provided by an ASPI driver. Take care when creating partitions for operating systems with inherent partition-size limitations.

Chapter 25

Manipulating files and directories using OmniFS

This chapter includes the following topics:

About OmniFS

OmniFS is a general-purpose utility for manipulating files and directories in a locally attached NTFS, FAT, or EXT3 file system (including hidden partitions).

OmniFS.exe performs these functions from DOS or WinPE. OmniFS32 performs the same functions but runs them in a Windows environment. The Linux version, omnifs, performs the corresponding functions under Linux.

OmniFS performs selected file input/output operations on a file system that is not accessible from a utility's operating environment.

OmniFS supports scripting and batch mode execution.

OmniFS operating environments

Table 25-1 lists the versions of OmniFS.

Table 25-1 OmniFS versions

Executable	Operating system
OmniFS.exe	PC-DOS, MS-DOS
omnifs	Linux
OmniFS32	Windows Vista/XP/2000

Long file names are supported on NTFS file systems, but support for long file names on FAT file systems depends on the operating system and access method. If you use the OmniFS library to access a file system, then long file names are supported. You can use the access method switches to directly access a file system.

Using OmniFS

You can execute OmniFS from the command line only. Running OmniFS without any arguments provides a list of the interfaces and lists the access method switches.

The following interfaces are supported for OmniFS.exe, OmniFS32.exe, and omnifs for Linux:

omnifs [/accessmethods]<operation to perform> <operation arguments, if any>	Performs the file operation and exits. It uses the exit code to signal whether or not the operation was successful, making it suitable for batch mode execution.
omnifs [/accessmethods]script<script file name>	Performs all of the operations that are nominated in the script file and exits. It uses the exit code to signal whether the operation was successful. If any operation in the script file is unsuccessful, the script stops running and the utility exits, which signifies that the operation failed.
omnifs help	Lists the available commands.

To run OmniFS32 in Microsoft Vista, you must run the command prompt as an administrator.

To run the command prompt as an administrator

1 On the taskbar, click **Start > All Programs > Accessories**, right-click **Command Prompt** and click **Run as administrator**.

2 In the User Account Control dialog box, type the administrator credentials.

3 Click **OK**.

Access method switches

Table 25-2 lists the access method switches that you can use in any operation. Not all access methods are relevant to the Win32 version, OmniFS32.exe.

Table 25-2 Access method switches

Switch	Description
/ad=image file name /addDisk=image file name	Mounts the specified vmdk, pqi, v2i, or iv2i image file ("add" the image as a disk). Once added, a vmdk disk can be used in all normal operations, but the pqi, v2i, and iv2i disks are read-only.
/cp=codepage	Handles the code page in the same way as the current OEM page. The code page is specified as a number.
/diskfs	Specifies that the preferred file system access is through the application file system code.
/diskvol	Specifies that the preferred volume access is through the application volume code.
/dl=n	Specifies the number of hard drives present.
/ffi	Prefers use of Direct IDE Access (DOS only).
/ffs	Prefers use of Direct ASPI/SCSI Access.
/ffx	Prefers use of Extended Int13h.
/fna	Disables asynchronous I/O.
/fni	Disables Direct IDE Access support (DOS only).
/fns	Disables Direct ASPI/SCSI Access support.
/fnx	Disables Extended Int13h support.
/force1394	Forces the IEEE1394 device (Firewire) to start (DOS only).

Table 25-2 Access method switches *(continued)*

Switch	Description
/forceusb	Forces USB support to start, even when the USB controller is being run by something else (DOS only).The -forceusb switch attempts to take over the USB Host Controller and then attempts to return it to the previous state once the Ghost operation is complete. This works for controllers as follows: ■ EHCI controllers with BIOS support are taken over and then returned to the BIOS. ■ UHCI controllers with BIOS support are taken over and then returned to the BIOS. For example, the keyboard is returned after the Ghost operation is finished. ■ OHCI controllers with BIOS support are taken over but not returned to the BIOS. Note the following: ■ Use this switch with caution. ■ Avoid using the forceusb switch to take over a USB controller from a driver, for example, the Ghost peer-to-peer USB driver. You may encounter problems if you do this.
/no1394	Tuns off the IEEE1394 (Firewire) support (DOS only).
/noide	Tuns off the IDE support (DOS only).
/noscsi	Tuns off the SCSI support.
/nousb	Tuns off USB support (DOS only).
/osfs	Specifies that the preferred file system access is through the operating system.
/osvol	Specifies that the preferred volume access is through the operating system.
/pfpath=path	Sets the path to the directory in which the recovery file system resides.
/usbtimeout=n	Sets the USB emulation timeout in microseconds, where n is greater than or equal to 1 (DOS only). The default setting is 3000ms.
/vdw	Verifies every disk write.

Accessing files and folders with names that contain spaces

When using any of the OmniFS operations on files or folders that contain spaces in the file name or folder name, you must use one of these methods.

To display the directory for the folder My Documents in volume 1, use one of the following:

```
OmniFS dir “1.1:\My Documents” OmniFS dir 1.1:“\My Documents”
```

The following example would not work:

```
OmniFS dir 1.1:\“My Documents”
```

Listing drive identifiers

An NTFS file system cannot be mounted by DOS and, therefore, does not have a drive letter assigned by DOS. Use the info or diskinfo command to list the drive identifiers that are assigned by OmniFS on a computer.

In all cases, the characters :\ distinguish the volume identifier from the path name.

For example, the output of c:\>omnifs info might look like the following:

```
Disk:     1        (95.42GB)    M:[Maxtor 4 G100H5 GAK8]
                                S:[G5001MGF]

          1.1      (87.89GB)    [C:\] Active Volume NTFS
                                l:[Rasfline] Primary

                   (7.53GB)     Unused Space Primary

Disk:     2        (3.01GB)     M:[QUANTUM FIREBALL
                                EX3 A0A.] S:[673826342323]

          2.1      (55.09MB)    Active Volume EXT2 Primary

          2.2      (2.95GB)     [E:\] Volume FAT32 Primary

                   (3.94MB)     Unused Space Primary
```

The output provides additional information that is required to address partitions by the physical arrangement on the drives. Volume labels can also be used. To copy a file from the NTFS partition to the FAT32 partition in the example above, you can use the following syntax:

```
omnifs copy Rasfline:\test\data.txt 2.2:\test\data.txt
```

OmniFS operations

The supported OmniFS operations are as follows:

- Attrib
- Copy
- Rename
- Delete
- Deltree
- Dir
- Info
- Help
- Version
- Mkdir

Commands are not case sensitive.

Setting the attribute for a file

The syntax for the attrib command is as follows:

```
attrib [+r][-r][+s][-s][+h][-h][+w][-w][+x][-x] <source>
```

Table 25-3 lists the attributes. Some attributes are not available for some file systems.

Table 25-3 Attribute descriptions

Attribute	Description
r	Readable
s	System
h	Hidden
w	Writable
x	Executable

You must set the source argument as an absolute path. This command sets or clears the file attributes to read only, system or hidden.

Copying files and directories

The syntax for the copy command is as follows:

```
copy <source> <destination>
```

Both the source and destination arguments must be specified as absolute paths.

For example, as follows:

Copy a file from a volume that is accessible to the current operating system to a folder test on a volume that is inaccessible to it.	`copy a:\temp\test.txt 2:1\user\data.txt`
Copy a file from a volume that is inaccessible to the current operating system to a volume that is accessible to it.	`copy 2:1\user\data.txt a:\temp\test.txt`

In both examples, the absolute path to the files must be valid.

If the source argument points to a directory, the copy operation copies all of the files and subdirectories from the source location to the destination location. In this case, the destination argument must point to a valid directory. The last portion of the destination path is created if required.

If the first argument points to a file and the second argument points to a directory, the file is created with the same name as the source file in the destination directory.

Renaming files and folders

The syntax for the rename command is as follows:

```
rename <source> <destination>
```

Both the source and destination arguments must be specified. The source argument must be specified as an absolute path, and the destination argument must contain the new name only. To move the file or folder to a new location use the copy command.

For example:

```
rename 2:1\user\data.txt "my data.txt"
```

This renames 2:1\user\data.txt to 2:1\user\ my data.txt.

The following operation is illegal because the destination argument contains a location:

```
rename 2:1\user\data.txt 2:1\temp\"my data.txt"
```

Deleting a file

The syntax for the delete command is as follows:

```
delete <source>
```

The source argument must be specified as an absolute path, and the path must be valid. No wildcard characters are accepted.

For example:

```
delete 2:1\user\data.txt
```

A directory can be deleted only if it is empty.

Deleting a folder

The syntax for the deltree command is as follows:

```
deltree <source>
```

This command is similar to delete, but the source is a directory. The contents of the directory, including all subdirectories, are deleted before the directory is deleted.

Listing a folder

The syntax for the directory listing command is as follows:

```
dir <source>
```

The source argument must be specified as an absolute path, and the path must be valid.

For example:

```
dir 2:1\user
```

The output is similar to that of the 4Dos dir command.

Listing all volumes on a computer

The syntax for the info command is as follows:

```
info
```

The info operation has no parameters, and outputs the list of all the volumes that OmniFS is able to detect on the computer, regardless of whether they are recognizable by the current operating system.

Listing the commands

The syntax for the help command is as follows:

```
help
```

The help command lists the OmniFS commands.

Displaying the OmniFS version and copyright

The syntax for the version command is as follows:

```
version
```

This command displays the OmniFS version number and copyright.

Creating a directory

The syntax for the mkdir command is as follows:

```
mkdir <destination>
```

This command creates a directory. The destination argument must include an absolute path, and all components of the path except for the last directory must exist.

For example:

```
mkdir 2:1\user\test
```

The directory 2:1\user must already exist.

Using OmniFS to recover files

If a Clone task has failed on a client computer and the computer cannot start in Windows, you can use OmniFS to do a directory listing of preserved files in the File Preservation Metadata File and to copy the files to other locations.

Table 25-4 displays the formats that you can use for designating drives.

Table 25-4 Designating drives formats

Format	Example
Format c_drive when the origin partition was a FAT partition accessible from DOS.	`omnifs dir pf:\e_drive\data`

Table 25-4 Designating drives formats *(continued)*

Format	Example
Format disk_1\partition_2 when the origin partition was NTFS or hidden FAT.	`omnifs dir pf:\disk_1\partition_2\data`

Table 25-5 lists the commands you can use for recovering files. No other OmniFS commands are supported for use with the File Preservation Metadata File.

Table 25-5 OmniFS recovery commands

Command line	Description
omnifs dir pf:\c_drive\path	Displays a directory listing from the File Preservation Metadata File of the preserved files if the File Preservation Metadata File is in the current directory. If a path is not included, a full listing is displayed. The drive must be included in the command, in the format c_drive or e_drive. For example, omnifs dir “pf:\c_drive\My Documents” Displays all preserved files from c:\My Documents.
omnifs dir pf:\c:\recovery:\c_drive\path	Displays a directory listing from the File Preservation Metadata File of the preserved files if the File Preservation Metadata File is not in the current directory. If a path is not included, a full listing is displayed. The drive must be included in the command, in the format c_drive or e_drive. For example, omnifs dir pf:\c:\recovery:\c_drive\Data Displays all preserved files from c:\Data from the File Preservation Metadata File, which is located in c:\recovery.
omnifs copy pf:\source destination	Copies all files listed in the File Preservation Metadata File to the specified location. For example, omnifs copy pf:\1.2:\ 1:1\temp Copies all files listed in the File Preservation Metadata File, which is in the root directory of the second partition of the first disk, to the temp directory on the first partition on the first disk. This example uses the notation that lets you avoid having to use a drive letter.

Table 25-5 OmniFS recovery commands *(continued)*

Command line	Description
omnifs delete pf:\source destination	Deletes specified file. For example, omnifs delete pf:\1.2:\ghost: disk_0\partition_1\recovery\extra.txt Deletes the extra.txt file in the directory recovery listed in the File Preservation Metadata File that is in the Ghost directory on the second partition on the first disk.
omnifs deltree pf:\source destination	Deletes specified directory. For example, omnifs deltree pf:\1.2:\ghost: \recovery Deletes the recovery directory and all files within the directory.

Using a script file

The script file format that is recognized by the utility uses the following rules:

- Each line in the script file begins with the operation and is followed by all of the required arguments for the nominated operation.
- When specifying operation arguments with long file names, use quotation marks (as you would on the command line).
- Empty lines in the script file will be ignored.

An example of the script file is as follows:

```
copy a:\temp\user.dat 2:1\user\profile.dat
copy a:\userdir 2:1\user\data
delete 2:1\user\data\copy.bat
rename 2:1\user\data\catalog.cpy catalog.dat
```

The user can execute the set of commands provided in the script file using the following command:

```
omnifs script scriptfs.txt
```

Each command in the script file is echoed to the screen immediately before execution.

OmniFS scenarios

OmniFS can be used from the command line with a batch file and with a script file.

Using OmniFS from the command line

In this scenario, OmniFS is executed from the command line.

The user executes a single operation. For example:

```
omnifs copy a:\temp\user.dat 2:1\user\profile.dat
```

Or, the user executes a set of commands provided in the script file. For example:

```
omnifs script scriptfs.txt
```

Following are the contents of Scriptfs.txt:

```
copy a:\temp\user.dat 2:1\user\profile.dat
copy a:\userdir 2:1\user\data
delete 2:1\user\data\copy.bat
rename 2:1\user\data\catalog.cpy catalog.dat
```

Using OmniFS with a script file

This scenario uses a batch file and a script file to copy, delete, and rename files on a volume that is not recognized by the operating system on the computer.

Following are the contents of a batch file, Goomnifs.bat:

```
omnifs script scriptfs.txt
```

Following are the contents of Scriptfs.txt:

```
copy a:\temp\user.dat 2:1\user\profile.dat
copy a:\userdir 2:1\user\data
delete 2:1\user\data\copy.bat
rename 2:1\user\data\catalog.cpy catalog.dat
```

This scenario would be more efficient than using a batch file.

Using OmniFS with a batch file

This scenario uses a batch file to copy, delete, and rename files on a volume that is not recognized by the operating system on the computer.

Following are the contents of a batch file, Goomnifs.bat:

```
omnifs copy a:\temp\user.dat 2:1\user\profile.dat
omnifs copy a:\userdir 2:1\user\data
omnifs delete 2:1\user\data\copy.bat
omnifs rename 2:1\user\data\catalog.cpy catalog.dat
```

OmniFS error handling

If an error occurs during the OmniFS operation, an error file, OmniFSer.txt, is created in the current directory.

Correcting the date and time

When you copy files from a FAT partition to an NTFS partition under DOS, there is a time-zone issue that must be addressed.

The date and time data in the FAT file system are local to the computer that the files are on. NTFS, however, uses UTC (Universal Time Coordinated) dates and times, also known as Greenwich Mean Time. Therefore, to set the date and time data correctly, OmniFS needs to know the time zone that the computer is in. This can be done either in the autoexec.bat file or from the command line, using the DOS environment variable, tz. For example:

```
set tz=aaa[+|-]h[h][bbb]
```

Where:

aaa	The abbreviation for your standard time.
[+|-]h[h][:mm]	A one-two digit signed number that indicates the difference as number of hours West of Greenwich.
bbb	The abbreviation for your daylight (summer) time zone (can be omitted).

For example:

Auckland, Wellington

```
set TZ=NST-12
```

U.S. and Canada Central Time

```
set TZ=EST+6
```

Central America

```
set TZ=CST+5
```

There is no significance in the abbreviation string other than it must be three alphanumeric characters.

Following are examples with part hour time differences:

India (Delhi)

```
set TZ=IST-5:30
```

Nepal (Katmandu)

```
set TZ=NST-5:45
```

These settings are in contrast to Windows times zones, which are the number of hours East of Greenwich, in which Auckland would be GMT+12.

Editing registry keys and values using GhRegEdit

This chapter includes the following topics:

- About GhRegEdit
- Using GhRegEdit

About GhRegEdit

GhRegEdit lets you edit Windows registry keys and values.

Table 26-1 lists the versions of GhRegEdit.

Table 26-1 GhRegEdit versions

Executable	Operating system
GhRegEdt.exe	PC-DOS, MS-DOS
ghregedit	Linux
GhRegEdit32	Windows Vista/XP/WinPE/2000
GhRegEdit64	64-bit Windows operating systems.

Note: On a 64-bit operating system, you can run GhRegEdit64.exe to manipulate the registry as normal. You can also run GhRegEdit32 on a 64-bit operating system, where it manipulates the Wow6432Node. You need to specify the "wow64_64key" to make GhRegEdit32 function like GhRegEdit64 on 64-bit operating systems.

For example: `GhRegEdit64 enumkey HKLM\Software` and `GhRegEdit32 enumkey wow64_64key HKLM\Software` will enumerate all keys under HKLM\Software, whereas `GhRegEdit32 enumkey HKLM\Software` will enumerate all keys under HKLM\Software\wow6432node.

Using GhRegEdit

You can run GhRegEdt and GhRegEdit32 from the command line or from a batch file. Before you use GhRegEdit, you should verify that the registry is not read-only.

You can use GhRegEdit32 to edit the registry without starting the operating system. You can also edit the registry as the operating system runs.

All GhRegEdt command-line switches can be run with GhRegEdit32.

Where the Windows directory is listed as a parameter, it is not optional if you are running GhRegEdit in DOS. The Windows directory is optional if you are running GhRegEdit32 in Windows, and you want to edit the current operating system registry. If you are running GhRegEdit32 in WinPE, the Windows directory is required, otherwise the WinPE registry is opened instead of the Windows registry.

If the OEM code page language is not English, then GhRegEdit does not recognize path names. In this case, you should specify the code page to use for accessing the file system. For example, on a Japanese operating system, you should use the following command:

```
ghregedt.exe -cp=932 export 1.1:\windows 1.1:\exported.reg
```

For information about the file system OEM code page, see the following registry key:

HKLM\System\CurrentControlSet\Control\Nls\ Codepage\OEMCP

Table 26-2 lists the display operations.

Table 26-2 GhRegEdit display switches

Switch	Description
-ad=image file name -addDisk=image file name	Mounts the specified vmdk, pqi, v2i, or iv2i image file to GhRegEdit ("add" the image as a disk). Once added, the disk can be used in all normal operations.
windows	Displays Windows installations. GhRegEdit looks for a Boot.ini or Msdos.sys file. If it finds one of these files, it displays the following: ■ The location of the boot.ini or msdos.sys file in the format disk.partition:\filename For example: 1.1:\Windows The Windows installation is located on the first partition of the first disk. ■ Operating systems to which the file points See "Accessing files and folders with names that contain spaces" on page 497. **Note:** The format for displaying in GhRegEdit is disk.partition, not disk:partition. To access registry files stored in an NTFS partition from within DOS, you must use the disk.partition notation because NTFS volumes do not have drive letters assigned in DOS. **Note:** The windows switch is not available on GhRegEdit32 when running on Vista, but it is available on WinPE.
help	Displays a help file listing command-line switches.

Table 26-3 lists the import and export switches.

Table 26-3 GhRegEdit import and export switches

Switch	Description
import [windowsdir] filename	Imports a registry import file as follows: ■ Windowsdir is the location of the Windows directory For example, 1.1:\Windows. ■ Filename is the name and location of the .reg file.

Table 26-3 GhRegEdit import and export switches *(continued)*

Switch	Description
export [windowsdir] filename	Exports the entire registry as follows: ■ Windowsdir is the location of the Windows directory. For example, 1.1:\Windows. ■ Filename is the name and location of the .reg file.

Key operations switches must include the hive and can only operate on the local computer (HKEY_LOCAL_MACHINE) or the local user (HKEY_USERS). HKLM and HKU can be used as shorthand for HKEY_LOCAL_MACHINE and HKEY_USERS respectively.

Table 26-4 lists the key operations switches.

Table 26-4 GhRegEdit key switches

Switch	Description
addkey [windowsdir] key	Adds the specified key to the registry as follows: ■ Windowsdir is the location of the Windows directory. For example, 1.1:\Windows. ■ Key is the name and location of the key to be set. For example: `ghregedt addkey 1.1:\Windows HKEY_LOCAL_MACHINE\Software\MyTestApp`
delkey [windowsdir] key	Deletes the specified key from the registry as follows: ■ Windowsdir is the location of the Windows directory. For example, 1.1:\Windows. ■ Key is the name and location of the key to be deleted. For example: `ghregedt delkey 1.1:\Windows HKEY_LOCAL_MACHINE\Software\MyTestApp`

Table 26-4 GhRegEdit key switches *(continued)*

Switch	Description
enumkey [windowsdir] key	Enumerates the subkeys for the specified key as follows: ■ Windowsdir is the location of the Windows directory. For example, 1.1:\Windows. ■ Key is the name and location of the key. For example: `ghregedt enumkey 1.1:\Windows HKEY_LOCAL_MACHINE\Software`
export [windowsdir] filename key	Exports the key with subkeys as follows: ■ Windowsdir is the location of the Windows directory. For example, 1.1:\Windows. ■ Filename is the name and location of the .reg file. ■ Key is the name and location of the key to be exported.

Table 26-5 lists the value switches.

Table 26-5 GhRegEdit value switches

Switch	Description

addvalue [windowsdir] key [value] type data	Modifies the specified value as follows:
	■ Windowsdir is the location of the Windows directory.
	For example, 1.1:\WINNT.
	■ Key is the name and location of the key to be modified.
	■ Value is the name of the value to be modified.
	If value is not specified then the operation executes on the default value.
	■ Type is the type of the value to be modified.
	Type can be any supported by Windows, for example, REG_SZ, REG_DWORD, REG_BINARY.
	■ Data is the data to be set for the value.
	For example:
	`ghregedt addvalue 1.1:\Windows HKEY_LOCAL_MACHINE\Software\MyTestApp REG_SZ "This is my test app"`
	If you add a value of type REG_MULTI_SZ (multiple strings), you must use the following syntax:
	`addvalue [WINDOWSDIR] KEY [VALUE] TYPE [ESC] DATA`
	The [ESC] optional parameter represents escape sequence. It is used in DATA to mark the end of one string and the beginning of another. You must always use the [ESC] parameter when you add values of type REG_MULTI_SZ. You must always terminate DATA with [ESC].
	For example:
	`addvalue`
	`1.1:\WINNT HKEY_LOCAL_MACHINE\Software\Test`
	`TestValue REG_MULTI_SZ`
	`:: "First string"::"Second string"::"Third string"::`

Table 26-5 GhRegEdit value switches *(continued)*

Switch	Description
delvalue [windowsdir] key value	Deletes the specified value as follows: ■ Windowsdir is the location of the Windows directory. For example, 1.1:\Windows. ■ Key is the name and location of the key to be modified. ■ Value is the name of the value to be modified. If value is not specified, then the operation executes on the default value. For example, `ghregedt delvalue 1.1:\Windows HKEY_LOCAL_MACHINE\Software\MyTestApp Version`
enumvalue [windowsdir] key	Enumerates the specified key's value as follows: ■ Windowsdir is the location of the Windows directory. For example, 1.1:\Windows. ■ Key is the name and location of the key to be modified. For example, `ghregedt enumvalue 1.1:\Windows HKEY_LOCAL_MACHINE\Software\MyTestApp`

Chapter 27

Running DeployAnywhere from the command line

This chapter includes the following topics:

Running DeployAnywhere from the command line

The Deploy Anywhere feature lets you retarget an image to suit a computer that has different hardware from the model computer from which the image was created. This lets you deploy a generic image to a range of different computers and perform a retargeting of the computers, rather than requiring a separate image for each hardware set.

If you want to use DeployAnywhere outside the managed environment, you can run the DeployAnywhere executable, `ghDplyAw32.exe`, from the command line. The executable is located in the same folder as the Ghost standard tools.

When you use ghDplyAw32.exe you need to do the following:

- Firstly, evaluate the target volume to verify that the necessary drivers are available.
  If all of the required drivers are available, the evaluation step returns "Success".
  See "Evaluating the target volume" on page 516.
- Retarget the image. You should perform this step only after the evaluation step has verified that all the necessary drivers are available.
  See "Retargeting the image" on page 517.

Table 27-1 describes the GhDplyAw32.exe command line switches.

Table 27-1 ghDplyAw32.exe command line switches

Switch	Description
/target	The Windows volume to scan. For example, C: or 1.1:. If necessary, you can determine this by using GhConfig32 with the /findactivewindows switch.
/eval	Performs the evaluation step. When this switch is excluded, the retargeting step is performed. **Note:** Do not exclude this switch until after you have performed the evaluation step and verified that all of the necessary drivers are available. Attempting to retarget a computer with missing drivers may corrupt the Windows volume.
/ddb	The location of the DeployAnywhere driver database, if you want to use it. If you exclude this switch, ghDplyAw32.exe evaluates only the drivers that are available on the target volume. If you include this switch in the evaluation step, you must also include it in the retargeting step. If you create a boot package using Ghost Boot Wizard, you can include the DeployAnywhere driver database with the image. Alternatively, you can copy it from your Ghost installation (C:\Documents and Settings\All Users\Application Data\Symantec\Ghost\Template) to the appropriate media. If you want, you can create your own driver database by copying a subset of the drivers from the DeployAnywhere driver database, and use it with this switch. However, if you need to add new drivers to the database, you need to do so using the Ghost Boot Wizard. This operates only on the DeployAnywhere driver database.

Note: ghDplyAw32.exe may require GhConfig32.exe to perform some tasks. You should ensure that GhConfig32.exe is in the same directory as ghDplyAw32.exe before you run DeployAnywhere from the command line.

Evaluating the target volume

When you evaluate the target volume, `ghDplyAw32.exe` searches for the drivers that are required to boot the OS installation on the target computer's hardware. If any of the required drivers are not available, a list of missing drivers is returned. The list is also available in the `ghDplyAw.txt` file.

You need to ensure that the missing drivers are available in the DeployAnywhere driver database, and then run `ghDplyAw32.exe` again. You use the Ghost Boot Wizard to add new drivers to the DeployAnywhere driver database.

If all of the required drivers are available, the evaluation step returns "Success".

To perform the evaluation step, use the following command line:

```
ghDplyAw32.exe /target=[Windows disk] /eval /ddb=[DeployAnywhere
driver database location]
```

Retargeting the image

When the evaluation step has verified that all the necessary drivers are available, you can retarget the image. The retargeting step installs the appropriate drivers and performs other necessary configuration tasks.

To perform the retargeting step, use the following command line:

```
ghDplyAw32.exe /target=[Windows disk] /ddb=[DeployAnywhere driver
database location]
```

Section 9

Appendixes

Appendix A

Command-line switches

This appendix includes the following topics:

About Symantec Ghost switches

Symantec Ghost can be run in the following ways:

- Interactively with no command-line switches
- Interactively with selected switches
- Automated in batch files (batch mode)

The Symantec Ghost command-line switches are used to alter Symantec Ghost behavior and automate procedures.

A hyphen (-) or a slash (/) must precede all switches except @filename. Switches are not case sensitive.

If you are adding switches from the Advanced Options dialog box, some of the switches, for example the -clone switch, are not applicable to your task. Because you are already performing a backup, restore, or clone operation, the -clone switch is redundant.

Listing command-line switches

The Ghost switches can be listed in the command-line.

To list Symantec Ghost command-line switches

◆ In the Ghost directory, type one of the following:

- ghost.exe -h
- ghost.exe -?

Command-line switches

This section describes the command-line switches that you can use with Ghost. In most cases, these switches apply to all versions of the Ghost executable. Any exceptions are noted in the switch description.

@filename

@filename specifies a file that contains additional command-line switches that Symantec Ghost should read. Filename indicates the path and file name of the command-line switch file. The command-line switch file can include any Symantec Ghost command-line switch. The Symantec Ghost command-line switch file must be a text file with each switch on a separate line. This lets you exceed the DOS command-line limit of 150 characters.

For example:

```
ghost.exe @ghswitch.txt
```

For this command-line switch, the Ghswitch.txt file reads:

-clone,mode=pcreate,src=1:2,dst=g:\part2.gho

-fcr

-sure

-ad=image file name

-addDisk=image file name

Mounts the specified vmdk, pqi, v2i, or iv2i image file ("add" the image as a disk). Once added, a vmdk disk can be used in all normal operations, and pqi, v2i, or iv2i disks are mounted as read-only.

-afile=filename

Replaces the default abort error log file name, Ghosterr.txt, with the directory and file given in filename.

-align = chs

-align = 1mb

Lets you override the way in which the partitions are aligned when an individual partition or disk full of partitions is restored. This switch aligns the partition to the boundary as follows:

- CHS: Aligns to a track or cylinder boundary
- 1MB: Aligns with a boundary of 1 MB

By default, a partition is aligned on the destination computer as it was on the source computer.

Note: The 1MB alignment option supports Windows Vista.

-auto

Automatically names spanned image files during creation. Using this switch avoids the user prompt that asks for confirmation of the next destination location for the remainder of the image file that is being restored.

This switch is the default behavior for Symantec Ghost.

-batch

Batch mode switch. Prevents abort messages from waiting for user acknowledgment and removes user interaction prompts. The return value of Ghost.exe must be checked to identify whether the operation was successful. Symantec Ghost returns 0 on success and 1 or higher on failure or error.

See “Batch file example” on page 547.

-bfc

Handles bad FAT clusters when writing to disk. If this switch is set and the target partition is FAT, Symantec Ghost checks for and works around bad sectors, and all free sectors are verified.

This option may slow Symantec Ghost operation substantially.

-blind

Prevents any GUI display. The blind switch must be used with switches that do not require any user input, for example, the clone switch. Using this switch lets you execute Ghost operations on a computer with no video adapter.

-bootcd

When writing an image directly to a CD/DVD writer, makes the CD/DVD bootable. You need a bootable floppy disk in drive A. If you use the -sure switch with -bootcd and a floppy disk is not in drive A, then a non-bootable CD/DVD is created.

-buffersize=x

Ghost creates an image file using a buffer of size x where x = number of KB. The default size of the buffer is automatically calculated by Symantec Ghost. The buffersize switch lets you override this size. You can set the buffer size value from 1 to 32.

-chkimg,filename

Checks the integrity of the image file indicated by filename.

-clone

Ghost.exe operation switch. This switch allows automation of Ghost.exe operations and has a series of arguments that define the operation parameters.

See “Using the clone switch” on page 539.

-cns

Reverts the naming of spanned files to the system used by versions of Symantec Ghost prior to Symantec Ghost 6.5. If this switch is not used, then the naming of spanned files conforms to Microsoft application guidelines. You do not need to use this switch when reading an existing file. Use this switch when the first five characters in a file name must be unique.

Note: Symantec Ghost supports long file names.

Table A-1 lists some examples of how spanned files are named.

Table A-1 Spanned file naming examples

With -cns	Without -cns
Filename.gho	Filename.gho
Filename.001	Filen001.ghs
Filename.002	Filen002.ghs

-CRC32

The -CRC32 switch lists the files on a disk or partition or creates an image file with CRC values and then verifies the list against the original or a copy. The purpose is to allow both quick listing of the contents of an image file and verification that a disk created by Symantec Ghost contains the same files as the original.

See "Using the -CRC32 switch" on page 548.

-crcignore

Ignores CRC errors. CRC errors indicate data corruption. This switch overrides CRC error detection and may allow a corrupted image file to be used. Using this switch leaves the corrupted files in an unknown state. You can use this switch to help you extract files from a corrupted image file.

-cvtarea

Creates a file, Cvtarea.tmp, that is the location of the MFT when the FAT32 partition is converted to NTFS. This switch operates in a similar manner to the cvtarea program that Microsoft provides in Deploy.cab on the Windows XP installation CD.

For more information, see the Microsoft Web site:

http://www.microsoft.com/whdc/system/winpreinst/ntfs-preinstall.mspx

The file is created in the root directory of the partition during a partition or disk restore and is created as a contiguous space on the disk. The largest size allowed is 4 GB. If the file is larger than this, it is truncated to 4 GB.

The syntax for this switch is as follows:

```
-cvtarea,filename=xxx,size=yyy{%disk,%free,KB,MB,GB},
firstcluster=zzz{%disk,%free,KB,MB,GB}
```

The default settings are as follows:

filename	cvtarea.tmp
size	12%disk
firstcluster	1|3 GB|33%disk Defaults to the following: ■ 1/3 of the partition size if the partition size is less than 2 GB ■ 1 GB if the partition size is less than 6 GB ■ 3 GB if the partition size is equal to or greater than 6 GB

-dd

Dumps disk metrics information to the dump log file, Ghststat.txt. The file location can be altered using the -dfile=filename switch.

-dfile=filename

Changes the path and file name of the dump log file created using the -dd switch.

-disabledrive=drive

The specified drive is not available in the file requestor dialogs. You can use this switch with Ghost.exe only.

-dl=number

Specifies the number of hard disks present. Valid numbers are between 1 and 8. This may help when the BIOS does not report the number of drives correctly.

-dlist=drives

Specifies a list of drives to search for span files. If a span file cannot be found, then the drive letters in dlist are substituted one by one to look for the file on other drives.

For example, the command ghost -dlist=CDEFG instructs Symantec Ghost to look for files on C, D, E, F, and G drives. The path remains the same.

-f32

Lets Symantec Ghost convert all FAT16 volumes to FAT32 volumes when the destination partition to convert is larger than 256 MB in size. Ensure that the installed operating systems can access the volumes that will be converted to support FAT32.

-f64

Lets Symantec Ghost resize FAT16 partitions to be larger than 2047 MB using 64 KB clusters. This is only supported by Windows 2000. Do not use on computers with other operating systems.

-fatlimit

Limits the size of FAT16 partitions to 2047 MB.

-fcr

Creates a CRC32 file, Ghost.crc, while creating an image file.

See "Using the -CRC32 switch" on page 548.

-fdsp

Preserves the signature bytes on the destination disk when performing a disk-to-disk or image-to-disk cloning operation.

-fdsz

Clears the signature bytes on the destination disk. This is the default for disk-to-disk and image-to-disk operations.

-femax

When an extended partition is created in a disk-to-disk or image-to-disk operation, the femax switch ensures that the extended partition takes up all free space.

-fgpt

Forces the disk to restore to a GPT disk.

-ffatid

Forces the FAT partition id. This switch changes the partition id to the recommended partition id for the FAT partition within the destination image file or the destination partition table. This switch only takes effect if the source is a disk or partition, not an image file.

For example, if you are cloning a partition of type 0xA0 (some unknown partition id), and Symantec Ghost sees it as a valid FATx (FAT12/FAT16/FAT32) partition, then the partition id is changed from 0xA0 to FATx.

This was default Symantec Ghost behavior before Symantec Ghost 7.5. This switch allows for backward compatibility.

-ffi

Prefers the use of direct IDE access for IDE hard-disk operations.

-ffs

Prefers the use of direct ASPI/SCSI disk access for SCSI hard-disk operations.

-ffx

Prefers the use of Extended Interrupt 13h disk access for hard-disk operations.

-finger

Shows the fingerprint details written on a hard disk created by Symantec Ghost. The fingerprint details include the process used to create the disk or partition and the time, date, and disk on which the operation was performed.

Reports the presence of a Ghost fingerprint with the following return code:

- If any of the disks that Ghost can access have a fingerprint: 1
- If none of the disks that Ghost can access have a fingerprint: 0
- If the computer has no disk or none of the disks can be accessed: 2

-fis

Uses all available disk space when creating partitions. By default, Symantec Ghost often leaves a small amount of free space at the end of the disk. Because partitions must be aligned to cylinder boundaries, Symantec Ghost may leave up to 8 MB free even when -fis is specified.

-fmbr

Forces the disk to restore to a MBR-based disk.

-fmount

Force mounting of volumes even if they have not been cleanly unmounted.

-fni

Disables direct IDE access support for IDE hard-disk operations.

-fns

Disables direct ASPI/SCSI access support for SCSI hard-disk operations.

-fnx

Disables extended INT13 support for hard-disk operations.

-force1394

Forces FireWire support to start, even when the FireWire controller is being run by something else. The -force1394 switch attempts to take over the FireWire Host Controller. To enable native BIOS support you must restart the computer.

Note the following:

- Use this switch with caution.
- Avoid using the force1394 switch to take over a FireWire controller from a driver, for example, Iomega FireWire drivers. You may encounter problems if you do this.

-forceusb

Forces USB support to start, even when the USB controller is being run by something else. The -forceusb switch attempts to take over the USB Host Controller and then attempts to return it to the previous state once the Ghost operation is complete. This works for controllers as follows:

- EHCI controllers with BIOS support are taken over and then returned to the BIOS.
- UHCI controllers with BIOS support are taken over and then returned to the BIOS.
  For example, the keyboard is returned after the Ghost operation is finished.
- OHCI controllers with BIOS support are taken over but not returned to the BIOS.

Note the following:

- Use this switch with caution.
- Avoid using the forceusb switch to take over a USB controller from a driver, for example, the Ghost peer-to-peer USB driver. You may encounter problems if you do this.

-forcevolumesnapshot

Forces an attempt to use volume SNAPSHOT on volumes in preference to standard volume locking.

-fpr

Forces destination partitions to be resized proportionally to their original size. By default, Ghost evenly distributes free space to the destination partitions based on the amount of free space that is available in each source partition. The fpr switch determines the size of the destination partitions based on the size of the source partitions.

-fro

Forces Symantec Ghost to continue cloning even if the source contains bad clusters.

-ftxp

This switch prevents Ghost from updating the transactional NTFS (TxF) Resource Manager GUIDs. You can use this switch to keep the same identity in transactions for a single computer that you are restoring from an image. The ftxp switch maintains all existing transactions in progress instead of flushing them as part of the volume GUID change.

-fx

Causes Symantec Ghost to exit to DOS or Win PE after an operation is complete. By default, Symantec Ghost prompts the user to restart or exit when the operation has finished. If Symantec Ghost is run as part of a batch file, it is sometimes useful to exit back to the DOS prompt after completion so that further batch commands are processed.

For more information, see the -rb switch.

-ghostoncd

Includes Ghost.exe on a CD/DVD when writing an image to a CD/DVD.

-h or -? or -help

Shows the Symantec Ghost command-line switch Help page.

-hasfingerprint

Reports the presence of a Ghost fingerprint with the following:

- If any of the disks that Ghost can access have a fingerprint:
  Display to screen: 1
  Return code: 1
- If none of the disks that Ghost can access have a fingerprint:
  Display to screen: 0
  Return code: 0
- If the computer has no disk or none of the disks can be accessed:
  Display to screen: unknown
  Return code: 2

The display to the screen can be interpreted by any script language that is executing Ghost. However, it is easiest to use the return value.

-ia

The image all switch forces Symantec Ghost to perform a sector-by-sector copy of all partitions. By default, when copying a partition from a disk to an image file or to another disk, Symantec Ghost examines the source partition and decides whether to copy just the files and directory structure or to do a sector-by-sector copy. If it understands the internal format of the partition, it defaults to copying the files and directory structure. Generally, this is the best option. However, if a disk has been set up with special hidden security files that are in specific positions on the partition, the only way to reproduce them accurately on the target partition is through a sector-by-sector copy. If you use this switch to create an image of a dynamic disk, then the image must be restored to a disk with identical geometry.

-ial

Forces a sector-by-sector copy of Linux partitions. Other partitions are copied normally.

-ib

The image boot switch copies the entire boot track, including the boot sector, when creating a disk image file or copying disk-to-disk. Use this switch when installed applications, such as boot-time utilities, use the boot track to store information. By default, Symantec Ghost copies only the boot sector and does not copy the remainder of the boot track. You cannot perform partition-to-partition or partition-to-image functions with the -ib switch.

-id

The image disk switch is similar to -ia (image all), but also copies the boot track, as in -ib (image boot), extended partition tables, and unpartitioned space on the disk. When looking at an image with -id, you see the unpartitioned space and extended partitions in the list of partitions. The -id switch is primarily used by law enforcement agencies that require forensic images.

When Symantec Ghost restores from an -id image, it relocates partitions to cylinder boundaries and adjusts partition tables accordingly. Head, sector, and cylinder information in partition tables is adjusted to match the geometry of the destination disk. Partitions are not resizeable. You will need an identical or larger disk than the original.

Symantec Ghost does not wipe the destination disk when restoring from an -id image. Geometry differences between disks may leave tracks on the destination disk with their previous contents.

Use the -ia (image all) switch instead of the -id switch when copying partition-to-partition or partition-to-image. An individual partition can be restored from an image created with -id.

-ignoreLVM

Disable parsing of Linux LVM volumes.

-imgdesc

Adds a single-line image file description to the image file with the following restrictions:

- Cannot include any new lines
- Cannot be used with -imgdescfile
- Must be used with the clone switch
- Clone switch mode must be create, dump, pcreate, or pdump

-imgdescfile=filename

Specifies a text file that contains an image file description to be added to the image file with the following restrictions:

- Cannot be used with -imgdesc
- Must be used with the clone switch
- Clone switch mode must be create, dump, prcreate, or pdump

-ir

The image raw switch copies the entire disk, ignoring the partition table. This is useful when a disk does not contain a partition table in the standard PC format, or you do not want partitions to be realigned to track boundaries on the destination disk. Some operating systems may not be able to access unaligned partitions. Partitions cannot be resized during restore and you need an identical or larger disk.

-ja=sessionnm

Connects to the GhostCast Server using the specified session name. Set the disk and possibly partition to be cloned on the GhostCast Server.

-jaddr=<ip_address>

Use the IP address for the GhostCast Server.

-jl:x=filename

Creates a log file to assist in diagnosing GhostCasting and TCP/IP peer-to-peer problems. The amount of information logged is set by the log level x. The log level x can be E (errors), S (statistics), W (warnings), I (information), or A (all) in increasing order of logging detail. The file name indicates the path and file name of the log to be created. In general, the error and statistic levels do not affect session performance. All other levels may reduce performance and should be used for diagnostic purposes only.

-jm=[u|d|m]

Use unicasting, direct broadcast, or multicasting.

-js=n

Sets to n the number of router hops Symantec Ghost is allowed to cross in an attempt to find the GhostCast Server. (Default is 16.)

-limitswap

Limits the Linux swap space to 2GB.

-lockinfo

Shows the type code and information stored in the BIOS or the Pentium III Processor ID.

Table A-2 shows some examples of type codes and provides example values.

Table A-2 Lockinfo type codes

Type	Based On	Value
M	Manufacturer	Compaq
P	Product name	Deskpro EN Series SFF
V	Version	Award Software
S	Serial number	H925CKH60020
U	UUID	2DA9379B4707D31185E8C800A4F232BC
C	M&P combined	Compaq Deskpro EN Series SFF
I	PIII ID	0000067200028E72A6994A20

-locktype= Type

Lets you lock an image file for use with a specific set of computers defined by the type chosen and the source computer.

For example, ghost -locktype=P creates an image that can be used only on systems that have the same product name type as the source computer.

On computers with multiple processors, the processorID bios lock option does not work as intended when running Ghost32.exe. In this situation, do not create or restore images with the -locktype parameter set to I. Other -locktype values work as intended.

-lpm

The LPT master mode switch causes Symantec Ghost to automatically go into LPT master mode and is the equivalent of selecting LPT Master from the main menu.

-lps

The LPT slave mode switch causes Symantec Ghost to automatically go into LPT slave mode and is the equivalent of selecting LPT Slave from the main menu.

-mcyl=[1022|1023]

Forces the cylinder value to either 1022 or 1023 when the cylinder value is insufficient to address the whole partition.

This switch works in DOS only.

When Ghost restores the partitions on an MBR disk, it initializes the starting sector, the sector count, and ending sector of the partition. Ghost stores the starting sector and ending sector in an MBR disk as a cylinder, head, and sector address. Ghost also stores an absolute start sector and count. The cylinder value has a maximum value of 1023. However, the cylinder maximum of 1023 is often insufficient to represent the size of the partition. When the cylinder maximum is insufficient, the cylinder is set to a predetermined value. Ghost sets the cylinder maximum to 1022 for FAT partitions and 1023 for other partitions. For some tools, the cylinder value must be set specifically for the tool to recognize that it is insufficient.

-nfwm

Turn off firewall manipulation.

This switch applies to Vista and Linux only.

-noauto

Disables the automatic naming of spanned image files during creation. The user is prompted for confirmation of the next destination location for the remainder of the image file that is being restored.

-noautoskip

Includes the hibernation and skip files in the image file. These files are excluded by default.

See “Hibernation and swap files” on page 321.

-nofile

Disables the Image File Selection dialog box. Useful when opening directories with large numbers of files and slow links.

-noide

Disables access to IDE devices. This is equivalent to -fni for IDE disks, but noide also affects ATAPI CD writers, tape drives, and other IDE devices.

-noindex

Prevents Symantec Ghost from creating an index when creating an image file. This slightly reduces the size of the image file and saves memory, but Ghost Explorer is much slower in reading the image file. This switch is useful if you are saving an image file from a large disk with very little memory.

-nolilo

Does not attempt to patch the LILO or GRUB boot loader after a clone. If you use the -nolilo switch, you can restart your computer from a floppy disk or CD after a clone and then run /sbin/lilo or the GRUB install script as the root user to reinstall the boot loader.

-noOSdisk

Prevents Ghost from creating the virtual OS volumes disk.

By default Ghost creates a virtual disk to represent each volume (drive letter or Linux device) available from the OS. This allows you to create and restore images of volumes that Ghost cannot otherwise enumerate on a hard disk, for example, virtual disk partitions mounted as drive letters.

-noOSlayout

Prevents Ghost from updating the OS after a restore.

By default, Ghost passes information about the restore to Windows, which then makes updates. This switch disables that function and preserves the disk exactly as restored.

-noscsi

Disables access to SCSI devices using ASPI. This is equivalent to -fns for SCSI disks, but noscsi also affects SCSI CD writers, tape drives, and other SCSI devices.

-no1394

Disables FireWire

-nousb

Disables USB support.

-novolumesnapshot

Prevents Ghost from creating a volume SNAPSHOT.

-ntc-

Disables NTFS contiguous run allocation.

-ntchkdsk

Sets the CHKDSK bit set on a copied NTFS volume. This causes Windows NT to check the integrity of the volume when it is started.

-ntd

Enables NTFS internal diagnostic checking.

-ntexact

Attempts to arrange the restored NTFS volume in the same way as the source volume.

-ntic

Ignores the NTFS volume CHKDSK bit. Symantec Ghost checks the CHKDSK bit on an NTFS volume before performing operations. When Symantec Ghost indicates that the CHDSK bit is set, you should run CHKDSK on the volume to ensure that the disk is in a sound state before cloning.

-ntiid

This switch forces Symantec Ghost to ignore the partition table system ids and instead to check the partition contents when detecting NTFS file systems. This switch is useful when the system id is not set to 0x07 for partitions containing NTFS file systems. The partitions would otherwise be inefficiently imaged sector-by-sector. This switch can be used when it is necessary to image a Windows NT4 FTDisk mirrored partition.

Take care when using this switch. Do not use the -ntiid switch with volume sets and stripe sets.

To clone mirrored partitions (also known as Windows NT software RAID partitions), do the following:

1. With Windows NT disk administrator, break the mirror set.
2. Using the -ntiid switch, clone one of the mirror partitions.
3. Resize as desired. Partitions can only be resized by Symantec Ghost during a disk operation. When performing a partition operation, the target partition size must already be established.
4. After cloning, recreate the mirror set using the Windows NT disk administrator. The disk administrator creates the partitions in the mirror set.

-ntil

Ignores NTFS log file check (inconsistent volume).

-or

The override switch allows the override of internal space and integrity checks and lets you put a very big image into a small partition. The operation fails if it is unable to write to the limited partition size. This switch lets you override spanning, which fails if there is limited space. Avoid using this switch.

-pfile

Saves the File Preservation Metadata File that holds the location of preserved files to a specified location. By default, it is saved to the current directory.

For example:

```
ghost - pfile=c:\pathname
```

Where pathname is the directory for the File Preservation Metadata File.

-pmbr

Specifies that the master boot record of the destination disk is to be preserved when performing a disk-to-disk or image-to-disk operation.

-prefghst

If Symantec Ghost has a choice, it attempts to use internal Ghost file system access as opposed to using the operating system for file system access.

This switch is intended for use under instruction from Symantec Technical Support when troubleshooting.

-prefos

If Symantec Ghost has a choice, it attempts to use the operating system for file system access as opposed to using the internal Ghost file system access.

This switch is intended for use under instruction from Symantec Technical Support when troubleshooting.

-preserve

Preserves the specified files. The task fails if the specified files do not exist. To preserve files or directories other than the image file, the syntax is as follows:

```
-preserve=filepath[=newpath] [,filepath[=newpath]...]
```

Each filepath can refer to an individual file or a directory. All files and subdirectories of a specified directory are preserved. If a file does not exist, then the restore fails. After a Clone step in a task, all preserved files are added back to the partition that is specified by the-preservedest=n switch. Ghost renames them to newpath where it is specified. You must use -preserve with -preservedest.

If you are running Ghost from a CD, you must use the -pfile switch with the -preserve command. You also must specify a writeable location for the file-preservation metadata file. Otherwise, Ghost tries to write the file-preservation metadata file to the CD. Because the CD is read-only. the data cannot be written, and the process fails.

-preservedest=n

Where n is the number of the partition relative to the destination disk, not relative to the partitions being restored. Specifies the partition to which files specified with the preserve switch are restored.

-preservedimage
deleteafterclone

Deletes a preserved image file once the restore has completed successfully. This switch overrides the default, which is to retain the preserved image file.

-preserveifexists

Preserves the specified files if they exist. The task does not fail if the specified files do not exist. To preserve files or directories other than the image file, the syntax is as follows:

```
-preserveifexists=filepath[=newpath] [,filepath[=newpath]...]
```

Each filepath can refer to an individual file or a directory. All files and subdirectories of a specified directory are preserved. If a file does not exist, then the restore fails. After a Clone step in a task, all preserved files are added back to the destination specified by the -preservedest=n switch, renaming them to newpath where specified. You must use the -preserveifexists switch with -preservedest.

-pwd and -pwd=x

Specifies that password protection be used when creating an image file.

x indicates the password for the image file. If no password is given in the switch, Symantec Ghost prompts for one. You can enter a maximum of 10 alphanumeric characters.

-quiet

The quiet mode switch disables status updates and user intervention.

-rb

Restarts after finishing a restore or copy. After completing a restore or copy operation, the target computer must be restarted so that the operating system can restore the new disk/partition information. Normally, Symantec Ghost prompts the user to restart or exit. The -rb switch tells Symantec Ghost to restart automatically after it completes the restore or copy. This is useful when automating Symantec Ghost in a batch command file.

For more information, see the -fx switch.

-recover

Sets the default to recover preserved files if a previous restore has failed and the File Preservation Metadata File still exists. If this switch is not used, the default is set to abort.

-script

Allows you to specify a series of commands (one per line) that Symantec Ghost will execute in sequential order.

For example:

```
ghost -script=script.txt
```

Following is an example of script.txt:

```
-clone,mode=create,src=2,dst=1:1\drv2.gho
-chkimg,1:1\drv2.gho
-clone,mode=create,src=2,dst=c:\part2.gho
-chkimg,c:\part2.gho
```

In this example 1:1 is equivalent to c:\.

-skip=x

The skip file switch causes Symantec Ghost to exclude the indicated files during a create or restore operation. A skip entry can specify a single file, a directory, or multiple files using the * wildcard. File names must be given in short file name format and all path names are absolute. Only FAT system files can be skipped. It is not possible to skip files on NTFS or other file systems. The skip switch may only be included in the command line once. To specify multiple skip entries, they must be included in a text file indicated using -skip=@skipfile. The format of the skip text file, skipfile, matches the format used with the CRC32 vexcept option.

For example, as follows:

- `-skip=\windows\user.dll`
  Skips the file User.dll in the Windows directory.
- `-skip=*\readme.txt`
  Skips any file called Readme.txt in any directory.
- `-skip=\ghost\*.dll`
  Skips any file ending with .dll in the Ghost directory.
- `-skip=\progra~1\`
  Skips the program files directory (note the short file name).
- `-skip=@skipfile.txt`
  Skips files as outlined in Skipfile.txt. For example:

```
*\*.tmt
[partition:1]
\windows\
*\*.exe
[Partition:2]
*\*me.txt
```

This Skipfile.txt file would skip all *.tmt files on any partition, the Windows directory, all *.exe files on the first partition, and any file that ends with me.txt on the second partition.

When using the skip switch with a wildcard extension, only those files with an extension are skipped. For example:

-skip=asdf.* skips asdf.txt but does not skip asdf.

-span

Enables spanning of image files across volumes.

Do not use this switch if you are running Ghost.exe to write an image file directly to a CD-R/RW. Ghost.exe automatically spans CD-R/RW disks if required.

-split=x

Splits image file into x MB spans. Use this switch to create a forced-size volume set. For example, if you want to force smaller image files from a 1024-MB drive, you could specify 200-MB segments.

For example:

```
ghost.exe -split=200
```

This divides the image into 200-MB segments.

If this switch is not used then an image is split at 2 GB in the following operations:

- GhostCast
- Peer-to-peer
- Creating an image on a mapped-network drive

If the operation runs locally on a FAT partition, then the image splits at 4 GB.

If this switch is explicitly set to 0, the image does not split.

-sure

Use the -sure switch in conjunction with -clone to avoid being prompted with the final question “Proceed with disk clone - destination drive will be overwritten?” This command is useful in batch mode.

-sze

Sets the size for the destination partitions for either a disk restore or disk copy operation. When numbering partitions in the -sze switch, do not include the hidden Ghost partition. This switch is intended to be used in the Additional command line in the Console. All functionality of -sze switches are supported.

See “Setting a destination size for the clone switch” on page 544.

-szee

Forces Symantec Ghost to keep the sizes of all destination partitions the same size as in the source partition (no resizing).

This switch can be used with or without the -clone switch.

See “Setting a destination size for the clone switch” on page 544.

-szef

Forces Symantec Ghost to keep the sizes of all destination partitions, except for the first one, the same size as in the source partition. The first partition uses the remaining disk space.

This switch can be used with or without the -clone switch.

See “Setting a destination size for the clone switch” on page 544.

-szel

Forces Symantec Ghost to keep the sizes of all destination partitions, except for the last one, the same size as in the source partition. The last partition uses the remaining disk space.

This switch can be used with or without the -clone switch.

See “Setting a destination size for the clone switch” on page 544.

-tapebuffered

Default tape mode. Sets the ASPI driver to report a read/write as successful as soon as the data has been transferred to memory. Useful when using older or unreliable tape devices or sequential media.

-tapeeject

Forces Symantec Ghost to eject the tape following a tape operation. If the tape drive does not support remote ejection, you must eject and insert the tape manually before further use. Earlier versions ejected the tape by default. By default, Symantec Ghost does not eject the tape. It rewinds the tape before exiting to DOS.

-tapebsize=x

Specifies the tape block size in units of 512 bytes, where x is a number between 1 and 128.

-tapespeed=x

Allows control of tape speed, where x is 0 to F. 0 is the default. 1 to F increases tape speed. Only use this when the tape does not work correctly at the speed used by Symantec Ghost.

-tapeunbuffered

Sets the ASPI driver to report a read/write as successful only when the data has been transferred to the tape drive. This can occur before the data is physically written to the medium.

-tcpm[:slave IP address]

The TCP/IP master mode switch causes Symantec Ghost to go into TCP/IP master mode automatically and is the equivalent of selecting TCP/IP Master from the main menu. The IP address of the slave computer may be specified.

See “Peer-to-peer connections” on page 552.

-tcps

The TCP/IP slave mode switch causes Symantec Ghost to go into TCP/IP slave mode automatically and is the equivalent of selecting TCP/IP Slave from the main menu.

See “Peer-to-peer connections” on page 552.

-unpreserveimage

After a failed restore, do not preserve the image file that was used on the failed restore.

-usbm

The USB master mode switch causes Symantec Ghost to go into USB master mode automatically and is the equivalent of selecting USB Master from the main menu.

See “Peer-to-peer connections” on page 552.

-usbs

The -usbs switch causes Symantec Ghost to go into USB slave mode automatically and is the equivalent of selecting USB Slave from the main menu.

See “Peer-to-peer connections” on page 552.

-vdw

If the -vdw switch is set, Symantec Ghost uses the disk's verify command to check every sector on the disk before it is written. This option may slow Symantec Ghost operation substantially.

-ver

Shows the version number of Symantec Ghost.

-vmdkType=val

When creating a virtual disk (the virtual disk is the destination of the clone), this switch specifies the type of vmdk disk to create.

The valid values are:

- sparse
- flat

-vmdkSplit

When creating a virtual disk (the virtual disk is the destination of the clone), this switch specifies the vmdk should be split into 2GB maximum extent size.

-vmdkAdatper=val

When creating a virtual disk (the virtual disk is the destination of the clone), this switch specifies the type of disk adapter for the created vmdk.

The valid values are:

- ide
- lsiLogic (scsi)
- busLogic (scsi)

Note: For SCSI adapters, choose busLogic for the Windows 2000 family or Windows XP. Choose lsiLogic for later operating systems.

-vmdkSize=val

When creating a virtual disk (the virtual disk is the destination of the clone), this switch specifies the size in MB of the of the created vmdk disk.

-z

Runs compression when saving a disk or partition to an image file. The greater the compression, the slower the transmission, as follows:

- -z or -z1: Low compression (fast transmission)
- -z2: High compression (medium transmission)
- -z3 through -z9: Higher compression (slower transmission)

See "Image files and volume spanning" on page 316.

Accessing files

Table A-3 lists the formats that you can use to access files.

Table A-3 Accessing file format

Format	Example
Drive letter	c:\My Images\image.gho

Table A-3 Accessing file format *(continued)*

Format	Example
Disk and partition This lets you specify an otherwise inaccessible file, for example, a file located on a file system not recognized by DOS, such as NTFS, or a file on a hidden partition. It provides an alternative to using drive letters.	src=1:2\image.gho In this example, Image.gho resides on an NTFS file system on the second partition of the first disk. This format cannot be used with the -afile=filename switch.

Using the clone switch

Some cloning switches for use in Ghost can be specified on the GhostCast Server.

The syntax for the clone switch is:

```
-clone,MODE={operation},SRC={source},DST={destination},
[SZE{size},SZE{size}.......]
```

Defining the type of clone command

MODE defines the type of clone command.

The syntax is as follows:

```
MODE={copy | restore | create | pcopy | prestore | pcreate}
```

Table A-4 lists the mode commands.

Table A-4 Mode commands

Switch	Action
copy	Disk-to-disk copy
restore **Note:** The load switch is replaced by the restore switch. The load switch is still fully functional and is interchangeable with restore.	File-to-disk restore

Table A-4 Mode commands *(continued)*

Switch	Action
create **Note:** The dump switch is replaced by the create switch. The dump switch is still fully functional and is interchangeable with create.	Disk-to-file backup
pcopy	Partition-to-partition copy
prestore **Note:** The pload switch is replaced by the prestore switch. The pload switch is still fully functional and is interchangeable with prestore.	File-to-partition restore
pcreate **Note:** The pdump switch is replaced by the pcreate switch. The pdump switch is still fully functional and is interchangeable with pcreate.	Partition-to-file backup (allows multipartition Ghost backup selection)

Cloning combination options

Table A-5 illustrates the possible cloning operations that you can perform.

Table A-5 Cloning operations

Mode	Source	Destination
copy	■ disk	■ disk
restore	■ file (.gho, .vmdk, .pqi, .v2i, .iv2i) ■ GhostCast Server ■ tape ■ CD-ROM ■ USB 1.1 and 2.0 Mass Storage Device ■ DVD ■ FireWire hard disk	■ disk

Table A-5 Cloning operations *(continued)*

Mode	Source	Destination
create	■ disk	■ file (.vmdk) ■ GhostCast Server ■ tape ■ CD writer ■ USB 1.1 and 2.0 Mass Storage Device ■ DVD ■ FireWire hard disk
pcopy	■ disk:partition	■ disk:partition
prestore	■ file:partition ■ GhostCast Server (no partition specified) tape:partition ■ CD:image:partition ■ USB 1.1 and 2.0 Mass Storage Device ■ FireWire hard disk	■ disk:partition
pcreate	■ disk:partition ■ partition:partition You can specify more than one partition.	■ file ■ GhostCast Server tape ■ CD writer ■ USB 1.1 and 2.0 Mass Storage Device ■ DVD ■ FireWire hard disk

Setting a source for the clone switch

The syntax for this switch is as follows:

```
SRC={disk | file | multicast | tape | cd writer }
```

SRC defines the source for the operation that is selected by the clone mode option.

Table A-6 lists the source switches.

Table A-6 Source options for cloning

Switch	Source	Explanation

disk	drive number	Source disk drive number. Numbers start at 1. For example:
		SRC=1
		A partition on a drive can also be specified. Numbers start at 1. For example:
		SRC=1:2

file	filename	The source image file name. For example: SRC= g:\source.gho A partition in an image file can also be specified. For example: SRC=g:\source.gho:2 Files can also be read from a CD-ROM drive. The following files types are supported: .gho, .vmdk, .pqi, .v2i, .iv2i. **Note:** .pqi, .v2i, and .iv2i are only available in Ghost32 with the v2idisklib.dll present.
multicast	@mcsessionname	The name of the multicast session.

tape	@MTx	The tape drive number. Numbers start at 0. For example:
		SRC=@MT0
		A partition on a tape can also be specified. For example:
		SRC=@MT0:3

CD ROM	@CDx	The CD or DVD drive number. If you have a CD reader and a CD writer, in the Ghost.exe user interface you would see @CD1 and @CD2. The number is optional if you are specifying an operation from the command line. You can specify partitions for the image stored on a CD for a restore operation. For example: SRC=@CD1:2

Table A-6 Source options for cloning *(continued)*

Switch	Source	Explanation
Preservation file	@PF	An image file that was preserved during a restore that failed. For example: ghost -recover -clone,mode=[p] load, src=@pf,...
Operating System Volumes	@OS	SRC=@OS will take an image containing all volumes that have been mounted by the operating system, enabling an image to contain volumes from multiple drives. For example: SRC=@OS:C:D clones the mounted volumes C:\ and D:\

Setting a destination for the clone switch

The syntax for this switch is as follows:

```
DST={disk | file | multicast | tape | cdwriter}
```

DST defines the destination location for the operation.

Table A-7 lists the destination options for cloning.

Table A-7 Destination options for cloning

Switch	Destination	Explanation
disk	drive	The destination disk drive number, such as DST=2. A partition on a drive can also be specified. For example: DST=2:1 To create a new partition, type a destination partition one greater than the existing number of partitions, if there is enough free space.

Table A-7 Destination options for cloning *(continued)*

Switch	Destination	Explanation
file	filename	The destination image file name. For example: DST= g:\destination.gho **Note:** The file type may be .gho or .vmdk. If the specified .vmdk file exists, Ghost treats it as a normal disk. If the vmdk file does not exist, Ghost will create it from scratch. There are additional -vmdk switches to control the creation of .vmdk files.
multicast	@mcsessionname	The name of the multicast session.
tape	@MTx	The tape drive number. Numbers start at 0. For example: DST=@MT0
cd/dvdwriter	@CDx	The CD or DVD writer drive number. Numbers start at 1. For example: DST=@CD1 If you have a CD reader and a CD writer, in the Ghost.exe user interface you would see @CD1 and @ CD2. The number is optional if specifying an operation from the command line.
Operating System Volumes	@OS:D	DST=@OS:D restores a partition to the mounted volume D:\.

Setting a destination size for the clone switch

The SZE switch sets the size of the destination partitions for either a disk restore or disk copy operation. This is optional. Multiple partition size switches are supported.

The number of size switches depends on the number of partition sizes that you want to specify. There may be none.

You can use the sze switch in the Advanced command-line options in the Console.

```
SZE{E | F | L | n={xxxxM | mmP| F | V}}
```

Table A-8 lists the destination size switches.

Table A-8 Destination size options for cloning

Switch	Explanation
n=xxxxM	Indicates that the nth destination partition is to have a size of xxxxMB (for example, SZE2=800M indicates partition two is to have 800 MB).
n=mmP	Indicates that the nth destination partition is to have a size of mm percent of the target disk. Due to partition size rounding and alignment issues, 100% physical use of disk space may not be possible.
n=F	Indicates that the nth destination partition is to remain the same size on the destination as it was on the source. This is referred to as a fixed size.
n=V	Indicates that the partition may be made bigger or smaller depending on how much disk space is available. This is the default.
E	Indicates that the sizes of all partitions remain fixed.
F	Indicates that the sizes of all partitions except the first remain fixed. The first partition uses the remaining space.
L	Indicates that the sizes of all partitions except the last remain fixed. The last partition uses the remaining space.

Examples of clone switch usage

Table A-9 describes clone switches and their functions.

Table A-9 Clone switch usage examples

Switch	Function
ghost.exe -clone,mode=copy,src=1,dst=2	Copies local disk one to local disk two.
ghost.exe -lpm -clone,mode=create,src=2,dst=c:\drive2.gho	Connects a master computer using LPT to another computer running Ghost.exe in slave mode and saves a disk image of local disk two to the remote file c:\drive2.gho. The slave computer can be started with ghost.exe -lps.
ghost.exe -clone,mode=pcopy,src=1:2,dst=2:1 -sure	Copies the second partition of local disk one to the first partition of local disk two without the final warning prompt.
ghost.exe -clone,mode=restore,src=e:\savedsk.gho,dst=1 -sure	Restores the disk image file Savedsk.gho that is held on the server drive that is mapped locally to drive E onto local disk one. Performed without the final warning prompt. This example is typical of a command line included in a batch file to automate workstation installations from a network file server.

Table A-9 Clone switch usage examples *(continued)*

Switch	Function
ghost.exe -clone,mode=pcreate,src=1:2,dst=g:\part2.gho	Saves the second partition of disk one to an image file on mapped network drive G.
ghost -clone,mode=prestore,src=g:\part2.gho:2,dst=1:2	Restores partition two from a two-partition image file on mapped drive G onto the second partition of the local disk.
ghost.exe -clone,mode=restore,src=g:\3prtdisk.gho,dst=2,sze1=60P,sze2=20P	Restores disk two from an image file and resizes the destination partitions into a 60:20:20 allocation, assuming that the image contains 3 partitions.
ghost.exe -clone,mode=copy,src=1,dst=2,sze2=F	Clones a two-partition disk and keeps the second partition on the destination disk the same size as on the source disk and lets the first partition use the remaining space, leaving no unallocated space.
ghost.exe -clone,mode=create,src=1,dst=2:3\image.gho	Saves disk one to the image file image.gho located on the third partition of the second disk. This works only if the third partition of the second disk is an NTFS file system.
ghost.exe -clone,mode=prestore,src=2:3\image.gho:5,dst=4:2	Restores the fifth partition of the image file image.gho, which is located on the third partition of the second disk, to the second partition on the fourth disk. This switch only works if the third partition on the second disk is NTFS.
ghost.exe-clone,mode=restore,src=g:\3prtdisk.gho,dst=1,sze1=450M,sze2=1599M,sze3=2047M	Restores disk one from an image file and resizes the first partition to 450 MB, the second to 1599 MB, and the third to 2047 MB.
ghost.exe -clone,mode=restore,src=g:\2prtdisk.gho,dst=1,szeL	Restores a disk from an image file and resizes the last partition to fill the remaining space.
ghost.exe -clone,src=@MCsessionname,dst=1 -sure	Restores disk one from an image file being sent from the GhostCast Server with the session name “sessionname” without the final warning prompt.
ghost.exe -clone,src=1,dst=@MCsessionname -sure	Creates an image file of disk one to an image file being created by the GhostCast Server with the session name “sessionname” without the final warning prompt.
ghost.exe -clone,mode=create,src=2:2,dst=@MT0	Creates an image file of the second partition on disk 2 onto the first tape drive.
ghost.exe -clone,mode=pcreate,src=2:1:4:6,dst=d:\part146.gho	Creates an image file with only the selected partitions. This example selects partitions 1, 4, and 6 from disk 2.

Table A-9 Clone switch usage examples *(continued)*

Switch	Function
ghost.exe -clone, mode=restore, src=VirtualMachine.vmdk,dst=1	
ghost.exe -clone, mode=prestore, src=VirtualMachine.vmdk:1,dst=1:1	
ghost32.exe -clone, mode=create, src=@OS,dst=allvols.gho	Includes all mounted volumes in the image.
ghost32.exe -clone, mode=pcreate, src=@OS:C:D,dst=2vols.gho	Includes the specified volumes in the image.

Batch file example

This example restores disk one from an image file sent by the GhostCast Server using session name SN and resizes the first partition to 450 MB, the second to 1599 MB, and the third to 2047 MB. This is done in a batch file with no user intervention. The batch file commands change depending on the success or failure of the Symantec Ghost operation.

Batch file contents:

```
@ECHO OFF
ghost.exe
-clone,src=@mcSN,dst=1,sze1=450M,sze2=1599,sze3=2047M -batch
IF ERRORLEVEL 1 GOTO PROBLEM
ECHO Symantec Ghost exited with value 0 indicating success.
REM ** Add any commands required to run if Symantec Ghost
REM succeeds here**
GOTO FINISH
:PROBLEM
ECHO Symantec Ghost returned with an Error value 1 or higher
ECHO Symantec Ghost operation was not completed successfully
REM **Add any commands required to run if Symantec Ghost
REM fails here **
:FINISH
ECHO Batch File Finished
```

Using the -CRC32 switch

CRC checking works file-by-file with FAT partitions. NTFS partitions are CRC-checked within an image file by each MFT table. It is not possible at present to obtain a list of files failing a CRC check with an NTFS file system. When a CRC file is created for an NTFS partition, only a single CRC value is generated. You can also create a CRC file from an image file and verify it against a disk.

The full syntax for this switch is as follows:

```
-CRC32,action={create|verify|pcreate|pverify|dcreate|dverify},
src={{disk}|{partition}|{file}},crcfile={file}|{partition},vlist={file},
vexcept={file}
```

Table A-10 describes the parameters that can be used with the -CRC32 switch.

Table A-10 Parameters for the -CRC32 switches

Parameter	Explanation
create	Create an ASCII CRC32 file from a disk
verify	Verify a disk from a CRC32 file
pcreate	Create an ASCII CRC32 file from a partition
pverify	Verify a partition from an ASCII CRC32 file
dcreate	Create an ASCII CRC32 file from an image file
dverify	Verify an image file from an ASCII CRC32 file
crcfile	ASCII CRC32 file (default=Ghost.crc)
vlist	Verification list file (default=Ghost.ls)
vexcept	Verification exception file (no default)

Examples of -CRC32 usage

Table A-11 provides some examples of how you can use the -CRC32 switch.

Table A-11 -CRC32 usage examples

Switch	Function
ghost.exe -fcr	Creates a CRC32 file (called Ghost.crc) while making an image file.
ghost.exe -fcr=d:\test.crc	Creates a CRC32 file (called Test.crc) while making an image file.

Table A-11 -CRC32 usage examples *(continued)*

Switch	Function
ghost.exe -crc32,action=create,src=1, crcfile=ghost.crc	Creates a list of files and CRC32 values for a disk.
ghost.exe -crc32,action=dverify, src=x:dumpfile.gho,crcfile=ghost.crc	Verifies the list against an image file.
ghost.exe -crc32,action=pverify,src=1:2, crcfile=filename.crc:2	Verifies a partition on a disk with multiple partitions. This example verifies that partition 2 on disk 1 is the same as partition 2 in the CRC file.
ghost.exe -crc32,action=create	Creates an ASCII CRC32 file from the primary hard drive. Note that the default disk is the primary drive. The default ASCII CRC32 file is Ghost.crc.
ghost.exe -crc32,action=create,src=2, crcfile=myfile.txt	Creates an ASCII CRC32 file, Myfile.txt. This example uses disk 2 as the source drive and the output file.
ghost.exe -crc32,action=verify	Verifies the contents of the primary disk against a default ASCII CRC32 file, Ghost.crc (in the current directory). The default disk is the primary drive. The default verification list file is Ghost.ls. **Note:** If you want to keep Ghost.crc then copy Ghost.crc to a new location to ensure that it is accessible after you restart the computer.
ghost.exe -crc32,action=verify,src=1, crcfile=myfile.txt,vlist=myfile.out	Verifies the contents of the primary disk, 1, against the CRC32 file, Myfile.txt. Same as previous example, but specifies the disk, CRC file, and list file. This example uses disk 1 as the source drive, Myfile.txt as the ASCII CRC32 file, and Myfile.out as the verification list file.
ghost.exe -crc32,action=verify,src=1, crcfile=myfile.txt,vlist=myfile.out, vexcept=myfile.exc	Verifies the contents of the primary disk against a CRC32 file. Same as above with the inclusion of the EXCEPTION argument that excludes compared files based upon its entries.

Files not checked with CRC

The switch vexcept=filename specifies files that are not checked with CRC. This is normally used to exclude files that are always changed on start up. A sample exception file follows:

```
[ghost exclusion list]
\PERSONAL\PHONE
[partition:1]
\WINDOWS\COOKIES\*.*
\WINDOWS\HISTORY\*
```

```
\WINDOWS\RECENT\*
\WINDOWS\USER.DAT
\WINDOWS\TEMPOR~1\CACHE1\*
\WINDOWS\TEMPOR~1\CACHE2\*
\WINDOWS\TEMPOR~1\CACHE3\*
\WINDOWS\TEMPOR~1\CACHE4\*
[partition:2]
*\*.1
[end of list]
```

The exclusion list is case-sensitive. All files should be specified in uppercase. The (*) wildcard symbol follows UNIX rules, and is more powerful than the MS-DOS (*) wildcard. In particular, it matches the (.) character, as well as any other character, but other characters can follow the *. Therefore, a wildcard of *br* matches any files containing the letters br, such as, Brxyz.txt, Abr.txt, and Abc.dbr.

The specification of \WINDOWS\COOKIES\*.* in the previous example means match all files in the \WINDOWS\COOKIES subdirectory that have extensions. To match all files with or without extensions, use WINDOWS\COOKIES\*.

Use short file names in exclusion files. Files specified before the first [Partition:x] heading are used to match files in any partition.

A directory of * matches any subdirectory, regardless of nesting. The previous exclusion file matches any file with an extension of .1 in any subdirectory on the second partition. Apart from this, use wildcards for files, not for directories.

About numbering the Virtual Partition

Ghost.exe does not see the Virtual Partition when it runs from the command line. The numbering of the partitions is consistent with the numbering that appears when you run the Ghost.exe user interface.

If you use GDisk to view the disk, the Virtual Partition is displayed with the volume label VPSGHBOOT. Therefore, the partition numbering that you can see in GDisk is not the same as the partition numbering in Ghost.exe.

Transfer methods and hardware setup

This appendix includes the following topics:

Transfer and hardware requirements

Before using Symantec Ghost, consider the transfer and hardware requirements for the transfer method that you want to use. Ensure that all hard drives are installed correctly and that the BIOS of the system is configured and shows the valid parameters of the drives.

Peer-to-peer connections

Peer-to-peer connections enable Symantec Ghost to run on two computers, copying drives and partitions and using image files between them.

Note: Ghost32, Ghost64, and Ghost for Linux support peer-to-peer connections over TCP, but LPT and USB connections are not supported.

LPT or USB connections

On an LPT/parallel port connection, use a parallel connection cable and a parallel port to connect the computers. For data transfer of approximately 19-25 MB per minute, Symantec Ghost provides support for the Parallel Technologies universal DirectParallel cable. For peer-to-peer USB port connections, use a USB 1.1 cable that supports a host-to-host connection and a data transfer of approximately 20-30 MB per minute. Symantec Ghost does not support the following:

- Removal or addition of drives while Symantec Ghost is running
- USB 2.0 peer-to-peer
- Starting from a USB floppy disk drive

Due to problems with USB controllers, you should disable BIOS USB keyboard and mouse support when using Symantec Ghost with a USB device. In most cases, this is identified as Legacy support in the BIOS.

Symantec Ghost supports one USB 1.1 controller; therefore, you may have to try different ports to execute a Ghost USB peer-to-peer operation.

ECP is the best option for LPT connections and has a data transfer rate of approximately 5 MB/min. Symantec Ghost must be running under DOS on both computers.

See “Parallel Technologies cables” on page 557.

TCP/IP connections

Connect the computers with an Ethernet or token-ring network interface card and an established network connection, which includes one of the following:

- Crossover cable
- Coaxial or twisted pair cable
- Ethernet or token ring (network interface card)
- Ethernet or MSAU hub

SCSI tape drives

To use Symantec Ghost with a SCSI tape device, the tape media and the tape device must have an Advanced SCSI Programming Interface (ASPI) driver for DOS installed. The driver is installed in the Config.sys file as shown in the following example:

```
device=C:\scsitape\aspi4dos.sys
```

Note: Ghost for Linux does not support SCSI tape drives.

The driver can be included on a Ghost boot disk with the Standard Ghost Boot Disk option.

Refer to the documentation included with your SCSI tape device for more information.

GhostCast transfers

For GhostCasting transfers, the following hardware and software are required:

- Ethernet or token ring NIC
- Established network connection
- Optional multicast-enabled router
- Optional BOOTP/DHCP software

Set up the NIC using the manufacturer's installation program and run the NIC test program to check the NIC and cabling.

Removable media

The removable media drive, media, and media drivers for use in DOS are required.

CD/DVD usage

Note: Ghost for Linux does not support writing to CD/DVD. Reading from CD/DVD is available.

A CD/DVD writer and blank CD-R/RW or DVD media as suitable by the writer's manufacturers are required.

See “Image files and CD/DVD writers” on page 307.

Mapped network volume

An installed network interface card and established network connection are required to use a mapped network volume for cloning.

Network file server access within Windows is unavailable when Symantec Ghost runs in DOS. To access a network file server, a DOS network client boot disk must be created. A network client boot disk contains the appropriate network drivers and network client software to allow connection to a network. You can create a boot disk for connecting to a Microsoft network volume or an IBM LAN server.

See “About the Symantec Ghost Boot Wizard” on page 254.

Internal drives

To work with internal drives, ensure that each of the drives is properly configured. This means that if fixed IDE drives are in use, then the jumpers on the drives are set up correctly and the BIOS of the computer is configured for the disk arrangement. Both the source and the destination drives must be free from file corruption and physical hard-drive defects.

USB devices

When using a USB device Symantec Ghost supports the following:

- USB hubs
- Devices that must comply to the Mass Storage Specification, Bulk only

Symantec Ghost does not support the removal or addition of drives while Symantec Ghost is running.

Symantec Ghost does not support using a peer-to-peer USB cable with peer-to-peer drivers from a boot disk and another USB mass storage device on the same controller. Ghost internal USB support only starts when nothing else is controlling the controllers. You can use the switches -forceusb and -nousb to force USB support or disable USB support, but these switches should be used with caution.

See “About Symantec Ghost switches” on page 521.

FireWire devices

Symantec Ghost does not support the removal or addition of drives while Symantec Ghost is running.

To be supported by Symantec Ghost, the FireWire drive must comply to the following standards:

- Controllers must comply to the 1394 Open Host Controller Interface (OHCI) 1.0 Specification.
- Devices must comply to the Serial Bus Protocol 2 (SBP-2).
- Devices must support SCSI Primary Commands 2.0 (SPC-2).

Third-party device

Install the DOS driver as outlined in the device documentation.

USB and DirectParallel cables

This appendix includes the following topics:

Parallel Technologies cables

Parallel Technologies USB and DirectParallel Universal Fast Cable provide high-speed data transfer and can significantly increase Symantec Ghost performance.

USB and DirectParallel connection cables are available directly from Parallel Technologies as follows:

- http://www.ptnet.com
- Telephone:
  - 800.899.1652 (U.S.)
  - 952.920.7185 (International)
- Fax: 952.920.7475
- Email: sales@ptnet.com

For peer-to-peer connections, Symantec Ghost supports USB 1.1 cables and USB 1.1 controllers. Some USB 2.0 controllers may work, but Symantec Ghost does not support this configuration.

The USB and DirectParallel connection cables can also be used for high-speed computer-to-computer file transfer and networking in Windows 2000. Symantec

Ghost contains DirectParallel driver technology from Parallel Technologies, Inc., the developers of the Direct Cable Connection computer-to-computer technology built into Windows 2000. The DirectParallel drivers and cables contain patent-pending parallel port interface technology.

Other USB cables

The following USB peer-to-peer cables can also be used with Symantec Ghost:

- EzLink USB Instant Network, model 2710
- USB LinQ Network
- BusLink USB to USB File Transfer cable, model UFT06
- USB Net Linq Network Bridge cable, model 2K398
- USB Net Linq Network Bridge cable, model 00115G

Appendix D

Wattcp.cfg network configuration file

This appendix includes the following topics:

About the Wattcp.cfg configuration file

The Wattcp.cfg configuration file contains the TCP/IP networking configuration details for Symantec Ghost. The Wattcp.cfg file is not required for the GhostCast Server, Ghostsrv.exe.

Wattcp.cfg is created automatically in the virtual partition and when you create a boot package using the Ghost Boot Wizard.

The Wattcp.cfg file specifies the IP address and the subnet mask of the computer and lets you set other optional network parameters. The file should be located in the current directory where Ghost.exe is started.

Comments in the file start with a semicolon (;). Options are set using the format option = value. For example:

```
receive_mode=5;set receive mode
```

Wattcp.cfg keywords

The keywords in the Wattcp.cfg configuration file are listed in Table D-1.

Table D-1 Wattcp.cfg keywords

Keyword	Description
IP	Specifies the IP address of the local computer. Each computer must have a unique IP address. Symantec Ghost supports the use of DHCP and BOOTP servers and defaults to using them when the IP address is left blank or is invalid. DHCP and BOOTP provide automatic assignment of IP addresses to computers. This lets identical boot disks be used on computers with similar network cards. For example: IP=192.168.100.10
Netmask	Specifies the network IP subnet mask. For example: NETMASK=255.255.255.0
Gateway (optional)	Specifies the IP address of the gateway. This option is required when routers are present on the network and when participating computers are located on different subnets. For example: GATEWAY=192.168.100.1
Bootpto (optional)	Overrides the timeout value in seconds for BOOTP/DHCP. For example: BOOTPTO=60
Receive_Mode (Ethernet only)	Overrides the automatically configured packet driver mode used by Symantec Ghost. The modes, in order of preference, are 4, 5, and 6. The default mode is 4. Some packet drivers misrepresent their abilities in receiving multicast information from the network and allow the use of packet receive modes that they do not support. The packet driver should be set to mode 4 so that it only accepts the multicast packets required. If the packet driver does not support this mode, mode 5 can be used to collect all multicast packets. The final option, mode 6, configures the packet driver to see all packets being sent on the network. For example: RECEIVE_MODE=6
share_mode	Must be set to 1 to allow GhostCast or peer-to-peer operations on a mapped network drive. You should set this option to 0 for all other operations.

Ghost for Linux

This appendix includes the following topics:

- Supported configurations
- Supported Linux distributions for running Ghost
- Symantec Ghost utility support

Supported configurations

Symantec Ghost can copy or clone many different Linux distributions. However, Symantec Ghost is sensitive to any possible changes in Ext2/3 file systems and LILO and GRUB specifications. If changes are made to these specifications, Symantec Ghost may no longer support the Linux distribution.

Symantec Ghost is not sensitive to kernel versions. Use the -ial and -nolilo command-line switches to resolve problems with any incompatibilities.

See "Command-line switches" on page 522.

The following table shows the Linux boot loaders, filesystems and file system features that are supported:

GRUB		Ghost supports version 0.97 and earlier of GRUB. Later versions may also work. Any references to a disk other than the first hard disk in the system (/dev/hda or /dev/sda) are not supported. The /boot and root file systems must be on the first hard disk. The /boot directory can be a directory within the root file system. Symantec Ghost assumes that GRUB has been installed in the standard /boot/grub directory or /grub in a /boot partition and uses the standard file name /boot/grub/stage 2. Non-standard GRUB installations are not supported. **Note:** It is recommended that you use GRUB in preference to LILO.
LILO		Ghost supports version 22.5.1 and earlier of LILO. It only supports the linear mode, not the lba32 mode. This means the /boot files must be in the first 8.4Gb on the disk. Symantec Ghost uses the /etc/lilo.conf file to determine the boot configuration. If this file does not match the boot configuration, Symantec Ghost may be unable to patch LILO during cloning.
SysLinux		Used, for example, on bootable USB sticks. Ghost supports version 3.11 (other versions may also work).
ext2, ext3	Resize inode	Ghost drops the resize inode. When Ghost restores a partition it resizes the file system within it to use all of the available space.

	LVM	Ghost has limited support for LVM volumes. It clones only single-striped or non-mirrored logical volumes with a single segment. When creating an image, or cloning disk-to-disk Ghost operates as though the LVM volumes are simple partitions. Therefore Ghost, cannot recreate the LVM volumes on the destination. These volumes are cloned as though they were simple partitions. You may need to manually edit the config files. Ghost can clone or restore a single partition into an already existing LVM volume on the destination disk. In this case, the volume is still part of the LVM in the operating system. With Ghost running on Linux there is also the option of dealing with LVM volumes via the OS Volumes feature.
	Extended ACLs	Symantec Ghost fully supports ACLs.
	Journaling	Ghost supports journaling. It does not support having the journal on another device, but this is an extremely uncommon case.
	H-trees/Dirindexes	H-tree directory indexes are not cloned, but can easily be recreated by the user after the restore operation
ext4		There is no support for ext4 (except on a sector by sector basis).
Reiserfs		There is no support for Reiserfs (except on a sector by sector basis).
		Type 0 and type 1 Linux swap file systems (type 0x82) are supported.
		Skip file is not supported.
		Linux extended partitions (type 0x85) are partially supported. Ghost copies file systems inside these extended partitions, but restores them as DOS extended partitions. This is not known to cause problems with Linux systems after cloning.

Symantec Ghost provides the following support:

- LVM partitions are created as extended/logical partitions.
- Symantec Ghost does not support Linux if there is no valid boot record in the disk MBR and more than one partition on a disk is installed with LILO or GRUB.

If the Linux disk is set up to start from a partition MBR, there can be only 1 partition with a LILO or GRUB boot record in its MBR.

Warning: Always have a boot disk available in case of problems with starting a Linux system after cloning.

Supported Linux distributions for cloning

Symantec Ghost can copy or clone many different Linux distributions.

Note: Installing unsupported versions or features of the bootloaders and filesystems may cause Ghost to fail.

Symantec Ghost can copy or clone the following versions of Linux in their default configurations:

- Red Hat Enterprise Linux ES release 5.1
- Red Hat Enterprise Linux ES release 5
- Red Hat Enterprise Linux ES release 4
- Red Hat Enterprise Linux ES release 3
- Red Hat Enterprise Linux ES release 2
- Red Hat Enterprise Linux ES release 1
- Fedora Core 8 (Werewolf)
- Fedora Core 7 (Moonshine)
- Fedora Core 6 (Zod)
- Fedora Core 5 (Bordeaux)
- Red Hat Linux 9
- Ubuntu 7.10 (Gutsy Gibbon)
- Ubuntu 7.04 (Feisty Fawn)
- Ubuntu 6.10 (Edgy Eft)
- Ubuntu 6.06 (Dapper Drake)
- SuSE Linux Enterprise Server 10

Note: Symantec Ghost Solution Suite 2.5 supports 64-bit Linux if it is AMD64 and EMT64. Itanium 64-bit Linux is not currently supported.

Supported Linux distributions for running Ghost

Symantec Ghost for Linux (ghost) and the Linux tools (ghregedit, ghconfig, omnifs, and gdisk) are supported on the following Linux distributions:

- Red Hat Enterprise Linux ES release 5.1
- Fedora Core 8 (Werewolf)
- Ubuntu 7.10 (Gutsy Gibbon)
- SuSE Linux Enterprise Server 10

Symantec Ghost utility support

Ghost Explorer substantially supports Ext2/3 file systems within image files, including the restoration, deletion, and addition of files within these file systems. Problems arise when files that have names that are illegal on Windows are manipulated. Ghost Explorer cannot manipulate device files or symbolic links. Sparse files are expanded on restoration, and hard links are broken.

Appendix F

GDisk disk-wipe specifications

This appendix includes the following topics:

About GDisk disk-wipe specifications

GDisk is a tool for partitioning hard drives that also has a secure, disk-wiping function.

The disk-wipe feature in GDisk conforms to the standards that are detailed in the following documents:

- U.S. Department of Defense NISPOM (National Industrial Security Program Operating Manual), DoD 5220.22-M, January 1995.
  The NISPOM document is available at the following URL:
  www.usaid.gov/policy/ads/500/d522022m.pdf
- Assistant Secretary of Defense, Memorandum of Disposition of Unclassified DoD Computer Hard Drives, 4 June 2001.

Clearing, sanitizing, and viewing hard disks

Chapter 8 of the NISPOM (Automated Information System Security) contains a matrix of actions required to clear and sanitize magnetic disks of various types.

Table F-1 is an extract from Section 8-306 of the NISPOM.

Table F-1 Clearing and sanitizing a hard disk

Magnetic disk type	Clear	Sanitize
Bernoullis	a, b, c	m
Floppy disk	a, b, c	m
Non-removable rigid disk	c	a,b,d,m
Removable rigid disk	a,b,c	a,b,d,m

Where Clear is as follows:

a Degauss with a Type I degausser

b Degauss with a Type II degausser

c Overwrite all addressable locations with a single character

d Overwrite all addressable locations with a character, its complement, then a random character and verify

Note: This method is not approved for sanitizing media that contains Top Secret information.

m Destroy (disintegrate, incinerate, pulverize, shred, or melt)

Table F-2 lists the GDisk operations for clearing, sanitizing, or viewing a disk.

Table F-2 GDisk clearing, sanitizing or viewing operations

Operation	Description
Clearing a disk	GDisk performs a clear operation, as defined by action c, as the default disk-wipe operation. All addressable locations are overwritten with 0x00.

Table F-2 GDisk clearing, sanitizing or viewing operations *(continued)*

Operation	Description
Sanitizing a disk	GDisk performs a sanitize operation, as defined by action d, when performing a disk-wipe operation with the /diskwipe /dodwipe command modifier. The following cycle occurs six times: ■ All addressable locations are overwritten with 0x35. ■ All addressable locations are overwritten with 0xCA. ■ All addressable locations are overwritten with a pseudo-random character. ■ All addressable locations are verified in hardware using the Verify Sectors command to the disk.
Viewing a disk	You can use GDisk to view the overwrite pattern on the disk to confirm the overwrite has occurred. This lets you display one or more sectors to the screen, starting at sector n, of a physical disk (by default, 1 sector is displayed).

About completeness of coverage

Table F-3 details the control that GDisk has over the disk and, therefore, the completeness of the wipe.

Table F-3 Completeness of coverage

Control	Description
Addressable locations	The smallest addressable unit on a hard disk is the sector. The sector comprises 512 bytes in IDE drives but may have larger numbers of bytes in SCSI or ATAPI disks. The NISPOM assumes that the smallest addressable location is the size of a character, presumably an 8-bit character, which occupies 1 byte of storage. GDisk assumes that the smallest addressable location on the disk is a byte. Byte addressing is achieved by constructing a block of data, one or more sectors in size with the chosen character filling each byte in the block, and writing that block to the disk.

Table F-3 Completeness of coverage *(continued)*

Control	Description
Wiping Host Protected Area (HPA) PARTIES	During execution of a DoD disk wipe, GDisk attempts to detect an HPA/PARTIES area on the disk. If an HPA/PARTIES area is detected, then you are asked if this area is to be wiped. If the area is not password protected, then the area is wiped. In all cases, you are informed of the success or failure of the wipe.
Confirming the wipe	GDisk provides the view:n command to view the overwrite pattern on the disk to confirm the overwrite has occurred by sampling. You can use the view:n command-line switch to display one or more sectors, starting at n, of a physical disk on stdout (by default, 1 sector is displayed). Sector numbers start at 0. Each sector is displayed as a table with 16 columns containing the sector offset, then hex bytes, and lastly 16 ASCII characters representing each byte. This table has n rows, where n depends on the sector size and is usually 32 rows (sector size of 512 bytes).

Table F-3 Completeness of coverage *(continued)*

Control	Description
Non-addressable locations	There may be storage on the disk that is not directly addressable by GDisk. GDisk does not support the following features: ■ Bad sector remapping The disk may have spare sectors available that are used to automatically remap, or substitute, bad sectors by the disk firmware. This is a potential security risk, for example, if a bad sector may have been remapped and the original location on the disk platter previously used by that sector becomes inaccessible. However, it is possible that the bad sector may still contain readable data that could be accessed by a skilled hard-drive engineer. ■ Host Protected Area (HPA) If the HPA is password protected, then this area of the disk is not addressable by GDisk. ■ Inaccurate disk geometry detection An error in determining the disk size could result in non-accessibility. ■ Specialized disk commands Specialized disk commands, such as those used to access SMART logs, indicate that a disk may store data that is not accessible using standard commands. ■ Wiping of locked sectors The operating system may lock some of the sectors on the disk. These sectors cannot be accessed by GDisk and are not wiped. This is more likely to happen when you run GDisk in Windows than in DOS. GDisk gives notification of which sectors were not overwritten.

Determining disk size

The BIOS function calls, or disk commands, used for determining the size of the disk are as follows:

- Int13h, Get Drive Parameters (08h)
- Extended Int13h, Get Drive Parameters (48h)
- Direct IDE, IDENTIFY DEVICE(ECh)
- Direct SCSI, READ CAPACITY (25h)

Appendix G

Customizing Symantec Ghost functionality

This appendix includes the following topics:

About customization

Symantec Ghost functionality can be customized. In some situations, the holder of a license may want to provide versions of Symantec Ghost that have some features disabled.

Limiting functionality from the environment file

To limit Symantec Ghost functionality, edit the Symantec Ghost environment file. The environment file includes the following:

- The licensed user's details
- The maximum number of licensed, concurrent users
- Additional product licensing information
- Functionality switches

Table G-1 lists the available switches.

Table G-1 Environment file switches

Switch	Description
LOAD	Loads disk or partition from image file actions
DUMP	Dumps disk or partition to image file actions
WRITE	Stops Symantec Ghost from writing to destination partition or disk
DISK	Performs disk-to-disk and partition-to-partition actions
PEER	Connect via LPT, USB, or TCP/IP peer-to-peer
FPRNT	Creates a fingerprint that is a hidden mark on a cloned drive or partition that includes the following: ■ Process used to create the drive or partition ■ Time the operation was performed ■ Date the operation was performed ■ Disk number
IMGTMO	Sets the maximum age of an image file in days
TIMEOUT	Disables Symantec Ghost until a valid license is reapplied

Note: Ghost on Linux works in the same way as Ghost on DOS (uses the -#e switch).

To limit Symantec Ghost functionality

1. Manually edit the environment file, `Ghost.env`.
2. Add a switch parameter line as the first line of the environment file.

   Each feature except IMGTMO can be activated with switchname=y or deactivated with switchname=n in the bound executable.
3. Ensure that the `Ghost.env` file is in the same directory as `Ghost.exe`.
4. Run Symantec Ghost using the following command:

   ```
   C:\ghost> ghost.exe
   ```
5. If you have an environment file with a name other than Ghost.env, at the command line, run Symantec Ghost with the following switch and your environment file name:

   ```
   C:\ghost> ghost.exe -#e=filename.env
   ```

Customizing Ghost32

You cannot modify a running executable in Windows, so you cannot limit the functionality of ghost32.exe in the same way as ghost.exe. When limiting the functionality of Ghost32, you create a copy of the Ghost32 executable and place it in a suitable location. You can then run the original instance of Ghost32 to modify the copy. The modified copy is the limited-functionality executable that you want.

To modify a copy of Ghost32 you must use the switch `-envexe` in conjunction with the switches described above.

To limit Symantec Ghost32 functionality

1. Manually edit the environment file, Ghost.env.
2. Add a switch parameter line as the first line of the environment file.

   Each feature except IMGTMO can be activated with switchname=y or deactivated with switchname=n in the bound executable.
3. Ensure that the Ghost.env file is in the same directory as the copy of Ghost32.exe that you want to modify.
4. Run Symantec Ghost using the following command:

   ```
   C:\ghost32> Ghost32 -envexe=fullpath\Ghost32.exe -file
   ```

   where `fullpath` is the full path to the copy of Ghost32.exe (the executable that is not currently running).

   For example:

   ```
   C:\ghost32> Ghost32 -envexe=c:\folder\Ghost32.exe -file
   ```

Examples of customized functionality

You can customize functionality for end users of Symantec Ghost as follows:

- Image file restoration only
- Backup tool only

Image file restoration only

A company may have 100 laptops in use by its sales staff with the IT system administrator controlling the organization and maintenance of these laptops. Each laptop in use could include a copy of Symantec Ghost and a model image file burned on a CD-ROM for fast system restoration by the user. The system administrator can configure the Symantec Ghost edition that is burned onto the

CD-ROM to enable only image file restoration, thus removing the possibility of end users attempting to use other Symantec Ghost functions.

The administrator's version of Symantec Ghost has all of the options available after binding the original environment file. The CD-ROM version of Symantec Ghost is activated with:

Switches: load=y,dump=n,disk=n,peer=n

KeyNum: 12345

License: BM-512

MaxUsers: 10

Name: ABC Inc.

Address1: 200 John Wayne Blvd.

Address2: Irvine, CA 91024

Backup tool only

Symantec Ghost can be used as a backup tool. In the example above, it may be advisable to disable the load option so that image file creation procedures can be carried out without the possibility of users accidentally overwriting their local drives. Restoration would require the availability of another executable or the use of Ghost Explorer.

You can use Symantec Ghost as a backup tool with the following switches:

load=n,dump=y,disk=n,peer=n

OEM version of Symantec Ghost

The Symantec Ghost Recovery Kit lets OEM customers modify Symantec Ghost to suit their requirements. The Symantec Ghost Recovery Kit is supplied with Symantec Ghost Solution Suite.

The Symantec Ghost Recovery Kit is a suite of tools designed for original equipment manufacturers (OEMs) and value-added resellers (VARs). It adds tools and functionality to the applications included in Symantec Ghost Solution Suite.

Symantec Ghost Recovery Kit includes the following tools:

- GhostOEM (DOS version)
- GhostOEM32
- PQIDeploy (DOS version)
- PQIDeploy32

- SRFixMbr

Used in conjunction with the Recovery Kit, Symantec Ghost Solution Suite can provide a fully automated PC management solution for your network environment.

For more information, refer to the documentation, *Symantec Ghost Recovery Kit* (Recovery_Kit.pdf).

Adding DOS drivers to the Ghost Boot Wizard

This appendix includes the following topics:

About adding DOS drivers

The process described here details how to add DOS drivers to the Ghost Boot Wizard. You can create a boot disk that supports network interface cards (NICs) that are not currently available in Symantec Ghost.

See "About the Symantec Ghost Boot Wizard" on page 254.

Note: If you are using WinPE in the Ghost Boot Wizard, you can create and modify new versions of Win PE by copying an existing image and adding or removing drivers as appropriate. You can also add new drivers to the Ghost Deploy Anywhere driver database, and then include the new drivers in your Win PE versions.

See "Adding new drivers to the Ghost Deploy Anywhere driver database" on page 261.

The following is an overview of the process for adding DOS drivers to the Ghost Boot Wizard:

- Download the driver from the manufacturer's Web site.
- Make a driver template.

- Get the PCI information.

Downloading the driver from the manufacturer's Web site

Download the latest drivers from the NIC manufacturer.

To download drivers from the manufacturer's Web site

1. Go to the manufacturer's Web site.

   Use a search engine if the name is not obvious. Once you have found the Web site, there is usually a section titled Support or Driver downloads.

2. Download the driver archive.

   Often there is more than one archive for a card. If you have a choice, then download the archive for DOS and the archive for Windows. The SCO, Linux, and NetWare drivers are not required.

3. Unpack the archive into a directory.

   The archives are usually self-extracting.

4. Read Readme.txt from the archive to see which drivers are included.

   All cards should come with NDIS drivers, and some cards also have packet drivers.

Making a driver template

The second step in the process is to create a driver template.

When you make a driver template in the Ghost Boot Wizard, the setup boxes may be automatically completed. If this does not happen, you must manually complete the boxes.

To start creating a driver template

1. On the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Boot Wizard**.
2. In the Symantec Ghost Boot Wizard, in the PreOS Version page, select **PC-DOS**.
3. Click **Next**.
4. In the Image Type page, click **Network Boot Package**.
5. Click **Next**.
6. In the Network Interface Card page, click **Add**.

7. In the Template Type dialog, click **NDIS2 Driver**.
8. Click **OK**.
9. In the Template Properties window, on the NDIS Driver tab, click **Setup**.
10. Select the folder that holds the NDIS2 driver that you previously downloaded.

    The NDIS2 driver is usually in a subdirectory called ndis\dos. If this directory does not exist, the NDIS driver will be in a directory with a similar name.
11. Click **OK**.

    All boxes in the Template Properties window are automatically completed. If this is not successful, then you must complete the details manually.
12. Click **OK**.

To complete details on the NDIS driver tab

1. On the NDIS driver tab, click **Browse**.
2. Find the NDIS2 driver file.
3. Open Windows Explorer.
4. In the NDIS2 driver file directory, use Notepad to open Protocol.ini.

    The Protocol.ini file looks similar to this:

```
;Module description for Adaptec 69XX Ethernet PCI Adapter Family
; DriverName = EMPCI$
;
; Optional Parameters :
;
;   NetAddress   = "000000000000"
;   MaxTransmits = 1 - 8
;   MaxReceives  = 1 - 8
```

5. Copy the text that follows Drivername =.

    In the above example, you would copy the text EMPCI$. Ensure that you maintain the case.
6. Click **OK**.

    If the template is new, then rename it.

    The standard convention for naming a template is <Manufacturer><Name of card>. Readme.txt usually lists the cards with which the driver can be used, so name the template to reflect this.

    For example, Adaptec 69XX Ethernet PCI Adapter Family.

Getting the PCI information

The Ghost Boot Wizard and the Symantec Ghost Console require PCI information. It can be accessed only by manually opening the hidden Ghost Boot Wizard template.

To get the PCI information

1. Press **Control** on the keyboard and select the copyright message on the first page of the Ghost Boot Wizard.

   The folder in which the templates are stored appears.

2. Open Windows Explorer, and open the folder containing the templates.

   Ensure that you can view hidden files.

3. Double-click **Mcassist.cfg**.

   The contents of Mcassist.cfg looks similar to this:

   ```
   # This file is used by the Ghost Boot Wizard.
   # You should not attempt to edit this file yourself
   DRIVER-TYPE = NDIS
   DRIVER-NAME = El90x.dos
   NDIS-NAME = EL90X$
   RECEIVE-MODE = 0
   PCI-TAG = 10B7 9000 : 3C900-TPO Fast Ethernet$
   PCI-TAG = 10B7 9001 : 3C900-Combo Fast Etherlink$
   ```

4. In Notepad, open the Windows 95 driver configuration file downloaded from the manufacturer's Web site. This is called *name of driver*.inf and is usually in its own directory.

   Find the lines that look similar to the following:

   ```
   [HP]
   %en1207d.DeviceDesc%=en1207d.ndi,PCI\VEN_1113&
   DEV_1211&SUBSYS_1207103C
   %en1207d.DeviceDesc%=en1207d.ndi,PCI\VEN_1113&DEV_1211&
   SUBSYS_9207103C
   ```

5. Copy the PCI vendor ID and the PCI Device ID.

   These are stored as 4-digit hexadecimal numbers. In the example above, the correct numbers follow VEN_ and &DEV_, namely 1113 and 1211.

6 Add a new line to Mcassist.cfg that reads as follows:

```
PCI-TAG = <vendor ID> <device ID> : <name of card>$
```

In this example, both lines in the Windows configuration file are the same. Only one line is added to Mcassist.cfg.

For example,

```
PCI-TAG = 1113 1211 : HP EN1207D-TX PCI Fast Ethernet Adapter$
```

7 Save **Mcassist.cfg**.

8 Restart the Ghost Boot Wizard.

Installing Symantec Ghost from the command line

This appendix includes the following topics:

About installation interface types

Microsoft Windows Installer lets you choose the user interface that you see during installation. If you are installing in Basic or Silent mode, you must run the installation from the command line.

Symantec Ghost does not support the Microsoft Windows Installer modifier, or the Reduced UI mode.

Full interface mode

The Full interface mode guides you through a series of dialog boxes to install Symantec Ghost. You can change installation settings. For example, you can select components and change installation directories. Because a user interface is provided, you do not need to include parameters in the command line.

Basic interface mode

The Basic interface mode shows a progress bar and any system-level error messages. If you alter any default installation settings, you must pass this information through as parameters from the command line.

Table I-1 lists the syntax for this installation.

Table I-1 Basic installation syntax

Installation package	Syntax
Symantec Ghost Console	msiexec /I “<path to msi package>\Symantec Ghost.msi” /qb
Standard Tools AutoInstall	msiexec /I “<path to msi package>\Symantec Ghost.msi” /qb GHOSTINSTALLTYPE=“xxxxxxx” where xxxxxxx is one of the following: ■ Server Tools = Standard Tools ■ AutoInstall = AutoInstall
Console client	msiexec /I “<path to msi package>\Client.msi” /qb
Configuration client (standalone)	msiexec /I “<path to msi package>\Client.msi” /qb GHOSTINSTALLTYPE=“Standalone Client”
Symantec User Migration Wizard	msiexec /I "<path to msi package>\SUMWizard.msi /qb

Silent interface mode

The Silent interface mode does not show any dialog boxes or error messages. If you alter any default settings, you must pass this information through as parameters from the command line. To install a component of Symantec Ghost, use the syntax in Table I-1 but with the switch /q, not /qb.

For example, to install Symantec Ghost Console, the syntax is:

```
msiexec /I "c:\temp\Symantec Ghost.msi" /q
```

About installation modes

Microsoft Windows Installer lets you choose the way you install Symantec Ghost. Unless you choose a Normal installation, run the installation from the command line.

Table I-2 describes the installation modes.

Table I-2 Installation Modes

Mode	Description
Normal	The Normal installation mode provides dialog boxes to guide you through installation. It lets you install Symantec Ghost on the target computer by selecting the location and the required components.
Administrative	The Administrative installation mode installs the entire installation package to a network location. All installation files are copied from the CD to the specified location. This lets users with access to the network location install Symantec Ghost from this location. This installation requires administrative privileges. The syntax for this installation is as follows: `msiexec /a "<path to msi package> \"installation package".msi"`
Repair	The Repair installation lets you repair the current installation. It is accessed once Symantec Ghost is installed on your computer. You can activate this by using Add/Remove Programs in the Control Panel. You can also run this mode from the command line. The syntax for this installation is as follows: `msiexec /f "<path to msi package> \ "installation package".msi"` The switch /fa reinstalls all files, /fu rewrites all required user registry entries, and /fs overwrites any existing shortcuts. The /f switch reinstalls all required files, registry entries, and shortcuts, but it ignores any property values entered in the command line.
Modify	The Modify installation mode lets you change the user's current configuration. To do this, use Add/Remove Programs in the Control Panel. On Windows 2000/XP, click Change. You cannot use this mode for a client package.
Advertised	The Advertised installation mode creates shortcuts of the components on the target computer and registers the file type extensions associated with the components' features. When the user selects the shortcut or opens one of the associated files, the component is installed. Therefore, only those components that the user needs are installed. You cannot install a client package using this mode. The syntax for this installation is: `msiexec /j` *`path to msi package`*`\SUMWizard.msi`

Installing from the command line

You can specify parameters when installing Symantec Ghost from the command line by setting installer properties. The syntax for these properties is as follows:

```
msiexec /I “c:\temp\Symantec Ghost.msi” /q PROPERTY = VALUE
```

The property name must be in uppercase, and the value is case-sensitive.

In Windows Vista/XP/2003/2000, Msiexec.exe is in the path by default, so it can be called from any directory.

If you are not running Windows XP and you do not have Windows Installer version 2 installed, then the installation must be performed through a setup file.

Console Setup.exe	In the Symantec Ghost \Install directory.
ClientSetup.exe	In the Symantec Ghost \Install\Client directory.
Symantec User Migration Setup.exe	In the Symantec Ghost \SUMWizard directory.

If you are installing in Administrative mode, you do not need to set these properties because you are copying the installation package to a location on the network. Set these properties once you run the installation from the network location.

If the installation fails review the Windows Installer log file to help determine the cause of the failure. To increase the amount of logged information you can execute msiexec.exe with the /l*v <log-file-name> command line.

When installing the Symantec Ghost Console, you must set company name in the command line, or the installation fails. When installing Standard Tools or AutoInstall, these properties are optional.

Table I-3 shows the package properties that can be set from the command line when installing one of these components.

Table I-3 Symantec Ghost package properties

Property	Default value	Description
INSTALLDIR	Program files\ Symantec\Ghost	Destination directory
USERNAME	Registered user	User name
COMPANYNAME	Registered company	Company name

Table I-3 Symantec Ghost package properties *(continued)*

Property	Default value	Description
EMAILADDRESS		Email address
GHOSTINSTALLTYPE	Server	Installs one of the following: ■ Symantec Ghost Console (value=Server) ■ Standard Tools (value=Server Tools) ■ AutoInstall (value=AutoInstall)

Table I-4 shows the package properties that can be set from the command line when you install a client.

Table I-4 Client package properties

Property	Default value	Description
GHOSTCONSOLENAME	No default	Symantec Ghost Console
INSTALLDIR	Program files\ Symantec\Ghost	Destination directory
GHOSTINSTALLTYPE	Client	Installs one of the following: ■ Console client (value=Client) ■ Configuration client Standalone (value=Configuration)

Table I-5 contains the switches that can be used with Setup.exe and ClientSetup.exe.

Table I-5 Setup.exe switches

Switch	Description
/a	Runs installation in Administrative installation mode.
/s	Hides the initialization dialog.
/s /v/qn	Runs the installation in Silent installation mode.
/x	Uninstalls the application.

Table I-5 Setup.exe switches *(continued)*

Switch	Description
/v	Passes the parameters to the installation. All of the parameters must be enclosed in quotation marks, and the opening quotation mark must immediately follow the /v switch. Any other quotation marks must be preceded by a backslash.

The following command line installs Symantec Ghost in a specified folder, registering Symantec Ghost with the user name in silent mode:

```
setup.exe /v"USERNAME=\"Me\" INSTALLDIR=\"c:\temp\" /qn"
```

Uninstalling from the command line

You can uninstall Symantec Ghost from the command line using Microsoft Installer.

See "Installing from the command line" on page 588.

To uninstall Symantec Ghost from the command line

- At the command prompt, type the following command:

  ```
  Msiexec /x "<path to msi package> \msipackagename.msi” [/q or /qb]
  ```

  The switches /q and /qb are optional.

Installing a boot partition

This appendix includes the following topics:

- About boot partitions
- Installing a boot partition on a client computer

About boot partitions

If the computer that you want to connect to the Ghost Console does not have an operating system, you can do one of the following:

- Install a Ghost boot partition on the client computer.
- Create a boot package that lets you use 3Com Boot Services to start the client computer from the network.
  See "Using 3Com Boot Services and Symantec Ghost" on page 40.
  See "Creating a TCP/IP Network Ghost Client Boot Image" on page 271.

You could also create a Ghost boot partition on a computer if you do not want to keep the existing operating system and configuration settings on the Console.

See "The Symantec Ghost partition" on page 37.

Installing a boot partition on a client computer

The process for installing a boot partition is as follows:

- Use the Ghost Boot Wizard to create a network boot package.
  The GhostCast Server uses this boot package to copy the boot partition image to the client computers.
  See "Creating a Network Boot Package" on page 272.
- Use the Ghost Boot Wizard to create a Console Boot Partition image file.

The Console Boot Partition image file includes the Console client, the Symantec Ghost executable, and the drivers for your network card.
See "Creating a boot image that contains a Console boot partition" on page 268.

- Restart the client computers by using the network boot package, and then connect to the GhostCast session.
  See "To join a GhostCast session to restore an image file to client computers" on page 370.
- Use the GhostCast Server to image the client computers from the boot partition image file that you have created.
  See "To restore an image onto client computers using the GhostCast Server" on page 369.

Configuring firewalls

This appendix includes the following topics:

- Symantec Ghost port configuration

Symantec Ghost port configuration

Table K-1 lists the ports that must be open in a firewall to allow the Ghost Console and the Console client to work.

Table K-1 Ghost Console and Console client port configuration

Sent by	Source port	Destination address	Destination port	Type	Volume
Stage 1: Server Discovery					
Client	1346	229.55.150.208	1345	UDP	Low
Client	Varies	WINS server	137	UDP	Low
Server	1345	Client IP	Varies	UDP	Low
Stage 2: Status update					
Client	1346	Server IP	1347	UDP	Low
Server	1347	Client IP	1346	UDP	Low
Stage 3: Task execution					
Client	Varies	Server IP	1347	TCP	Low
Server	1347	Client IP	Varies	TCP	Medium
File transfer steps using Multicast					

Table K-1 Ghost Console and Console client port configuration *(continued)*

Sent by	Source port	Destination address	Destination port	Type	Volume
Client	7777	Server IP	Varies	UDP	Medium
Server	Varies	224.77.xxx.xxx	7777	UDP	High

Table K-2 lists the ports that must be open in a firewall to allow GhostCast multicasting to work.

Table K-2 GhostCast server multicasting port configuration

Sent by	Source port	Destination address	Destination port	Type	Volume
Stage 1: Server discovery					
Client	Varies	224.77.0.0 Client IP	6666	UDP	Low
Server	6666	Client IP	Varies	UDP	Low
Stage 2: Status update					
Client	Varies	Server IP	Varies	TCP	Low to Medium
Server	Varies	Client IP	Varies	TCP	Low to medium
Stage 3: Task execution					
Client	7777	Server IP	Varies	UDP	High
Server	Varies	224.77.1.0	7777	UDP	Low
Server	Varies	224.77.xxx.xxx	7777	UDP	High

Table K-3 lists the ports that must be open in a firewall to allow the GhostCast directed broadcasting to work.

Table K-3 GhostCast server directed broadcasting port configuration

Sent by	Source port	Destination address	Destination port	Type	Volume
Stage 1: Server discovery					
Client	Varies	224.77.0.0 Client IP	6666	UDP	Low
Server	6666	Client IP	Varies	UDP	Low
Stage 2: Status update					

Table K-3 GhostCast server directed broadcasting port configuration *(continued)*

Sent by	Source port	Destination address	Destination port	Type	Volume
Client	Varies	Server IP	Varies	TCP	Low to medium
Server	Varies	Client IP	Varies	TCP	Low to medium
Stage 3: Task execution					
Client	7777	Server IP	Varies	UDP	High
Server	Varies	Clients's subnet broadcast address	7777	UDP	High

Table K-4 lists the ports that must be open in a firewall to allow the GhostCast unicasting to work.

Table K-4 GhostCast server unicasting port configuration

Sent by	Source port	Destination address	Destination port	Type	Volume
Stage 1: Server discovery					
Client	Varies	224.77.0.0 Client IP	6666	UDP	Low
Server	6666	Client IP	Varies	UDP	Low
Stage 2: Status update					
Client	Varies	Server IP	Varies	TCP	Low to medium
Server	Varies	Client IP	Varies	TCP	Low to medium
Stage 3: Task execution					
Client	7777	Server IP	Varies	UDP	High
Server	Varies	Client IP	7777	UDP	High

Troubleshooting

This appendix includes the following topics:

- Ghost.exe errors messages
- Ghost.exe problems
- Symantec Ghost Console errors
- Symantec GhostCast errors
- Symantec Ghost and legacy network cards
- About command-line or scheduled tasks
- Problems running Symantec Ghost
- About writing to or restoring from a recordable CD or DVD

Ghost.exe errors messages

A Symantec Ghost error message consists of an error number and a description.

A Ghosterr.txt file is generated when an abort error occurs.

See "Hard-drive detection and diagnostic information" on page 619.

More information about Ghost.exe error messages is available on the Symantec Ghost Technical Support Web site:

www.symantec.com/techsupp

Table L-1 details some error messages that you may encounter.

Table L-1 Error messages

Error code	Description
8006, 8008	The trial period of the evaluation has expired. Visit the Symantec Web site at http://www.symantec.com for details on how to purchase Symantec Ghost.
10030	Symantec Ghost was unable to communicate with the GhostCast Server. Check that the GhostCast session name is correct and, the GhostCast Server is ready to accept clients.
10098	The partition number must be included in the command-line switches. See “Command-line switches” on page 522.
10010	Incorrect path/file syntax. Ensure that the path and file name are correct. Also make sure that you have the proper user rights to read or create the image file.
19906	Symantec Ghost was unable to establish a connection with the GhostCast Server. See “About the Wattcp.cfg configuration file” on page 559.
19910, 20070	No packet driver was found. See Table L-5 on page 606.
19913	Cannot find the BOOTP/DHCP server. Ensure that the computer is connected to the network and that a BOOTP or DHCP server is set up for this subnet.
19916	Duplicate IP address detected. An IP address has been allocated that is already in use.
19900	The GhostCast session is set up incorrectly. Ensure that the TCP/IP settings are correct.
29005	If you restore an image to a disk configured as a dynamic disk with a single simple volume on it on a Vista RTM Ultimate computer then Ghost32 fails with the following error: write sector failure 29005. The workaround is as follows: In Disk Manager, convert the disk to an mbr disk and then restore the image.

Table L-1 Error messages *(continued)*

Error code	Description
CDR101: Not ready reading drive X, Abort, Retry, Fail	A system error message. This error is not caused by Symantec Ghost. It is caused by malfunctioning hardware or software configurations. The image file on the CD is not readable. To verify this, go into DOS and copy the image file off of the CD-ROM using copy verification, copy /v.

Universal Network Driver errors

If you have problems when starting a computer from a boot disk set that includes the Universal Network Driver(UNDI driver), ensure that the LAN cable is plugged in.

Table L-2 lists errors that you may encounter when using the UNDI driver on specific computers.

Table L-2 UNDI driver error messages

Error	Description
UNDI Option ROM not detected!	This error may be encountered on DELL laptops as the BIOS does not support the UNDI installer. Create the boot package again using the specific network driver template for the computer.
Multicast session starts and then hangs	If this error is encountered on the following computers then the work around for this error is to use Directed Broadcast or Unicast: ■ Computer based on a "ABIT AV8 - 3rd Eye" motherboard with a "VIA K8T800 PRO" chipset that includes an integrated "VIA Networking Velocity Family Gigabit Ethernet Adapter". ■ HP ProLiant ML350 G3 Server (specific model is ML350T03) with HP NC7760 Gigabit server network adapter. ■ HP Compaq D330 Microtower Desktop PC with BroadCom NetExtreme Gigabit Ethernet for hp network adapter. If this problem is encountered in other computers, set the RECEIVE_MODE to 6 which may allow the UNDI driver to work in multicast mode.
Bad UNDI Image Load undi driver failed with status code 0xC6	To use the UNDI driver with the 3Com PXE server, verify that in the 3Com PXE boot image properties, Keep UNDI is set to Yes.

Ghost.exe problems

Some errors may occur that do not produce an error code.

Vista volume containing system restore points

When a Vista volume containing system restore points is mounted in a Windows XP/2003 volume, the restore points are deleted. The following error is displayed:

Question 1854: A source volume could not be locked as it is in use by another process. Do you wish to attempt to force a dismount on the volume?

Run the task on Vista WinPE or in DOS as a work-around for this error.

Resolving interrupt conflicts

Ghost might hang when running a task. This might be caused by an interrupt conflict between a network device, and a mass storage device. You can use the Symantec Ghost tool Irqcfg in several different ways to solve this problem.

You can find this tool in the following template directories:

- \Documents & Settings\All Users\Symantec\Ghost\Templates\Universal Packet Driver v2 [irqcfg]\
- \Documents & Settings\All Users\Symantec\Ghost\Templates\Universal NDIS Driver v2 [irqcfg]\

You can run Irqcfg in the command line with the summarize switch. The summarize switch causes Irqcfg to display PCI devices and IRQ that are on the computer and any conflict between the devices. The syntax for this switch is as follows:

```
irqcfg /summarize
```

You can also run Irqcfg without parameters. Irqcfg tries to resolve conflicts between devices. This might cause other problems, depending upon the configuration that you are using. Run the Irqcfg tool before the template installs the network driver.

You can run Ghost using a boot package that includes Irqcfg. Irqcfg attempts to resolve the conflicts. You must use the Ghost Boot Wizard to create the boot package and you must use the driver templates that include the tool.

The following driver templates include Irqcfg:

- Universal Packet Driver v2.0 [irqcfg]
- Universal NDIS Driver [irqcfg]

You can run the Irqcfg tool as a driver in Config.sys using the following syntax:

```
DEVICE=\net\irqcfg.exe
```

You can also add the Irqcfg tool to a network template if you have an interrupt conflict using the template. Use the Ghost UNDI irqcfg templates as an example.

Writing to USB CD/DVD

Ghost does not always detect that a USB CD/DVD writer is available to be written to because some USB CD/DVD writers can take several seconds to respond. The work-around to this problem is to wait several seconds and then open the file requestor dialog again. This workaround usually gives the device time to respond.

Booting from a 3Com PXE image

Some newer (PXE 2.1) clients may hang when starting from a 3Com PXE image if the Base Code is set to keep. By default, the Ghost Boot Wizard has the base code set to keep. This ensures that earlier versions of the clients (for example, PXE 0.99) start correctly and retain backward compatibility with earlier Ghost releases. The backward comparability is required because older PXE clients require the base code to enable the UNDI drive to operate correctly and therefore the Universal Packet Driver to operate correctly. To prevent this problem modify the PXE image using the 3Com boot image editor and turn off the keep base code option.

Starting from a PXE image on a Dell Dimension 8100 computer

On a Dell Dimension 8100 computer a conflict between the PXE BIOS and the Ghost USB code causes Ghost.exe to fail. Run Ghost with the -nousb switch to overcome this problem.

USB and FireWire support

Ghost.exe may not start if you have created the boot disk with the Ghost Boot Wizard and one of the following options:

- You have specified to override BIOS USB support when creating the boot disk
- You have specified to override BIOS FireWire support when creating the boot disk
- You have started Ghost with either the -forceusb or -force1394 switch

With these specifications Ghost takes control of either the USB or FireWire controller. The control is not always successful especially if the BIOS actively uses them. If you use the -forceusb switch then no USB device is usable. In most cases if you want to use either a FireWire or USB disk then Ghost can do so without using the override or switch.

Phoenix-Award BIOS computers

A computer with a Phoenix-Award BIOS does one of the following:

If the computer is started from a USB flash drive, which includes PC DOS	Hang
If started from an ISO image or CD/DVD with PC DOS	Display the error; Boot disk failure

The work-around for this problem is to start the computer with a floppy disk boot package. You can also create a boot package on an ISO image or USB flash drive with MS DOS taken from a Windows 98 installation.

Symantec Ghost Console errors

If a task to restore a backup fails and your backups are stored in a mapped network location, ensure that the network connection is still available.

Table L-3 details some error messages that you may encounter.

Table L-3 Console error messages

Error	Description
Conflict with existing set of credentials	The Ghost Configuration Server has a domain logon that is used to create computer accounts for Windows 2000/XP clients. Only one sessions is allowed from a client to a server when using Microsoft networking. If you have mapped a drive to a share on the Primary Domain Controller (PDC) the configuration Server cannot log on to the domain. The conflict error is displayed. For more information see the following Microsoft Knowledgebase article at the following URL: http://support.microsoft.com/?kbid=106211

Table L-3 Console error messages *(continued)*

Error	Description

Connection: Credentials conflict	This error appears when you are attempting a remote client install and the Console already has a connection to the client computer.
	Try the following:
	1 From the command line, execute the following to establish a connection to the client computer:
	`net user \\machine\c$`
	2 Execute the following to force shut the open connection to the client computer:
	`net use /delete \\machine\c$`
	3 Retry the remote client installation.
	If the remote client install fails again, restart the Console computer.

Unable to obtain IP address via DHCP	This message may appear after loading the boot partition and restarting the computer. Try configuring the network interface card (NIC) using the utility that came with it. You may need to alter the speed and duplex settings. This error can also be caused when using dual NIC computers. See "About Symantec Ghost support for multiple network interface cards " on page 290.
Mixed domain issue	If you have installed the Symantec Ghost Console on a Windows 2000 SP 4 computer that is a member of a Windows 2000 mixed domain, then the Console does not add client computers to Windows 2003 native domains.

About using Ghost with NTFS files

There are some errors that may occur when using Ghost with NTFS files.

Table L-4 Errors when using Ghost with NTFS files

Error message	Description
Error 25002 - Unhandled condition encountered: Attr translation will result in corruption of MFT table	This error occurs when Ghost has finished mapping the location of disk clusters used to store data for an NTFS file and determines that it cannot allocate enough space to store those cluster mappings. This situation can occur with very fragmented or compressed NTFS files. Possible workarounds include the following: ■ Defragmenting the source drive before cloning or creating an image. ■ Using the -ntc- switch, which lets Ghost attempt to allocate disk clusters at or near their original location on the source volume. This minimizes the amount of disruption to the cluster mappings and the subsequent space required to store the mappings.
Error 25058 - "Unable to locate enough contiguous free space to load run. Increase the destination partition size or run Ghost with -NTC- switch."	This error occurs when Ghost cannot find a large enough free space to store a section of an NTFS file. There may be enough total free space in smaller allocations scattered about the volume to store the contents of the file, but due to the fact that Ghost does not attempt to break up contiguous sections of files as they are cloned, it produces this error. When cloning volumes with minimal free space and containing large files comprised of a small number of contiguous sections, the operation will be particularly vulnerable to this error. Possible workarounds include the following: ■ Defragmenting the source drive before cloning or creating an image. ■ Using the -ntc- switch, which lets Ghost attempt to allocate disk clusters at or near their original location on the source volume. This minimizes the amount of disruption to the cluster mappings and the subsequent space required to store the mappings.

Table L-4 Errors when using Ghost with NTFS files *(continued)*

Error message	Description
Error 24010 - "Encountered BAD used MFT Record - run CHKDSK"	This error can occur when cloning or creating an image from a source NTFS volume. It may be caused by either corruption or by a bad sector on the drive. Possible workarounds include the following: ■ If the file system is corrupted, running CHKDSK /F on the NTFS volume before attempting to clone it again will pick this up. ■ If the problem is due to a bad sector, run Ghost with the -fro switch to force Ghost to read sectors one-by-one if it detects a bad sector during a read of a range of bad sectors.
Error 25030 - "NTFSGetClusterCount failed"	This error can occur when Ghost is cloning or creating an image of an NTFS volume. It is most likely to have been caused by file system corruption. A possible workaround is to do the following: ■ If this is a file system corruption, run CHKDSK /F on the volume.

Symantec GhostCast errors

If you are having problems using Symantec Ghost or the Symantec GhostCast Server ensure that you have the latest drivers for your network card installed. The manufacturer of your network card or computer should have the latest drivers available on its Web site.

Table L-5 lists specific answers to GhostCasting errors. Use the solution most closely related to the problem that you are experiencing.

Table L-5 Symantec GhostCast errors

Problem	Solution
When I launch Symantec Ghost, I am unable to select GhostCasting.	Symantec Ghost uses a packet driver or NDIS2 drivers to perform GhostCasting. If Symantec Ghost does not detect a packet driver in memory or if the packet driver is inappropriate for your network card, the GhostCasting option is not available. You must have a boot disk that loads the appropriate packet driver or NDIS2 drivers for your network card. Use the Ghost Boot Wizard to create a packet-driver boot disk. See "Creating a Network Boot Package" on page 272.

Table L-5 Symantec GhostCast errors *(continued)*

Problem	Solution
Symantec Ghost times-out after I type a session name.	This is usually caused by a connectivity problem between the server and the client. To determine the source of the problem try the following: ■ Verify the spelling of the session name on both the client and the GhostCast Server. ■ Check all physical connections, including cabling, hubs, routers, switches, and so on for physical problems. ■ Verify that any routers present between the server and the client are configured properly and have GhostCasting enabled. ■ Check the Wattcp.cfg file for a valid IP address and subnet mask if you are using static IP. ■ Confirm that a network communication topology problem exists by connecting the GhostCast Server and client to a dumb hub or cross-over cable. Then use, static IP to try to complete the task. You can also try pinging the IP address of the client computer from the server computer. If you are not able to ping the client, there is a communication problem, and IP packets are not being passed between these computers. To ping the IP address of the client computer: ■ Start the client computer. ■ On the Symantec Ghost main menu, click GhostCast and select one of the following: ■ Unicast ■ Direct Broadcast ■ Multicast Do not enter a session name. Stop at the dialog box requesting the session name. This will initialize the IP address. ■ Ping the client from the server.

Table L-5 Symantec GhostCast errors *(continued)*

Problem	Solution
When I begin sending data via GhostCasting, the session fails or times out.	Add a RECEIVE_MODE=X value to the Wattcp.cfg file. Add RECEIVE_MODE=5 first, then try 6. See "About the Wattcp.cfg configuration file" on page 559. If you are GhostCasting across routers or switches, you must enable a GhostCasting protocol on these devices. For more information on GhostCast protocols, refer to your router or switch documentation.

Symantec Ghost and legacy network cards

Windows 95 and 98 are plug-and-play operating systems. They reconfigure most network cards if they find an IRQ conflict. Because GhostCasting runs on a DOS level and DOS is not a plug-and-play operating system, IRQ conflicts may arise.

Most newer network cards come with a software configuration utility that automatically checks for IRQ conflicts and reconfigures the card if a conflict exists. Otherwise, you must manually change the IRQ of the network card. Refer to your network adapter manual for more information on changing the IRQ address of your card.

DOS drivers can also have problems detecting the type and speed of your network. A DOS configuration utility that may have been supplied by the network card manufacturer lets you set these explicitly.

About command-line or scheduled tasks

Normal task logging can be viewed from the Console task log.

See "Monitoring Symantec Ghost Console activity" on page 241.

When you launch a task from the command line or from Scheduler, you can also check two error log files for the cause of failure of a task.

Console log.txt logs the success or failure of a task launched from the command line or Scheduler. However, if a task has been initiated from the Scheduler, then the Console might not start. In this case, you can check Schedulgu.txt for a cause of failure.

Failure is most often caused by a lack of user name and password.

See "Setting up backup regimes" on page 167.

Problems running Symantec Ghost

Some errors may occur that do not produce an error code.

Cloning Windows 2000/XP computers

If a Windows 2000/XP computer fails to start after being cloned it may not have the correct mass storage controller driver configured and loaded for the hardware on which it starts. This failure may be due to hardware differences between the source and destination computers. You can fix this problem by editing the section SyprepMassStorage in Sysprep.inf to specify one or more mass storage controllers that you want Windows to load.

Vista partition restore

After a NTFS Vista partition is restored the following error is reported in the event viewer:

The default transaction resource manager on volume <drive> encountered an error while starting and its metadata was reset. The data contains the error code.

The warning is issued, but does not affect the successful restore of the partition.

Incremental backup of Symantec AntiVirus 10.0.2

An incremental backup of a computer installed with Symantec AntiVirus 10.0.2 fails to restore Symantec AntiVirus successfully. The backup is successful, but on the client the following error is displayed:

Symantec AntiVirus Auto-Protect failed to load.

The workaround for this problem is to repair the installation of Symantec AntiVirus after restoring the backup.

AutoInstall limitations

Table L-6 lists some limitations when using AutoInstall to install specific applications.

Table L-6 AutoInstall limitations

Application	Description
Lotus Smart Suite Millennium Edition	Lotus Smart Suite Millennium Edition cannot be installed to multiple users on a single computer. It must be installed for each user as a licensing protection. If the AutoInstall package is deployed when a user is logged onto the computer then it is installed for that user. If no user is logged on then it is installed for the last logged-on user.
McAfee Office Suite	An AutoInstall package containing McAfee Office Suite installs, but may produce an error message when the application is launched. The error is due to a font being installed to the McAfee installation directory, and not the Windows fonts directory. A work-around for this problem is to install the fonts as follows: **1** In the Control Panel, open the fonts folder. **2** Install the font.

Executing a clone and configuration change task

A clone and configuration change task may fail to apply the configuration with the following setup:

- The image file contains a Console client from a version previous to Symantec Ghost 8.2.
- The configuration settings specify that the client computer is added to an Active Directory container or that the Netbios name be overwritten.

If the Console client does not support Active Directory containers or the option to overwrite Netbios names then you do one of the following:

- Recreate the image with a new Console client.
- Change the configuration settings.

Installing a client remotely

If a remote install to Windows 2000/XP clients, which are members of an Active Directory domain fails check that the time on the client computer matches the Primary Domain Controller (PDC) time. Windows 2000/XP computers use the time as a part of security authentication.

Transferring files to clients with Firewalls installed

The file transfer part of a task may time-out with the following setup:

- When you are transferring files to one or more clients
- The client computer is using the default Windows XP firewall.

The firewall causes the time-out by preventing the Ghost Client seeing the multicast packets. To solve this problem do one of the following:

- In the Task Properties window, on the Network tab, select Unicast
- Disable the Windows XP firewall.

Wake on LAN (WOL)

WOL does not work correctly for some hardware and software configurations when you fully shut down the computer. In all cases, the Ghost Console sends the required message to the computer but sometimes the computer does not wake up. A computer in standby mode always wakes up using WOL.

Check the following:

- Ensure that WOL is enabled on the card itself using DOS or Windows configuration programs for the card.
- Ensure that WOL is enabled in the network card drivers under the operating system.
- Ensure that WOL is enabled in the BIOS of the computer.

Joining client computers to Active Directory Domains

If you have problems joining clients to Active Directory-based domains ensure that the Domain Name Server (DNS) is configured correctly.

You may want to use the DCDIAG tool available from the Windows 2000 Server resource kit.

Network card not found/Card not installed

This error can occur if a driver cannot find a network card installed on your computer. The error can occur when you start your computer with a Ghost boot disk or run a task in the virtual partition. . Check the following:

- Ensure that you selected the correct network card template when you created the Ghost boot disk.

- Ensure that the plug-and-play operating system setting in the BIOS does set up plug-and-play devices.

  Locate the Plug and Play OS setting in the BIOS configuration screens. Some network cards require that this setting be set to No before they function in DOS. See your computer manual for instructions specific to your computer. If the driver still fails to load, set the plug-and-play operating system setting explicitly to Yes and try again.

  Your BIOS may phrase the name of this setting differently; its function is the same.

Cannot start from drive A

If your computer does not check drive A first on startup, use your computer's Setup program to change its settings. The Setup program may be named differently on your computer, for example, BIOS settings or CMOS settings. You may need to refer to the computer manufacturer's documentation for the key sequence to enter the Setup program.

Be careful when you make changes using your computer's Setup program. If you have never used it before, you may want to refer to your computer manufacturer's documentation.

To change your computer's settings

1. Restart your computer.
2. When a message appears telling you the key or keys to press to run Setup, press the appropriate key or keys.
3. Set the Boot Sequence to boot drive A first and drive C second.

   Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program's Help system, refer to the documentation that came with your computer, or contact your computer manufacturer.
4. Save the changes, then exit the Setup program.

Windows blue screen

If you are restoring, backing up, or cloning a computer onto another Windows computer with incompatible hardware, you may get a blue screen. To prevent this problem, do not use incompatible hardware, or on Windows 2000/XP, use Sysprep when creating the image file.

Try restoring the computer using the -fdsp or -fdsz switch and ensuring the partition sizes are the same on the destination drive as in the image file.

See “About Sysprep” on page 459.

See “About Symantec Ghost switches” on page 521.

Missing hibernation file

If the hibernation file is missing, the following message may appear:

“Cannot hibernate because there is no hibernation file or the hibernation file has an error.”

Recreate the hibernation files according to the instructions for your Windows operating system.

Getting out of the virtual partition

If your client computer is stuck in the virtual partition, you can use the executable Ngctdos.exe to restart your computer back into Windows.

To restart your client computer back into Windows

1. At the command line, type **ngctdos -hide**
2. Press **Enter**.

About cancelling a Ghost.exe operation

If you start a Ghost.exe operation, you can abort the process by pressing Ctrl+C. Be aware that pressing Ctrl+C leaves the destination image file, disk, or partition in an unknown state.

Installing and uninstalling Symantec Ghost

If you have problems installing or uninstalling Symantec Ghost, providing a log file of the installation or uninstallation assists Technical Support in analyzing the problem.

Add the following to the end of a command line to create a Logfile.txt file in the root directory of drive C: – `/l*v c:\logfile.txt`

See “About installation interface types” on page 585.

To add logging to the end of a command line for Windows NT/2000/XP installations, use the following command line:

```
Msiexec.exe /I <install package location> /l*v c:\logfile.txt
```

Where <install package location> is the path to the installation package that you want to install.

For example,

d:\Install\SymantecGhost.msi, or d:\Install\Client\Client.msi.

About connecting using USB peer-to-peer

If you cannot connect using USB peer-to-peer, then try altering the drivers that are installed. You could also try different ports.

About writing to or restoring from a recordable CD or DVD

If you are having problems saving a file directly to or restoring from a CD-R/RW or DVD, there are a number of possible solutions.

Supported CD-R/RW and DVD drives

Symantec Ghost supports a large number of CD-R/RW and DVD drives. Check that your drive is listed here at the following URL:

http://www.symantec.com/techsupp/cddvddriver

Inaccessible CD-ROM drive

When writing to a compatible CD-R/RW drive, the drive may not be accessible to Symantec Ghost. To discover whether this is a problem, check Ghosterr.txt, located in the same directory as the Ghost executable.

See “Hard-drive detection and diagnostic information” on page 619.

IDE CD-ROM drives

To see if an IDE CD-R/RW drive is inaccessible to Symantec Ghost, open Ghosterr.txt or the log file.

The IDE sections are named one or more of the following:

- IDE
- IDE for PIO
- IDE for UDMA

If the word Unavailable appears under these headings, then check the following:

Ensure that the firmware for your CD-R/RW drive is current.	Check the Web site for the CD-R/RW drive manufacturer for the most current firmware.
Update the computer BIOS with the latest version, following the computer manufacturer's instructions.	The computer BIOS may not be enabled to detect the IDE drive.
Check the controller to which the IDE drive is attached.	The IDE drive might be attached to a controller that requires a driver for access. Check the documentation for the controller to determine whether you need to load an IDE driver when starting your computer. Drivers may be needed for controllers that are included on the computer's motherboard. Reading and writing from a CD-R/RW drive are different processes. You may be able to access a CD-R/RW drive from DOS to read the drive, but not to write to the drive.

SCSI CD-R/RW drives

To see if a SCSI CD-R/RW drive is inaccessible to Symantec Ghost, open Ghosterr.txt or the log file. The SCSI section is named ASPI.

If the word Unavailable appears under the ASPI heading, then check the ASPI files loaded from Config.sys. The following files must be loaded:

- aspi2dos.sys
- aspi4dos.sys
- aspi8dos.sys
- aspi8u2.sys

All SCSI controllers require an ASPI driver. The listed ASPI files are sufficient for most SCSI controllers. The controller might require a driver that is usually supplied with the controller. Copy the driver to the bootable floppy disk and edit Config.sys to load the driver. The controller's documentation should include the correct syntax for loading the driver from DOS. If you do not have the driver, then contact the controller's manufacturer.

If the correct ASPI drivers are loaded, then update the computer BIOS and the controller BIOS with the latest versions, following the manufacturer's instructions.

For example, older versions of the BIOS for the Adaptec 2940 controller card are not compatible with Symantec Ghost.

CD-R/RW disc

The CD disc to which you are writing may have a problem. Try the following:

Use an unformatted CD-RW disc.	To write an image to a CD-RW disc that you have already used, use the CD-RW utility to wipe all information off the disc, including the file system.
Try a second disc.	If you have tried one disc only, then you have not eliminated the possibility of a damaged disc. Try again, using an unused new disc.
Try a different brand of disc.	Some CD-R/RW drives do not work with low-quality discs or specific manufacturers of discs. Try a different brand.
Use a standard 650 MB CD-R/RW disc.	Symantec Ghost or the CD-R/RW drive may have problems with high-speed discs or with discs that record more information.

Loading Ghost.exe from the floppy disk drive

If you have problems loading Ghost.exe from a floppy disk, you can sometimes resolve a problem by loading Ghost.exe from a hard drive.

For example, if you are creating an image file of the first partition, copy Ghost.exe to the second partition. Edit Autoexec.bat to start Ghost.exe from the second partition as follows:

```
d:\ghost.exe
```

Do not load Ghost.exe from the partition that is being cloned.

Outdated computer BIOS

Your computer might have an old BIOS version. Check the manufacturer's Web site for an update. Follow the manufacturer's instructions for updating the BIOS.

Outdated CD-R/RW drive BIOS

The CD-R/RW drive might have an old BIOS version. An update to the BIOS often fixes problems. Check the manufacturer's Web site for an update. Follow the manufacturer's instructions for updating the BIOS.

About PC-DOS or MS-DOS

If you put PC-DOS system files on the boot disk, recreate the boot disk with MS-DOS system files. You can choose MS-DOS while creating the boot disk.

See “Selecting the PreOS version to use” on page 258.

High compression

Try using a lower or no compression when creating the image file.

Using third-party software to write to the CD-R/RW disc

If you are unable to write directly to a CD-R/RW disc using Symantec Ghost, you can create the Ghost image and then use third-party software to write to the CD-R/RW disc. If you use software to write an image file directly to the CD, you may experience problems when restoring the image file. Software designed to write directly to a CD, such as Adaptec Direct CD, uses a different file format. Therefore, the copied files are not recognized by Ghost.

If you are writing directly to a CD using third-party software, use a program that lays out the format of the disc before it writes it, such as Adaptec E-Z CD Creator.

Symantec Ghost does not provide technical support for third-party software, but details on this method can be found in the Knowledge Base on the Symantec Support Web site.

To write an image to CD using third-party software

1. Create the Ghost image file and save it to a temporary location.
2. Collect and edit the other required files.
3. Use third-party software to save the image file and other required files to the CD-R/RW disk.
4. Do one of the following:
   - Make the CD bootable, including the drivers to let Ghost read the CD.
   - Create a boot disk using the CD/DVD Startup Disk with Ghost option in the Ghost Boot Wizard. This disk will be required when you want to restore the image from the CD.

About restoring from an image spanned over multiple CD/DVDs

Using GhostCast to restore from an image that is spanned over multiple CD/DVDs fails because GhostCast cannot find the second Ghost image on the second CD. A GhostCast session cannot be interrupted to prompt for the second CD. The workaround is to copy each of the image files to the same directory and use GhostCast to restore the image from that directory.

Diagnostics

This appendix includes the following topics:

- Hard-drive detection and diagnostic information
- Elementary network testing techniques
- Testing TCP/IP functionality

Hard-drive detection and diagnostic information

Symantec Ghost can generate diagnostic reports that outline the hard-drive devices detected, other system-related information, and error conditions when they are detected.

View Log

If you are running tasks from the Console, a task log may be generated. This can help in diagnosing problems.

See "To view the Task Log" on page 242.

Abort error file (Ghosterr.txt)

An error message consists of an error number, a description, and possibly a suggestion of how to remedy the problem.

The Symantec Ghost abort error file includes these details along with additional drive diagnostics and details required to assist Technical Support in diagnosing the cause of the problem.

The Symantec Ghost abort error file is generated when Symantec Ghost detects an erroneous condition that Symantec Ghost is unable to recover from or work around. The Ghosterr.txt file is generated in the current directory. If this location is read-only, the Ghosterr.txt file output location should be redirected. The location and file name of the abort file can be altered using the -afile=drive:\path\filename command-line switch.

See "Ghost.exe errors messages" on page 597.

Creating a full diagnostic statistics dump summary

A full diagnostic statistics dump summary file contains the detected hard-disk geometry details along with other Symantec Ghost statistics. The full Symantec Ghost diagnostic statistics dump can be created using the command-line switch -dd. The default statistics dump file name is Ghststat.txt. You can alter the location and file name by adding the -dfile=drive:\path\filename command-line switch.

For example:

```
ghost.exe -dd -dfile=c:\diagnose\log.txt
```

Elementary network testing techniques

Following are the methods that you can use to test networking functionality:

- Testing TCP/IP functionality
- Generating a GhostCast log file for Technical Support to use in diagnosing problems

Testing TCP/IP functionality

There are several testing utilities available in the Microsoft TCP/IP application suite. Examples are the output of two Windows TCP/IP utilities, Ping.exe and Ipconfig.exe.

The Ping.exe utility shows TCP/IP networking response and can be used to show connectivity between computers. For a mapped network volume connection, a client can ping the server and vice versa to check that they have basic connectivity at any time.

For GhostCast connections, Symantec Ghost only responds to a ping request sent from another computer if it is in GhostCast or TCP/IP peer-to-peer mode and running Ghost in that mode.

Ping utilities that do not indicate multicast packets can traverse between two points on a network. This determines that Unicast will work but not necessarily Multicast or Direct Broadcast. For example, a ping test may indicate successful TCP/IP operation between two computers on differing subnets, while GhostCast packets may not be able to cross due to a nonmulticast-enabled router that separates the subnets.

Pinging a local host shows basic local TCP/IP functionality.

Pinging another computer

The address used in this example identifies the local host on the network.

On the GhostCast Server, a DOS prompt dialog box is run with the following session:

```
C:\> Ping 192.168.100.3
Pinging [192.168.100.3] with 32 bytes of data:
Reply from 192.168.100.3: bytes=32 time<10ms TTL=128
Reply from 192.168.100.3: bytes=32 time<20ms TTL=128
Reply from 192.168.100.3: bytes=32 time<20ms TTL=128
Reply from 192.168.100.3: bytes=32 time<20ms TTL=128
```

The outcome of the first command indicates that the client using the IP address 192.168.100.3 received the ping request and replied. This indicates basic TCP/IP operation between the two computers. This does not indicate that multicast packets can traverse between the two computers.

On Windows Vista/XP/2000 computers, you can run the ipconfig to get information about the Windows IP configuration and the IP address for the local area connection.

Generating a GhostCast log file

You can generate a GhostCast log file for Technical Support diagnostic purposes. Logging can slow down the GhostCasting process and should be used to assist in diagnosing problems noted during normal use.

The diagnostic levels in order of increasing detail are shown in Table M-1.

Table M-1 Diagnostic levels

Diagnostic level	Description
Error	Reports any unrecoverable error that occurs during the GhostCast session. Use of this level should not affect session performance.
Statistics	Reports all errors and additional statistic information on completion of the session. Use of this level should not affect session performance.
Warning	Reports all statistic level details and includes any additional warning messages. Use of this level may affect session performance.

Table M-1 Diagnostic levels *(continued)*

Diagnostic level	Description
Information	Reports all warning level details and adds additional diagnostic information. Use of this level may affect session performance.
All	Reports all logging messages. Use of this level reduces GhostCast session performance.

Generating a GhostCast Server log file

You can generate a log file while running the Symantec GhostCast Server.

To generate a GhostCast Server log file

1. On the GhostCast Server, on the File menu, click **Options**.
2. Use the Symantec GhostCast Server as required.

   The Symantec GhostCast Server can be used for normal operation and the log file can be inspected upon completion.

Generating a GhostCast Client log file

You can generate a log file while running Ghost.exe on a client computer.

To generate a GhostCast Client log file

1. Add the logging switch -jl:loglevel = filename, where loglevel specifies the diagnostic reporting level. (E, S, W, I, or A.)

   For example:

   ```
   ghost.exe -jl:a=d:\filename
   ```

   See “About Symantec Ghost switches” on page 521.
2. Select a location for the log file other than the drive being written to by Symantec Ghost. It should have sufficient space to create the file.

   For example, to create a GhostCast log file, D:\Logs\Multi.log, to log all information while using GhostCasting in interactive mode:

   ```
   ghost.exe -jl:a=d:\logs\multi.log
   ```
3. Run Ghost.exe.
4. Connect to the GhostCast Server.

   On completion, the log is written to the selected location.

User Migration supported applications

This appendix includes the following topics:

- Microsoft Outlook
- Microsoft Outlook Express
- Microsoft PowerPoint
- Microsoft Project
- Microsoft Visio
- Microsoft Word
- Mozilla FireFox
- Mozilla Thunderbird
- MSN Messenger
- NetMeeting
- Palm Desktop
- Symantec Norton AntiVirus
- Symantec pcAnywhere
- Windows Desktop Display
- Windows Explorer
- Windows Accessibility Settings
- Windows Mouse Settings
- Windows Regional Settings
- Windows Sound and Multimedia Settings
- Windows Taskbar and Start Menu
- WinZip
- Yahoo Messenger

About supported applications

Symantec Ghost supports migrating application settings using the Ghost Console user migration feature and Symantec User Migration. Details of the supported applications and any caveats are listed here.

Adobe Acrobat Reader

Ghost User Migration supports the following:

- Adobe Acrobat Reader 5.0
- Adobe Acrobat Reader 5.1
- Adobe Acrobat Reader 6.0
- Adobe Acrobat Reader 7.0

Adobe Acrobat Reader 5.0

Table N-1 describes the Adobe Acrobat Reader 5.0 supported settings.

Table N-1 Adobe Acrobat Reader 5.0 supported settings

Settings Location	Exceptions
Edit->Preferences->Accessibility->Display	
Edit->Preferences->Accessibility->Custom Scheme	
Edit->Preferences->Accessibility->Content Delivery	
Edit->Preferences->Comments->Comments	
Edit->Preferences->General->Display	
Edit->Preferences->General->Magnification	
Edit->Preferences->General->Smoothing	
Edit->Preferences->General->Options	
Edit->Preferences->Forms->Forms	
Edit->Preferences->Full Screen->Full Screen Navigation	
Edit->Preferences->Full Screen->Full Screen Appearance	
Edit->Preferences->Identity->Identity	
Edit->Preferences->Options->Web Browser Options	
Edit->Preferences->Options->Startup	
Edit->Preferences->Options->Miscellaneous	
Edit->Preferences->Search->Include in Query	

Table N-1 Adobe Acrobat Reader 5.0 supported settings *(continued)*

Settings Location	Exceptions
Edit->Preferences->Search->Results	
Edit->Preferences->Search->Display	
Edit->Preferences->Search->View Dialog Options	
Edit->Preferences->Update	
Edit->Preferences->Web Buy	
Edit->Preferences->Web Buy->Warnings	
Edit->Preferences->Web Buy->Select Other Identifiers	
Edit->Preferences->Web Buy->Bookshelf	
Edit->DocBox->Preferences	
Document->Select Reading Order	

Adobe Acrobat Reader 5.1

Table N-2 describes the Adobe Acrobat Reader 5.1 supported settings.

Table N-2 Adobe Acrobat Reader 5.1 supported settings

Settings Location	Exceptions
Edit->Preferences->Accessibility->Alternate Document Color	
Edit->Preferences->Accessibility->Custom Scheme	
Edit->Preferences->Accessibility->Content Delivery	
Edit->Preferences->Comments->Comments	
Edit->Preferences->Digital Signatures	
Edit->Preferences->General->Display	
Edit->Preferences->General->Magnification	
Edit->Preferences->General->Smoothing	
Edit->Preferences->Forms->Forms	
Edit->Preferences->Full Screen->Full Screen Navigation	

Table N-2 Adobe Acrobat Reader 5.1 supported settings *(continued)*

Settings Location	Exceptions
Edit->Preferences->Full Screen->Full Screen Appearance	
Edit->Preferences->Identity->Identity	
Edit->Preferences->Options->Web Browser Options	
Edit->Preferences->Options->Startup	
Edit->Preferences->Options->Miscellaneous	
Edit->Preferences->Search->Include in Query	
Edit->Preferences->Search->Results	
Edit->Preferences->Search->Display	
Edit->Preferences->Search->View Dialog Options	
Edit->Preferences->Self-Sign Security	
Edit->Preferences->Update	
Edit->Preferences->Web Buy	
Edit->Preferences->Web Buy->Warnings	
Edit->Preferences->Web Buy->Select Other Identifiers	
Edit->Preferences->Web Buy->Bookshelf	
Edit->DocBox->Preferences	
Document->Select Reading Order	

Adobe Acrobat Reader 6.0

Table N-3 describes the Adobe Acrobat Reader 6.0 supported settings.

Table N-3 Adobe Acrobat Reader 6.0 supported settings

Settings Location	Exceptions
Edit->Preferences->Accessibility->Document Color Options	
Edit->Preferences->Accessibility->Tab Order	
Edit->Preferences->Digital Signatures->Appearance	

Table N-3 Adobe Acrobat Reader 6.0 supported settings *(continued)*

Settings Location	Exceptions
Edit->Preferences->Digital Signatures->Signing Method	
Edit->Preferences->Digital Signatures->Verifying Signatures	
Edit->Preferences->Digital Signatures->Advanced Preferences	
Edit->Preferences->Forms->General	
Edit->Preferences->Forms->Background Color	
Edit->Preferences->Forms->Auto-Complete	
Edit->Preferences->Full Screen->Full Screen Navigation	
Edit->Preferences->Full Screen->Full Screen Appearance	
Edit->Preferences->General->Selection	
Edit->Preferences->General->Miscellaneous	
Edit->Preferences->Identity->Identity	
Edit->Preferences->Internet->Web Browser Options	
Edit->Preferences->Internet->Internet Options	
Edit->Preferences->JavaScript	
Edit->Preferences->Multimedia->Player Options	
Edit->Preferences->Multimedia->Accessibility Options	
Edit->Preferences->PageDisplay	
Edit->Preferences->Magnification	
Edit->Preferences->Reading->ReadingOrderOptions	
Edit->Preferences->Reading->ReadingOutLoudOptions	
Edit->Preferences->Reading->ScreenReaderOptions	
Edit->Preferences->Search->Search	
Edit->Preferences->Search	
Edit->Preferences->Search->Fast Find	
Edit->Preferences->Smoothing	

Table N-3 Adobe Acrobat Reader 6.0 supported settings *(continued)*

Settings Location	Exceptions
Edit->Preferences->Startup->Opening Documents	
Edit->Preferences->Startup->Application Startup	
Edit->Preferences->Trust Manager	
Edit->Preferences->Trust Manager->Multimedia	
Edit->Preferences->Units	
Edit->Preferences->Update	
Edit->Search	

Adobe Illustrator

Ghost User Migration supports the following:

- Adobe Illustrator 8.0
- Adobe Illustrator 9.0
- Adobe Illustrator 10.0
- Adobe Illustrator CS
- Adobe Illustrator CS2

Adobe Illustrator 8.0

Table N-4 describes the Adobe Illustrator 8.0 supported settings.

Table N-4 Adobe Illustrator 8.0 supported settings

Settings Location	Exceptions
Preferences->General	Settings not migrated to higher versions
Preferences->Type & Auto Tracing	Settings not migrated to higher versions
Preferences->Units & Undo	Settings not migrated to higher versions
Preferences->Guides & Grid	Settings not migrated to higher versions
Preferences->Smart Guides	Settings not migrated to higher versions
Preferences->Hyphenation Options	Settings not migrated to higher versions

Table N-4 Adobe Illustrator 8.0 supported settings *(continued)*

Settings Location	Exceptions
Preferences->Plug-ins & Scratch Disk	Settings not migrated to higher versions
Color Settings->Profiles	Settings not migrated to higher versions

Adobe Illustrator 9.0

Table N-5 describes the Adobe Illustrator 9.0 supported settings.

Table N-5 Adobe Illustrator 9.0 supported settings

Settings Location	Exceptions
Preferences->General	Settings not migrated to higher versions
Preferences->Type & Auto Tracing	Settings not migrated to higher versions
Preferences->Units & Undo	Settings not migrated to higher versions
Preferences->Guides & Grid	Settings not migrated to higher versions
Preferences->Smart Guides	Settings not migrated to higher versions
Preferences->Hyphenation Options	Settings not migrated to higher versions
Preferences->Plug-ins & Scratch Disk	Settings not migrated to higher versions
Preferences->Files & Clipboard	Settings not migrated to higher versions
Color Settings	Settings not migrated to higher versions
Color Settings->Working Spaces	Settings not migrated to higher versions
Color Settings->Color Management Policies	Settings not migrated to higher versions

Adobe Illustrator 10.0

Table N-6 describes the Adobe Illustrator 10.0 supported settings.

Table N-6 Adobe Illustrator 10.0 supported settings

Settings Location	Exceptions
Preferences->General	
Preferences->Type & Auto Tracing	

Table N-6 Adobe Illustrator 10.0 supported settings *(continued)*

Settings Location	Exceptions
Preferences->Units & Undo	
Preferences->Guides & Grid	
Preferences->Smart Guides & Slices	
Preferences->Hyphenation Options	
Preferences->Plug-ins & Scratch Disk	
Preferences->Files & Clipboard	
Preferences->Workgroup	
Color Settings	
Color Settings->Working Spaces	
Color Settings->Color Management Policies	

Adobe Photoshop

Ghost User Migration supports the following:

- Adobe Photoshop 6.0
- Adobe Photoshop 7.0
- Adobe Photoshop CS
- Adobe Photoshop CS2

Adobe Photoshop 5.5

Table N-7 describes the Adobe Photoshop 5.5 supported settings.

Table N-7 Adobe Photoshop 5.5 supported settings

Settings Location	Exceptions
File->Preferences->General	Settings not migrated to higher versions
File->Preferences->Saving Files	Settings not migrated to higher versions
File->Preferences->Display & Cursors	Settings not migrated to higher versions

Table N-7 Adobe Photoshop 5.5 supported settings *(continued)*

Settings Location	Exceptions
File->Preferences->Transparency & Gamut	Settings not migrated to higher versions
File->Preferences->Units & Rulers	Settings not migrated to higher versions
File->Preferences->Guides & Grid	Settings not migrated to higher versions
File->Preferences->Plug-Ins & Scratch Disks	Choose Plug-Ins folder not supported.
File->Preferences->Memory & Image Cache	Available RAM used by Photoshop not supported.
File->Color Settings->RGB Set Up	Settings not migrated to higher versions
File->Color settings->CMYK Setup	Settings not migrated to higher versions
File->Color settings->Grayscale Setup	Settings not migrated to higher versions
File->Color settings->Profile Setup	Settings not migrated to higher versions

Table N-8 describes the Adobe Image Ready 2.0 supported settings.

Table N-8 Image Ready 2.0 supported settings

Settings Location	Exceptions
Edit->Preferences->General	
Edit->Preferences->Saving Files	
Edit->Preferences->Slices	
Edit->Preferences->HTML	
Edit->Preferences->Optimization	
Edit->Preferences->Cursors	
Edit->Preferences->Transparency	
Edit->Preferences->Plug-ins	Not supported

Adobe Photoshop 6.0

Table N-9 describes the Adobe Photoshop 6.0 supported settings.

Table N-9 Adobe Photoshop 6.0 supported settings

Settings Location	Exceptions
File->Preferences->General	Settings not migrated to higher versions
File->Preferences->Saving Files	Settings not migrated to higher versions
File->Preferences->Display & Cursors	Settings not migrated to higher versions
File->Preferences->Transparency & Gamut	Settings not migrated to higher versions
File->Preferences->Units & Rulers	Settings not migrated to higher versions
File->Preferences->Guides & Grid	Settings not migrated to higher versions
File->Preferences->Plug-Ins & Scratch Disks	Additional Plug-Ins Directory not supported.
File->Preferences->Memory & Image Cache	Memory used by Photoshop not supported.
File->Color Settings	Settings not migrated to higher versions
File->Color settings->Working Spaces	Settings not migrated to higher versions
File->Color settings->Color Management Policies	Settings not migrated to higher versions

Table N-10 describes the Adobe Image Ready 3.0 supported settings.

Table N-10 Image Ready 3.0 supported settings

Settings Location	Exceptions
Edit->Preferences->General	
Edit->Preferences->Slices	
Edit->Preferences->Image Maps	
Edit->Preferences->Optimization	
Edit->Preferences->Cursors	
Edit->Preferences->Transparency	
Edit->Preferences->Plug-ins	Not supported

Adobe Photoshop 7.0

Table N-11 describes the Adobe Photoshop 7.0 supported settings.

Table N-11 Adobe Photoshop 7.0 supported settings

Settings Location	Exceptions
File->Preferences->General	
File->Preferences->File Handling	
File->Preferences->Display & Cursors	
File->Preferences->Transparency & Gamut	
File->Preferences->Units & Rulers	
File->Preferences->Guides & Grid	
File->Preferences->Plug-Ins & Scratch Disks	Additional Plug-Ins Directory not supported.
File->Preferences->Memory & Image Cache	Memory used by Photoshop not supported.
Edit->Color Settings	
Edit->Color Settings->Working Spaces	
Edit->Color Settings->Color Management Policies	
Edit->Color Settings->Conversion Options	
Edit->Color Settings->Advanced Controls	

Table N-12 describes the Adobe Image Ready 7.0 supported settings.

Table N-12 Image Ready 7.0 supported settings

Settings Location	Exceptions
Edit->Preferences->General	
Edit->Preferences->Slices	
Edit->Preferences->Image Maps	
Edit->Preferences->Optimization	
Edit->Preferences->Cursors	
Edit->Preferences->Transparency	
Edit->Preferences->Plug-ins	Not supported

AOL Instant Messenger

Ghost User Migration supports the following:

- AOL Instant Messenger 4.8
- AOL Instant Messenger 5.x

AOL Instant Messenger 4.8

Table N-13 describes the AOL Instant Messenger 4.8 supported settings.

Table N-13 AOL Instant Messenger 4.8 supported settings

Settings Location	Exceptions
Buddy List	
Privacy->Who can contact me	
Privacy->Allow users to see	
Privacy->Allow users who know my email address to find	
Sign On->Sign On	Starting AIM when window starts not supported.
Sign On->Internet Connection	
Sign On->Auto Upgrade	
Sign On->Connection	
Idle message	
Away Message->When away	
Buddy Icons	Images to use for buddies not supported. For buddy icons set by others not supported.
Buddy Icons->Display Buddy Icons	
Mail->Mail alert notification	
Mail->Sound	
Stock Ticker->Display	
News Ticker	
News Ticker->Topics	

Table N-13 AOL Instant Messenger 4.8 supported settings *(continued)*

Settings Location	Exceptions
IM Chat->IM Window	
IM Chat->Chat Room Window	
IM/Buddy Chat->Defaults for Composing Windows	
IM/Buddy Chat->Text Magnification	
IM Image->When I open an IM Image	
IM Image->When others send an IM Image	
Talk->when I start a talk session	
Talk->when others want to talk to you	
Talk->Sounds	
File sharing	
File Transfer	
Send buddy list	
Add-ins	

AOL Instant Messenger 5.x

Table N-14 describes the AOL Instant Messenger 5.x supported settings.

Table N-14 AOL Instant Messenger 5.x supported settings

Settings Location	Exceptions
Buddy List	
Privacy->Who can contact me	
Privacy->Allow users to see	
Privacy->Allow users who know my email address to find	
Sign On->Sign On	Automatically signing on when AIM starts not supported.
Sign On->Internet Connection	

Table N-14 AOL Instant Messenger 5.x supported settings *(continued)*

Settings Location	Exceptions
Sign On->Auto Upgrade	
Sign On->Connection	
Sign On	Make AIM my default instant messenging program not supported.
Idle message	
Away Message->When away	
Buddy Icons	Images to use for buddies not supported. For buddy icons set by others not supported.
Buddy Icons->Display Buddy Icons	
Mail->Mail alert notification	
Mail->Sound	
News Ticker	
News Ticker->Topics	
IM Chat->IM Window	
IM Chat->Chat Room Window	
Font->Default for Composing Windows	
Font	
AIM Expressions	
IM Image->When I open an IM Image	
IM Image->When others send an IM Image	
Talk->when I start a talk session	
Talk->when others want to talk to you	
Talk->Sounds	
File sharing	
File Transfer	

Table N-14 AOL Instant Messenger 5.x supported settings *(continued)*

Settings Location	Exceptions
Send buddy list	
Add-ins	

Symantec BackupExec System Recovery

Ghost User Migration supports the following:

- Symantec BackupExec System Recovery 6.5

Table N-15 describes the Symantec BackupExec System Recovery 6.5 supported settings.

Table N-15 Symantec BackupExec System Recovery 6.5 supported settings

Settings Location	Exceptions
Tools > options > Settings	
Tools > options > notification > Log file > properties	
Tools > options > notification > Event Log > properties	
Tools > options > notification > SMTP > properties	
Tools > options > notification > SNMP Trap > properties	
Tools > options > Performance	
Tools > options > Tray Icon	
View	

Cisco VPN Client

Ghost User Migration supports the following:

- Cisco VPN Client 3.6.3
- Cisco VPN Client 4.0
- Cisco VPN Client 4.6
- Cisco VPN Client 4.7
- Cisco VPN Client 4.8

Cisco VPN Client 3.6.3

Table N-16 describes the Cisco VPN Client 3.6.3 supported settings.

Table N-16 Cisco VPN Client 3.6.3 supported settings

Settings Location	Exceptions
Connection Entries (For Each Connection) -> Properties	
Connection Entries (For Each Connection) -> Properties -> Authentication	
Connection Entries (For Each Connection) -> Properties -> General	
Connection Entries (For Each Connection) -> Properties -> Connections	
Options->Application Launcher	
Options->Windows Logon Properties	Enable start before logon not supported.

Cisco VPN Client 4.0

Table N-17 describes the Cisco VPN Client 4.0 supported settings.

Table N-17 Cisco VPN Client 4.0 supported settings

Settings Location	Exceptions
Connection Entries (For Each Connection) -> Properties	
Connection Entries (For Each Connection) -> Properties -> Authentication	
Connection Entries (For Each Connection) -> Properties -> Transport	
Connection Entries (For Each Connection) -> Properties -> Backup Servers	
Connection Entries (For Each Connection) -> Properties -> DialUp	
Log > Log Settings	
Options->Application Launcher	
Options->Application Launcher	
Options->Windows Logon Properties	Enable start before logon not supported.

Symantec LiveState Recovery Desktop

Ghost User Migration supports the following:

- Symantec LiveState Recovery Desktop 6.0

Note: Migration to Symantec BackupExec System Recovery 6.5 is supported.

Table N-18 describes the Symantec LiveState Recovery Desktop 6.0 supported settings.

Table N-18 Symantec LiveState Recovery Desktop 6.0 supported settings

Settings Location	Exceptions
Tools > options > Settings	
Tools > options > notification > Log file > properties	
Tools > options > notification > Event Log > properties	
Tools > options > notification > SMTP > properties	
Tools > options > notification > SNMP Trap > properties	
Tools > options > Performance	
Tools > options > Tray Icon	
View	

Lotus Notes

Ghost User Migration supports the following versions:

- Lotus Notes 6.0
- Lotus Notes 6.5
- Lotus Notes 7.0

Note: If you restore a user migration package without first starting the Lotus Notes client on the target machine, the Lotus Notes client will start automatically and go though the first run process. The Lotus Notes client will prompt you to provide the user ID (user mail file). The user ID has been migrated to the default Lotus Notes location on the target machine. To enable Lotus Notes to start, you need to browse to that location and select the appropriate file.

Lotus Notes 6.0

Table N-19 describes the Lotus Notes 6.0 supported settings.

Table N-19 Lotus Notes 6.0 supported settings

Settings Location	Exceptions
File->Tools->User Preferences->Basics -> Display Options	
File->Tools->User Preferences->Basics->Startup Options	
File->Tools->User Preferences->Basics->Additional Options	
File->Tools->User Preferences->Basics->Additional Options -> Customize Logout Screen	
File->Tools->User Preferences->International	
File->Tools->User Preferences->Mail and News	
File->Tools->User Preferences->Ports	

Lotus Organizer

Ghost User Migration supports the following versions:

- Lotus Organizer 6.0

Table N-20 describes the Lotus Organizer 6.0 supported settings.

Table N-20 Lotus Organizer 6.0 supported settings

Settings Location	Exceptions
File->User Setup->Organizer Preferences ->Default File	
File->User Setup->Organizer Preferences ->Environment	
File->User Setup->Organizer Preferences ->Folders	
File->User Setup->Organizer Preferences ->Alarms	
File->User Setup->Mail and Scheduling	
File->User Setup->SmartIcon Setup	
File->User Setup->Telephone Dialing	
Edit->Layouts->Layouts	

McAfee VirusScan

Ghost User Migration supports the following versions:

- McAfee VirusScan 6.0
- McAfee VirusScan 7.0
- McAfee VirusScan 8.0

McAfee VirusScan 6.0

Table N-21 describes the McAfee VirusScan 6.0 supported settings.

Table N-21 McAfee VirusScan 6.0 supported settings

Settings Location	Exceptions
McAfee VirusScan->Service	
McAfee VirusScan->Components	
View and edit scheduled scans	
System Scan Properties->Detection	
System Scan Properties->Action	
System Scan Properties->Alert	
System Scan Properties->Report	
System Scan Properties->Exclusion	
E-Mail Scan Properties->Detection	
E-Mail Scan Properties->Action	
E-Mail Scan Properties->Alert	
E-Mail Scan Properties->Report	
Download Scan Properties->Detection	
Download Scan Properties->Action	
Download Scan Properties->Possible actions	
Download Scan Properties->Alert	
Download Scan Properties->Report	

Table N-21 McAfee VirusScan 6.0 supported settings *(continued)*

Settings Location	Exceptions
Internet Filter Properties->Detection	
Internet Filter Properties->Action	
Internet Filter Properties->Alert	
Internet Filter Properties->Report->Log file	
Hostile Activity Watch Kernel Properties->Outlook	
Instant Updater->Configure automatic updates	
Instant Updater->Configure advanced settings	

McAfee VirusScan 7.0

Table N-22 describes the McAfee VirusScan 7.0 supported settings.

Table N-22 McAfee VirusScan 7.0 supported settings

Settings Location	Exceptions
McAfee VirusScan->Service	
View and edit scheduled scans	
System Scan Properties->Detection	
System Scan Properties->Action	
System Scan Properties->Report	
System Scan Properties->Exclusion	
E-Mail Scan Properties->Detection	
E-Mail Scan Properties->Action	
E-Mail Scan Properties->Alert	
E-Mail Scan Properties->Report	
Hostile Activity Watch Kernel Properties->E-mail	
Hostile Activity Watch Kernel Properties->Script Stopper	
Instant Updater->Configure automatic updates	

Table N-22 McAfee VirusScan 7.0 supported settings *(continued)*

Settings Location	Exceptions
Instant Updater->Configure advanced settings	

Microsoft Access

Ghost User Migration supports the following versions:

- Microsoft Access 2000
- Microsoft Access XP
- Microsoft Access 2003
- Microsoft Access 2007

Microsoft Access 2000

Table N-23 describes the Microsoft Access 2000 supported settings.

Table N-23 Microsoft Access 2000 supported settings

Settings Location	Exceptions
Tools -> Options -> View	
Tools -> Options -> Show in Macro Design	
Tools -> Options -> Database window Click Option	
Tools -> Options -> Dual Font Support	
Tools -> Options -> General	
Tools -> Options -> Edit/Find	
Tools -> Options -> Keyboard	
Tools -> Options -> Datasheet	
Tools -> Options -> Tables/Queries	
Tools -> Options -> Forms/Reports	
Tools -> Options -> Advanced	
Toolbars -> Customize -> Toolbars	

Microsoft Access XP

Table N-24 describes the Microsoft Access XP supported settings.

Table N-24 Microsoft Access XP supported settings

Settings Location	Exceptions
Tools -> Options -> View	
Tools -> Options -> Show in Macro Design	
Tools -> Options -> Database window Click Option	
Tools -> Options -> General	
Tools -> Options -> Edit/Find	
Tools -> Options -> Keyboard	
Tools -> Options -> Datasheet	
Tools -> Options -> Tables/Queries	
Tools -> Options -> Forms/Reports	
Tools -> Options -> Advanced	
Tools -> Options -> Pages	
Tools -> Options -> International	
Tools -> Options -> Spelling	
Toolbars -> Customize -> Toolbars	

Microsoft Access 2003

Table N-25 describes the Microsoft Access 2003 supported settings.

Table N-25 Microsoft Access 2003 supported settings

Settings Location	Exceptions
Tools -> Options -> View	
Tools -> Options -> Show in Macro Design	
Tools -> Options -> Database window Click Option	
Tools -> Options -> General	

Table N-25 Microsoft Access 2003 supported settings *(continued)*

Settings Location	Exceptions
Tools -> Options -> Edit/Find	
Tools -> Options -> Keyboard	
Tools -> Options -> Datasheet	
Tools -> Options -> Tables/Queries	
Tools -> Options -> Forms/Reports	
Tools -> Options -> Advanced	
Tools -> Options -> Pages	
Tools -> Options -> Error Checking	
Tools -> Options -> International	
Tools -> Options -> Spelling	
Toolbars -> Customize -> Toolbars	

Microsoft Access 2007

Table N-26 describes the Microsoft Access 2007 supported settings.

Table N-26 Microsoft Access 2007 supported settings

Settings Location	Exceptions
Personalize	
Current Database	
DataSheet	
Object Designers	
Proofing	
Advanced -> Editing	
Advanced -> Display	
Advanced -> Printing	
Advanced -> General	

Table N-26 Microsoft Access 2007 supported settings *(continued)*

Settings Location	Exceptions
Advanced -> Advanced	
Trust Center -> Trust Center settings	

Microsoft Excel

Ghost User Migration supports the following versions:

- Microsoft Excel 2000
- Microsoft Excel XP
- Microsoft Excel 2003
- Microsoft Excel 2007

Microsoft Excel 2000

Table N-27 describes the Microsoft Excel 2000 supported settings.

Table N-27 Microsoft Excel 2000 supported settings

Settings Location	Exceptions
Tools->Options->View->Show	
Tools->Options->View->Comments	
Tools->Options->View->Objects	Not supported
Tools->Options->View->Windows options	Not supported
Tools->Options->Calculation->Calculation	
Tools->Options->Calculation->Iteration	
Tools->Options->Calculation->Workbook options	Not supported
Tools->Options->Edit->Settings	
Tools->Options->General	
Tools->Options->Transition -> Settings	
Tools->Options->Transition -> Sheet Options	Not supported

Table N-27 Microsoft Excel 2000 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Custom Lists	
Tools->Options->Chart->Active chart	Not supported
Tools->Options->Chart->Chart tips	
Tools->Options->Colors	
View -> Toolbars Customize -> Commands	
View -> Toolbars Customize -> Options	

Microsoft Excel XP

Table N-28 describes the Microsoft Excel XP supported settings.

Table N-28 Microsoft Excel XP supported settings

Settings Location	Exceptions
Tools->Options->View->Show	
Tools->Options->View->Comments	
Tools->Options->View->Objects	Not supported
Tools->Options->View->Windows options	Not supported
Tools->Options->Calculation->Calculation	
Tools->Options->Calculation->Iteration	
Tools->Options->Calculation->Workbook options	Not supported
Tools->Options->Edit->Settings	
Tools->Options->General	
Tools->Options->Transition -> Settings	
Tools->Options->Transition -> Sheet Options	Not supported
Tools->Options->Custom Lists	
Tools->Options->Chart->Active chart	Not supported
Tools->Options->Chart->Chart tips	

Table N-28 Microsoft Excel XP supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Colors	
Tools->Options->International	
Tools->Options->Save	
Tools->Options->Error Checking	
Tools->Options->Spelling	
Tools->Options->Security	
View -> Toolbars Customize -> Commands	
View -> Toolbars Customize -> Options	

Microsoft Excel 2003

Table N-29 describes the Microsoft Excel 2003 supported settings.

Table N-29 Microsoft Excel 2003 supported settings

Settings Location	Exceptions
Tools->Options->View->Show	
Tools->Options->View->Comments	
Tools->Options->View->Objects	Not supported
Tools->Options->View->Windows options	Not supported
Tools->Options->Calculation->Calculation	
Tools->Options->Calculation->Iteration	
Tools->Options->Calculation->Workbook options	Not supported
Tools->Options->Edit->Settings	
Tools->Options->General	
Tools->Options->Transition -> Settings	
Tools->Options->Transition -> Sheet Options	Not supported
Tools->Options->Custom Lists	

Table N-29 Microsoft Excel 2003 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Chart->Active chart	Not supported
Tools->Options->Chart->Chart tips	
Tools->Options->Colors	
Tools->Options->International	
Tools->Options->Save	
Tools->Options->Error Checking	
Tools->Options->Spelling	
Tools->Options->Security	
View -> Toolbars Customize -> Commands	
View -> Toolbars Customize -> Options	

Microsoft Excel 2007

Table N-30 describes the Microsoft Excel 2007 supported settings.

Table N-30 Microsoft Excel 2007 supported settings

Settings Location	Exceptions
Personalize -> Top options for working with Excel	
Personalize -> When creating new work book	
Personalize -> Personalize your copy	
Formulas >calculation options	
Formulas > working with formulas	
Formulas > Error checking	
Formulas > Error checking rules	
Proofing -> Autocorrect Options	
Proofing ->When correcting spelling in Office	
Save > preserve backup info	

Table N-30 Microsoft Excel 2007 supported settings *(continued)*

Settings Location	Exceptions
Save > autorecover exceptions for	
Save >offline editing options	
Save > preserve	
Advanced > editing options	
Advanced >cut copy and paste	
Advanced > display	
Advanced > display options for this workbook	
Advanced > formulas	
Advanced > when calculating this work book	
Advanced >General	
Trust Center-> Trust center settings	

Microsoft Internet Explorer

Ghost User Migration supports the following versions:

- Microsoft Internet Explorer 5.0 and 5.5
- Microsoft Internet Explorer 6.0
- Microsoft Internet Explorer 6.0 SP1
- Microsoft Internet Explorer 7.0

The following applies to all versions of Microsoft Internet Explorer, when running on Windows XP with German language.

The following settings are not migrated:

- Tools->folder Options->Clickitems
  The single click/double click option button is migrated, but if a single click option is selected, the subsequent option setting is not.
- Tools->folder options->view->Use simple file sharing (recommended)
- Tools->folder options->Offline files->Enable offline files

Microsoft Internet Explorer 5.0 and 5.5

Table N-31 describes the Microsoft Internet Explorer 5.0 and 5.5 supported settings.

Table N-31 Microsoft Internet Explorer 5.0 and 5.5 supported settings

Settings Location	Exceptions
Tools->Internet Options->General	Amount of disk space not supported.
Tools->Internet Options->Security	
Tools->Internet Options->Content	
Tools->Internet Options->Programs	
Tools->Internet Options->Advanced	
Favorites	
Tools->Internet Options->General->Colors	
Tools->Internet Options->General->Fonts	
Tools->Internet Options->General->Accessibility	

Microsoft Internet Explorer 6.0

Table N-32 describes the Microsoft Internet Explorer 6.0 supported settings.

Table N-32 Microsoft Internet Explorer 6.0 supported settings

Settings Location	Exceptions
Tools->Internet Options->General	Amount of disk space not supported.
Tools->Internet Options->Security	
Tools->Internet Options->Content	
Tools->Internet Options->Programs	
Tools->Internet Options->Advanced	
Favorites	
Tools->Internet Options->General->Colors	
Tools->Internet Options->General->Fonts	

Table N-32 Microsoft Internet Explorer 6.0 supported settings *(continued)*

Settings Location	Exceptions
Tools->Internet Options->General->Accessibility	
Tools->Internet Options->Privacy	

Microsoft Internet Explorer 7.0

Table N-33 describes the Microsoft Internet Explorer 7.0 supported settings.

Table N-33 Microsoft Internet Explorer 7.0 supported settings

Settings Location	Exceptions
Tools->Internet Options->General	Amount of disk space not supported.
Tools->Internet Options->Security	
Tools->Internet Options->Content	
Tools->Internet Options->Programs	
Tools->Internet Options->Advanced	
Favorites	
Tools->Internet Options->General->Colors	
Tools->Internet Options->General->Fonts	
Tools->Internet Options->General->Accessibility	
Tools->Internet Options->Privacy	
Tools->Internet Options->General->Languages	
Tools->Internet Options->Connections	

Microsoft Office Publisher

Ghost User Migration supports the following versions:

- Microsoft Office Publisher 2002
- Microsoft Office Publisher 2003
- Microsoft Office Publisher 2007

Microsoft OneNote

Ghost User Migration supports the following versions:

- Microsoft OneNote 2003
- Microsoft OneNote 2007

Microsoft OneNote 2003

Table N-34 describes the Microsoft OneNote 2003 supported settings.

Table N-34 Microsoft OneNote 2003 supported settings

Settings Location	Exceptions
Tools->AutoCorrect Options->AutoCorrect	
Tools->Customize->Options	
Tools->Options->Display	
Tools->Options->Editing	
Tools->Options->Spelling	
Tools->Options->Handwriting	
Tools->Options->E-Mail	
Tools->Options->Note Flags	
Tools->Options->Audio and Video	
Tools->Options->Open and Save	
Tools->Options->Backup	
Tools->Options->Passwords	
Tools->Options->Other	
Tools->Options->Live Sharing	

Microsoft OneNote 2007

Table N-35 describes the Microsoft OneNote 2007 supported settings.

Table N-35 Microsoft OneNote 2007 supported settings

Settings Location	Exceptions
Tools->AutoCorrect Options->AutoCorrect	
Tools->Customize->Options	
Tools->Options->Display	Adjust Darkness setting not available.
Tools->Options->Editing	Empty deleted pages and Permanently delete pages settings not available.
Tools->Options->Pen	
Tools->Options->Spelling	
Tools->Options->Synchronization	
Tools->Options->Filing Rules	
Tools->Options->E-Mail	
Tools->Options->Note Flags	
Tools->Options->Audio and Video	
Tools->Options->Open and Save	
Tools->Options->Backup	
Tools->Options->Passwords	
Tools->Options->Other	Online Content options not supported.
Tools->Options->Live Sharing	

Microsoft Outlook

Ghost User Migration supports the following versions:

- Microsoft Outlook 2000
- Microsoft Outlook XP
- Microsoft Outlook 2003
- Microsoft Outlook 2007

Microsoft Outlook 2000

Table N-36 describes the Microsoft Outlook 2000 supported settings.

Table N-36 Microsoft Outlook 2000 supported settings

Settings Location	Exceptions
Tools->Options->Preferences->E-mail Options	
Tools->Options->Preferences->Calendar	
Tools->Options->Preferences->Calendar Options	
Tools->Options->Preferences->Tasks	
Tools->Options->Preferences->Task Options	
Tools->Options->Preferences->Contact Options	
Tools->Options->Preferences->Journal Options	
Tools->Options->Preferences->Notes Options	
Tools->Options->Mail Services	
Tools->Options->Mail Format	
Tools->Options->Spelling	
Tools->Options->Security	
Tools->Options->Other->General	
Tools->Options->Other->AutoArchive	
Tools->Options->Other->Preview Pane	
Tools->Options->Internet E-mail	
View	
Tools	
Rules and Alerts	

Microsoft Outlook XP

Table N-37 describes the Microsoft Outlook XP supported settings.

Table N-37 Microsoft Outlook XP supported settings

Settings Location	Exceptions
Tools->Options->Preferences->E-mail Options	
Tools->Options->Preferences->Calendar	
Tools->Options->Preferences->Calendar Options	
Tools->Options->Preferences->Tasks	
Tools->Options->Preferences->Task Options	
Tools->Options->Preferences->Contact Options	
Tools->Options->Preferences->Journal Options	
Tools->Options->Preferences->Notes Options	
Tools->Options->Mail Setup	
Tools->Options->Mail Format	
Tools->Options->Spelling	
Tools->Options->Security	
Tools->Options->Other->General	
Tools->Options->Other->AutoArchive	
Tools->Options->Other->Preview Pane	
View	
Tools	
Rules and Alerts	

Microsoft Outlook 2003

Table N-38 describes the Microsoft Outlook 2003 supported settings.

Table N-38 Microsoft Outlook 2003 supported settings

Settings Location	Exceptions
Tools->Options->Preferences->Junk E-mail	
Tools->Options->Preferences->E-mail Options	

Table N-38 Microsoft Outlook 2003 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Preferences->Calendar	
Tools->Options->Preferences->Calendar Options	
Tools->Options->Preferences->Tasks	
Tools->Options->Preferences->Task Options	
Tools->Options->Preferences->Contact Options	
Tools->Options->Preferences->Journal Options	
Tools->Options->Preferences->Notes Options	
Tools->Options->Mail Setup	
Tools->Options->Mail Format	
Tools->Options->Spelling	
Tools->Options->Security	
Tools->Options->Other->General	
Tools->Options->Other->AutoArchive	
Tools->Options->Other->Reading Pane	
View	
Tools	
Rules and Alerts	

Microsoft Outlook Caveats

There are a number of issues that may cause problems when migrating Microsoft Outlook settings and files.

User Migration does not support the migration of POP services. The source computer must be configured to use the Microsoft Exchange Server service.

The following sections describe the caveats for migrating Microsoft Outlook:

- Migrating the default profile
- Profiles and services
- Restoring multiple packages

- Setting the default profile
- Migrating signature files
- Troubleshooting Microsoft Outlook migration

Migrating the default profile

User Migration supports the migration of the Outlook Default Profile only.

If multiple profiles exist on the same computer, only the profile that is set as the default is migrated. The exception is Outlook 2003, in which all the profiles are migrated.

For example, user A creates a package on the source computer. User B logs on to the Windows 2000 target computer and restores user A's package. User B now has user A's profile.

Profiles and services

Outlook profiles have a set of associated files and services. User Migration migrates the following services with each profile:

- Microsoft Exchange Server
- Personal Address Book and associated *.pab files
- Personal Folders and associated *.pst files

The following are details about migrating Mail Service settings:

- The migration process moves one Personal Address Book (.pab file) for each profile.
- To migrate other profiles from the source to the target computer, change the default profile (select the desired profile) on the source computer and follow the migration process. After the restore process, a new profile is created on the target computer. This process does not overwrite existing profiles with different profile names on the target computer.
- To move the default signature settings, the default editor must be set to use the internal editor in Outlook.
  For example, the default editor must not be set to Microsoft Word.
- The migration process only moves the Mail Service profile identified as the default profile. A profile of the same name is created on the target computer.
  Outlook does not need to be initiated beforehand. However, when a user starts Outlook on the target computer, the application sometimes prompts the user to create a profile. This occurs when Outlook runs for the first time. It does not mean that the profile did not migrate to the target computer. If prompted

to create a profile, create one for the corporate or workgroup environment and type a name other than the one that is being moved by User Migration. Services should not be added to this profile. This is not a profile that you need to use and you can safely delete it later.

- User Interface settings are found in the Outlook Mail Service. These settings are an entirely separate class of functions from the Mail Service settings. They do not share restrictions.
- Delegation settings are only accessible if the Microsoft Exchange Server service is migrated to the target computer. Delegation settings are stored on the Exchange Server and, while these settings are not moved directly, if the Microsoft Exchange Server service is moved, the user still has access.

To view the Mail Service settings for Outlook 2000

◆ In Outlook 2000, click **Tools > Services > Mail Control Panel**.

Restoring multiple packages

Because of the way in which Outlook 2000 and later versions store user settings, restoring multiple packages after changing the default profile overwrites the user settings on the target computer.

To view these settings

◆ In Outlook 2000/2002/2003, click **Tools > Options**.

Setting the default profile

If Outlook prompts you to select a profile from the list when you launch Outlook on the source computer, there is not a default account from which User Migration can copy the settings. The Outlook profile information does not migrate unless there is a default profile selected.

To set the default profile

1. On the target computer, on the Windows desktop, click **Start > Control Panel > Mail**.
2. Click **Show Profiles**.
3. Select the profile that you want to use.
4. Click **Apply**.

Migrating signature files

Signature files are migrated if they are available in the locations listed in Table N-39.

Table N-39 Signature file location

Outlook version	Signature file location on source computer
Outlook 2000	Either of the following locations: ■ <user profiles path>\<user name>\Applications Data\Microsoft\Shared\Signatures ■ <user profiles path>\<user name>\Applications Data\Microsoft\Signature
Outlook 2002/2003	Either of the following locations: ■ <user profiles path>\<user name>\Applications Data\Microsoft\Shared\Signatures ■ <user profiles path>\<user name>\Applications Data\Microsoft\Signature

Troubleshooting Microsoft Outlook migration

Table N-40 lists some of the problems that you may encounter when using User Migration, and the workarounds.

Table N-40 Microsoft Outlook migration troubleshooting

Problem	Workaround
Some of your Outlook profiles do not move to the target computer.	User Migration only moves settings that are associated with the default profile setup. It does not move settings for other profiles. This is a limitation of how Outlook 2000/2002/2003 stores settings.
You cannot access your delegation settings.	If the Microsoft Exchange Server service is not moved, delegation settings are not accessible. Delegation settings are stored on the Exchange Server, and while these settings do not move directly, if the Microsoft Exchange Server service is moved, the user still has access.

Microsoft Outlook Express

Ghost User Migration supports the following versions:

- Microsoft Outlook Express 4.0
- Microsoft Outlook Express 5.0 and 6.0

Microsoft Outlook Express 4.0

Table N-41 describes the Microsoft Outlook Express 4.0 supported settings.

Table N-41 Microsoft Outlook Express 4.0 supported settings

Settings Location	Exceptions
Tools->Options->General	
Tools->Options->Send	
Tools->Options->Read	
Tools->Options->Security	
Tools->Options->Dial Up	
Tools->Options->Advanced	
Tools->Accounts->Mail->Properties->General	
Tools->Accounts->Mail->Properties->Servers	
Tools->Accounts->Mail->Properties->Connection	
Tools->Accounts->Mail->Properties->Security	
Tools->Accounts->Mail->Properties->Advanced	

Microsoft Outlook Express 5.0 and 6.0

Table N-42 describes the Microsoft Outlook Express 5.0 and 6.0 supported settings.

Table N-42 Microsoft Outlook Express 5.0 and 6.0 supported settings

Settings Location	Exceptions
Tools->Options->General	
Tools->Options->Send	
Tools->Options->Read	
Tools->Options->Receipts	
Tools->Options->Compose	
Tools->Options->Signatures	
Tools->Options->Spelling	

Table N-42 Microsoft Outlook Express 5.0 and 6.0 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Security	
Tools->Options->Connection	
Tools->Options->Maintenance	
Tools->Accounts->Mail->Properties->General	
Tools->Accounts->Mail->Properties->Servers	
Tools->Accounts->Mail->Properties->Connection	
Tools->Accounts->Mail->Properties->Security	
Tools->Accounts->Mail->Properties->Advanced	

Microsoft PowerPoint

Ghost User Migration supports the following versions:

- Microsoft PowerPoint 2000
- Microsoft PowerPoint XP
- Microsoft PowerPoint 2003
- Microsoft PowerPoint 2007

Microsoft PowerPoint 2000

Table N-43 describes the Microsoft PowerPoint 2000 supported settings.

Table N-43 Microsoft PowerPoint 2000 supported settings

Settings Location	Exceptions
Tools->Options->View->Show	
Tools->Options->View->Slide Show	
Tools->Options->General->General options	
Tools->Options->General->User Information	
Tools->Options->General->Web Options	

Table N-43 Microsoft PowerPoint 2000 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Edit	
Tools->Options->Print	
Tools->Options->Save	
Tools->Options->Spelling and Style	
Tools->Customize->Toolbars	
View -> Toolbars->Customize->Toolbars	Custom toolbars are not migrated between different versions.

Microsoft PowerPoint XP

Table N-44 describes the Microsoft PowerPoint XP supported settings.

Table N-44 Microsoft PowerPoint XP supported settings

Settings Location	Exceptions
Tools->Options->View->Show	
Tools->Options->View->Slide Show	
Tools->Options->View->Default View	
Tools->Options->General->General options	
Tools->Options->General->User Information	
Tools->Options->General->Web Options	
Tools->Options->Edit	
Tools->Options->Print	
Tools->Options->Save	
Tools->Options->Security	
Tools->Options->Spelling and Style	
Tools->Customize->Toolbars	
Tools->AutoCorrect Options->AutoFormat As You Type	

Table N-44 Microsoft PowerPoint XP supported settings *(continued)*

Settings Location	Exceptions
View -> Toolbars->Customize->Toolbars	Not supported.

Microsoft PowerPoint 2003

Table N-45 describes the Microsoft PowerPoint 2003 supported settings.

Table N-45 Microsoft PowerPoint 2003 supported settings

Settings Location	Exceptions
Tools->Options->View->Show	
Tools->Options->View->Slide Show	
Tools->Options->View->Default View	
Tools->Options->General->General options	
Tools->Options->General->User Information	
Tools->Options->General->Web Options	
Tools->Options->General->Service Options	
Tools->Options->Edit	
Tools->Options->Print	
Tools->Options->Save	
Tools->Options->Security	
Tools->Options->Spelling and Style	
Tools->Customize->Toolbars	
Tools->AutoCorrect Options->AutoFormat As You Type	
View -> Toolbars->Customize->Toolbars	Migration to higher versions not supported.

Microsoft PowerPoint 2007

Table N-46 describes the Microsoft PowerPoint 2007 supported settings.

Table N-46 Microsoft PowerPoint 2007 supported settings

Settings Location	Exceptions
Personalize > Top options	
Personalize > Personalize	
Proofing > AutoCorrect options	
Proofing > When correcting spelling in Office programs	
Proofing > When correcting spelling in PowerPoint	
Save	
Advanced > Editing options	
Advanced > Cut, copy, and paste	
Advanced > Display	
Advanced > Slide Show	
Advanced > Print	
Advanced > When Printing this doc	
Advanced > Save	
Advanced > General > Web options	
Advanced > General > Service options	
Trust Center-> Trust center settings	

Microsoft Project

Ghost User Migration supports the following versions:

- Microsoft Project 2000
- Microsoft Project 2002
- Microsoft Project 2003
- Microsoft Project 2007

Microsoft Project 2000

Table N-47 describes the Microsoft Project 2000 supported settings.

Table N-47 Microsoft Project 2000 supported settings

Settings Location	Exceptions
Tools->AutoCorrect	
Tools->Resource Leveling	
Tools->Customize->Toolbar->Options	Custom toolbars are not migrated between different versions.
Tools->Options->View	
Tools->Options->General	
Tools->Options->Edit	
Tools->Options->Calendar	
Tools->Options->Schedule	
Tools->Options->Calculation	
Tools->Options->Spelling	
Tools->Options->Workgroup	
Tools->Options->Save	

Microsoft Project 2002

Table N-48 describes the Microsoft Project 2002 supported settings.

Table N-48 Microsoft Project 2002 supported settings

Settings Location	Exceptions
Tools->AutoCorrect	
Tools->Resource Leveling	
Tools->Customize->Toolbar->Options	Custom toolbars are not migrated between different versions.
Tools->Options->View	
Tools->Options->General	
Tools->Options->Edit	
Tools->Options->Calendar	

Table N-48 Microsoft Project 2002 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Schedule	
Tools->Options->Calculation	
Tools->Options->Spelling	
Tools->Options->Collaborate	
Tools->Options->Save	
Tools->Options->Interface	

Microsoft Project 2003

Table N-49 describes the Microsoft Project 2003 supported settings.

Table N-49 Microsoft Project 2003 supported settings

Settings Location	Exceptions
Tools->AutoCorrect Options -> AutoCorrect	
Tools->Level Resources	
Tools->Customize->Options	
Tools->Options->View	
Tools->Options->General	
Tools->Options->Edit	
Tools->Options->Calendar	
Tools->Options->Schedule	
Tools->Options->Calculation	
Tools->Options->Spelling	
Tools->Options->Collaborate	
Tools->Options->Save	
Tools->Options->Interface	
Tools->Options->Security	

Microsoft Project 2007

Table N-50 describes the Microsoft Project 2007 supported settings.

Table N-50 Microsoft Project 2007 supported settings

Settings Location	Exceptions
Tools->AutoCorrect Options -> AutoCorrect	
Tools->Level Resources	
Tools->Customize->Toolbar->Options	Custom toolbars are not migrated between different versions.
Tools->Options->View	
Tools->Options->General	
Tools->Options->Edit	
Tools->Options->Calendar	
Tools->Options->Schedule	
Tools->Options->Calculation	
Tools->Options->Spelling	
Tools->Options->Collaborate	
Tools->Options->Save	
Tools->Options->Interface	
Tools->Options->Security	
Tools->Enterprise Options->Project Server Accounts/When starting	

Microsoft Visio

Ghost User Migration supports the following versions:

- Microsoft Visio 2000
- Microsoft Visio 2002
- Microsoft Visio 2003
- Microsoft Visio 2007

Microsoft Visio 2000

Table N-51 describes the Microsoft Visio 2000 supported settings.

Table N-51 Microsoft Visio 2000 supported settings

Settings Location	Exceptions
Tools -> Options -> General	
Tools->Options->File Paths	Not supported
Tools -> Options -> Drawing	
Tools -> Options -> Regional Settings	
Tools->Options->Spelling	
Tools -> Options -> Advanced	

Microsoft Visio 2002

Table N-52 describes the Microsoft Visio 2002 supported settings.

Table N-52 Microsoft Visio 2002 supported settings

Settings Location	Exceptions
Tools -> Options -> General	
Tools->Options->File Paths	Not supported
Tools -> Options -> View	
Tools -> Options -> Regional	
Tools->Options->Save	
Tools -> Options -> Advanced	

Microsoft Visio 2003

Table N-53 describes the Microsoft Visio 2003 supported settings.

Table N-53 Microsoft Visio 2003 supported settings

Settings Location	Exceptions
Tools -> Options -> General	

Table N-53 Microsoft Visio 2003 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Advanced->File Paths	Not supported
Tools -> Options -> View	
Tools -> Options -> Regional	
Tools->Options->Save	
Tools -> Options -> Advanced	
Tools -> Options -> Units	
Tools -> Options -> Advanced -> Color Settings	
Tools -> Options -> Security	
Tools->Options->Shape Search	
Tools -> Options -> Spelling	

Microsoft Visio 2007

Table N-54 describes the Microsoft Visio 2007 supported settings.

Table N-54 Microsoft Visio 2007 supported settings

Settings Location	Exceptions
Tools -> Options -> General	
Tools->Options->Advanced->File Paths	Not supported
Tools -> Options -> View	Startup Task Pane and Choose Drawing Type Pane not supported.
Tools -> Options -> Regional	Not supported.
Tools->Options->Save/Open	
Tools -> Options -> Advanced	
Tools -> Options -> Units	
Tools -> Options -> Advanced -> Color Settings	
Tools -> Options -> Security	

Table N-54 Microsoft Visio 2007 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Shape Search	
Tools -> Options -> Spelling	
Tools -> Customize -> Toolbar	
Tools->Autocorrectoptions->Autocorrect	
Tools->Autocorrectoptions->Auto Format As you Type	

Microsoft Word

Ghost User Migration supports the following versions:

- Microsoft Word 2000
- Microsoft Word XP
- Microsoft Word 2003
- Microsoft Word 2007

Microsoft Word 2000

Table N-55 describes the Microsoft Word 2000 supported settings.

Table N-55 Microsoft Word 2000 supported settings

Settings Location	Exceptions
Tools->Options->View	
Tools->Options->General	
Tools->Options->Edit	
Tools->Options->Print	
Tools->Options->Save	
Tools->Options->Spelling and Grammar	
Tools->Options->Track Changes	
Tools->Options->User Information	

Table N-55 Microsoft Word 2000 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Compatibility	
Tools->Options->File Locations	
View -> Toolbars -> Customize -> Toolbars	Not migrated to higher versions.

Additional custom dictionaries for Word 2000 are not migrated. The package contains only custom.dic. Any additional dictionaries are not included in the package.

Microsoft Word XP

Table N-56 describes the Microsoft Word XP supported settings.

Table N-56 Microsoft Word XP supported settings

Settings Location	Exceptions
Tools->Options->View	
Tools->Options->General	
Tools->Options->E-Mail Options	Word email signature pictures are not migrated.
Tools->Options->Edit	
Tools->Options->Print	
Tools->Options->Save	
Tools->Options->Security	
Tools->Options->Spelling and Grammar	
Tools->Options->Track Changes	
Tools->Options->User Information	
Tools->Options->Compatibility	
Tools->Options->File Locations	
Tools->AutoCorrect Options	
View -> Toolbars -> Customize -> Toolbars	

Microsoft Word 2003

Table N-57 describes the Microsoft Word 2003 supported settings.

Table N-57 Microsoft Word 2003 supported settings

Settings Location	Exceptions
Tools->Options->View	
Tools->Options->General	
Tools->Options->E-Mail Options	Word email signature pictures are not migrated.
Tools->Options->Edit	
Tools->Options->Print	
Tools->Options->Save	
Tools->Options->Security	
Tools->Options->Spelling and Grammar	
Tools->Options->Track Changes	
Tools->Options->User Information	
Tools->Options->Compatibility	
Tools->Options->File Locations	
Tools->AutoCorrect Options	
View -> Toolbars -> Customize -> Toolbars	
Office Assistant->Options	Not supported

Microsoft Word 2007

Table N-58 describes the Microsoft Word 2007 supported settings.

Table N-58 Microsoft Word 2007 supported settings

Settings Location	Exceptions
Personalize > Top options	
Personalize > Personalize	

Table N-58 Microsoft Word 2007 supported settings *(continued)*

Settings Location	Exceptions
Display > Page display options	
Display > Always show formatting	
Display > Printing options	
Proofing > AutoCorrect options	
Proofing > When correcting spelling in Office programs	
Proofing > When correcting spelling in Word	
Proofing > When correcting grammar in Word	
Proofing > Exceptions for	
Save	
Advanced > Editing options	
Advanced > Cut, copy, and paste	
Advanced > Show document content	
Advanced > Display	
Advanced > Print	
Advanced > When Printing this doc	
Advanced > Save	
Advanced > Preserve	
Advanced > General	
Advanced > General > File location	
Advanced > General > Web options	
Advanced > General > Service options	
Advanced > Compatibility options	
Trust Center-> Trust center settings	

Mozilla FireFox

Ghost User Migration supports the following versions:

- Mozilla FireFox 1.5x
- Mozilla FireFox 2.0x

Mozilla Thunderbird

Ghost User Migration supports the following versions:

- Mozilla Thunderbird 1.5x
- Mozilla Thunderbird 2.0x

MSN Messenger

Ghost User Migration supports the following versions:

- MSN Messenger 5.0
- MSN Messenger 6.0
- MSN Messenger 7.0 and 7.5

MSN Messenger 5.0

Table N-59 describes the MSN Messenger 5.0 supported settings.

Table N-59 MSN Messenger 5.0 supported settings

Settings Location	Exceptions
Tools->Options-> General	Run this program when Windows starts not supported.
Tools->Options->Messages->Change Font	
Tools->Options->Messages	
Tools->Options->Personal	
Tools->Options->Accounts	
Tools->Options->Privacy	
Tools->Options->Connections	
Tools->Use Windows Color Scheme	

Table N-59 MSN Messenger 5.0 supported settings *(continued)*

Settings Location	Exceptions
View	

MSN Messenger 6.0

Table N-60 describes the MSN Messenger 6.0 supported settings.

Table N-60 MSN Messenger 6.0 supported settings

Settings Location	Exceptions
Tools->Options-> General	Run this program when Windows starts not supported.
Tools->Options->Messages->Change Font	
Tools->Options->Messages->File Transfer	
Tools->Options->Messages	
Tools->Options->Personal	
Tools->Options->Accounts	
Tools->Options->Privacy	
Tools->Options->Connections	
View	

MSN Messenger 7.0 and 7.5

Table N-61 describes the MSN Messenger 7.0 and 7.5 supported settings.

Table N-61 MSN Messenger 7.0 and 7.5 supported settings

Settings Location	Exceptions
Tools->Options-> General	Run this program when Windows starts not supported.
Tools->Options->Messages->Change Font	
Tools->Options->Messages->File Transfer	
Tools->Options->Messages	
Tools->Options->Personal	

Table N-61 MSN Messenger 7.0 and 7.5 supported settings *(continued)*

Settings Location	Exceptions
Tools->Options->Accounts	
Tools->Options->Privacy	
Tools->Options->Connections	
View	

NetMeeting

Ghost User Migration supports the following versions:

- NetMeeting 3.x

NetMeeting 3.x

Table N-62 describes the NetMeeting 3.x supported settings.

Table N-62 NetMeeting 3.x supported settings

Settings Location	Exceptions
Tools->Options->General	
Tools->Options->General -> Advanced Calling	
Tools->Options->Video	
Call	
Tools->Options->Security	
Tools->Chat->Options->Information Display	
Tools->Chat->Options->Fonts	
View	
Tools->Remote Desktop Sharing	

Palm Desktop

Ghost User Migration supports the following versions:

- Palm Desktop 3.0
- Palm Desktop 4.0.1
- Palm Desktop 4.1

Palm Desktop 3.0

Table N-63 describes the Palm Desktop 3.0 supported settings.

Table N-63 Palm Desktop 3.0 supported settings

Settings Location	Exceptions
Tools->Options->General	Data directory not supported.
Tools->Options->Date Book->Date and Time	
View	
HotSync->Setup	
Tools->Users	
Mail Setup	Synchronize with not supported.

Palm Desktop 4.0.1

Table N-64 describes the Palm Desktop 4.0.1 supported settings.

Table N-64 Palm Desktop 4.0.1 supported settings

Settings Location	Exceptions
Tools->Options->General	Data directory not supported.
Tools->Options->Date Book->Date and Time	
Tools->Options->Security	
Tools->Options->Address	
Tools->Options->To Do	
Tools->Options->Alarms	
Tools->Options->Themes	
View	
HotSync->Setup	

Table N-64 Palm Desktop 4.0.1 supported settings *(continued)*

Settings Location	Exceptions
Tools->Users	
Mail Setup	Synchronize with not supported.

Palm Desktop 4.1

Table N-65 describes the Palm Desktop 4.1 supported settings.

Table N-65 Palm Desktop 4.1 supported settings

Settings Location	Exceptions
Tools->Options->General	Data directory not supported.
Tools->Preferences->Date Book->Date and Time	
Tools->Options->Security	
Tools->Options->Alarms	
Tools->Options->Tools	
Tools->Options->Themes	
View	
HotSync->Setup	
Tools->Users	
Mail Setup	Synchronize with not supported.

Symantec Norton AntiVirus

Ghost User Migration supports the following versions:

- Symantec Norton AntiVirus 7.5 and 7.6
- Symantec Norton AntiVirus 8.1
- Symantec Norton AnitVirus 9.0
- Symantec Norton AnitVirus 10.0

Symantec Norton AntiVirus 7.5 and 7.6

Table N-66 describes the Symantec Norton AntiVirus 7.5 and 7.6 supported settings.

Table N-66 Symantec Norton AntiVirus 7.5 and 7.6 supported settings

Settings Location	Exceptions
Configure->File System Realtime Protection	
File->Configure Histories	
Configure->Lotus Notes Realtime Protection	
Configure->Microsoft Exchange Realtime Protection	
File->Schedule Updates	
Scan->Scan Floppy Disk	
Custom Scan	

Symantec Norton AntiVirus 8.1

Table N-67 describes the Symantec Norton AntiVirus 8.1 supported settings.

Table N-67 Symantec Norton AntiVirus 8.1 supported settings

Settings Location	Exceptions
File->Configure Histories	
File->Schedule Updates	
Configure->Lotus Notes Realtime Protection	
Configure->Microsoft Exchange Realtime Protection	
Configure->File System Realtime Protection	
Scan->Scan Floppy Disk	
Custom Task	

Symantec pcAnywhere

Ghost User Migration supports the following versions:

- Symantec pcAnywhere 10.0 and 10.5
- Symantec pcAnywhere 11.0
- Symantec pcAnywhere 11.5 and 12.0

Symantec pcAnywhere 10.0 and 10.5

Table N-68 describes the Symantec pcAnywhere 10.0 and 10.5 supported settings.

Table N-68 Symantec pcAnywhere 10.0 and 10.5 supported settings

Settings Location	Exceptions
pcAnywhere Options->Host Operation	
pcAnywhere Options->Remote Operation	
pcAnywhere Options->Host Communications -> Dial-up properties	
pcAnywhere Options->Host Communications -> TCP/IP options	
pcAnywhere Options->Host Communications -> Remote Communications	
pcAnywhere Options->File Transfer	
pcAnywhere Options->Event Logging	
pcAnywhere Options->Directory Services	
pcAnywhere Options->Remote Printing	
pcAnywhere Options->Encryption	

Symantec pcAnywhere 11.0

Table N-69 describes the Symantec pcAnywhere 11.0 supported settings.

Table N-69 Symantec pcAnywhere 11.0 supported settings

Settings Location	Exceptions
Tools-> Options->Host Operation	
Tools-> Options->Remote Operation	
Tools-> Options->Host Communications -> Dial-up properties	
Tools-> Options->Host Communications -> TCP/IP options	
Tools-> Options->Host Communications -> Remote Communications	

Table N-69 Symantec pcAnywhere 11.0 supported settings *(continued)*

Settings Location	Exceptions
Tools-> Options->Host Communications -> Session Manager	
Tools-> Options->File Transfer	
Tools-> Options->Event Logging	
Tools-> Options->Directory Services	
Tools-> Options->Encryption	

Symantec pcAnywhere 11.5 and 12.0

Table N-70 describes the Symantec pcAnywhere 11.5 and 12.0 supported settings.

Table N-70 Symantec pcAnywhere 11.5 and 12.0 supported settings

Settings Location	Exceptions
Edit -> Preferences ->Host Operation	
Edit -> Preferences ->Remote Operation	
Edit -> Preferences ->Host Communications -> Dial-up properties	
Edit -> Preferences ->Host Communications -> TCP/IP options	
Edit -> Preferences -> Remote Communications	
Edit -> Preferences -> Session Manager	
Edit -> Preferences ->File Transfer	
Edit -> Preferences ->Event Logging	
Edit -> Preferences ->Directory Services	
Edit -> Preferences ->Encryption	

Windows Desktop Display

Ghost User Migration supports the following versions:

- Windows Desktop Display 2000
- Windows Desktop Display XP

Windows Desktop Display 2000

Table N-71 describes the Windows 2000 Desktop supported settings.

Table N-71 Windows 2000 Desktop supported settings

Settings Location	Exceptions
Display Properties->Background	
Display Properties->Screen Saver	
Display Properties->Appearance	
Display Properties->Effects	
Display Properties->Web	

Windows Desktop Display XP

Table N-72 describes the Windows XP Desktop supported settings.

Table N-72 Windows XP Desktop supported settings

Settings Location	Exceptions
Display Properties->Themes	
Display Properties->Desktop	
Display Properties->Screen Saver	
Display Properties->Appearance	
Display Properties->Appearance -> Effects	
Display Properties->Appearance -> Advanced Appearance	
Power Options Properties->Power Schemes	
Power Options Properties->Advanced	

Windows Explorer

Ghost User Migration supports the following versions:

- Windows Explorer 2000
- Windows Explorer XP

Windows Explorer 2000

Table N-73 describes the Windows Explorer 2000 supported settings.

Table N-73 Windows Explorer 2000 supported settings

Settings Location	Exceptions
Folder Options->General->Active Desktop	
Folder Options->General-> Web View	
Folder Options->General-> Browse Folders	
Folder Options->General->Click Items as follows	Underline icon titles setting not supported.
Folder Options->View->Advanced settings->Files and Folders	
Folder Options->File Types	Registered File Types setting not supported.
Folder Options->Offline Files	

Windows Explorer XP

Table N-74 describes the Windows Explorer XP supported settings.

Table N-74 Windows Explorer XP supported settings

Settings Location	Exceptions
Folder Options->General-> Tasks	
Folder Options->General-> Browse Folders	
Folder Options->General->Click Items as follows	Underline icon titles setting not supported.
Folder Options->View->Advanced settings->Files and Folders	
Folder Options->File Types	Registered File Types setting not supported.

Windows Accessibility Settings

Ghost User Migration supports the following versions:

- Windows 2000 Accessibility Settings
- Windows XP Accessibility Settings
- Windows Vista Accessibility Settings

Windows 2000 Accessibility Settings

Table N-75 describes the Windows 2000 Accessibility Settings supported settings.

Table N-75 Windows 2000 Accessibility Settings supported settings

Settings Location	Exceptions
Accessibility Options\Keyboard	
Accessibility Options\Sound	
Accessibility Options\Display\High Contrast	
Accessibility Options\Mouse\MouseKeys	
Accessibility Options\General	

Windows XP Accessibility Settings

Table N-76 describes the Windows XP Accessibility Settings supported settings.

Table N-76 Windows XP Accessibility Settings supported settings

Settings Location	Exceptions
Accessibility Options\Keyboard	
Accessibility Options\Sound	
Accessibility Options\Display\High Contrast	
Accessibility Options\Mouse\MouseKeys	
Accessibility Options\General	

Windows Vista Accessibility Settings

Table N-77 describes the Windows Vista Accessibility Settings supported settings.

Table N-77 Windows Vista Accessibility Settings supported settings

Settings Location	Exceptions
Ease of access > Quick access common tools > Turn on Magnifier	
Ease of access > Quick access common tools > Turn on Narrator	
Ease of access > Quick access common tools > Turn on On screen keyboard	

Table N-77 Windows Vista Accessibility Settings supported settings *(continued)*

Settings Location	Exceptions
Ease of access > Quick access common tools > Turn on sticky keys	
Ease of access > Quick access common tools > Turn on High contrast	
Ease of access > Quick access common tools > Setup high contrast	
Ease of access > Quick access common tools > Turn on Filter keys	
Ease of access > Quick access common tools > Set up Filter keys	
Ease of access >windows can read and highlight	
Ease of access > explore all available settings > use computer without display	
Ease of access > explore all available settings > optomize visual display	
Ease of access > explore all available settings > Alternative input devices	
Ease of access > explore all available settings > Mouse -> Setup Mouse keys	
Ease of access > explore all available settings > keyboard	
Ease of access > explore all available settings > Sounds	
Ease of access > explore all available settings > Reasoning Tasks	

Windows Mouse Settings

Ghost User Migration supports the following versions:

- Windows 2000 Mouse Settings
- Windows XP Mouse Settings
- Windows Vista Mouse Settings

Windows 2000 Mouse Settings

Table N-78 describes the Windows 2000 Mouse Settings supported settings.

Table N-78 Windows 2000 Mouse Settings supported settings

Settings Location	Exceptions
Mouse Properties->Buttons->Button Configuration	

Table N-78 Windows 2000 Mouse Settings supported settings *(continued)*

Settings Location	Exceptions
Mouse Properties->Buttons->Files and Folders	
Mouse Properties->Buttons->Double-click speed	
Mouse Properties->Pointers	
Mouse Properties->Pointer Options->Motion	
Mouse Properties->Pointer Options->Acceleration	
Mouse Properties->Pointer Options->Snap to Default	

Windows XP Mouse Settings

Table N-79 describes the Windows XP Mouse Settings supported settings.

Table N-79 Windows XP Mouse Settings supported settings

Settings Location	Exceptions
Mouse Properties->Buttons->Button Configuration	
Mouse Properties->Buttons->Double-click speed	
Mouse Properties->Buttons->ClickLock	
Mouse Properties->Buttons->ClickLock -> Settings	
Mouse Properties->Pointers	
Mouse Properties->Pointer Options->Motion	
Mouse Properties->Pointer Options->Snap to	
Mouse Properties->Pointer Options->Visuality	
Mouse Properties->Wheel->Scrolling	

Windows Vista Mouse Settings

Table N-80 describes the Windows Vista Mouse Settings supported settings.

Table N-80 Windows Vista Mouse Settings supported settings

Settings Location	Exceptions
Ease of access > explore all available settings > Mouse > Mouse settings > Buttons	
Ease of access > explore all available settings > Mouse > Mouse settings > Buttons > ClickLock > Settings	
Ease of access > explore all available settings > Mouse > Mouse settings > Pointers	
Ease of access > explore all available settings > Mouse > Mouse settings > Pointer Options > Motion	
Ease of access > explore all available settings > Mouse > Mouse settings > Pointer Options > Snap To	
Ease of access > explore all available settings > Mouse > Mouse settings > Pointer Options > Visibility	
Ease of access > explore all available settings > Mouse > Mouse settings > Pointer Options > Wheel	

Windows Regional Settings

Ghost User Migration supports the following versions:

- Windows 2000 Regional Settings
- Windows XP Regional Settings
- Windows Vista Regional Settings

Windows 2000 Regional Settings

Table N-81 describes the Windows 2000 Regional Settings supported settings.

Table N-81 Windows 2000 Regional Settings supported settings

Settings Location	Exceptions
Date/Time Properties->Date & Time	
Date/Time Properties->Time Zone	
Regional Settings Properties->Regional Settings	
Regional Settings Properties->Language settings to the system	
Regional Settings Properties->Language settings to the system -> Advanced	

Table N-81 Windows 2000 Regional Settings supported settings *(continued)*

Settings Location	Exceptions
Regional Settings Properties->Numbers	
Regional Settings Properties->Currency	
Regional Settings Properties->Time->Appearance	
Regional Settings Properties->Time	
Regional Settings Properties->Date->Calendar	
Regional Settings Properties->Date->Short date	
Regional Settings Properties->Date->Long date	
Regional Settings Properties->Input Locales	
Keyboard Properties->Speed->Character repeat	
Keyboard Properties->Speed	
Keyboard Properties->Language	
Keyboard Properties->Input Locales	

Windows XP Regional Settings

Table N-82 describes the Windows XP Regional Settings supported settings.

Table N-82 Windows XP Regional Settings supported settings

Settings Location	Exceptions
Date and Time Properties->Date & Time	
Date and Time Properties->Time Zone	
Date and Time Properties->Internet Time	
Regional and Language Options ->Regional Settings	
Regional and Language Options->Language settings to the system	
Regional and Language Options->Language settings to the system -> Advanced	
Regional and Language Options->Customize->Numbers	
Regional and Language Options->Customize->Currency	

Table N-82 Windows XP Regional Settings supported settings *(continued)*

Settings Location	Exceptions
Regional and Language Options->Customize->Time	
Regional and Language Options->Customize->Date->Calendar	
Regional and Language Options->Customize->Date->Short date	
Regional and Language Options->Customize->Date->Long date	
Regional and Language Options->Languages->Text Services and Input Languages->Settings	
Regional and Language Options->Languages->Text Services and Input Languages->Settings->Preferences->Language Bar	
Regional and Language Options->Languages->Text Services and Input Languages->Key Settings	
Regional and Language Options->Advanced	
Regional and Language Options->Advanced->Default user account settings	
Keyboard Properties->Speed->Character repeat	
Keyboard Properties->Speed	
Keyboard Properties->Input Locales	

Windows Vista Regional Settings

Table N-83 describes the Windows Vista Regional Settings supported settings.

Table N-83 Windows Vista Regional Settings supported settings

Settings Location	Exceptions
Date and Time Properties->Date & Time	
Date and Time Properties->Additional Clocks	
Date and Time Properties->Internet Time -> Change Settings	
Regional and Language Options -> Formats	
Regional and Language Options->Formats -> Customize this Format -> Formats	
Regional and Language Options->Formats -> Customize this Format -> Currency	

Table N-83 Windows Vista Regional Settings supported settings *(continued)*

Settings Location	Exceptions
Regional and Language Options->Formats -> Customize this Format -> Time	Time Separator setting not supported.
Regional and Language Options->Formats -> Customize this Format -> Date	
Regional and Language Options->Location	
Regional and Language Options-> Keyboards and Languages -> Settings -> General	
Regional and Language Options-> Keyboards and Languages -> Settings -> Language Bar	
Regional and Language Options-> Keyboards and Languages -> Settings -> Advanced Key Settings	Turn off advanced text services setting not supported.
Regional and Language Options-> Keyboards and Languages -> Settings -> Advanced Key Settings -> Change Key Sequence	
Regional and Language Options-> Administrative->Change System Locale	
Regional and Language Options-> Administrative->Reserved Account Settings...	
Keyboard ->Speed	
Keyboard Properties->Input Locales	Settings not supported

Windows Sound and Multimedia Settings

Ghost User Migration supports the following versions:

- Windows 2000 Sound and Multimedia Settings
- Windows XP Sound and Multimedia Settings
- Windows Vista Sound and Multimedia Settings

Windows 2000 Sound and Multimedia Settings

Table N-84 describes the Windows 2000 Sound and Multimedia Settings supported settings.

Table N-84 Windows 2000 Sound and Multimedia Settings supported settings

Settings Location	Exceptions
SoundsMM Properties->Sounds->Sound Events	
SoundsMM Properties->Sounds->Sound Volume	
SoundsMM Properties->Audio->Sound Playback	Settings not supported
SoundsMM Properties->Audio->Sound Recording	Settings not supported
SoundsMM Properties->Audio->MIDI Music Playback	Settings not supported
SoundsMM Properties->Audio	

Windows XP Sound and Multimedia Settings

Table N-85 describes the Windows XP Sound and Multimedia Settings supported settings.

Table N-85 Windows XP Sound and Multimedia Settings supported settings

Settings Location	Exceptions
SoundsAD Properties->Volume	
SoundsAD Properties->Volume -> Advanced	
SoundsAD Properties->Volume -> Speaker Settings	Settings not supported
SoundsMM Properties->Sounds	
SoundsMM Properties->Sounds->Sound Events	
SoundsMM Properties->Sounds->Sound Volume	
SoundsMM Properties->Audio->Sound Playback	Settings not supported
SoundsMM Properties->Audio->Sound Recording	Settings not supported
SoundsMM Properties->Audio->MIDI Music Playback	Settings not supported
SoundsMM Properties->Audio	

Windows Vista Sound and Multimedia Settings

Table N-86 describes the Windows Vista Sound and Multimedia Settings supported settings.

Table N-86 Windows Vista Sound and Multimedia Settings supported settings

Settings Location	Exceptions
Audio Devices and Sound Themes> Audio Devices	
Audio Devices and Sound Themes> Audio Devices> Volume Control> General	
Audio Devices and Sound Themes> Audio Devices> Volume Control> Configuration	
Audio Devices and Sound Themes> Audio Devices> Volume Control> Other	
Audio Devices and Sound Themes> Audio Devices> Volume Control> Levels	
Audio Devices and Sound Themes> Audio Devices> Volume Control> Options	
Audio Devices and Sound Themes> Audio Devices> Microphone > General	
Audio Devices and Sound Themes> Audio Devices> Microphone > Other	
Audio Devices and Sound Themes> Audio Devices> Microphone > Levels	
Audio Devices and Sound Themes> Audio Devices> Line In > General	
Audio Devices and Sound Themes> Audio Devices> Line In > Levels	
SoundsMM Properties->Sounds->Sound Volume	
Audio Devices and Sound Themes> Sound Events	

Windows Taskbar and Start Menu

Ghost User Migration supports the following versions:

- Windows 2000 Taskbar and Start Menu
- Windows XP Taskbar and Start Menu

Windows 2000 Taskbar and Start Menu

Table N-87 describes the Windows 2000 Taskbar and Start Menu supported settings.

Table N-87 Windows 2000 Taskbar and Start Menu supported settings

Settings Location	Exceptions
Taskbar and Start Menu Properties->General	Settings not supported
Taskbar and Start Menu Properties->Advanced->Start Menu Settings	

Windows XP Taskbar and Start Menu

Table N-88 describes the Windows XP Taskbar and Start Menu supported settings.

Table N-88 Windows XP Taskbar and Start Menu supported settings

Settings Location	Exceptions
Taskbar and Start Menu Properties->Taskbar->Taskbar Appearance	Settings not supported
Taskbar and Start Menu Properties->Taskbar->Notification area	
Taskbar and Start Menu Properties->Start Menu	
Taskbar and Start Menu Properties->Start Menu>Start menu->Customize->General->Select an icon size for program	
Taskbar and Start Menu Properties->Start Menu>Classic Start menu->Customize->Advanced Start menu options	

WinZip

Ghost User Migration supports all versions of WinZip.

Table N-89 describes the WinZip supported settings.

Table N-89 WinZip supported settings

Settings Location	Exceptions
Options->Configuration->View->Columns	
Options->Configuration->View->General	
Options->Configuration->View->Mouse Selection	
Options->Configuration->View->Mouse Selection->Single Click To Open File	
Toolbar	
Folders	
Folders->Working Folders	
Folders->Startup Folders	
Folders->Extract Folder	
Folders->Add Folder	

Table N-89 WinZip supported settings *(continued)*

Settings Location	Exceptions
System->General	
System->Show Add Dialog When Dropping Files On	
System->Explore Shell Extension->	
System->Explore Shell Extension->Use Shell Extensions	
System->Explore Shell Extension->Check For Self Extracting CAB Files	
Miscellaneous->Start up	
Miscellaneous->Other	

Yahoo Messenger

Ghost User Migration supports the following version:

- Yahoo Messenger 5.6

Table N-90 describes the Yahoo Messenger 5.6 supported settings.

Table N-90 Yahoo Messenger 5.6 supported settings

Settings Location	Exceptions
Login -> Preferences -> General	
Login -> Preferences -> General->Misc	
Login -> Preferences -> Content	
Login -> Preferences -> Appearance->Main Messenger Window	
Login -> Preferences -> Appearance->Display of friend names	
Login -> Preferences -> Appearance -> Fonts and Colors	
Login -> Preferences -> Appearance -> Fonts and Colors -> Choose Effects	
Login -> Preferences -> Appearance	
Login -> Preferences -> Messages	
Login -> Preferences -> Messages-Misc	
Login -> Preferences -> Archive	

Table N-90 Yahoo Messenger 5.6 supported settings *(continued)*

Settings Location	Exceptions
Login -> Preferences -> File Transfer	Port Number to Use setting not supported.
Login -> Preferences -> Alerts and Sounds	
Login -> Preferences -> Alerts and Sounds -> A friend comes online	
Login -> Preferences -> Alerts and Sounds -> A friend goes offline	
Login -> Preferences -> Alerts and Sounds -> A friend buzzes me	
Login -> Preferences -> Alerts and Sounds -> I receive an instant message	
Login -> Preferences -> Alerts and Sounds -> I receive a stock alert	
Login -> Preferences -> Alerts and Sounds -> I receive a mail message	
Login -> Preferences -> Alerts and Sounds -> I receive a calendar reminder	
Login -> Preferences -> Chat	
Login -> Preferences -> WebCam	
Login -> Preferences -> Super WebCam	
Login -> Preferences ->Mobile->Mobile Friends	
Login -> Preferences ->Mobile->Mobile Login	
Login -> Preferences ->Mobile	
Login -> Preferences ->WebCam	
Login -> Preferences ->Privacy	
Login -> Preferences -> Privacy->Online Status	
Login -> Preferences ->Connection	

Glossary

baseline image A full image of client computer. You take the image as part of a backup regime. Subsequent backups are saved as incremental backups. Incremental backups include only changes made to the client computer since you created the baseline image/

boot disk set A disk set that contains the Symantec Ghost executable and any necessary drivers. You start a computer from the boot disk set and start Symantec Ghost to perform a cloning operation. Any drivers required to run supported hardware can be saved onto the boot disk set.

boot package A file, bootable disk, Ghost image, or PXE image of a bootable disk that contains the Symantec Ghost executable and any necessary drivers. It lets you start a client computer from the boot package and start Symantec Ghost to perform a cloning operation from the Ghost executable, the GhostCast Server, or the Console.

boot partition A hidden partition on a client computer containing the necessary software to allow communication with the Console and the execution of Console tasks. Usually created as a Ghost image boot package by the Ghost Boot Wizard.

cloning The creation of one or more replicas of a source computer.

command line The direct DOS interface that lets you type commands to be executed.

create To copy the contents of a hard disk or partition to an image file. This includes the disk system area (for example, the partition table) and the data contents.

DHCP (Dynamic Host Configuration Protocol) The program used on client-server networks, as opposed to peer-to-peer networks. When a network uses DHCP, the network includes a DHCP server that automatically assigns IP addresses to computers on the network as needed. Each time that a computer disconnects from the network and then reconnects, the DHCP server assigns a new IP address. Most client-server networks have either a DHCP server or a Bootp server. Bootp is a program that performs the same function as DHCP. When a computer is not on a network, or the network does not have a DHCP server or similar server, then the computer uses a static IP address. The computer static IP address does not change until is it changed manually. A static IP address is retained during a system restart.

DOS (disk operating system) An operating system that can be run from within Windows from a command shell. You cannot run Symantec Ghost from a command shell. A Windows 9x computer can be restarted into DOS. Windows Vista/NT/Me/XP/2000 computers cannot be restarted into DOS except with the use of a boot package containing DOS or using the Ghost virtual or boot partition.

dump See create.

dynamic disk A proprietary disk partitioning structure used by Microsoft Windows 2000/XP. Dynamic disks can be created and deleted within the operating system without having to reboot. Dynamic disks cannot be accessed by other operating systems.

external mass storage device A device that is attached to your computer with a network or cable that is capable of storing large amounts of data. For example, a hard disk attached to a computer with a USB or FireWire cable.

GhostCasting A method of cloning to one or a group of computers simultaneously across a network.

GPT (GUID Partition Table) Part of the Extensible Firmware Interface (EFI) standard, which is the replacement for the PC BIOS. GPT is the standard for the layout of the partition table on a disk.

hard disk A physical disk in your computer or attached as a external device.

image file definition A description of the properties of an image file, including the image file's name, location, and status.

IP (Internet Protocol) address A number that uniquely identifies a computer on a network or on the Internet. IP addresses for computers on a client-server network might change daily or more often. The address for a computer must be unique within a network.

load See restore.

model computer A computer that is used as a model for other computers on the network. It has been installed with an operating system and application software and has had an image file taken. The image file taken from this computer is applied to other computers.

multicast The simultaneous delivery of a file to a number of computers. Multicasting reduces load on a network by sending one file to multiple client computers.

native copy A copy of only the disk structure information and the files, rather than all sectors on the disk. In addition, on FAT partitions, native copying saves the files contiguously. That is, when you write the image to the destination drive, the files are no longer fragmented.

NIC (network interface card) A physical device inside a computer that coordinates communications between the computer and a network.

partition A divided part of a hard disk. An operating system sees a partition as a separate disk if it recognizes the file system.

PreOS An operating system that contains the code that is used to perform tasks on a client computer that cannot be performed while the client computer's operating system is running. Also used when the client computer has no operating system installed (a "bare metal" computer), for example, when restoring images.

properties A set of criteria for a computer. For example, available memory, operating system, or hard disk size.

resources The data stored in the Symantec Ghost Console. For example, images, migration packages, configuration sets, tasks, and client computers.

restore To overwrite all existing data on a computer either with an image file or directly with a copy of another computer. To write information to a disk or partition.

sector copy A copy of an entire disk, including the boot track, all sectors, and unpartitioned space. A sector copy does not filter extraneous or erroneous information from the boot track.

SID (Security Identifier) An identifier that uniquely identifies a computer.

snapshot An image file of a source computer created by AI Snapshot before or after installation of a software application. Two snapshots are compared and used to create a configuration file that captures the changes made to the source computer.

source computer A computer installed with drivers and applications that is used as a template. An image file is created of this computer and restored onto other client computers.

task A series of steps to be performed on targeted client computers.

template task A task which has not had all fields completed. A template task can be executed from the command line with the addition of parameters.

unattended files Files that are used by Sysprep to apply computer-specific information to a computer after cloning to ensure that the computer has a unique name and SID.

user migration package A container for the data captured by a Symantec Ghost User Migration: Capture operation, or Symantec User Migration Wizard operation. These packages can be used to restore a user’s data and settings to another computer.

user migration template A template that defines files, application settings, and registry entries to include in a User Migration task.

Virtual Partition A partition that is created when you perform a backup, restore, clone, or other Symantec Ghost operation from Windows. The Ghost operation is performed from the Virtual Partition.

WMI (Windows Management Instrumentation) WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. It lets you obtain management data from remote computers. In Symantec Ghost you can used this data to provide inventory details for the computers on your network.

Index