

Symantec Ghost™ Implementation Guide

Symantec Ghost™

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 7.5

PN: 07-30-00482

Copyright Notice

Copyright © 1998–2001 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Symantec Ghost, Ghost Walker, Ghost Explorer, and GDisk are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. IBM, OS/2, and OS/2 Warp are registered trademarks of International Business Machines Corporation. Novell and NetWare are registered trademarks of Novell Corporation. 3Com and EtherLink are registered trademarks of 3Com Corporation. Compaq is a registered trademark of Compaq Corporation. Zip and Jaz are registered trademarks of Iomega Corporation. SuperDisk is a trademark of Imation Enterprises Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

SYMANTEC SOFTWARE LICENSE AGREEMENT

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE:

The software and documentation which accompanies this license (collectively, the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

(i) use the Software to clone a hard drive or multiple hard drives from another disk, partition, or disk image file. If a License Module accompanies, precedes, or follows this license, you may make and use that number of copies of the Software licensed to you by Symantec as provided in your License Module on an equal number of individual computers pursuant to the terms of this license. Your License Module shall constitute proof of your right to make and use such copies;

(ii) use the Software to create disk image files of hard drives commensurate with the License Module and store the disk image files on removable media for disaster recovery purposes;

(iii) use the Software to reapply, upgrade, refresh, or recover a hard drive an unlimited number of times provided that the hard drive is part of the original License Module granted by Symantec under this license;

(iv) use the Software to manipulate hard drives and their contents, in the manner described in the software documentation;

(v) make one copy of the Software for archival purposes, or copy the Software onto the hard disk of a computer and retain the original for archival purposes;

(vi) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;

(vii) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license;

(viii) use the Software as described in the documentation; and

(ix) use the Software as described in the documentation to apply changes to a replacement hard drive provided the replaced hard drive has been permanently decommissioned.

You may not:

(i) use the Software for the purpose of creating multiple computers or hard drives for resale or external distribution except as stipulated in a License Module;

(ii) copy the documentation which accompanies the Software except as provided herein;

(iii) sublicense, rent or lease any portion of the Software;

(iv) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or

(v) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version. Upon upgrading the Software, all copies of the prior version must be destroyed.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60)

days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, USA.

6. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

C O N T E N T S

Section 1 Getting started

Chapter 1 About Symantec Ghost

New features in Symantec Ghost	17
How Symantec Ghost works	19
Quick reference guide	21

Chapter 2 Understanding Symantec Ghost basics

Choosing a method to create an image file	23
The Symantec Ghost partition	24
Using the virtual partition to connect to the Console	25
Using the Ghost boot partition to connect to the Console	26
Symantec Ghost components	26
Symantec Ghost Console	26
Symantec Ghost Console client	27
Symantec Ghost GhostCast Server	28
Ghost Boot Wizard	28
Symantec Ghost AutoInstall	29
Symantec Ghost executable	30
Standalone configuration	30
Ghost Walker	30
Ghost Explorer	31
GDisk	31
License Audit Utility	32
Accessibility in Symantec Ghost	32
Accessibility features in Symantec Ghost	32
Support documentation formats	33

Chapter 3 Installing Symantec Ghost

Preparing for installation	36
System requirements	36
What to install	37
Installing the Symantec Ghost Console	38
Installing the Console client	39
Remotely installing the Console client	40
Manually installing the Console client	41
Installing the standalone configuration client	41

Installing Symantec Ghost Standard Tools	42
Registering Symantec Ghost	43
Generating a registration file	43
Obtaining a validation key	44
Entering a validation key	45
Adding additional licenses	45
Registering the Symantec Ghost Console after reinstallation	45
Clearing an outstanding registration request	46
Updating Symantec Ghost	47
Updating the Symantec Console client	47
Uninstalling Symantec Ghost	48
Creating Configuration Server accounts	49
Removing a domain account	51

Section 2 Creating image files and managing tasks from the Console

Chapter 4 Managing image files, configuration resources, and computers

Introducing the Symantec Ghost Console	55
Creating and executing a Symantec Ghost Console task	56
Starting the Symantec Ghost Console	57
Grouping Console client computers	58
Adding or moving a computer to a group	59
Removing a computer from a group	60
Renaming a computer	61
Setting properties for computers in a subnet	61
Storing the Console client computer details	63
Checking client software and status	63
Viewing and changing Console client computer properties	64
Editing and applying new default configuration settings	66
About the Configuration Resources folder	69
Creating and viewing image definitions	70
Creating and viewing configuration sets	71
Creating and viewing AI package definitions	78

Chapter 5 Creating and executing tasks

Understanding tasks	81
Starting a task from a client computer	82

Creating the model computer	82
Creating image dump tasks	83
Setting image dump task properties	84
Creating tasks	87
Setting task properties	88
Reviewing tasks	96
Scheduling and executing tasks	97
Scheduling a task	97
Executing a task manually from the Symantec Ghost Console	98
Initiating a task from a client computer	98
Initiating a task from the client command line	99

Chapter 6 Incremental backups and rollbacks

Introducing incremental backups and backup regimes	101
Creating a backup regime	102
Setting backup regime properties, task, and schedule details	102
Creating a backup manually	105
Viewing computer backups	105
Viewing a backup regime	105
Restoring a computer	106

Chapter 7 Move the User

Introducing Move the User	107
Creating a data template	108
Viewing a data template	111
Creating a User Profile	111
Viewing a User Profile	113
Capturing and restoring user data	113
Variables for use with Move the User	115
Absolute and relative paths	116
User settings that can be moved	117
Accessibility settings	117
Display settings	118
International settings	119
Keyboard settings	120
Mouse settings	120
Sound settings	121
Screen Saver	121
Mapped network drive settings	121
Internet settings	122
Taskbar and Start menu options	122
Desktop options	123

Chapter 8	Sysprep	
	Introducing Sysprep	125
	Setting up Sysprep	126
	Adding a Sysprep configuration	127
	Overwriting a Sysprep configuration	128
	Deleting a Sysprep configuration	128
	Cloning with Sysprep	129
	Editing, restoring or reloading Sysprep.inf	130
	How Sysprep works with cloning and the Console	
	post-configuration process	131
	Configuring Sysprep.inf	132
 Chapter 9	 Creating boot images and disks with the Ghost Boot Wizard	
	Introducing the Ghost Boot Wizard	133
	Opening the Ghost Boot Wizard	134
	Creating boot disks and boot images	134
	Standard boot disks with the option of LPT and USB support	135
	Boot disks with network support	136
	Creating boot disks that support mapping network drives	138
	Boot disks with CD-ROM support	140
	Creating a boot image containing the Console boot partition	141
	Boot packages that support RIS	142
	Starting client computers from the network	144
	Multicard templates and the boot disk	145
	Adding network drivers to the Ghost Boot Wizard	145
	Adding packet drivers to the Ghost Boot Wizard	146
	Adding NDIS2 drivers to the Ghost Boot Wizard	146
	Customizing the template	147
	Adding command-line parameters to a boot package	148
	Selecting a version of DOS	150
 Chapter 10	 Additional Console options	
	Monitoring the Symantec Ghost Console activity	151
	Launching the Configuration Server	154
	Setting the Symantec Ghost Console options	154
	Symantec Ghost Console security	159
	Updating the boot partition certificates	160
	Generating new certificates	160

Chapter 11 Image file options

About Symantec Ghost image files	161
Image files and compression	162
Performance expectations on a network	162
Image files and CRC32	163
Image files and volume spanning	164
Standard image files	164
Size-limited, multisegment image files	164
Spanned image files	164
Spanning across multiple volumes and limiting span sizes	165
Loading from a spanned image	166
Image files and tape drives	166
Image files and CD writers	168
Cloning dynamic disks in Windows 2000	169
Hibernation and swap files	170

Section 3 GhostCasting image files in a networked environment

Chapter 12 Using GhostCasting to create and load images

About Symantec Ghost GhostCasting	175
Preparing for GhostCasting	176
Creating the model computer	177
Creating a GhostCast Server	178
Starting a GhostCast session	178
Controlling the GhostCast session from the server	183
Setting Auto Start parameters	186
Setting the data transfer mode	187
Controlling the amount of network bandwidth used	188
Viewing and changing GhostCast Server session options	190
Running the Symantec Ghost executable	190

Chapter 13 GhostCasting from the command line

Running the GhostCast Server for Windows from the command line	193
Running the DOS-based GhostCast Server	194
Starting the GhostCast session	194
GhostCast Server command-line options	195
Examples using GhostCast Server command-line options	196

Creating a DOS boot disk manually	198
Setting up packet drivers	199

Chapter 14 GhostCasting and IP addresses

Introducing IP addresses for GhostCasting	205
Locally specified IP addresses	206
Examples of Wattcp.cfg client configuration files	206
Using BOOTP/DHCP to assign IP addresses	208
BOOTP/DHCP automatically defined IP address	208
Examples of BOOTP/DHCP defined addresses	209

Section 4 Cloning image files locally

Chapter 15 Symantec Ghost as a standalone program

Starting the Symantec Ghost executable	213
Navigating without a mouse	214
Using Ghost.exe on a standalone computer	215
Cloning disks	215
Cloning disk to disk	216
Cloning a disk to an image file	217
Cloning a disk from an image file	219
Cloning partitions	221
Cloning from partition to partition	221
Cloning a partition to an image file	222
Cloning a partition from an image file	224
Saving an image file to a CD-R/RW	226
Create Ghost boot disks	226
Start your computer	226
Create and save the image file	227
Adding switches to your cloning task	227
Creating a DOS boot disk	228

Chapter 16 Standalone configuration

Introducing the standalone configuration	229
Generating the configuration data file	230
Running the standalone configuration	231
Errors logged during a standalone configuration	231

Section 5 Creating executables to roll out applications

Chapter 17 Getting started with AutoInstall

How AutoInstall works	235
Using AutoInstall	236
Installing AI Snapshot and AI Builder on the model computer	237
Setting up target computers	238
Installing Microsoft products using AutoInstall	238
Letting the model computer restart	238
Adding uninstall commands	238
Using AutoInstall to clone Office XP	238
Microsoft system file protection (SFP) limitations on deploying AI packages	239

Chapter 18 Creating AI packages

Creating an installation script for a software installation	241
Capturing existing system information	241
Installing the software that you would like to package	242
Capturing system information again to determine changes	244
Customizing and building AI packages	245
Customizing installation scripts	247
Building AI packages	250
Modifying installation scripts and AI packages	251
Executing and rolling out AI packages	252

Section 6 Symantec Ghost utilities

Chapter 19 Using Ghost Explorer to modify image file contents

Understanding Ghost Explorer	255
Viewing image files	256
Restoring a file or directory from an image file	257
Modifying image files in Ghost Explorer	258
Adding, moving, and deleting files	258
Saving a list of contents of an image file	258
Setting span file sizes	259
Compiling a file	259

Determining Symantec Ghost image file version	260
Using Ghost Explorer from the command line	260

Chapter 20 Managing partitions using GDisk

Introducing GDisk	263
Overview of main command-line switches	264
Online Help for command-line switches	265
Switches common to all GDisk commands	266
Creating a partition	266
Reinitializing the Master Boot Record	268
Showing information about disks	269
Performing multiple GDisk operations using batch mode	269
FAT16 partitions in Windows NT	271
Deleting and wiping your disk	271
Activate or deactivate a partition	273
Hide or unhide a partition	273
Modify the Windows NT/2000/XP boot menu	274
Specifying the boot.ini path and file name	274
Displaying the list of current boot entries	274
Adding an entry to Boot.ini	275
Removing an entry from Boot.ini	277
Setting the default boot option and timeout	278
Support for large hard disks	278

Chapter 21 Tracking Symantec Ghost license numbers

Setting up the License Audit Utility	281
Running the License Audit Utility	282
Viewing the database file	283
Removing the License Audit Utility	283

Chapter 22 Updating Security Identifiers (SIDs) and computer names

Making SID changes with Sysprep and Ghost Walker on NT based clients	285
Symantec Ghost Walker capabilities	285
Symantec Ghost Walker shortcomings	286
Microsoft Sysprep capabilities	286
Microsoft Sysprep shortcomings	287
Problems with SID changing	287
Using Ghost Walker	287
Running Ghost Walker from the command line	289

Loss of access to external data objects	293
Identical user names and passwords across workstations	293

Section 7 Appendices

Appendix A Command-line switches

Symantec Ghost command-line switches	297
Clone switch syntax	314
Defining the type of clone command	314
Setting a source for the clone switch	315
Setting a destination for the clone switch	316
Setting a destination size for the clone switch	316
Examples of clone switch usage	317
Batch file example	319
CRC32 switch usage	320
Examples of -CRC32 usage	321

Appendix B Setting up the hardware and transfer methods

Hardware and transfer requirements	325
Peer-to-peer connections	325
SCSI tape driver	327
GhostCasting	327
Removable media	327
CD-ROM usage	327
Mapped network volume	328
Internal drives	328
Third party device	328

Appendix C USB and DirectParallel Cables

Parallel Technologies cables	329
Other USB cables	330

Appendix D The Wattcp.cfg network configuration file

The Wattcp.cfg configuration file	331
---	-----

Appendix E Cloning with Linux

Supported configurations	333
Position of disk	334

Boot configuration	334
Symantec Ghost utility support	334

Appendix F Customizing Symantec Ghost functionality

Limiting functionality from the environment file	335
Examples of customized functionality	337
Image file restoration only	337
Backup tool only	337
OEM version of Symantec Ghost	338

Appendix G Troubleshooting

Symantec Ghost error message	339
Symantec Ghost Console errors	341
Symantec Ghost GhostCast errors	341
Symantec Ghost and GhostCast DOS errors	343
Running command-line or scheduled tasks	344

Appendix H Diagnostics

Hard drive detection and diagnostic information	345
Symantec Ghost abort error file (Ghosterr.txt)	345
Creating a full diagnostic statistics dump summary	346
Elementary network testing techniques	346
Testing TCP/IP functionality	346
Generating a GhostCast log file	348

Appendix I Installing Symantec Ghost from the command line

Choosing an interface type for installation	351
Choosing an installation mode	352
Installing from the command line	353
Installing from the command line in Windows 9x or NT	354
Uninstalling from the command line	355

Service and support solutions

CD Replacement Form

Glossary

Index

1

G e t t i n g s t a r t e d

- [About Symantec Ghost](#)
- [Understanding Symantec Ghost basics](#)
- [Installing Symantec Ghost](#)

About Symantec Ghost

This chapter contains the following:

- [New features in Symantec Ghost](#)
- [How Symantec Ghost works](#)
- [Quick reference guide](#)

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

It also makes PC management and deployment issues easy and cost effective. Functionality, including computer configuration management, computer/user migration, and incremental backup, makes Symantec Ghost the solution for removing the problems associated with PC management.

New features in Symantec Ghost

New features in Symantec Ghost 7.5 include:

- Virtual partition

The virtual partition frees you from having to visit a client computer and install the boot partition. It is no longer necessary to perform a destructive clone of a computer to include the boot partition on a client.

- Remote client installation

You can remotely install the Console client from the Symantec Ghost Console on Windows NT/2000/XP client computers. You can browse for computers on a network and install the Console client without physically visiting the computers.

- GhostCast Server

The GhostCast Server replaces the Multicast Server to provide three methods of transferring image files to optimize their deployment. You can choose from:

- Unicast: One copy of the data sent to each computer
- Directed broadcast: Data sent to all computers on a specified subnet
- Multicast: Data sent to all computers on the network that are included in the multicast session

- Reducing GhostCast traffic on the network

You can control how much network bandwidth is used and therefore avoid overloading the network with GhostCast traffic.

- Client initiated tasks

You can initiate tasks from the client computer, freeing you from having to return to the Symantec Ghost Console. This lets you perform a task without having to return to the Symantec Ghost Console computer. Users can initiate tasks.

- Tuning the Console heartbeat

You can configure the ping rate of the Console client, which reduces the network noise associated with Symantec Ghost.

- Microsoft Terminal Services support

Enables the remote control of the Symantec Ghost Console via Microsoft Terminal Server.

- GDisk32

GDisk32 runs from a command line within Windows NT/2000/XP/9x. It updates Boot.ini to change the boot order and lets you create partitions at the end of free space.

- Enhanced dynamic disk support

Symantec Ghost supports a full dynamic disk dump.

- Section 508 of the US Rehabilitation Act of 1973 supported

- Additional security options

New security options include password protection and BIOS-lock.

- Updated post clone configuration support

Symantec Ghost includes Novell NetWare client information.

- Standalone configuration
You can configure computers without using the Symantec Ghost Console.
- Windows XP Professional, Windows 2000 Professional, and Server
Logo Certification

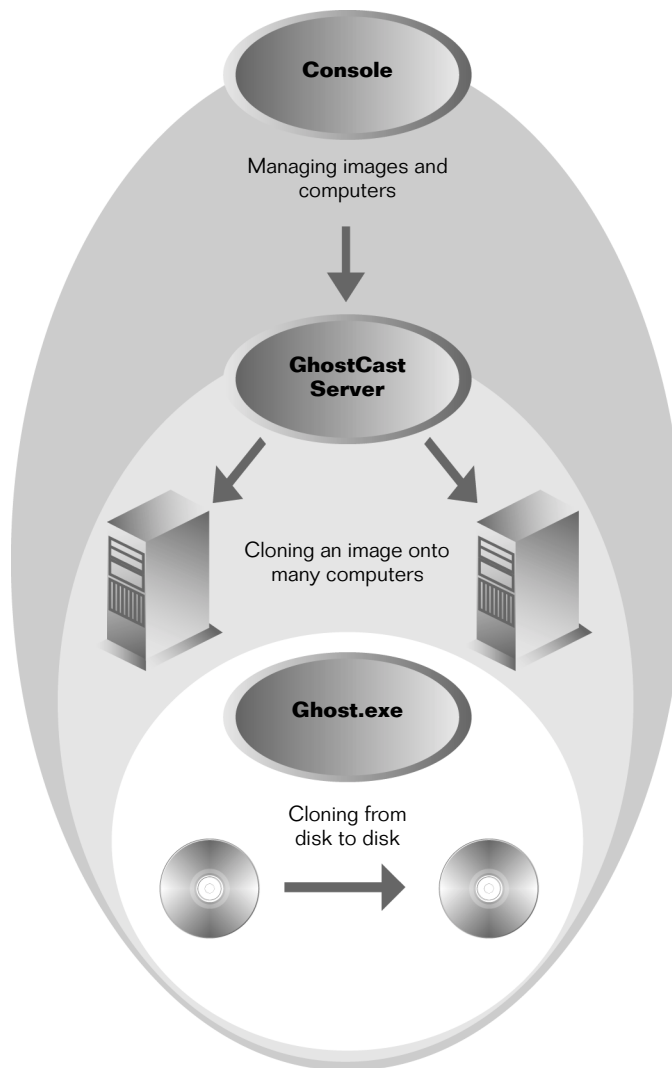
How Symantec Ghost works

The basis of Symantec Ghost is a cloning function that creates an image file containing all of the information required to recreate a complete disk or partition. Image files store and compress images of model system configurations (computers with all of the necessary software installed and configured), or create backup copies of complete drives or partitions. The image file is cloned onto one or more partitions or disks, replacing existing data.

GhostCasting extends this functionality to cloning multiple computers simultaneously across a network, rolling out a standard image file to a group of computers.

Leveraging the cloning and GhostCasting functions, Symantec Ghost lets you manage computers from a central Console. Once the Symantec Ghost client software is installed on the client computers, you can execute operations from the central Console without revisiting the clients.

This graphic describes the relationship between the Symantec Ghost console, the GhostCast Server, and Ghost.exe.



Quick reference guide

This *Implementation Guide* contains procedures that guide you through Symantec Ghost tasks. Listed below are the main tasks that you can perform using Symantec Ghost, and cross-references to the associated procedures.

- Create an image of a model computer from a standalone computer.
For more information, see [“Cloning disks”](#) on page 215.
- Create an image of a networked computer.
 - Use the Console if the Corporate Tools are installed.
For more information, see [“Creating image dump tasks”](#) on page 83.
 - Use GhostCasting if the Standard Tools are installed.
For more information, see [“Starting a GhostCast session”](#) on page 178.
- Create a boot disk for use with a cloning job.
For more information, see [“Boot disks with network support”](#) on page 136.
- Configure a client computer after cloning.
 - Use Ghost Walker to change the computer name and Security Identifiers (SID).
For more information, see [“Using Ghost Walker”](#) on page 287.
 - Use the Console to alter configuration settings.
For more information, see [“Creating and viewing configuration sets”](#) on page 71.
 - Use the standalone configuration to configure a computer without the Symantec Ghost Console.
For more information, see [“Introducing the standalone configuration”](#) on page 229.
- Clone a group of computers with one task.
For more information, see [“Creating tasks”](#) on page 87.
- Clone one or more computers using GhostCasting.
For more information, see [“Loading an image file onto client computers”](#) on page 181.

- Clone a computer that is not networked.
For more information, see [“Cloning disks”](#) on page 215.
- Create an executable to install an application.
For more information, see [“Getting started with AutoInstall”](#) on page 235.
- Create a backup regime.
For more information, see [“Incremental backups and rollbacks”](#) on page 101.
- Migrate a user to a new operating system.
For more information, see [“Move the User”](#) on page 107.

Understanding Symantec Ghost basics

This chapter contains the following:

- [Choosing a method to create an image file](#)
- [The Symantec Ghost partition](#)
- [Symantec Ghost components](#)
- [Accessibility in Symantec Ghost](#)

Choosing a method to create an image file

There are three ways to create an image and clone it onto a computer:

- Standalone
- GhostCasting
- Console

Which method you choose depends on how many computers you are cloning, the operating system installed, and the functions required.

Cloning option	Explanation
Cloning a standalone computer disk-to-disk	Use the Symantec Ghost executable to clone one drive or partition onto another. This can be within a computer, or between computers with an LPT/USB, mapped network drive, or network connection. This is fast and efficient. Only Ghost.exe and the relevant drivers on a floppy disk are required.
Cloning over a network using GhostCasting	<p>You can use the Standard Tools on a server computer and run the Symantec Ghost executable on the client computers to create an image file. You can then clone a number of computers simultaneously.</p> <p>The Symantec Ghost executable is used on each client computer from a boot disk created with the Symantec Ghost Boot Wizard.</p>
Cloning using a Console task	The Console draws on the functionality of standalone and GhostCasting but offers many more functions. A cloning task is created that can be run concurrently with other tasks. After cloning is complete, you can apply configuration settings to the computer.

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
- Ghost boot partition

When 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 DOS is executed.

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 clone onto the client computer.

For more information, see the *Installing the Ghost boot partition* PDF on the Symantec Ghost CD.

You can check the Ghost partition settings for each client computer.

For more information, see [“Storing the Console client computer details”](#) on page 63.

Using the virtual partition to connect to the Console

The virtual partition is created on client computers that:

- Have an operating system installed
- Do not have the Ghost boot partition installed

The virtual partition is created on a computer once the Console client is installed and a task that requires a restart in DOS is run. This process is transparent to you and the user on the client computer.

Once you have installed the Console client on the client computer, and a task requiring a restart in DOS is executed from the Console for that client, then the virtual partition is created to let the task execute.

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

Note the following points regarding the virtual partition:

- A free primary slot in the partition table is required.
- Compressed drives on Windows 9x computers are not supported.
- Support of dynamic disks is limited to simple dynamic disks. The virtual partition is not supported on spanned, striped, and RAID-5 volumes.
- If a client computer is using static IP, then the same static IP address is used in the virtual partition.
- If you select MS-DOS in the Ghost Boot Wizard, then the virtual partition is updated to use MS-DOS.

Using the Ghost boot partition to connect to the Console

The Ghost boot partition is used on client computers that:

- Have a previous version of the Console client for Symantec Ghost installed. If you have upgraded the Console to version 7.5, then the boot partition exists on your client computers.
- Have no operating system installed. If you have a computer that has no operating system installed, then you cannot install the Console client on the computer. However, you can create a Ghost boot partition that contains the Console client, which then connects to the Console.

If the Ghost boot partition exists on a client computer, then it is used when a task is run. Client computers that have a previous version of the Console client installed have the boot partition. You don't have to use the virtual partition if the Ghost boot partition exists on the computer.

For more information, see [“Adding Advanced features for cloning”](#) on page 90.

The process of creating a Ghost boot partition on a client computer consists of several steps. This process is described in the *Installing the Ghost boot partition* PDF on the Symantec Ghost CD.

Symantec Ghost components

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

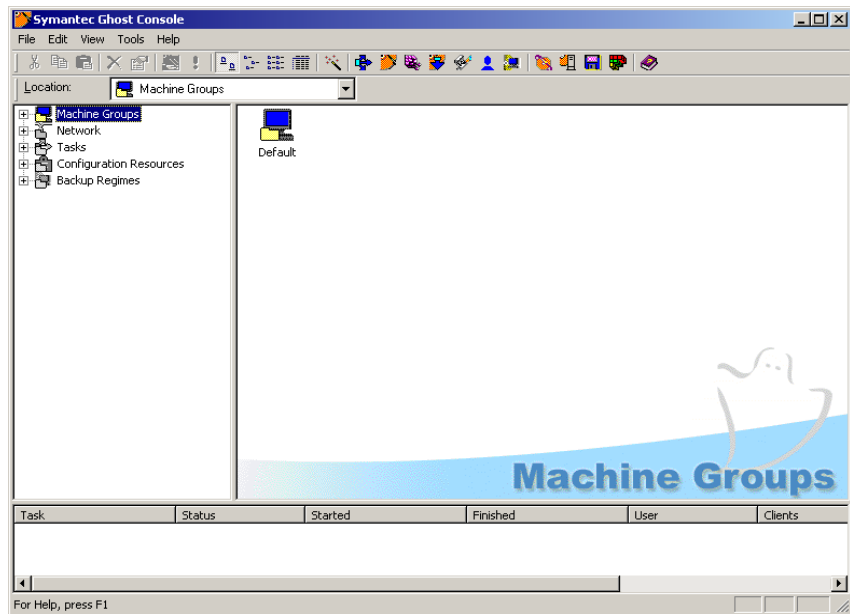
The Symantec Ghost Console is a Windows server-based application for remote management of cloning operations, post-cloning configuration, and AutoInstall operations.

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

The Symantec Ghost Console stores workstation configuration data, allowing the reconfiguration of a computer after the cloning operation. Stored workstation data includes:

- Computer name
- Workgroup or domain
- Computer description
- TCP/IP settings

Symantec Ghost Console main window



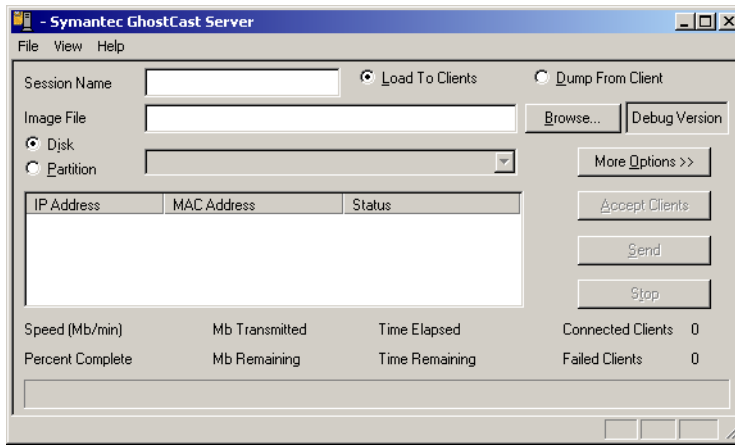
Symantec Ghost Console client

The Console client is comprised of a Windows agent and a Ghost partition. The client is installed on all Windows 9x/NT/XP/Me/2000 computers, enabling remote control from the Symantec Ghost Console. The Windows agent is an unobtrusive application that lets the computer start from the Ghost partition when required by the Console. The Ghost partition is a hidden DOS partition installed on the computer that lets the Symantec Ghost executable perform cloning operations.

Symantec Ghost GhostCast Server

The GhostCast Server delivers an image file to multiple computers simultaneously using a single IP GhostCast transmission. This minimizes the impact on network bandwidth. The GhostCast Server sends or receives images to or from one or more computers rather than accessing a mapped network drive, which is slower than GhostCasting.

Symantec Ghost
GhostCast Server
main window

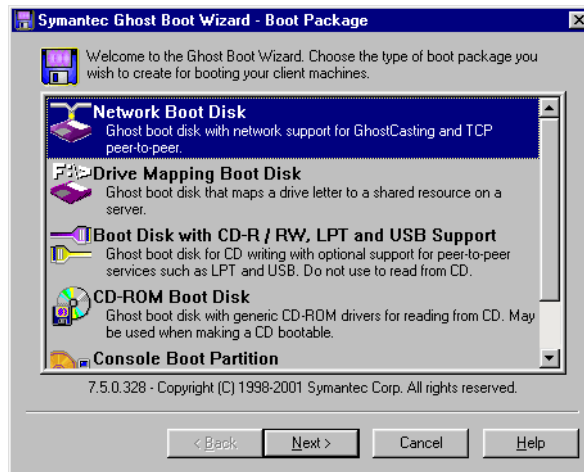


Ghost Boot Wizard

Use the Ghost Boot Wizard to create boot packages. A boot package can be a boot disk, a Ghost image file, or a Preboot eXecution Environment (PXE) image. Boot packages are used for all cloning jobs, from creating a simple boot disk for GhostCasting, to providing a boot image for use with PXE applications such as 3Com's DynamicAccess boot services or

Microsoft's Remote Installation Service. The wizard guides you to the drivers needed to create a boot package.

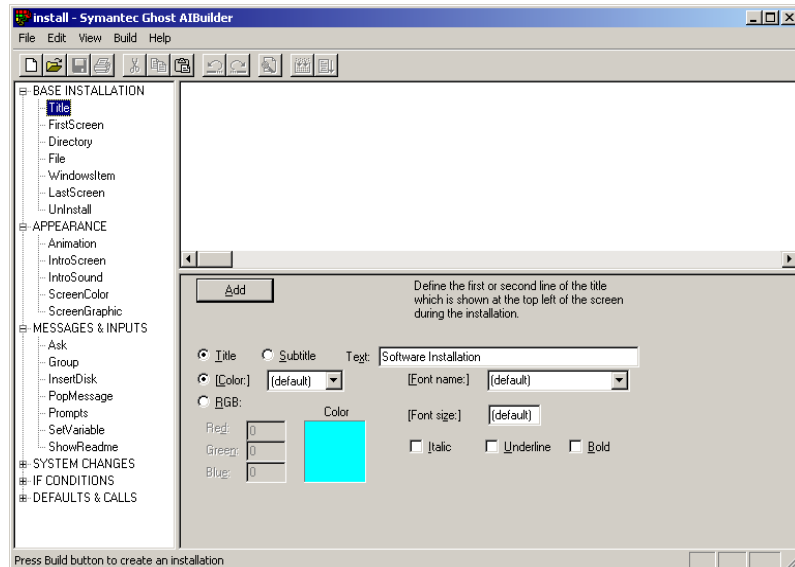
Symantec Ghost
Boot Wizard
main window



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 workstations from the Symantec Ghost Console.

AI Builder main
window

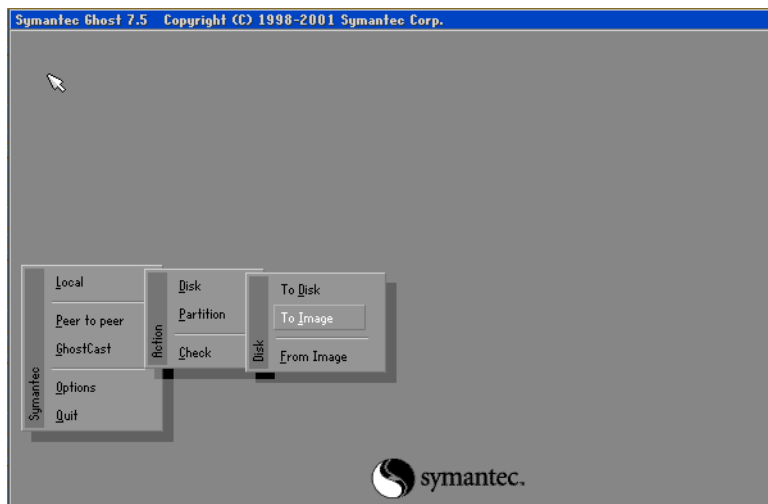


Symantec Ghost executable

The Symantec Ghost executable (Ghost.exe) makes disk cloning possible. Because the executable is small with minimal conventional memory requirements, you can run it easily from a DOS boot disk or hard drive. Symantec Ghost can load a workstation from an image file containing both Windows 98 and the full installation of Office 97 in under a minute.

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

Ghost.exe menu



Standalone configuration

The standalone configuration feature lets you apply configuration settings directly to a computer. This lets you run a post clone configuration without using the Symantec Ghost Console.

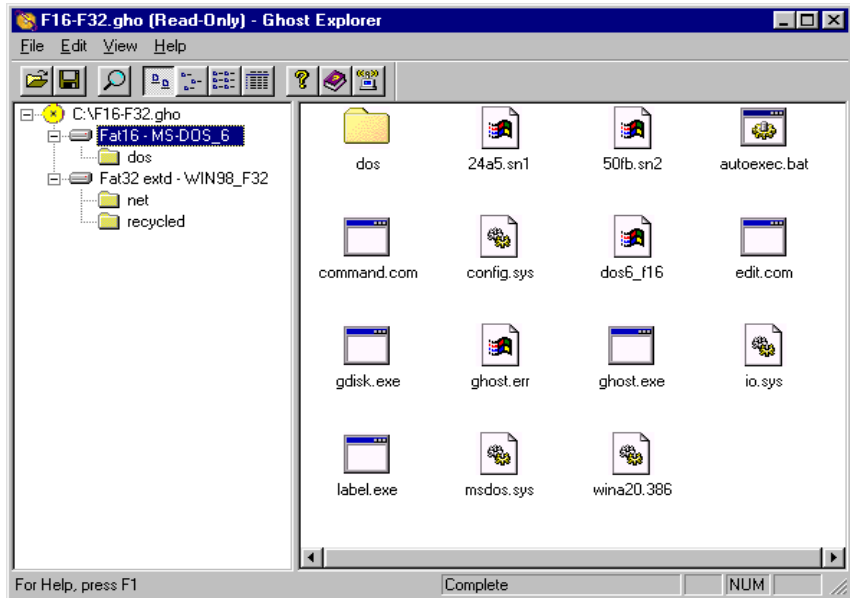
Ghost Walker

Ghost Walker assigns statistically unique security identifiers (SIDs) to cloned Microsoft Windows NT/2000/XP workstations. The SID is an important part of the Windows NT/2000/XP security architecture as it provides a unique identifier when a computer is networked.

Ghost Explorer

Ghost Explorer lists all of the files and directories within image files. On FAT and Linux file systems, you can also add, recover, and delete individual directories and files to or from an image file.

Ghost Explorer
main window



GDisk

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

- FAT file system formatting
- Batch mode operation
- Hiding and unhiding of partitions
- Secure disk wiping
- 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.

Two versions of GDisk are supplied:

- GDisk: Runs in DOS
- GDisk32: Runs from the command-line in a Windows operating system

License Audit Utility

The License Audit Utility measures the usage of Symantec Ghost on a network. It counts the number of computers that have been cloned using Symantec Ghost and stores the results in a file. Tools are provided to add this program to users' logon scripts to let the process occur automatically, and then to view the results.

Accessibility in Symantec Ghost

Symantec Ghost includes two features for accessibility:

- Optional Ghost watermarks
- Alternative documentation formats

For more information on accessibility features, contact your Symantec sales representative.

Accessibility features in Symantec Ghost

Turn off the Ghost watermarks on the Symantec Ghost Console if you are using the Windows high contrast accessibility option with white text on a black background.

For more information, see [“Setting the Symantec Ghost Console options”](#) on page 154.

Support documentation formats

The user documentation for Symantec Ghost is available in the following formats.

Document	Format
<i>Symantec Ghost Implementation Guide</i>	<ul style="list-style-type: none">■ Printed manual■ Ghost_guide.pdf, PDF document
Getting Started Guide Card	<ul style="list-style-type: none">■ Printed card■ Getting_Started.pdf, PDF document
Installing the boot partition	<ul style="list-style-type: none">■ Boot_partition.pdf, PDF document
Readme	<ul style="list-style-type: none">■ Readme.txt, text document
Online help	<ul style="list-style-type: none">■ HTML compiled .chm files

Online help is available for the following components:

- AutoInstall
- Console
- GhostCast
- Ghost Boot Wizard
- Ghost Explorer
- License Audit Utility
- Registration

Installing Symantec Ghost

This chapter contains the following:

- [Preparing for installation](#)
- [Installing the Symantec Ghost Console](#)
- [Installing the Console client](#)
- [Installing the standalone configuration client](#)
- [Installing Symantec Ghost Standard Tools](#)
- [Registering Symantec Ghost](#)
- [Updating Symantec Ghost](#)
- [Uninstalling Symantec Ghost](#)
- [Creating Configuration Server accounts](#)

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.

For more information, see [“Creating AI packages”](#) on page 241.

Preparing for installation

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

System requirements

This sections lists the minimum requirements for each installation option.

Symantec Ghost Console

- For Windows NT/2000/XP: 48 MB RAM (96 MB recommended)
- Pentium processor
- VGA monitor
- One of the following:
 - Windows 2000 SP2 with Internet Explorer 4.0 installed
 - Windows NT 4.0 SP6A with Internet Explorer 5.0 installed
 - Windows XP

Ghost.exe

- IBM PC computer or 100% compatible
- 386 processor
- 8 MB RAM
- VGA monitor
- Microsoft compatible mouse recommended

To support CD writing:

- An additional 6.5 MB above the Ghost.exe requirements
- CD writer supported by Symantec Ghost

Symantec Ghost Console client

- Networked computer with Windows 95/98/2000/Me/XP, or Windows NT 4.0 SP4
- Single boot system

- Can have more than one physical disk, but backup functionality supports the first physical disk only
- DOS drivers for network card

For more information, see [“Creating boot images and disks with the Ghost Boot Wizard”](#) on page 133.

Standard Tools

- IBM computer or 100% compatible
- 386 processor
- 8 MB RAM
- VGA monitor
- Microsoft compatible mouse recommended
- Microsoft Windows 9x/2000/NT/Me/XP

File systems supported for standalone cloning

- All FAT
- All NTFS
- EXT2

For more information, see [“Cloning with Linux”](#) on page 333.

What to install

Symantec Ghost has five software packages. Use this table to determine what you need to install and where you need to install it.

Component	Description
Symantec Ghost Console	Install on the server computer from which you plan to remotely clone and configure other workstations. Install all components of Symantec Ghost on the server except for the Console client.
Symantec Ghost Console client	Install on your workstations to enable communication among your workstations and the Symantec Ghost Console.

Component	Description
Symantec Ghost standalone configuration client	Install on a workstation that is not to be managed by the Symantec Ghost Console. Install this client to apply configuration settings after a clone using Ghost.exe. For more information, see “Introducing the standalone configuration” on page 229.
Symantec Ghost Standard Tools	Install when the Console is not required. Install all components of Symantec Ghost except for the Console server and client.
AutoInstall	Install on the computer on which you want to create packages to install applications. For more information, see “Getting started with AutoInstall” on page 235.

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

Installing the Symantec Ghost Console

The Symantec Ghost Console must be installed by someone with administrator rights on the Console computer. When you install the Symantec Ghost Console, the Standard Tools are automatically installed.

Note: The user name, email address, and serial number that you enter during installation are used in the registration process.

To install the Symantec Ghost Console

- 1 Insert the Symantec Ghost CD into the CD-ROM drive.
- 2 In the Symantec Ghost installation window, click **Install Symantec Ghost Corporate**.
- 3 Click **Next**.
- 4 Accept the terms of the license agreement, then click **Next**.
- 5 Click **Next**.
- 6 In the User Information window, verify that the user and organization names are correct.

For more information, see [“Generating a registration file”](#) on page 43.

- 7 In the Email Address field, type the email address to which the registration file should be sent.
This must be a valid and working email address.
- 8 In the Serial Number field, type the serial number from your Symantec Ghost certificate.
For more information, see [“Generating a registration file”](#) on page 43.
- 9 Click **Next**.
- 10 Do one of the following:
 - Confirm the installation location.
 - To select a different installation location, click **Browse**.
- 11 Click **Next**.
- 12 In the Custom Setup window, click **Next**.
- 13 In the Symantec Ghost Console Service Account Registration window, click **Next**.
If required, change the Console Service Account Password to increase security.
For more information, see [“Creating Configuration Server accounts”](#) on page 49.
- 14 Click **Install** to start the installation.

Installing the Console client

You can install the Console client in one of two ways:

- Install the Console client remotely from the Symantec Ghost Console.
You can install the Console client on computers running Windows NT/2000/XP. Installing the client remotely lets you avoid physically visiting the client computer.
- Manually install the Console client on a workstation from the Symantec Ghost CD.

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

For more information, see [“Storing the Console client computer details”](#) on page 63.

Remotely installing the Console client

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

If you are installing on more than one computer in a workgroup, install each computer separately.

To remotely install the Console client

- 1 On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the Tools menu, click **Remote Client Install**.
- 3 Select the computers to include in the client installation.
You can select multiple computers under different domains.
- 4 Click **Install**.
- 5 In the Admin User name field, do one of the following:
 - Type the administrator name for the domain.
 - Type the fully qualified user name for a computer under the workgroup.

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

For example, machinename\username.

If you have selected more than one domain, this dialog box appears until you have entered the administrator details for each domain.

- 6 In the Password field, type the password for the account.
- 7 Click **OK**.

Manually installing the Console client

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

To manually install the Console client

- 1 Insert the Symantec Ghost CD into the CD-ROM drive of the client computer.
- 2 In the Symantec Ghost install window, click **Install Symantec Ghost Corporate**.
- 3 In the InstallShield Wizard window, click **Next**.
- 4 Accept the terms of the license agreement, then click **Next**.
- 5 Click **Console Client**.
- 6 Click **Next**.
- 7 In the Connect to server window, type the computer name of the Ghost Console server.
- 8 Click **Next**.
- 9 In the Destination Folder window, do one of the following:
 - Click **Next** to confirm the current folder as the destination folder for the Console client.
 - Click **Change** to change the destination folder for the Console client.
- 10 Click **Install** to start the installation process.

Installing the standalone configuration client

Install the standalone configuration client if the client is not to be managed by the Symantec Ghost Console and the only Symantec Ghost functionality to be performed on this computer is a post clone configuration.

To install the standalone configuration client

- 1 Insert the Symantec Ghost CD into the CD-ROM drive.
- 2 In the Symantec Ghost install window, click **Install Symantec Ghost Corporate**.
- 3 In the InstallShield Wizard window, click **Next**.
- 4 Accept the terms of the license agreement, then click **Next**.
- 5 Click **Standalone Client**.

- 6 Click **Next**.
- 7 In the Destination Folder window, do one of the following:
 - Click **Change** to change the destination folder for the Console client.
 - Click **Next** to confirm the current folder as the destination folder for the Console client.
- 8 Click **Install** to start the installation process.

Installing Symantec Ghost Standard Tools

Install Standard Tools to use the Ghost executable, Ghost Boot Wizard, Ghost Walker, GhostCast Server, GDisk, and Ghost Explorer.

To install Symantec Ghost Standard Tools

- 1 Insert the Symantec Ghost CD into the CD-ROM drive.
- 2 In the Symantec Ghost installation window, click **Install Symantec Ghost Corporate**.
- 3 Click **Next**.
- 4 Accept the terms of the license agreement, then click **Next**.
- 5 In the Choose Installation Type window, click **Standard Tools only (Ghost, Gdisk etc)**.
- 6 Click **Next**.
- 7 Do one of the following:
 - Confirm the installation location.
 - To select a different location for the installed files, click **Browse**.
- 8 Click **Next**.
- 9 In the Custom Setup window, click **Next**.
- 10 Click **Install** to start the installation.

Registering Symantec Ghost

After installing the Symantec Ghost Console, you must register Symantec Ghost. Until you register Symantec Ghost, your use of the Console is restricted. A registered version of Symantec Ghost tracks the number of client computers attached to the Console, and informs you when you have installed 90% of the licensed clients.

For new installations:

- You can run the Console for no more than 30 days after installation.
- You can have a maximum of 10 clients attached to the Console for new installations.

If you are upgrading from a previous version of Symantec Ghost, you can attach the existing number of clients to the Console for a period of 30 days.

To register Symantec Ghost:

- Generate a registration file.
- Obtain a validation key.
- Enter the validation key.

Generating a registration file

A registration file is generated in one of two ways:

- By entering the registration information, including a user name, email address, and a serial number in the User Information dialog box during installation

For more information, see [“Installing the Symantec Ghost Console”](#) on page 38.

- By generating a registration file manually after installing the Symantec Ghost Console

The registration file, Ghostreg.dat, is saved in the folder in which Symantec Ghost is installed.

You may need to manually generate a registration file if:

- You need to register the Console for additional licenses.
- A serial number was not entered at the time of installation.
- The registration file was lost.
- You are experiencing difficulty in getting a validation key using the existing registration file.

If you have generated a registration file and have not yet entered a validation key, you cannot generate a new registration file. If you have a problem with the existing registration file, you must clear the outstanding registration request before generating a new one.

For more information, see [“Clearing an outstanding registration request”](#) on page 46.

To manually generate a registration file

- 1 On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the Help menu, click **Generate Registration file**.
- 3 In the E-mail address field, type the email address to which to send the validation key.
This must be a valid and working email address.
- 4 In the Serial number field, type the serial number.
This is the 10 digit number usually found on the certificate confirming your Symantec purchase.
- 5 Click **OK**.

Obtaining a validation key

Once you have generated the registration file, Ghostreg.dat, email it to Symantec to receive a validation key.

To obtain a validation key

- Email Ghostreg.dat to ghostreg@symantec.com.
Email the file as an attachment and do not include any text in the email. Symantec will return a validation key to the email address entered when the registration file was generated. A validation key is usually returned within 48 hours.

Entering a validation key

Once Symantec has emailed a validation key to you, you can complete the registration process.

To enter a validation key

- 1 On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the Help menu, click **Register Console**.
- 3 In the Validation Key field, type the validation key that you received in the email from Symantec.
- 4 Click **OK**.

The Symantec Ghost Console is now registered for the number of clients for which you are licensed.

Adding additional licenses

To register the Console for additional licenses, you must generate a new registration file and complete the registration process.

The following details must be the same as the original installation:

- User name
- Email address

Registering the Symantec Ghost Console after reinstallation

If you uninstall the Symantec Ghost Console, and then reinstall it, you must reenter the original validation key. However, the following details must be the same as when the Console was first registered:

- Email address
- Serial number
- User name

If you bought additional licenses before reinstalling, then you must repeat the registration process for each set of licenses purchased.

- 1 Register the Console with the original validation key.
- 2 Generate a new registration file with the same information used to purchase the additional licenses.
- 3 Register the Console with the additional license validation key.
- 4 Repeat steps 2-3 until all of the additional license validation keys are registered.

Clearing an outstanding registration request

If you have generated a registration file and have not yet received and entered a validation key, you cannot generate another registration file. If you have a problem with the existing registration file, you must clear the outstanding registration request before generating a new one.

To clear an outstanding registration request

- 1 On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 Click **Close** to close the Console Wizard.
- 3 On the Help menu, click **Generate Registration file**.
- 4 Click **Clear outstanding request** to delete the current Ghostreg.dat file.
- 5 Click **Yes** to confirm the deletion.

You must generate a new registration file and complete the registration process.

For more information, see [“Generating a registration file”](#) on page 43.

The Symantec Ghost executable runs under DOS, but you must install Symantec Ghost in a Windows operating system.

To install Symantec Ghost

- 1 Insert the Symantec Ghost CD into the CD-ROM drive.
- 2 In the Symantec Ghost install window, click **Install Symantec Ghost 2002**.
- 3 Click **Next**.
- 4 Follow the on-screen instructions.

Updating Symantec Ghost

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

- Provide free updates to fix defects and provide additional features to the Symantec Ghost program. LiveUpdate connects to Symantec via the Internet to see if updates are available for Symantec Ghost.
- Update the Symantec Ghost Console if there is a new version. You receive the updated client version of the software through LiveUpdate.

Symantec does not charge for Symantec Ghost 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 > Corporate 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.

Updating the Symantec Console client

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

Uninstalling Symantec Ghost

Uninstall the Console in the Control Panel in Windows.

To uninstall the Symantec Ghost Console

- 1 On the Console server, on the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 Click **Symantec Ghost Corporate**.
- 4 Click **Remove**.

You can uninstall the client from the Symantec Ghost Console on Windows NT/2000/XP computers.

To remotely uninstall a client computer

- 1 In the left pane of the Symantec Ghost Console, 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**.

You can also uninstall the Console client on the client computer. On Windows 9x computers, the client must be uninstalled from the Control Panel in Windows.

To uninstall the Console client on the client computer

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 Click **Symantec Ghost**.
- 4 Click **Remove**.

Creating Configuration Server 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 user account must be created on the domain.

The user name and password are set for the Console Service Account during installation. The default user name is Ghost_computer name, and the default password is Ghost_computername. The Configuration Server logs on as this user. The user does not have interactive logon rights, is not a member of any groups, and only has the privilege to manage computer accounts.

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

You can either:

- Create a Configuration Server account from the Symantec Ghost Console.
- Create a Configuration Server account manually.

You must create a user with the same user name and password as the defaults that were set during installation, and you must set some rights for the account.

Example code for setting user rights is included on the Symantec Ghost CD in the following directory:

`\Extras\Source\Consoleaccount`

To create Configuration Server accounts from the Symantec Ghost Console

- 1 On the Console server, on the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate 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** and type a user name and password to create a Configuration Server account on the domain.
The user of the Configuration Server account must have the authority to create an account on the domain.
 - Uncheck **Create account in the domain**.
You must have previously created a user account on the domain.
- 6 Click **OK**.

Although it is unlikely to be a security risk, you might want to use Windows administration tools to change the password for this user. If you do this, you must inform the Configuration Server service of the new password by setting the registry value password under the following key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Ngserver
\Params

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 > Corporate Console**.
- 2 On the Tools menu, click **Supported Domains list**.
- 3 Select the domain to remove.
- 4 Click **Remove**.

2

C r e a t i n g i m a g e f i l e s a n d m a n a g i n g t a s k s f r o m t h e C o n s o l e

- Managing image files, configuration resources, and computers
- Creating and executing tasks
- Incremental backups and rollbacks
- Move the User
- Sysprep
- Creating boot images and disks with the Ghost Boot Wizard

-
- Additional Console options
 - Image file options

Managing image files, configuration resources, and computers

This chapter contains the following:

- [Introducing the Symantec Ghost Console](#)
- [Creating and executing a Symantec Ghost Console task](#)
- [Grouping Console client computers](#)
- [Storing the Console client computer details](#)
- [About the Configuration Resources folder](#)

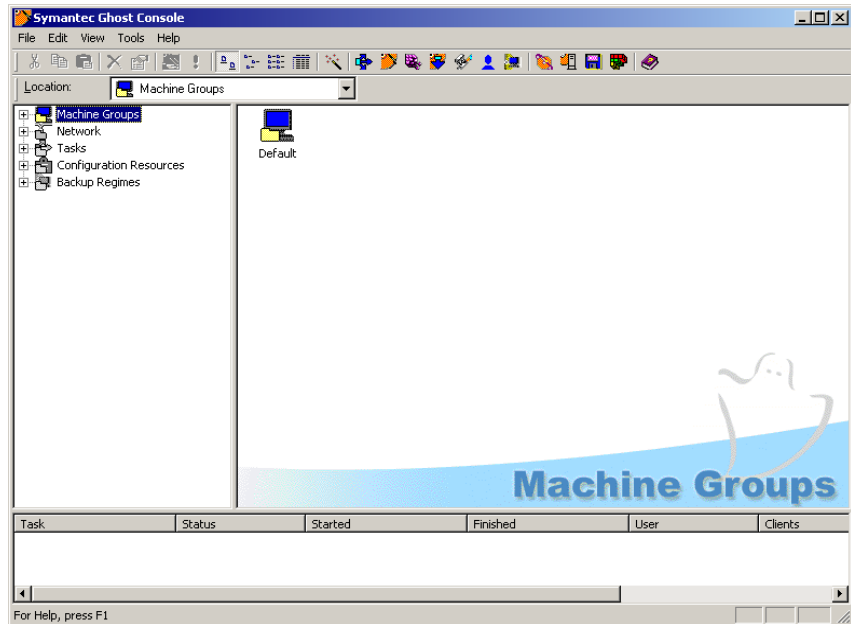
Introducing the Symantec Ghost Console

The Symantec Ghost Console lets you:

- Define and execute tasks that automate the distribution of image files
- Deploy AI packages
- Alter the configuration settings on a Console client computer, or a group of Console client computers
- Create backups
- Save user data
- Run the Microsoft Sysprep application
- Transfer files to client computers

- Execute commands on client computers
- Organize and manage your client computers, image files, configuration sets, and other resources required to complete these tasks

Symantec
Ghost Console
main window



Creating and executing a Symantec Ghost Console task

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

Warning: For a Symantec Ghost Console task to execute successfully, the Symantec Ghost client software must be installed on each client computer.

To create and execute a Symantec Ghost Console task

- 1 Install the Symantec Ghost client software on all Console client computers.
- 2 Group Console client computers to create a specific set of target computers to receive the task.
For more information, see [“Grouping Console client computers”](#) on page 58.
- 3 Define a task.
For more information, see [“Creating tasks”](#) on page 87.
- 4 Execute the task for a computer or group of computers.
For more information, see [“Scheduling and executing tasks”](#) on page 97.
- 5 Review the Task Log to check the statuses of executed tasks.
For more information, see [“To view the Task Log”](#) on page 152.

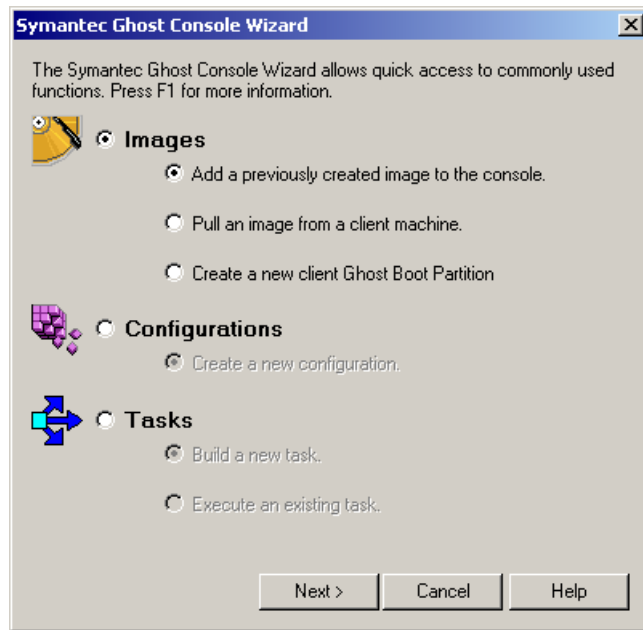
Starting the Symantec Ghost Console

To make the Symantec Ghost Console easier to use, a list of the most frequently used options and tasks appears when you first open the Console.

To start the Symantec Ghost Console

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 Click **OK** and read the Readme document.
The Symantec Ghost Console Wizard appears.

The wizard lets you access the most frequently executed tasks using the Symantec Ghost Console program.



Note: The Symantec Ghost Console runs in Windows Me, Windows NT, and Windows 2000. It does not run in Windows 9x.

Grouping Console client computers

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

To create a computer group

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Group folder.

To place your new group beneath an existing group, expand the folders until you open the parent group. If you do not select a Machine Group folder, the computers are stored in the Machine Group default folder.

- 2 On the File menu, click **New > Folder**.
- 3 Type a new name for the Machine Group.
- 4 Press **Enter** to confirm the rename.

You can now add computers to this group.

Adding or moving a computer to a group

When you install the Symantec Ghost software on a Console client computer, the Console client appears in the Default folder of the Symantec Ghost Console. You can then move the computer into another group if required.

There are two restrictions for adding computers to a group:

- You cannot have a computer in the root folder of the Machine Groups folder. You must have at least one folder below the root folder in which to place a computer or group of computers.
- You can have more than one copy of a computer. However, there can be only one copy in any folder below each main folder. (A main folder is a folder immediately below the Machine Groups folder.)

If you place a computer in a folder, you can't place the same computer in a subfolder of that folder. A warning message appears if you try to add more than one instance of a computer within a main folder.

To add or move a computer to a group

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Group folder.
- 2 Select the computer that you want to add to the group.
- 3 On the Edit menu, do one of the following:
 - Click **Copy** to add another instance of this computer.
 - Click **Cut** to move this computer to another folder.

The Console client computer remains visible in this folder until you paste it into a new folder.
- 4 Open the group in which you want to add the computer.
- 5 On the Edit menu, click **Paste**.

The computer appears in the new group.

Removing a computer from a group

You can remove a computer from a group temporarily. When the computer restarts, the Symantec Ghost Console detects it and it appears in the Console.

To remove a computer from a group temporarily

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to remove.
- 3 Select the computer that you want to remove.
- 4 On the File menu, click **Delete**.
- 5 Click **Yes** to confirm the deletion.

If you have two copies of the same computer in different groups, you can remove one. Removing one copy does not remove the other.

To remove the computer permanently, uninstall the client software from the computer, and overwrite the Symantec Ghost DOS boot partition if it exists.

For more information, see [“Uninstalling Symantec Ghost”](#) on page 48.

To remove the boot partition from a computer

- 1 Create an image file of the computer.
For more information, see [“Creating tasks”](#) on page 87.
- 2 Dump the image file onto the computer, including the option to overwrite the Ghost boot partition in the Advanced options dialog box.
For more information, see [“Creating tasks”](#) on page 87.
- 3 Remove the Symantec Ghost client from the computer.
For more information, see [“Uninstalling Symantec Ghost”](#) on page 48.

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 a computer

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to rename.
- 3 Select the computer that you want to rename.
- 4 On the File menu, click **Rename**.
- 5 Type a name for the computer.
- 6 Press **Enter**.

Setting properties for computers in a subnet

Each client computer is grouped by subnet. When a client computer is discovered by the Symantec Ghost Console, it is automatically grouped by subnet within the Network folder. This lets you set properties to apply to all computers within a subnet. You can set the following properties for a subnet:

- Client heartbeat interval: You can also set the client heartbeat interval globally and for client computers.

For more information, see [“Setting the client computer heartbeat interval”](#) on page 65 and [“Setting the Symantec Ghost Console options”](#) on page 154.

- Data throughput limits: Symantec Ghost lets you control how much network bandwidth is used when GhostCasting. Use this functionality to avoid overloading the network with GhostCasting traffic.

For more information, see [“Controlling the amount of network bandwidth used”](#) on page 188.

- Data transfer mode: You can select one of the following data transfer modes.

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

For more information, see [“Setting the data transfer mode”](#) on page 187.

To set properties for a subnet

- 1 In the left pane of the Symantec Ghost Console, expand the Network folder.
- 2 Click the subnet for which you want to set properties.
- 3 On the File menu, click **Properties**.
- 4 Click **Client Heartbeat Interval** and type the number of seconds for the heartbeat interval.
- 5 Click **Load** to set a limit for loading an image and type the maximum MB per minute for loading an image.
- 6 Click **Dump** to set a limit for dumping an image and type the maximum MB per minute for dumping an image.
- 7 Click **Data transfer mode** to set a transfer mode.
- 8 Select one of the following:
 - Multicast: Set the transfer method to multicast.
 - Direct Broadcast: Set the transfer method to direct broadcast.
 - Unicast: Set the transfer method to unicast.
- 9 Click **OK**.

Storing the Console client computer details

The Symantec Ghost Console stores a record for every Console client computer that it detects. A Console client computer automatically appears in the Symantec Ghost Console once the Console client software is installed. It appears in the Machine Groups Default folder with a title reflecting the computer name and default user.

When DOS is the only operating system installed on the Console client computer, the computer appears with a title matching the adapter address of the computer.

If the Console client computer is subsequently cloned with a Windows 9x/Me/NT/2000/XP operating system, do one of the following to update the computer title and other configuration settings in the Symantec Ghost Console:

- Execute a task for the computer to refresh the default configuration settings.

For more information, see [“Creating tasks”](#) on page 87.

- Remove the computer from the Symantec Ghost Console. When the computer is detected again, its details are updated.

For more information, see [“Removing a computer from a group”](#) on page 60.

Checking client software and status

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

- The left side of the Console client icon shows whether the current version of the client software is installed. A check mark means that the current version is installed.
- The right side of the icon shows the computer’s status. A red X means that the computer is offline or unavailable.

- A question mark means that the client heartbeat is 0 and that the client status is unknown.



— The computer is online and the client software is the current version



— The computer is offline, and the client software is the current version



— The computer is online but the client software is not the current version



— The client software isn't the current version and the computer is offline or unavailable



— The client software isn't the current version and the computer status is unknown



— The client software is the current version and the computer status is unknown

Viewing and changing Console client computer properties

Console client computer properties are on the Symantec Ghost Console and appear in the computer's Properties window. You can view the following details:

- Default configuration settings for the client computer
For more information, see [“Editing and applying new default configuration settings”](#) on page 66.
- Version of the Symantec Ghost Console client software on the computer
- Details of the backups created for this computer
- Heartbeat interval
- Last image file used to clone this computer
- Whether or not the Ghost boot partition is installed
- The DOS version under which the client computer runs

To view Console client computer properties

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to view.
- 3 Select the computer that you want to view.
- 4 On the File menu, click **Properties**.

Setting the client computer heartbeat interval

You can set the frequency with which status reports are sent from the Console client computers to the Symantec Ghost Console. You can also set the client heartbeat globally and for each subnet.

For more information, see [“Setting the Symantec Ghost Console options”](#) on page 154, [“Setting properties for computers in a subnet”](#) on page 61, and [“To set a client heartbeat”](#) on page 157.

To set the client computer heartbeat interval

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to view.
- 3 Select the computer that you want to view.
- 4 On the File menu, click **Properties**.
- 5 Click **Heartbeat interval**.
- 6 Type the number of seconds to set the rate at which status reports are sent from the computer to the Console.
- 7 Click **OK**.

Editing and applying new default configuration settings

The default configuration settings are taken from the client computer when it is first detected by the Symantec Ghost Console. You can edit default settings, or copy them to match those on another computer.

The default configuration settings can be updated at any time to match the settings on the computer by including the computer in a task that has the Configuration Refresh check box checked.

For more information, see [“Setting task properties”](#) on page 88.

When you edit the default configuration settings, you can apply them to the client computer by choosing to use the default settings in a task.

For more information, see [“Setting Configuration properties”](#) on page 91.

To edit default configuration settings

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to view.
- 3 Select the computer that you want to alter.
- 4 On the File menu, click **Properties**.
- 5 On the General tab, click **Edit**.
- 6 Make your changes to the default settings.

For more information, see [“Creating and viewing configuration sets”](#) on page 71.

You can use the same configuration settings for many computers by copying the settings.

To copy default configuration settings

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer from which you want to copy the configuration settings.
- 3 Select the computer from which you want to copy the configuration settings.
- 4 On the File menu, click **Properties**.
- 5 Click **Copy**.

- 6 Expand the Machine Groups folder.
- 7 Open the folder containing the computer to which you want to copy the configuration settings.
- 8 Select the computer to which you want to copy the configuration settings.
- 9 Click **OK**.

You can set the template that contains the DOS network drivers to use when the client computer starts in the virtual partition.

To set the DOS network driver template

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to view.
- 3 Select the computer that you want to alter.
- 4 On the File menu, click **Properties**.
- 5 On the Client tab, do one of the following:

- Click **Use Suggested Template** and select a template from the drop-down list box.

The drop-down list box 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.

- Click **Use Manually Selected Template**, then click **Browse** to select a template.

The Browse for template dialog box displays all of the templates that are included with the Ghost Boot Wizard. You can select one of these templates, or add and modify a template.

For more information, see [“Adding network drivers to the Ghost Boot Wizard”](#) on page 145.

You can select a version of DOS to install when the virtual partition is created on the client computer.

To set the version of DOS that the client runs under

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to view.
- 3 Select the computer that you want to alter.
- 4 On the File menu, click **Properties**.
- 5 On the Client tab, select one of the following:
 - Default: Set the DOS version to the default version.
For more information, see [“Setting the Symantec Ghost Console options”](#) on page 154.
 - MS-DOS: Set the DOS version to MS-DOS.
This option can be selected only if MS-DOS is installed on the Console server.
For more information, see [“Selecting a version of DOS”](#) on page 150.
 - PC-DOS: Set the DOS version to PC-DOS.

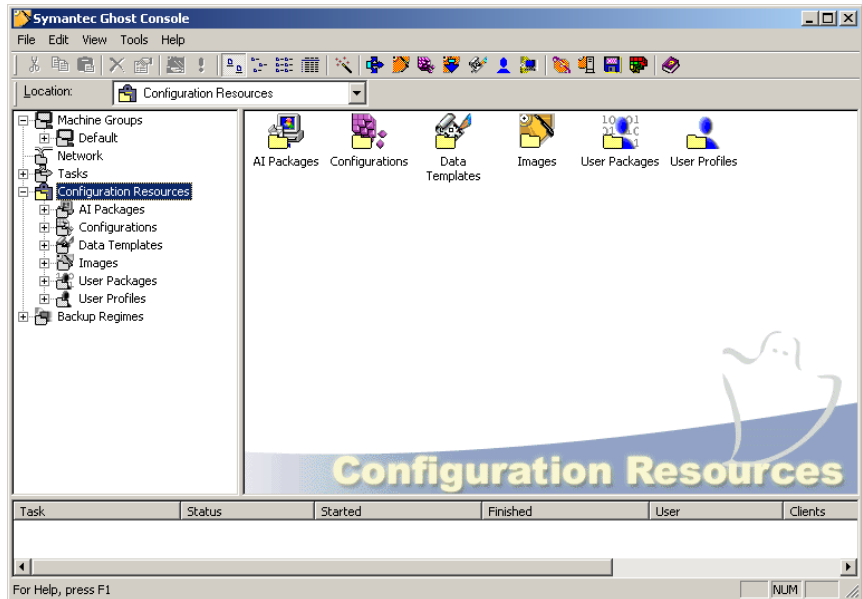
You can view details of any baseline images and incremental images that have been created for a computer.

To view backups created for a computer

- 1 In the left pane of the Symantec Ghost Console, expand the Machine Groups folder.
- 2 Open the folder containing the computer that you want to view.
- 3 Select the computer that you want to alter.
- 4 On the File menu, click **Properties**.
- 5 Click the **Backup** tab.

About the Configuration Resources folder

The Configuration Resources folder contains the information that tasks apply to target computers.



This information includes:

Folder	Description
AI Packages	Stores details of AutoInstall packages and AI Package definitions.
Configurations	Stores templates containing sets of registry parameters.
Data Templates	Stores the data templates created for inclusion in user profiles. For more information, see “Creating a data template” on page 108.
Images	Stores details of image files and image definitions.

Folder	Description
User Packages	<p>Stores the packages of user data taken from the Console client computers in Move the User tasks.</p> <p>For more information, see “Capturing and restoring user data” on page 113.</p>
User Profiles	<p>Stores user profiles used to define Move the User tasks.</p> <p>For more information, see “Creating a User Profile” on page 111.</p>

Creating and viewing image definitions

Image definitions contain the following details of image files created by Symantec Ghost or the Symantec Ghost Console that are used in image dump and load tasks:

- Name and location of the image file
- Image file status
- Details of the image:
 - Partition number
 - Type
 - Original size of the partitions
 - Size of data
 - A description of the image file

To create a new image definition

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration Resources folder.
- 2 Expand the Images folder.
- 3 Open the folder in which you want to create the new image definition.
If you do not select an Images folder, then the image definition is stored in the Images root folder.
- 4 On the File menu, click **New > Image**.
- 5 In the Properties for New Image window, type a name for the image.

- 6 Do one of the following:
 - Type the name and location of the image file.
 - Click **Browse** to select the image file.

The file information appears once you have selected an image file.

You can type the name and location of an image file that is not yet created. This is necessary when creating a new image file with the Symantec Ghost Console.
- 7 Type a description for the image file.
- 8 Click **Launch Ghost Explorer** to start Ghost Explorer and view the image file, if appropriate.

To view an image definition

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration Resources folder.
- 2 Expand the Images folder.
- 3 Select the image that you want to view.
- 4 On the File menu, click **Properties**.
- 5 Click **Launch Ghost Explorer** to view details of the selected image file.

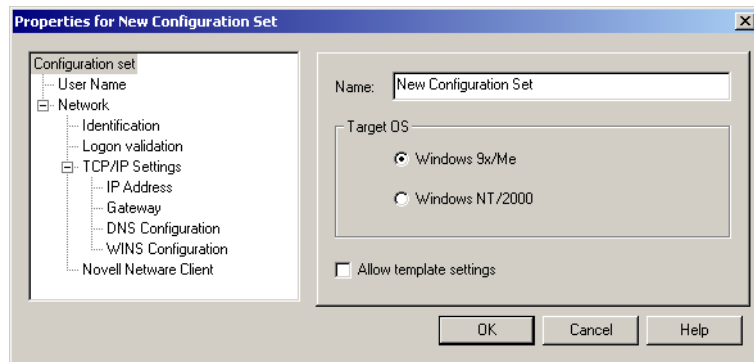
For more information, see [“Understanding Ghost Explorer”](#) on page 255.

Creating and viewing configuration sets

A configuration set is a number of registry settings that is saved and applied as part of a cloning task. The settings can be saved as a template and applied to a group of computers, or saved and applied to individual computers. You can create tasks that apply configuration settings after an image file load or as a separate task.

To create a configuration set

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration Resources folder.
- 2 Expand the Configurations folder.
- 3 Open the folder in which you want to store your configuration set.
If you don't select a folder, the configuration set is stored in the Configurations root folder.
- 4 On the File menu, click **New > Configuration**.
- 5 In the Properties For New Configuration Set window, type a name for your new configuration set.



- 6 Select a target operating system: Windows NT/2000/XP or Windows 9x/Me.
- 7 Check **Allow template settings** to create a template so that the configuration set can be applied to a group of computers.
Leave this unchecked to apply the settings to individual computers as a customized setting.
- 8 In the left hand window, click **User Name** to specify a user name.
- 9 Click **Identification** to specify identification parameters.
- 10 Click **Logon validation** to specify logon validation parameters.
This option is not available for Windows NT and Windows 2000 computers.
- 11 Click **TCP/IP Settings** to apply IP addresses to the Console client.

Specifying a user name

When creating a configuration set, you can specify a new user name to apply.

To specify a user name

- 1 In the Properties for New Configuration Set window, click **User Name**.
- 2 Click **Apply User Name** to specify a new user name.
- 3 In the space provided, type the new user name.

Specifying identification parameters

When creating a configuration set, you can specify identification parameters. The parameters available depend on the target operating system.

If you choose to apply this configuration set as a template, then the default name appears as Computer N*****. When the task runs, the wildcard stars are replaced with a number that is unique to each computer. You can increase or decrease the number of stars, and you can alter the alphabetical part of the name. For example, if you create computers for the Administration department, set this field to Admin *****.

To specify identification parameters for Windows 9x or Me computers

- 1 In the Properties for New Configuration Set window, click **Identification**.
- 2 Click **Apply Computer name** to specify a new computer name.
- 3 In the space provided, type a name to apply to the Console client.
You can change this name after cloning.
- 4 Click **Apply Workgroup** to specify a workgroup.
- 5 In the space provided, type the name of a workgroup for this Console client.
- 6 Click **Computer Description** to specify a computer description.
- 7 In the space provided, type a description that applies to the Console client.

To specify identification parameters for Windows NT/2000/XP computers

- 1 In the Properties for New Configuration Set window, click **Identification**.
- 2 Click **Apply Computer name** to specify a new computer name.
- 3 In the space provided, type a name to apply to the Console client.
This name can be changed after cloning so that there is a unique user name.
- 4 Click **Apply Member of** to make a computer a member of a workgroup or domain.
- 5 To make the client a member of a workgroup, click **Workgroup**, then type the name of a workgroup for this Console client to join.
- 6 To make the client a member of a domain, click **Domain**, then select a domain from the drop-down list box for this Console client to join.

Setting logon validation registry settings

You can set validation registry settings for logging on to Windows 9x or Me computers.

To set logon validation registry settings for Windows 9x or Me computers

- 1 In the Properties for New Configuration Set window, click **Logon Validation**.
- 2 Click **Log on to Windows NT/2000/XP domain** if you want Windows 9x or Me computers to log on to an NT/2000/XP domain.
- 3 In the Windows NT/2000/XP domain field, type the domain name.

Applying IP addresses

You can choose between DHCP or static IP address. This choice must match the image file when the configuration change is part of a cloning task. However, for a task that only changes the configuration, this setting must match the setting on the current computer.

To apply IP addresses to the Console client

- 1 In the Properties for New Configuration Set window, click **TCP/IP Settings**.
- 2 Do one of the following:
 - Click **Target computer uses DHCP server to obtain the IP Address** to let the DHCP server generate the IP address automatically.
 - Click **Target machine has static IP address** to enter the IP address information.

To specify IP address information

- 1 In the Properties for New Configuration Set window, click **Apply IP Address**.
- 2 Do one of the following:
 - Type the IP address for nontemplate settings.
 - Type a range of addresses for template settings.
- 3 In the subnet mask field, type the setting.

To specify default gateway information

- 1 In the Properties for New Configuration Set window, click **Apply Default Gateway**.
- 2 Type the default gateway address.

To specify DNS configuration information

- 1 In the Properties for New Configuration Set window, click **Apply DNS Configuration**.
- 2 In the space provided, type a host name.
- 3 Type the domain address.
- 4 Type the DNS server address.

To specify WINS server information

- 1 In the Properties for New Configuration Set window, click **Apply WINS Server**.
- 2 Type the WINS server address.

Applying Novell NetWare client configuration details

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.

Symantec Ghost supports the following Novell NetWare clients

- Computers running Windows 9x: Novell NetWare clients version 3.2 and later
- Computers running Windows 2000/NT: Novell NetWare clients version 4.7 and later

Note the following:

- 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.
- On a Windows 2000/NT client computer, when a task is executed that requires a restart, the client computer must not be 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 New Configuration Set window, click **Novell Netware Client**.
- 2 Click **Apply Novell Netware Client Settings** to apply the settings to the client.
- 3 In the Netware Tree field, type the NetWare tree.
- 4 In the Netware Context field, type the NetWare context.

- 5 Do one of the following:
 - Click **Use Current Username Setting for Novell Username** to set the user name entered in the User Name window to the Novell user name.
 - In the Novell Username field, type a user name for the Novell user name.

On Windows NT/2000/XP computers, the Novell local logon user name is set to the user name entered in the User Name window.
- 6 In the Preferred Server field, type the Novell NetWare preferred server.

Viewing configuration sets

You can view a configuration set. This can be a template setting created to apply to a group of computers, or a custom setting created to apply to one computer only.

To view a configuration set

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration folder.
- 2 Select the configuration set that you want to view.
- 3 On the File menu, click **Properties**.

The following configuration set information appears:

 - Name of the configuration set
 - Target operating system
 - Whether the set is a template that can be applied to a group of computers
- 4 Click **User Name** to view the specified User Name.
- 5 Click **Identification** to view the Identification parameters.
- 6 Click **Logon Validation** to view the logon validation registry settings for Windows 9x or Me computers.
- 7 Click **TCP/IP** settings to view the IP addresses.

- 8 If the static IP address check box is checked on the target computer, then you can select and view any of the following:
 - IP Address
 - Default Gateway
 - DNS Configuration
 - WINS Server
- 9 Click **Novell Netware Client** to view Novell NetWare client details.

Creating and viewing AI package definitions

AI package definitions contain details of AutoInstall packages created by the AutoInstall application. They are used in tasks that deploy the packages to client computers.

To create a new AI package definition

- 1 In the left pane of the Symantec Ghost Console, expand the AI package folder.
- 2 Open the folder in which you want to store the AI package.

If you do not select an AI package folder, then the package is stored in the AI package root folder.
- 3 On the File menu, click **New > AI Package Definition**.
- 4 In the Properties for New AI Package window, type a name for the package.
- 5 Do one of the following:
 - Type the name and location of the AI package.
 - Click **Browse** to locate and select the package.

AI packages can be stored locally, on a network share, or at an HTTP location.

The AI package and location information appears once you have selected the AI package. If the package is not located on an HTTP path, then the Package GUID appears.

For more information, see [“Customizing and building AI packages”](#) on page 245.

- 6 Click **Validate** to verify that the package is a valid AI Package if the package is located on an HTTP path.
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.

To view an AI package definition

- 1 In the left pane of the Symantec Ghost Console, expand the AI package folder.
- 2 Select the AI package that you want to view.
- 3 On the File menu, click **Properties**.
The name and location of the package appears. The package can be stored locally, on a network share, or at an HTTP location.
- 4 Click **AI Builder** to view the details of the selected package.
For more information, see [“Customizing and building AI packages”](#) on page 245.

Creating and executing tasks

This chapter contains the following:

- [Understanding tasks](#)
- [Creating image dump tasks](#)
- [Creating tasks](#)
- [Scheduling and executing tasks](#)
- [Initiating a task from a client computer](#)

Understanding tasks

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

- Create an image file
- Load an image file
- Apply configuration settings
- Apply user data files and registry settings
- Load AutoInstall packages

You can initiate (execute) a task from the Console server or a client computer.

To execute a Symantec Ghost Console task successfully, install the Symantec Ghost client software and Ghost partition on each client computer.

Starting a task from a client computer

You can initiate a task from a client computer. This lets an administrator execute a task at a user's desk instead of having to return to the Console Server to execute the task.

Creating the model computer

A model computer is created as a template for client computers. This is the first step in creating a Symantec Ghost model image. Set up a computer with Windows 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.

If you are creating a model computer for Windows NT computers, see the Online Knowledge Base article "How to clone an NT system" under the General Information section.

You may need to create a model computer for each unique hardware setup. For example, if you have some computers with different network or video cards, you must 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.

Creating image dump tasks

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

An image dump task includes the following components:

Option	Description
General	Details of the image dump.
Network	<ul style="list-style-type: none">■ An instruction to include all computers in the target group that are currently shut down and have this feature installed.■ Data transfer options.
Sysprep	Facilitates restoring of image files on computers that have different hardware configurations. For more information, see “To clone with Sysprep” on page 129.

To begin creating an image dump task

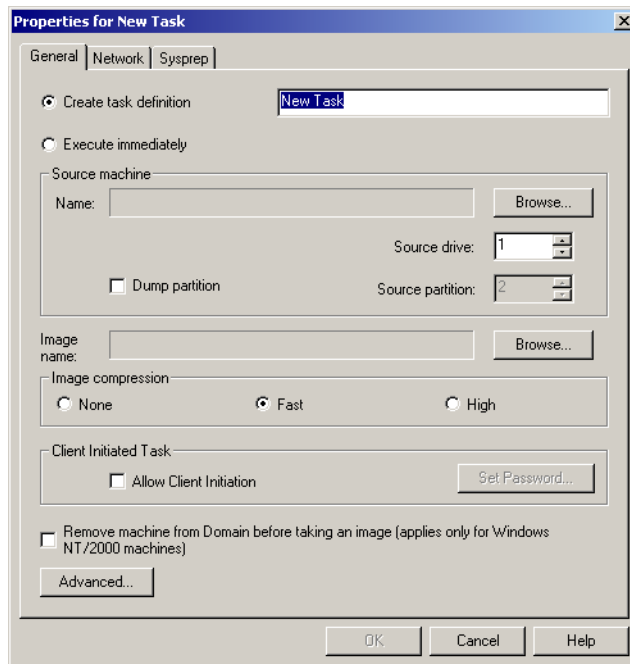
- 1 In the left pane of the Symantec Ghost Console, expand the Tasks folder.
- 2 Open the folder in which you want to add the new task.
If you do not select a task folder, the task is stored in the Tasks root directory.
- 3 On the File menu, click **New > Image Dump**.
- 4 Set the image dump task properties.

Setting image dump task properties

An image dump task includes details of the image file to be created and optionally the network and Sysprep components. You can select the computer from which to dump and enter the image definition details.

To set General image dump properties

- 1 In the Properties for New Task window, on the General tab, do one of the following:
 - Click **Execute immediately** to create an image file immediately.
 - Type a name for the task.



- 2 Click **Browse** to show the hierarchy of client computers.
- 3 In the Machine Groups folder, select the computer from which you want to take the image.
- 4 Double-click the computer icon to view the computer properties.
- 5 In the Source drive field, type a drive number, if required.
- 6 To extract the image of a partition, click **Dump partition**, then type a source partition number.

- 7 Click **Browse** to show the hierarchy of Image definitions.
- 8 In the Images folder, do one of the following:
 - Select the image definition to which you want to save the image.
 - Click **New** to create a new image definition.

For more information, see [“To create a new image definition”](#) on page 70.
- 9 To view or create the image definition properties, double-click the image definition icon.
- 10 Click **Remove machine from domain before taking an image** to remove the computer from a domain, if required.

Remove the computer from the domain if you are rolling out the image file to a number of computers. This is not necessary if you are using Sysprep. Sysprep does this automatically.
- 11 Select a compression option: None, Fast, or High.

For more information, see [“Image files and compression”](#) on page 162.
- 12 Click **Allow Client Initiation** to let the client computer execute the task.
- 13 Click **Set password** and type a password to be entered on the user computer for client initiated tasks.

For more information, see [“Initiating a task from a client computer”](#) on page 98.
- 14 Click **Advanced** to add more options to the task using the command line.

For more information, see [“To add Advanced features for cloning”](#) on page 90.
- 15 Click **OK** to save the image dump task.

Warning: If you checked Execute immediately, the task executes.

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 in which image files are transferred over your network. You can alter these settings globally, for a multicast session, and for a task.

For more information, see [“Setting the data transfer mode”](#) on page 187, [“Controlling the amount of network bandwidth used”](#) on page 188, and [“Setting the Symantec Ghost Console options”](#) on page 154.

To set data transfer mode and network bandwidth limits

- 1 In the Properties for New Task window, on the Network tab, check **Force data transfer mode** to set a data transfer mode.
- 2 Select one of the following:
 - Multicast: Set the data transfer mode to Multicast.
 - Direct Broadcast: Set the data transfer mode to direct broadcast.
 - Unicast: Set the data transfer mode to Unicast.
- 3 Check **Force data throughput limit** and type the maximum MB per minute to set a limit for dumping an image.

Setting Wake On Lan (WOL) properties

Set the Wake on Lan (WOL) properties 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 the BIOS Power Management.
- The connection light on the back of the NIC must be lit when the computer is turned off.

To set Wake on Lan properties

- 1 In the Properties for New Task window, on the Network tab, click **Use WOL when executing the task**.
- 2 Click **Shut down machines when task is finished** to turn off these computers once the task is executed.

Creating tasks

A task is a set of instructions. Tasks can be created, copied, changed, and reused as required.

A task includes some, or all, of the following components:

Option	Description
General	Defines the task steps and target computers.
Network	<ul style="list-style-type: none">■ Lets you include all computers in the target group that are currently turned off and have Wake on Lan installed.■ Optimizes data transfer.
Clone	Loads an image file onto client computers.
Configuration	Applies the specified configuration settings to the target computers.
Move the User	Captures or restores user packages from target computers.
Deploy AI packages	Lists the AutoInstall packages to be installed or uninstalled on the target computers.
File transfer	Lists the files to be copied onto the target computers.
Command	Executes the specified command on the target computers.

To begin creating a task

- 1 In the left pane of the Symantec Ghost Console, expand the Tasks folder.
- 2 Open the folder in which you want to add the new task.
If you do not select a task folder, the task is stored in the Tasks root directory.
- 3 On the File menu, click **New > Task**.
- 4 Set the task properties.
The OK button becomes active when you have completed all required fields on the properties tabs.

Setting task properties

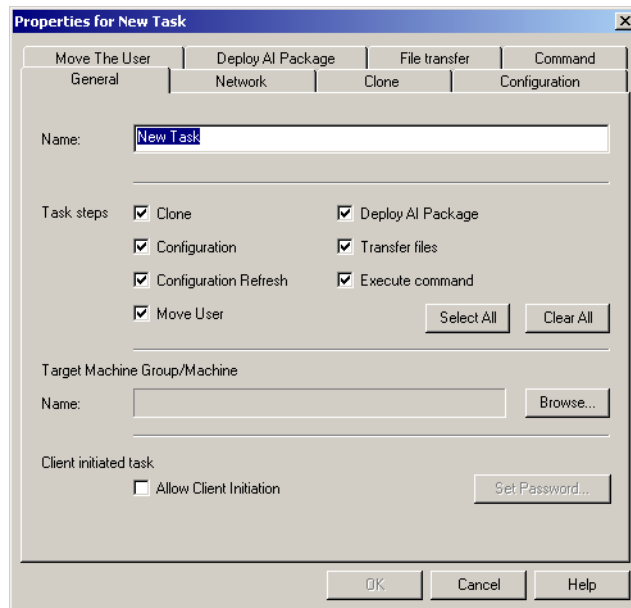
A task always includes General properties and Network properties. The other components depend on the steps required for the task being completed.

Setting General task properties

The General task properties include the steps in a task and the target computers on which they are performed.

To set General task properties

- 1 In the Properties For New Task window, on the General tab, type the title of the task in the Name field.



- 2 Select one or more task steps.
- 3 Click **Browse** to show the hierarchy of client computers.
- 4 Expand the Machine Groups folder.
- 5 Open the folder containing the machine group that you want to receive the task.

- 6 Select the machine group that you want to receive the task.
If you select a group folder, all computers in that folder and in the folders below are selected.
- 7 Double-click the computer icon to view the computer properties of any of the computers in the group.
- 8 Click **Allow Client Initiation** to let the client computer execute the task.
- 9 Click **Set password** and type a password to enter on the user computer for client initiated tasks.
For more information, see [“Initiating a task from a client computer”](#) on page 98.

Setting Network properties

Wake on Lan properties let you run tasks on computers that are turned off. You can also optimize the data transfer for your network hardware.

For more information, see [“To set Wake on Lan properties”](#) on page 86 and [“Optimizing data transfer over the network”](#) on page 85.

Setting Clone properties

The Clone properties specify the details of the cloning task. These include the target computers and the image file.

To set Clone properties

- 1 On the Clone tab, in the Destination drive field, type a drive number, if required.
- 2 To direct the image file to a partition, click **Partition Load**, then type a destination partition number.
- 3 Click **Browse** to show the hierarchy of Image definitions.
- 4 In the Image definitions folder, select the image definition to which you want to save the image.
If the image definition has not been created, you can create one.
For more information, see [“To create a new image definition”](#) on page 70.
- 5 To view or create the image definition properties, double-click the image definition icon.

- 6 In the Image definitions folder, select the image definition for the image file that you want to load.
- 7 Double-click the image definition icon to view the image definition properties.
- 8 If the image is being loaded to a partition, do one of the following:
 - If an image file exists for the image definition specified, select the Source partition from the Source partition drop-down list.
 - If an image file does not exist, select a Source partition number.
- 9 Click **SID Change** to alter the SID on each of your target computers using Symantec Ghost Walker if you are cloning onto a Windows NT/2000/XP operating system.

For more information, see [“Using Ghost Walker”](#) on page 287.

- 10 If required, add more advanced features to the task using the command line.

Adding Advanced features for cloning

In the Advanced dialog box, you can set more options for the cloning task using the command-line switches.

To add Advanced features for cloning

- 1 In the Properties for New Task windows, on the Clone tab, click **Advanced**.
- 2 In the Additional Options for Ghost Command Line field, type the extra commands.

For more information, see [“Command-line switches”](#) on page 297.

- 3 Click **Overwrite hidden partition** if you want to overwrite the Symantec Ghost DOS boot partition on the client computer.

If the image contains a Symantec Ghost DOS boot partition, this check box is checked. If the image does not contain a Symantec Ghost DOS boot partition, you can select this option.

- 4 Click **OK**.

Warning: The syntax of your command line 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.

Setting Configuration properties

Set Configuration properties to apply configuration settings to the target computers.

Option	Description
Default	<p>Restores the current default settings to the target computers.</p> <p>These settings are stored when a computer first connects to the Symantec Ghost Console. You can view and edit them in the computer's Properties window.</p> <p>For more information, see “Editing and applying new default configuration settings” on page 66.</p>
Template	Applies a template configuration set to the computers in your group.
Custom	Applies an individual template configuration set to each of the computers in your group.

To ensure that the computer's default settings are updated to the computer's new settings, the Configuration Refresh box must be checked on the General tab.

For more information, see [“Setting General task properties”](#) on page 88.

To apply a Default configuration to target computers

- 1 On the Configuration tab, click **Default**.
- 2 Check **Use default settings** to apply the default settings to those settings that are not specified when the Template or Custom options are chosen.

To apply a Template configuration to target computers

- 1 On the Configuration tab, click **Template**.
- 2 Click **Browse** to select the set from the Configuration Resources folder.
The names of configuration sets appear in bold. You can only select one set. Double-click the name to view the template settings.
- 3 Check **Use default settings** to apply the default settings to those settings that are not specified when the Template or Custom options are chosen.

To apply a Custom configuration to target computers

- 1 On the Configuration tab, click **Custom**.
- 2 Click **Customize**.

The Machine Group folder appears on the left, and the Configuration Resources folder appears on the right.
- 3 Drag a configuration set from the Configuration Resources folder onto the computer to which you want to apply the settings.

The icon for the configuration set appears below the selected computer. You can only select sets that are in bold. This marks individual computer settings.
- 4 Double-click the name of the configuration set for a detailed view.
- 5 Repeat steps 2 through 4 for each computer to which you want to apply settings.
- 6 Check **Use default settings** to apply the default settings to those settings that are not specified when Template or Custom is chosen.

Setting Move the User properties

Move the User lets you capture settings and place them on another computer or restore them on the same computer. Setting the Move the User properties is part of a process to run a Move the User task.

For more information, see [“Capturing and restoring user data”](#) on page 113.

Setting Deploy AI Package properties

AI packages to install applications on target computers are created in AutoInstall. The packages are deployed to the target computers by running a task from the Console. You can set properties for the task on the Deploy Package tab, selecting which packages to install and uninstall on the target computers.

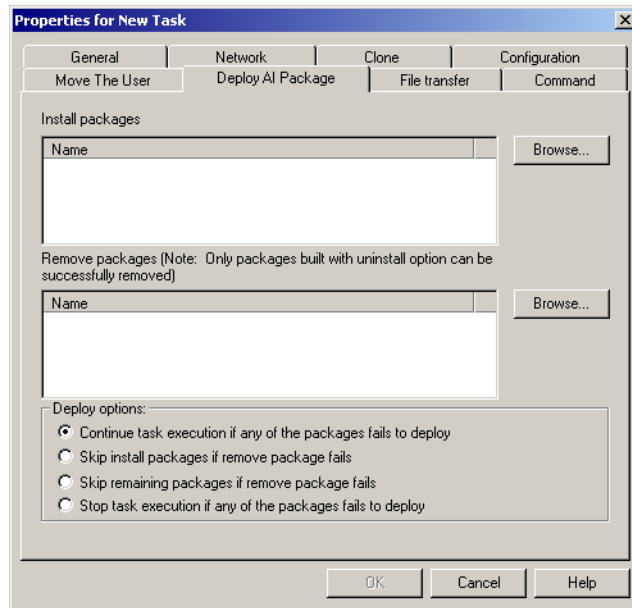
You cannot uninstall all packages. You can uninstall a package if it was created with an uninstall command included. If you are unsure, open the package with AI Builder to see if there is an uninstall command.

Also, if an AI package is rebuilt with a new identifying number (GUID), then 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 uninstall command is not included, or an AI package was built with a new GUID, then the software should be uninstalled by some other means.

To set Deploy AI Package properties

- 1 On the Deploy AI Package tab, under Install packages, click **Browse** to locate packages created with AutoInstall.



- 2 Select the package definition for the package that you want to install.
- 3 Under Remove packages, click **Browse** to locate uninstall packages created with AutoInstall.
- 4 Select the package definition for the package you want to uninstall.

- 5 Repeat steps 1 through 4 to include all required packages.
- 6 Do one of the following to specify how the selected packages should be deployed. These deployment options apply to individual target computers:
 - Click **Continue task execution if any of the packages fails to deploy** to continue to uninstall or install packages on the target computer if one package fails to deploy.
 - Click **Skip install packages if remove package fails to install packages** only if all packages are uninstalled successfully.
 - Click **Skip remaining packages if remove package fails to install or uninstall packages** only if previous packages are removed successfully.
 - Click **Stop task execution if any of the packages fails to deploy** to stop the task if any package is not removed or installed successfully.

Storing AI packages

AI packages can be stored locally, at an HTTP location, or on a network share.

Packages located on a nonUNC 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 NT and 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.

Setting File Transfer properties

You can transfer files to the operating system or the Ghost partition. The target is selected on a file-by-file basis. If you transfer the files to the virtual partition, then the files remain there only while the task is being executed.

When the task is executed, the files are transferred to the following folder:

c:\Program Files\Symantec\Ghost\Incoming

To set File Transfer properties

- 1 On the File Transfer tab, do one of the following:
 - Click **In Target Operating System** to transfer files to the operating system.
 - Click **In Ghost Partition** to transfer files to the Ghost partition.
- 2 Click **Add** to add a file to the list of files to transfer.
- 3 Locate the file that you want to transfer.
- 4 Double-click the file that you want to transfer.
- 5 Repeat steps 1 through 4 until all the files you want to transfer are in the list.

To remove a file from the file transfer

- 1 On the File Transfer tab, in the List of files to transfer field, select the file that you want to delete.
- 2 Click **Delete** to remove the file from the file transfer.

Setting Command properties

Commands are executed in the operating system or the Ghost partition. The target is selected on a command-by-command basis.

Note: Using GDisk from Command lets you alter partitions during a task.

To set Command properties

- 1 On the Command tab, do one of the following:
 - Click **In Target Operating System** to execute a command in the operating system.

You must include the full path for the command. The path is as follows:
C:\Ghost\Incoming
 - Click **In Ghost Partition** to execute a command in the Ghost partition.

You must include the full path for the command. The path is as follows:
C:\Program Files\Symantec\Ghost\Incoming
- 2 Type the command in the space provided to add a command to the Command list.
- 3 Click **Add**.
- 4 Repeat steps 1 through 3 until all of the commands that you want are in the list.

To remove a command from the Command list

- 1 On the Command tab, in the Command list field, select the command that you want to delete.
- 2 Click **Delete** to remove the command from the command list.

Reviewing tasks

You can check the details of the task in the task scenario dialog box before you execute it. The task scenario includes the clone properties, all configuration steps, and the client computers included in the task.

To view task details

- 1 In the left pane of the Symantec Ghost Console, expand the Tasks folder.
- 2 Select the task that you want to view.
- 3 On the View menu, click **Task Scenario**.

Scheduling and executing tasks

When you have finished setting task properties, the next step is to execute the task. Once defined, tasks can be scheduled for specific dates and times, or they can be executed at any time. You can execute tasks once or more than once on a scheduled basis, from the Symantec Ghost Console or from the client.

You can view tasks that are currently executing in the bottom pane of the Symantec Ghost Console.

For more information, see [“Setting the Symantec Ghost Console options”](#) on page 154.

A task may fail to execute if the correct network drivers are not found. If the task log indicates that this happened, amend the computer properties to use the correct template.

For more information, see [“Storing the Console client computer details”](#) on page 63, and [“Monitoring the Symantec Ghost Console activity”](#) on page 151.

Scheduling a task

You can schedule tasks to run automatically from the Symantec Ghost Console.

To schedule a task

- 1 On the View menu, click **Scheduler**.
All scheduled tasks appear.
- 2 On the Task menu, click **New Task**.
- 3 Expand the Tasks folder.
- 4 Select the task that you want to schedule, then click **OK**.
- 5 On the Schedule tab, set the date, time, and frequency with which to execute the task.
- 6 On the Task tab, in the Run as field, type the user name of the person who is running the task.
The default is the logged on user.
- 7 Click **Set Password**.

- 8 In the Password field, type your password.
You must type a password to run the task. The password is confirmed when the task runs.
- 9 In the Confirm field, type your password again to confirm that it is entered correctly.

Executing a task manually from the Symantec Ghost Console

You can execute a task manually at any time from the Symantec Ghost Console.

To execute a task manually

- 1 In the left pane of the Symantec Ghost Console, expand the Tasks folder.
- 2 Select the task that you want to execute.
- 3 On the File menu, click **Execute task**.

You can run tasks concurrently. Before tasks are executed, the following information is checked:

- The validity of an image file to be loaded.
- 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.

You can also execute a task from the command line using the following command:

```
ngcons.exe /e taskname
```

Initiating a task 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 the client without having to return to the Console computer.

Both global and task settings must allow for client initiated tasks.

For more information, see [“Setting task properties”](#) on page 88 and [“Setting the Symantec Ghost Console options”](#) on page 154.

To initiate a task from a client computer

- 1** On the client computer, click the Symantec Ghost Client icon.
- 2** Select the task to execute.
Unless a password is required to execute the task, there is no confirmation required. The task executes immediately.
- 3** In the Password field, 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 client command line

You can also initiate a task from the client computer command line or from a batch file. The syntax for this is:

```
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.

Incremental backups and rollbacks

This chapter contains the following:

- [Introducing incremental backups and backup regimes](#)
- [Creating a backup regime](#)
- [Creating a backup manually](#)
- [Viewing a backup regime](#)
- [Restoring a computer](#)

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.

Introducing incremental backups and backup regimes

You can schedule incremental backups, or you can create them manually. 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 made are too great to be stored as an incremental image, a new baseline image is created and stored, replacing the previous baseline. Full baseline images must be created when fundamental changes to the operating system are made (for example, installing service packs, Microsoft applications, drivers, or making

changes to operating system protected files). Create a new baseline image after every five incrementals. You can specify a maximum time between baseline images.

Creating a backup regime

Backups are stored in the directory specified in the Console Options dialog box.

For more information, see [“To set the location for incremental backups”](#) on page 159.

To create a backup regime

- 1 In the left pane of the Symantec Ghost Console, expand the Backup Regime folder.
- 2 Open the folder in which you want to store your regime.
- 3 On the File menu, click **New > Backup Regime**.
- 4 On the Properties tab, enter the properties.
For more information, see [“To set backup regime properties”](#) on page 103.
- 5 On the Task tab, enter the task details if you are scheduling the backup.
For more information, see [“To set backup regime task properties”](#) on page 104.
- 6 On the Schedule tab, enter the schedule details if you are scheduling the backup.
For more information, see [“To set up schedule properties”](#) on page 104.
- 7 Click **OK**.

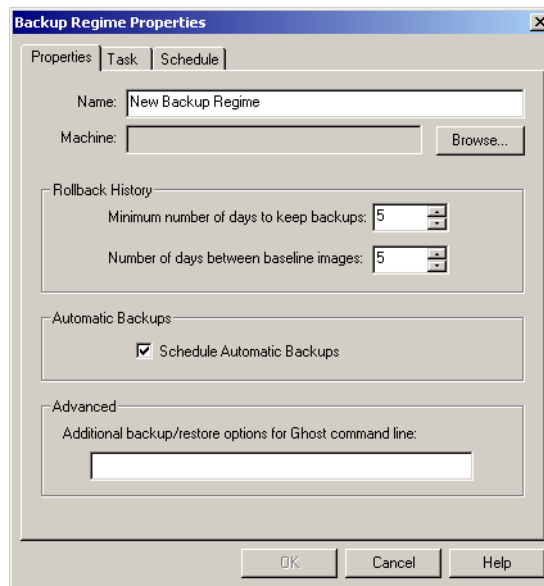
Setting backup regime properties, task, and schedule details

You can complete the properties of the backup regime on the following tabs:

- Properties: The name of the computer included in the regime.
- Task: Details on the backup task.
- Schedule: Scheduling of the backup task.

To set backup regime properties

- 1 On the Properties tab, in the Name field, type a name for the backup.
- 2 Click **Browse** to select the computer to be included in the backup regime.
Computers can only be placed in one backup regime.
- 3 On the Properties tab, in the Minimum number of days to keep backups field, 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 field, type the number of days after which to create a new baseline image.
- 5 Click **Schedule Automatic Backups** to create or edit the schedule for the automatic backup.



- 6 Under Advanced, in the Additional options for Ghost command line field, type any additional command line options.

For more information, see [“Command-line switches”](#) on page 297.

Warning: The syntax of your command line 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.

Incremental and baseline images are deleted as a set, so they may not be deleted when expected. Backups are not automatically deleted after the required number of days. Backups are not deleted until all dependent images are deleted.

For example:

- You have a baseline image, and several incremental images that rely on the baseline.
- The last incremental image that you created was within the specified number of days to keep backups.

Once the last incremental image is older than the specified number of days, it is deleted because no other backups rely on it. Each earlier incremental image is deleted until the final baseline image is reached and then it is deleted.

To set backup regime task properties

- 1 On the Task tab, in the Comments field, type identifying comments for the scheduled backup regime.
- 2 On the Task tab, in the Run as field, type the user name of the person who is running the backup task.
The default is the logged on user.
- 3 Click **Set password**.
- 4 In the Password field, type your password.
A password must be entered to run the backup task. The password is confirmed when the backup task runs.
- 5 In the Confirm field, type your password again to confirm that it is entered correctly.

To set up schedule properties

- 1 On the Schedule tab, in the Schedule Task drop-down list, select a schedule.
- 2 In the Start time field, select a time for the schedule to take effect.
- 3 Click **Advanced** to specify an end date or other advanced features.
- 4 In the Every field, select a number to schedule a task to be performed regularly.
- 5 Click **Show multiple schedules** to add, delete, or show other schedules.

Creating a backup manually

Computers are backed up manually as defined by a backup regime.

To create a backup manually

- 1 In the left pane of the Symantec Ghost Console, expand the Backup Regime folder.
- 2 Select the backup regime for the computer that you want to back up.
- 3 Right-click the regime, then click **Backup Now**.
- 4 In the Comments field, type notes that will accompany the backup. These are stored in the backup history, under Properties.
- 5 Check **Force new baseline image** to create a new baseline image. If this is not checked, the backup is performed as defined on the Properties tab of the backup regime.
- 6 Click **OK**.

Viewing computer backups

Details of the backup regime and the backups performed on a computer are in the computer's Properties window.

For more information, see [“To view Console client computer properties”](#) on page 65.

Viewing a backup regime

A backup regime includes a computer and a set of properties that control how the backup is created. Examples of these properties include how long the backup information is saved, whether automatic backups are scheduled, and any additional command line options.

To view a backup regime

- 1 In the left pane of the Symantec Ghost Console, expand the backup regime tree.
- 2 Select the regime that you want to view.
- 3 On the File menu, click **Properties**.

Restoring a computer

Computers can be rolled back to a previous backup at any time.

To restore a computer

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 Click **Close** to close the Console Wizard.
- 3 In the left pane of the Symantec Ghost Console, expand the Backup Regime folder.
- 4 Select the regime for the computer that you want to receive the rollback.
- 5 Right-click the regime, then click **Restore**.
- 6 On the list of incremental backups, select the one to which to roll back.

The status of each incremental 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.

- 7 In the bottom pane, you can view the status of the back up.

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.

- 8 Click **Safe Mode restore (non-system files only)** to restore user files only.

The operating system files and registry files are not restored.

- 9 Click **Finish** to initiate the rollback.
- 10 Click **OK** to confirm.

Note: You cannot cancel or undo a backup once it has started.

Move the User

This chapter contains the following:

- [Introducing Move the User](#)
- [Creating a data template](#)
- [Viewing a data template](#)
- [Creating a User Profile](#)
- [Viewing a User Profile](#)
- [Capturing and restoring user data](#)
- [Variables for use with Move the User](#)
- [Absolute and relative paths](#)
- [User settings that can be moved](#)

Introducing Move the User

Move the User lets you capture settings and files from a computer and restore them to the same computer or to another computer. For example, you can capture specified data and registry files from a computer with user, desktop, and configuration settings and restore them on the same computer after installing a new operating system. You can also restore them to a different computer. Move the User lets you quickly move a user from one computer to another, or complete cloning tasks that preserve a user's personal set up.

There are several steps involved in defining the settings and files to capture in a Move the User task. First, data templates are defined. Then a User Profile is created that lets you specify a user, the application-specific data, and data templates required.

Data templates define rules for excluding and including individual files and registry keys. You can create and use more than one data template to create a User Profile.

Once you've created a User Profile, you can use it to capture user settings from one computer or a number of computers, and restore them as required. You can then run a Move the User task.

Creating a data template

Data templates let you specify the data and registry files that you want to include in a capture. You specify a set of rules that define the files to include and exclude. You can also specify a reference path from which to take the files and a reference path to which the files are to be restored.

To create a data template

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration Resources folder.
- 2 Expand the Data Templates folder.
- 3 Expand the folders until you reach the parent folder in which to place the data template.
- 4 On the File menu, click **New > Data Template**.
- 5 On the Rules tab, define the directories, files, and settings to be captured.

For more information, see [“To specify the files to include or exclude in the data template”](#) on page 108.

- 6 On the Advanced tab, complete the fields to allow relative paths.
For more information, see [“To enable relative paths”](#) on page 110.

To specify the files to include or exclude in the data template

- 1 On the Rules tab, in the Template Name field, type a name for the template.
- 2 Click **Add Rule** to add a rule that defines the files covered by the template.

The order in which the rules are applied is the order in which they are listed.

- 3 In the Rule Definition dialog box, do one of following:
 - Click **Include** to include the files in the DirPath/RegPath field.
 - Click **Exclude** to exclude the files in the DirPath/RegPath field.
- 4 Do one of the following:
 - Click **V** to select a predefined variable that includes all files within a folder.

For more information, see [“Variables for use with Move the User”](#) on page 115.
 - Type a path and file to select a file.

The path and files must be fully defined or include wildcards unless relative paths are defined on the Advanced tab. For example, C:\Windows\Notes.cty.
- 5 Under Date, click **Apply to files** to include or exclude files from a date range.

For example, files that have been modified between selected dates.
- 6 Do one of the following:
 - Click **Between** to set a range of dates.

All files created between the start and end dates are selected.
 - Click **During the previous** to select files from a previous number of months.

All files created in the previous number of months are selected.
 - Click **During the previous** to select files from a previous number of days.

All files created in the previous number of days are selected.
- 7 Under Size, click **Apply to files** to include or exclude files of a certain size.
- 8 Do one of the following:
 - Click **Greater than** to include files that are greater than the specified size.
 - Click **Less than** to include files that are less than the specified size.
- 9 In the KB field type a file size.
- 10 Repeat steps 2 through 9 until all of the required files are included.

To include registry keys in a data template

- 1 On the Rules tab, click **Add Rule** to add a registry key to the data template.
- 2 In the Rule Definition dialog box, do one of following:
 - Click **Include** to include the registry keys in the DirPath/RegPath field.
 - Click **Exclude** to exclude the registry keys in the DirPath/RegPath field.
- 3 Do one of the following:
 - Click **V** to select a predefined variable that includes all registry keys within a path.

For more information, see [“Variables for use with Move the User”](#) on page 115.
 - Type a registry path and key to select a file.

The registry path and key can be relative to the reference path or specifically defined. For example, HKEY_LOCAL_MACHINE.

Date and size options do not apply to registry keys.
- 4 Click **OK**.

You can set a source directory path and a target directory path. This lets you move files from a source folder to a different folder on the target computer.

To enable relative paths

- 1 On the Advanced tab, click **Allow relative paths**.
- 2 In the Source Path field, type the reference path and directory on the source computer that contains the files to capture.

For example, c:\

You can specify a reference directory that is set up by the operating system, for example, My Documents is specified with the variable \$MYDOCUMENTS\$.

For more information, see [“Variables for use with Move the User”](#) on page 115.
- 3 In the Target Path field, type the reference path and directory on the target computer to which the files will be restored.

For example, d:\

Viewing a data template

Before including a data template in a User Profile, you can view it to select the appropriate templates for the profile.

To view a data template

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration Resources folder.
- 2 Expand the Data Templates folder.
- 3 Select the data template that you want to view.
- 4 On the File menu, click **Properties**.

The data template information includes the following:

- Name of the data template
 - Source reference path and directory
 - Target reference path and directory
 - Description
- 5 On the Rules tab, view the directories, files and settings to be included in the user package.

The rules are executed in the order in which they are listed when the user package is created.

Creating a User Profile

You define what to include in the capture and for whom in the User Profile. You also give the package a name. You define the data files and registry keys by selecting the appropriate data templates. You can select as many as you want to use. Specify the user and Windows settings by making the appropriate selections from the list.

To create a User Profile

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration Resources folder.
- 2 Expand the User Profile folder.

You do not have to be in a User Profile folder to store a profile. If you do not select a User Profile folder, then the profile is stored in the User Profile root directory.

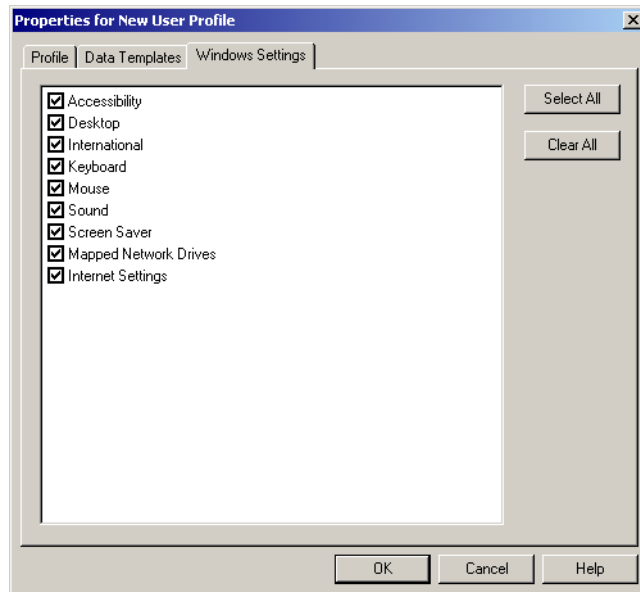
- 3 In the Name field, type a name for the User Profile.

- 4 Do one of the following:
 - Click **Last Logged User** to capture the settings for the last logged on user.
 - Click **All Domain Users** to capture the settings for all users from the current domain that have logged on to the computer.
 - Click **All Users** to capture the settings for all users that have logged on to the computer.
 - Click **Specified Users** and type the user names, separated by commas, in the fields below to capture the settings for particular users.

A domain name may be required. For example:

domainname\username

- 5 On the Data Templates tab, select the data templates that you want to add to this User Profile.
- 6 On the Windows Settings tab, select Windows settings to apply to the target computers.



Viewing a User Profile

When running a Move the User task, you can view User Profiles before including them in a task.

To view a User Profile

- 1 In the left pane of the Symantec Ghost Console, expand the User Profile folder.
- 2 Select the User Profile that you want to view.
- 3 On the File menu, click **Properties**.

The following User Profile information appears:

- Name given to the User Profile
 - Users whose settings should be selected
- 4 On the Data Templates tab, view the data templates to be applied when creating the User Profile.
 - 5 On the Windows Settings tab, view the Windows settings to be captured when creating the User Profile.

Capturing and restoring user data

User data is captured as a package and restored on a computer, or group of computers, as part of a task. The task can have other task properties set or just the required General properties. Data can be captured and restored in the same task or in separate tasks. The captured data is saved in packages, and the packages are stored in the application data folder. You can restore packages as often as needed.

The user account password is deleted on the target computer.

To capture user data

- 1 In the left pane of the Symantec Ghost Console, expand the Tasks folder.
- 2 Open the folder in which you want to add the new task.
If you do not select a task folder, the task is stored in the Tasks root directory.
- 3 On the File menu, click **New > Task**.
- 4 On the Move the User tab, check **Grab User Package(s)** to capture user data from a client computer.

- 5 To specify a name for the package generated, do one of the following:
 - Click **Automatically using Machine Name** to automatically name one or more packages.

Automatic Naming uses the computer name with the date and time the task is run to name a package.
 - Click **Specified** to type your own package name.

This option is available only if you are capturing data from a single computer.
- 6 Click **Browse** to display the User Profiles folder.
- 7 Select the User Profile that you want to use for the capture.

For more information, see [“Creating a User Profile”](#) on page 111.
- 8 Click **OK**.

To restore user data

- 1 In the left pane of the Symantec Ghost Console, expand the Tasks folder.
- 2 Open the folder in which you want to add the new task.

If you do not select a task folder, the task is stored in the Tasks root directory.
- 3 On the File menu, click **New > Task**.
- 4 On the Move the User tab, check **Restore User Package(s)** to restore user data on a client computer.
- 5 To specify the package that you want to restore on a specified computer, do one of the following:
 - Click **Automatically using Machine Name** to restore the package most recently taken from a computer with the matching computer name.
 - Click **As Specified in Grab Step** to restore a package that is captured in the same task.

Grab User Package(s) must be checked as part of the capture procedure.

For more information, see [“To capture user data”](#) on page 113.
 - Click **Specified** to select a package that you want to restore.

This option is available only if you are restoring a package to a single computer.

- 6 Click **Overwrite existing files on target machine** to overwrite files on the target computer.

You can view a user package to check the computer on which it was created and the date it was created.

To view a user package

- 1 In the left pane of the Symantec Ghost Console, expand the Configuration Resources folder.
- 2 Expand the User Packages folder.
- 3 Select the package that you want to view.
- 4 On the File menu, click **Properties**.
- 5 Click **Launch AI Builder** to start AI Builder.

Variables for use with Move the User

The locations of some paths and directories are determined by the operating system and are represented by variables.

You can use a variable within a path or append a directory or file to the end of a variable.

Variable	Automatically assigns the directory path for..
\$MYDOCUMENTS\$	Current user's My Documents folder
\$PROGFILES\$	Windows Program Files directory
\$USERHIVE\$	Registry path of current user's hive
\$USERPROFILE\$	Current user's profile directory
\$WINDIR\$	Windows directory
\$WINSYSDIR\$	Windows System directory
\$WINTMPDIR\$	Windows Temp directory

Other variables take on unique values depending on certain factors.

Variable	Automatically assigns...
\$MACHINENAME\$	Name of the computer
\$USERS\$	User's name
\$WINDRIVE\$	Drive containing Windows

Absolute and relative paths

In a data template, you can use absolute paths or relative paths. Absolute paths are paths that have a path from start to end, including a drive letter and directories. For example:

C:\Documents and Settings\msmith\My Documents

The relative path feature lets you set global source and target paths in the Advanced options. Once you have enabled this feature and entered source and target paths, then any path that is not an absolute path is set within the relative path.

For example, the source path in the Advanced feature dialog box is:

C:\Documents and Settings\msmith

The target path is:

C:\Documents and Settings\marysmith

If you add the rule Include “My Documents*.*”, then all of the files within C:\Documents and Settings\msmith\My Documents\ are included in the template. When you execute the Move the User task, the documents are moved to:

C:\Documents and Settings\marysmith\My Documents

User settings that can be moved

You can move certain user settings depending on the operating system that is installed.

Accessibility settings

This table displays the user settings that you can capture in the Control Panel under Accessibility.

Setting	95	98	Me	NT	2000	XP
Keyboard, StickyKeys	✓	✓	✓	✓	✓	✓
Keyboard, StickyKeys Settings	✓	✓	✓	✓	✓	✓
Keyboard, FilterKeys	✓	✓	✓	✓	✓	✓
Keyboard, FilterKeys Settings	✓	✓	✓	✓	✓	✓
Keyboard, ToggleKeys	✓	✓	✓	✓	✓	✓
Keyboard, ToggleKeys Settings	✓	✓	✓	✓	✓	✓
Show extra keyboard help in programs	✓	✓	✓		✓	✓
Sound, SoundSentry	✓	✓	✓	✓	✓	✓
Sound, SoundSentry Settings	✓	✓	✓	✓	✓	✓
Sound, ShowSounds	✓	✓	✓	✓	✓	✓
Display, High Contrast	✓	✓	✓		✓	✓
Display, High Contrast Settings	✓	✓	✓		✓	✓
CursorWidth			✓			✓
Mouse, MouseKeys	✓	✓	✓	✓	✓	✓
Mouse, MouseKeys Settings	✓	✓	✓	✓	✓	✓
General, Automatic reset	✓	✓	✓	✓	✓	✓
General, Give warning message when turning a feature on	✓	✓	✓		✓	✓

Setting	95	98	Me	NT	2000	XP
General, make a sound when turning a feature on or off	✓	✓	✓	✓	✓	✓
General, SerialKey devices	✓	✓	✓	✓	✓	✓
General, SerialKey devices Settings	✓	✓	✓	✓	✓	✓

Display settings

This table displays the user settings that you can capture in the Control Panel under Display.

Option	95	98	Me	NT	2000	XP
Background, Wallpaper	✓	✓	✓	✓	✓	✓
Background, Display mode (Tile, Center, Stretch)	✓	✓	✓	✓	✓	✓
Background, Pattern	✓	✓	✓	✓	✓	
Appearance, Scheme	✓	✓	✓	✓	✓	✓
Effects, Hide icons when desktop is viewed as a web page		✓	✓		✓	✓
Effects, Use large icons		✓	✓	✓	✓	✓
Effects, Show icons using all possible colors		✓	✓	✓	✓	✓
Effects, Animate windows, menus and lists		✓				
Effects, Use Transition Effects for menus and tooltips			✓		✓	✓
Effects, Choice of effects, scroll/fade			✓		✓	✓
Effects, Smooth edges of screen fonts		✓	✓	✓	✓	✓
Effects, Choice of effects, standard or clear type						✓

Option	95	98	Me	NT	2000	XP
Effects, Show window contents while dragging		✓	✓	✓	✓	✓
Effects, Change icons (My Documents, My Computer, Recycle Bin)		✓	✓	✓	✓	✓
Web, View my active desktop as a web page	✓	✓	✓	With IE	✓	✓
Effects: Hide keyboard navigation indicators until I use the Alt key					✓	✓
Effects, Show shadows under menus						✓
Plus, Stretch desktop wallpaper to fit the screen (available in background settings for Windows 98/Me/NT/2000, or 95 with Plus or IE installed)	With I/E	✓	✓	✓	✓	✓
Run Desktop Cleanup Wizard every 60 days						✓
Lock desktop items (to prevent moving or resizing of Web items on your desktop)						✓

International settings

This table displays the user settings that you can capture in the Control Panel under International.

Option	95	98	Me	NT	2000	XP
Regional settings	✓	✓	✓	✓	✓	✓
Number	✓	✓	✓	✓	✓	✓
Currency	✓	✓	✓	✓	✓	✓
Time	✓	✓	✓	✓	✓	✓
Date	✓	✓	✓	✓	✓	✓

Keyboard settings

This table displays the user settings that you can capture in the Control Panel under Keyboard.

Option	95	98	Me	NT	2000	XP
Speed, Character repeat	✓	✓	✓	✓	✓	✓
Speed, Repeat delay	✓	✓	✓	✓	✓	✓
Speed, Repeat rate	✓	✓	✓	✓	✓	✓
Speed, Cursor blink rate	✓	✓	✓	✓	✓	✓
Indicator on taskbar	✓	✓	✓	✓	✓	✓
Turn off caps lock					✓	
Hotkey to switch IME	✓	✓	✓	✓	✓	✓
Language (95/98/Me)	✓	✓	✓	✓	✓	✓
Input locales (NT/2000)	✓	✓	✓	✓	✓	✓

Mouse settings

This table displays the user settings that you can capture in the Control Panel under Mouse.

Option	95	98	Me	NT	2000	XP
Buttons, Double click speed	✓	✓	✓	✓	✓	✓
Buttons, Button configuration	✓	✓	✓	✓	✓	✓
Pointer, Scheme	✓	✓	✓	✓	✓	✓
Pointer, Speed	✓	✓	✓	✓	✓	✓
Pointer, Trail	✓	✓	✓		✓	✓
Single click to open an item	With IE	✓	✓	With IE	✓	✓
Double click to open an item	✓	✓	✓	✓	✓	✓
Snap mouse to the default button in dialog (NT)			✓	✓	✓	✓

Option	95	98	Me	NT	2000	XP
Acceleration			✓		✓	✓
Turn on Click Lock			✓			✓
Turn on Click Lock settings			✓			✓
Hide pointer when typing			✓			✓
Show location of pointer when pressing CTRL			✓			✓
Enable pointer shadow			✓		✓	✓

Sound settings

This table displays the user settings that you can capture in the Control Panel under Sound.

Option	95	98	Me	NT	2000	XP
Schemes	✓	✓	✓	✓	✓	✓

Screen Saver

This table displays the user settings that you can capture in the Control Panel under Screen Saver.

Option	95	98	Me	NT	2000	XP
Screen saver, with or without password	✓	✓	✓	✓	✓	✓
Energy saving features of monitor		✓	✓		✓	✓

Mapped network drive settings

This table displays the user settings that you can capture in the Control Panel under Mapped Network Drive.

Option	95	98	Me	NT	2000	XP
Mapped Network drive	✓	✓	✓	✓	✓	✓

Internet settings

This table displays the user settings that you can capture in the Control Panel under Internet.

Option	95	98	Me	NT	2000	XP
Home Page	✓	✓	✓		✓	✓
Proxy, bypass proxy server for local addresses	✓	✓	✓	✓	✓	✓
Proxy for http and ftp	✓	✓	✓	✓	✓	✓
Do not use proxy server for addresses beginning with....	✓	✓	✓	✓	✓	✓

Taskbar and Start menu options

This table displays the user settings that you can capture for Taskbar and Start menu options.

Option	95	98	Me	NT	2000	XP
Lock the taskbar						✓
Auto-hide the taskbar	✓	✓	✓	✓	✓	✓
Keep the taskbar on top of other windows						✓
Group similar taskbar buttons						✓
Show the clock	✓	✓	✓	✓	✓	✓
Hide inactive icons						✓
Start menu controls, start menu or classic start menu						✓
Auto-hide the taskbar						✓
Always on top	✓	✓	✓	✓	✓	✓
Show small icons on Start menu	✓	✓	✓	✓	✓	✓
Height of taskbar	✓	✓	✓	✓	✓	✓

Desktop options

Option	95	98	Me	NT	2000	XP
Toolbar, Address		✓	✓		✓	✓
Toolbar, Link		✓	✓		✓	✓
Toolbar, Desktop		✓	✓		✓	✓
Toolbar, QuickLaunch		✓	✓		✓	✓
Start menu controls			✓		✓	✓
Group similar taskbar buttons	✓	✓	✓	✓	✓	✓
Start menu style, XP or classic						✓

Sysprep

This chapter contains the following:

- [Introducing Sysprep](#)
- [Setting up Sysprep](#)
- [Cloning with Sysprep](#)
- [How Sysprep works with cloning and the Console post-configuration process](#)
- [Configuring Sysprep.inf](#)

Introducing Sysprep

Sysprep is a Microsoft utility that helps prepare Microsoft Windows 2000/XP 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.

If the source or target computers are running Microsoft Windows 2000 or Microsoft Windows XP Professional, then Sysprep uses a file called `Sysprep.inf` that you can edit to provide computer-specific information before and after completing a cloning task. Sysprep uses `Sysprep.inf` in three 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 Sysprep.inf is used to prepare the source computer for duplication and customization before creating the image. Some of the settings specified in Sysprep.inf are applied by Sysprep after you load the image back onto the destination computers. Sysprep.inf is not included with the Sysprep download from Microsoft. You must create Sysprep.inf 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.

Read the following documents, even if you are familiar with Sysprep.

Get information on	From
How to deploy Microsoft Windows 2000 using Sysprep	The Microsoft Windows 2000 Professional CD: <ul style="list-style-type: none">■ Support\Tools\Depoly.cab\Deptool.chm■ Support\Tools\Deploy.cab\Unattend.doc
How to deploy Microsoft Windows XP using Sysprep	The Microsoft Windows XP Professional CD: <ul style="list-style-type: none">■ Support\Tools\Deploy.cab\Deploy.chm■ Support\Tools\Deploy.cab\Ref.chm

Note: Do not use Sysprep and a configuration task to set the same configuration 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 contains reduced functionality.

Adding a Sysprep configuration

Once you have copied the Sysprep files on to your computer, you can set up and configure a version from the Console.

Download Sysprep version 1.1 for Windows 2000 from the Microsoft Web site:

<http://www.microsoft.com/windows2000/downloads/tools/sysprep/default.asp>

Copy Sysprep version 2.0 for Windows XP from the following directory on the Windows XP installation CD:

Support\Tools\Deploy.cab

To add a Sysprep configuration

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 Do one of the following to move the Sysprep files to the Symantec Ghost Console data directory:
 - On the Tools menu, click **Sysprep Configurations**.
 - On the File menu, click **New > Image Dump**, then, on the Sysprep tab, click **Sysprep Configurations**.

If you do not install the Sysprep files, your Sysprep tasks fail to execute.

- 3 Type a name for the version of Sysprep that you are installing.
- 4 In the Browse For Folder window, click the **Sysprep** folder.
- 5 Click **OK**.

Note: 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 (except for the empty ones) are installed in the Console local data area. Before you create a Sysprep image, all folders and files from that location are copied to the Console client computer.

Overwriting a Sysprep configuration

You can overwrite an existing Sysprep configuration with a new version. Do this if you want a later version of Sysprep, or you have made changes to any Sysprep files.

To overwrite a Sysprep configuration

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the Tools menu, click **Sysprep Configurations**.
- 3 Select a Sysprep configuration from the drop-down list.
- 4 Click **Create**.
- 5 Click **OK**.
- 6 In the Browse For Folder window, click the **Sysprep** folder.
- 7 Click **OK**.
- 8 Click **OK**.

Deleting a Sysprep configuration

If you delete a Sysprep configuration, all Sysprep files for that version are removed from your computer.

You cannot delete a Sysprep configuration if it has been selected within a task.

To delete a Sysprep configuration

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the Tools menu, click **Sysprep Configurations**.
- 3 Select a Sysprep configuration.
- 4 Click **Delete**.
- 5 Click **OK**.

Cloning with Sysprep

Sysprep is included in a cloning task by completing the Sysprep information in the Image Dump task.

To clone with Sysprep

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.

- 2 On the File menu, click **New > Image Dump**.

- 3 Complete the Network and the General image dump details.

For more information, see [“Setting image dump task properties”](#) on page 84.

- 4 On the Sysprep tab, click **Run Microsoft Sysprep on this machine before dumping the image**.

- 5 Select a Sysprep configuration.

- 6 Click **Tell Sysprep to perform a SID change when loading 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 loading an image onto client computers.

For more information, see [“Making SID changes with Sysprep and Ghost Walker on NT based clients”](#) on page 285.

- 7 Leave Run the MiniSetup wizard to process the sysprep.inf file selected for Sysprep to 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 when the computer is next started.

- 8 In the Extra Sysprep Command Line Arguments field, type Sysprep switches to execute commands that are not automatically generated by Symantec Ghost.

- 9 Click **Edit Sysprep** to make changes to the Sysprep.inf file for this task.

You can configure the file to let Sysprep set up the client computers without user interaction.

For more information, see [“Editing, restoring or reloading Sysprep.inf”](#) on page 130.

Some Sysprep switches are generated automatically by Symantec Ghost or affect the operation of the Console task. Do not use the following switches in a Sysprep image dump task:

- forceshutdown
- mini
- noreboot
- nosidgen
- quiet
- reboot
- reseal

Editing, restoring or reloading Sysprep.inf

You can edit the Sysprep template file included in a task. If you do not, the default Sysprep.inf in the Console's data folder is used.

For more information, see [“Configuring Sysprep.inf”](#) on page 132.

To edit, restore, or reload Sysprep.inf

- 1 In the Properties for New Task window, on the Sysprep tab, click **Edit Sysprep**.
- 2 Edit the Sysprep.inf file.

The file can be configured to let Sysprep set up the client computers without user interaction.

For more information, see [“Configuring Sysprep.inf”](#) on page 132.
- 3 Select one of the following:
 - OK: Save your changes.
 - Restore: Return to the Sysprep.inf file that was used when the task was first created.
 - Reload: Replace Sysprep.inf with the configuration template Sysprep.inf.

How Sysprep works with cloning and the Console post-configuration process

Sysprep and the Console client interact in many ways.

Image dump task

- Sysprep sets up the model computer before you dump an image.
- It then restarts the computer and the image dump task executes.
- After the image has been created, the client remains in DOS and does not process the Mini-Setup Wizard or Windows Welcome.

Image load task

- The image file is loaded onto the Console client computers and the computers start.
- The Console client updates the Sysprep.inf file before Sysprep runs so that the Sysprep Mini-Setup Wizard changes the computer name and workgroup to the values specified in the post-configuration task. If these aren't specified, then they remain as they were in the image file, unless specified in the Sysprep.inf file.

Note: If you requested that default settings be used, the default Computer Name or Workgroup settings are applied by the Ghost post-configuration process, overwriting any specific settings you may have included in the Sysprep.inf file. If you do not want your Sysprep.inf settings to be overwritten, ensure that you are not using the default settings.

- Each Console client then defers its own post-configuration until the Sysprep Mini-Setup Wizard or Windows Welcome is finished.
- 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.

For more information, see “[Configuring Sysprep.inf](#)” on page 132.

- If Sysprep has been enabled to change the SID, it changes it once the Console client computer has been configured.

For more information, see [“Making SID changes with Sysprep and Ghost Walker on NT based clients”](#) on page 285.

- The Console client completes the remainder of its post-configuration tasks after Sysprep has restarted a second time, and depending on the post-configuration tasks that the Console client has completed, it may restart the computer a third time.

Configuring Sysprep.inf

When you update a Sysprep configuration, the Sysprep.inf file that is copied by the Console becomes the template for all Sysprep tasks for that configuration. The template is copied for each Sysprep operation and can be edited and configured for a specific task. It is unique to the task. However, if you want to alter the template file, you must make the changes to the Sysprep.inf file and update the Sysprep configuration by overwriting the existing one.

For more information, see [“Overwriting a Sysprep configuration”](#) on page 128.

You can configure Sysprep in many ways. To have Sysprep.inf apply the computer name, you must request that Sysprep randomly generate the computer name. If you do not, Sysprep supplies a default to the Mini-Setup Wizard and the user is prompted to confirm it. To request a randomly generated computer name, use the following parameter:

```
[UserData]  
ComputerName=*
```

For more information, see [“Making SID changes with Sysprep and Ghost Walker on NT based clients”](#) on page 285.



Creating boot images and disks with the Ghost Boot Wizard

This chapter contains the following:

- [Introducing the Ghost Boot Wizard](#)
- [Creating boot disks and boot images](#)
- [Multicard templates and the boot disk](#)
- [Adding network drivers to the Ghost Boot Wizard](#)
- [Adding command-line parameters to a boot package](#)
- [Selecting a version of DOS](#)

Introducing the Ghost Boot Wizard

The Ghost Boot Wizard creates boot packages that let you complete various cloning tasks. You create boot packages using the Ghost Boot Wizard, a utility designed to easily create boot disks and images. For any task, the Ghost Boot Wizard guides you through the different steps to select the settings and drivers needed to create the boot package.

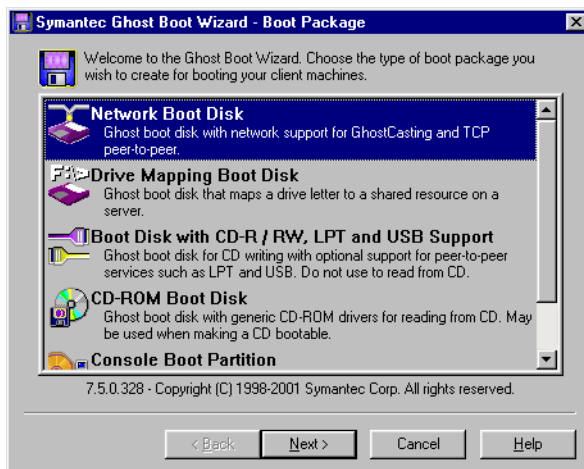
IBM DOS is supplied for the purpose of creating boot disks. The DOS files are installed automatically when you create the boot disk in Ghost Boot Wizard.

Opening the Ghost Boot Wizard

The procedures in this chapter assume that you know how to open the Ghost Boot Wizard.

To open the Ghost Boot Wizard

- On the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Boot Wizard**.



Creating boot disks and boot images

The processes for creating boot images and disks include how to create:

- Standard boot disks that enable the use of Symantec Ghost on a single computer
- Boot disks enabling peer-to-peer services for USB and LPT
- Network boot disks with network support for GhostCasting and TCP peer-to-peer connections
- A boot disk enabling you to write an image file to a CD-ROM on a CD writer supported by Symantec Ghost

For more information, see [“Image files and CD writers”](#) on page 168.

- Drive-mapping boot disks to map a drive on a workstation to a shared resource on a server
- CD-ROM boot disks with generic CD-ROM drivers for reading a Ghost image from a CD-ROM

- A disk used in the creation of a bootable CD-ROM
- Console boot partition images for installation on a workstation
- RIS boot packages that support Microsoft Remote Installation Service (RIS) using Symantec Ghost
- TCP/IP network boot images to allow access to Symantec Ghost without a boot disk using 3Com DynamicAccess Boot Services

Standard boot disks with the option of LPT and USB support

The Ghost Boot Wizard creates a boot disk that does any of the following:

- Lets you write Ghost images to a CD-R/RW on a CD writer supported by Symantec Ghost
For more information, see [“Image files and CD writers”](#) on page 168.
- Runs Ghost.exe on computers with LPT and USB support and peer-to-peer.
- Contains Ghost.exe only

Note: Symantec Ghost does not support writing to a CD-ROM drive that is connected with a USB cable.

To create a boot disk to run Ghost.exe, or with support for LPT and USB cables

- 1 In the Ghost Boot Wizard window, click **Boot Disk with CD-R/RW, LPT and USB Support**.
- 2 Click **Next**.
- 3 Do one or more of the following:
 - Check **USB support** to add USB support to the boot disk.
 - Check **LPT support** to add LPT support to the boot disk.
 - Uncheck to clear **USB support** and **LPT support** to create a boot disk that runs Symantec Ghost on a single computer.
 - Click **Advanced** to change the LPT mode or port.
 - Click **Include Adaptec ASPI drivers** to add drivers to support Adaptec ASPI drivers to the boot disk.
These drivers are required to write an image directly to a SCSI CD-R that is supported by Symantec Ghost.
- 4 Click **Next**.

- 5 Select one of the following:
 - Use PC-DOS: Include PC-DOS on the boot disk.
 - Use MS-DOS: Include MS-DOS on the boot disk.

For more information, see [“Selecting a version of DOS”](#) on page 150.
- 6 Click **Next**.
- 7 In the Ghost.exe, field type the correct path if the executable has been moved or you want to use a different version of Symantec Ghost.

The default path to the Symantec Ghost executable appears in the Ghost.exe field.
- 8 In the Parameters field, type any required command-line parameters.

For more information, see [“Adding command-line parameters to a boot package”](#) on page 148.
- 9 Click **Next**.
- 10 In the Floppy Disk Drive field, type the appropriate drive letter.
- 11 In the Number of disks to create field, type the number of disks that you want to create.
- 12 Click **Format disk(s) first** to format the disks before disk creation.
- 13 Click **Quick Format** to perform a quick format.
- 14 Click **Next**.

The default mode for an LPT connection is ECP/EPP High Speed. 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 disk, the mode is reset to the default ECP/EPP High Speed.

If you have multiple parallel ports and want to connect via any port other than the default LPT1, use the LPT port option to specify the port into which your cable is plugged.

Boot disks with network support

The Ghost Boot Wizard helps you create boot disks that provide network support for GhostCasting and TCP/IP peer-to-peer connections.

Before starting this process, you need to know the types of network cards that are installed on your client computers. Unless you use the multicard template, you must create a boot disk for each network card.

To create a boot disk with network support

- 1 In the Ghost Boot Wizard window, click **Network Boot Disk**.
- 2 Click **Next**.
- 3 Select the network driver for the make and model of the network card installed on the client computer.

If the correct driver isn't in the list, add the driver.

For more information, see [“Adding network drivers to the Ghost Boot Wizard”](#) on page 145.
- 4 Click **Next**.
- 5 Select one of the following:
 - Use PC-DOS: Include PC-DOS on the boot disk.
 - Use MS-DOS: Include MS-DOS on the boot disk.
For more information, see [“Selecting a version of DOS”](#) on page 150.
- 6 Do one of the following:
 - Click **Symantec Ghost** to create a boot package for the client that loads Symantec Ghost. You can connect to a running GhostCast Server to transfer image files to and from the client.
 - Click **Symantec GhostCast Server for DOS** to create a boot package that loads the DOS version of the GhostCast Server.

For more information, see [“Running the DOS-based GhostCast Server”](#) on page 194.
- 7 Do one of the following:
 - In the Ghost.exe field, type the correct path if the executable has been moved or you want to use a different version of Ghost.
 - In the Dosghsrv.exe field, type the correct path if the executable has been moved or you want to use a different version of GhostCast.
- 8 In the Parameters field, type any required command-line parameters.

For more information, see [“Adding command-line parameters to a boot package”](#) on page 148.
- 9 Click **Next**.

- 10 Do one of the following:
 - Click **DHCP will assign the IP settings** if your network contains a DHCP server.
 - Click **The IP settings will be statically defined** and complete the fields below this option if your network does not contain a DHCP server.

If you create more than one boot disk, then the static IP address incrementally increases as each boot disk is created.
- 11 Click **Next**.
- 12 In the Floppy Disk Drive field, type the appropriate drive letter.
- 13 In the Number of disks to create field, type the number of disks that you want to create.
- 14 Click **Format disk(s) first** to format the disks before disk creation.
- 15 Click **Quick Format** to perform a quick format.
- 16 Click **Next**.

Creating boot disks that support mapping network drives

When your client computers need to access a network drive, use the Ghost Boot Wizard to create boot disks that map a drive letter to a shared resource on a network server.

To create a boot disk that supports mapping network drives

- 1 In the Ghost Boot Wizard window, click **Drive Mapping Boot Disk**.
- 2 Click **Next**.
- 3 Select the network driver for the particular make and model of the network card installed on the client computer.

If the correct driver isn't in the list, add the driver.

For more information, see [“Adding network drivers to the Ghost Boot Wizard”](#) on page 145.

You can add more than one driver to the boot package.

For more information, see [“Multicard templates and the boot disk”](#) on page 145.
- 4 Click **Next**.

5 Select one of the following:

- Use PC-DOS: Include PC-DOS on the boot disk.
- Use MS-DOS: Include MS-DOS on the boot disk.

For more information, see [“Selecting a version of DOS”](#) on page 150.

6 Click **Get MS Client** and browse to the MS DOS Client files to include the Microsoft Client files if you are using MS-DOS.

If you are using MS-DOS, you need to have the Microsoft DOS Client files. You must install the files on the Ghost Boot Wizard computer before you can include them in the boot package. The files are usually installed in C:\Net.

7 Click **Next**.

8 In the Computer Name field, type the name of the client computer.

This specifies the name of the computer after starting from the floppy disk, and does not have to be the same name given to the computer in Windows. If you create more than one disk, a number is added to the computer name so that the names for subsequent disks are unique.

9 In the User Name field, type the user name that the boot disk will use to log on to the network.

This user must exist on the network and have sufficient access rights to the files and directories that you want to use.

10 In the Domain field, type the domain to which the user belongs.

11 In the Drive Letter field, select a drive letter to access a network share through a mapped drive.

This appears as though it is a hard drive connected to your computer.

12 Click **None** to prevent the boot package from mapping a drive when the computer starts.

In this case map a drive from the DOS prompt after the computer has started.

13 In the Maps To field, type the complete UNC path to the network share.

For example, to access a shared folder named Ghost on a computer named Boss, the UNC path is \\Boss\Ghost.

14 Click **Next**.

- 15 Do one of the following:
 - Click **DHCP will assign the IP settings** if your network contains a DHCP server.
 - Click **The IP settings will be statically defined** and complete the fields below this option if your network does not contain a DHCP server. Your network administrator can provide the values for these fields.
- 16 Click **Next**.
- 17 In the Floppy Disk Drive field, type the appropriate drive letter.
- 18 In the Number of disks to create field, type the number of disks that you want to create.
- 19 Click **Format disk(s) first** to format the disks before disk creation.
- 20 Click **Quick Format** to perform a quick format.
- 21 Click **Next**.

Boot disks with CD-ROM support

Boot disks with CD-ROM support let you access images stored on CD-ROM.

To create a boot disk with CD-ROM support

- 1 In the Ghost Boot Wizard window, click **CD-ROM Boot Disk**.
- 2 Click **Next**.
- 3 Select one of the following:
 - Use PC-DOS: Include PC-DOS on the boot disk.
 - Use MS-DOS: Include MS-DOS on the boot disk.

For more information, see [“Selecting a version of DOS”](#) on page 150.
- 4 Click **Next**.
- 5 In the Ghost.exe field, type the correct path if the executable has been moved or you want to use a different version of Ghost.

The default path to the Ghost executable appears in the Ghost.exe field.
- 6 In the Parameters field, type any required command-line parameters.

For more information, see [“Adding command-line parameters to a boot package”](#) on page 148.
- 7 Click **Next**.

- 8 In the Floppy Disk Drive field, type the appropriate drive letter.
- 9 In the Number of disks to create field, type the number of disks that you want to create.
- 10 Click **Format disk(s) first** to format the disks before disk creation.
- 11 Click **Quick Format** to perform a quick format.
- 12 Click **Next**.

Creating a boot image containing the 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.

For more information, see [“Installing the Console client”](#) on page 39.

To create a boot image that contains a Console boot partition

- 1 In the Ghost Boot Wizard window, click **Console Boot Partition**.
- 2 Click **Next**.
- 3 Select the network driver for the make and model of the network card installed on the client computer.

If the correct driver isn't in the list, add the driver.

For more information, see [“Adding network drivers to the Ghost Boot Wizard”](#) on page 145.

You can add more than one driver to the boot package.

For more information, see [“Multicard templates and the boot disk”](#) on page 145.

- 4 Click **Next**.
- 5 Type the correct path in the Ghost.exe field, if the executable has been moved, or you want to use a different version of Ghost.

The default path to the Ghost executable appears in the Ghost.exe field.

- 6 Type the correct path in the Ngctdos.exe field, if the executable has been moved, or you want to use a different version.

The default path to the Ghost DOS client executable appears in the Ngctdos.exe field.

- 7 Type the correct path in the Ghstwalk.exe field, if the executable has been moved, or you want to use a different version.

The default path to the Ghost Walker executable is entered in the Ghstwalk.exe field.

- 8 In the Machine Group, type the computer group folder, if required.
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.
- 9 Do one of the following:
 - Click **DHCP will assign the IP settings** if your network contains a DHCP server.
 - Click **The IP settings will be statically defined** and complete the fields below this option if your network does not contain a DHCP server.
- 10 Click **Next**.
- 11 Type a name and description for the image file.
- 12 Click **Next**.

Boot packages that support 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 or XP server with RIS installed. No floppy disk is required. An entry appears in the RIS menu.

This option only appears if Microsoft Remote Installation Service is installed on your computer.

To create a boot disk that supports RIS

- 1 In the Ghost Boot Wizard window, click **Microsoft RIS Boot Option**.
- 2 Select the generic PXE packet driver template.
- 3 Click **Next**.
- 4 Do one of the following:
 - Click **Symantec Ghost** to create a boot package that loads Symantec Ghost. You can connect to a running GhostCast Server to transfer image files to and from the client.
 - Click **Symantec GhostCast Server for DOS** to create a boot package that loads the DOS version of the GhostCast Server.
- 5 Do one of the following:
 - In the Ghost.exe field, type the correct path if the executable has been moved or you want to use a different version of Ghost.
 - In the Dosghsrv.exe field, type the correct path if the executable has been moved or you want to use a different version of the GhostCast Server.
- 6 In the Parameters field, type any required command-line parameters. For more information, see [“Adding command-line parameters to a boot package”](#) on page 148.
- 7 Click **Next**.
- 8 In the RIS Boot Menu Name field, type the name that will appear on the RIS Boot menu.

When you select this menu item, the client computer starts from the network card without a boot disk.
- 9 In the RIS Boot Description field, type a description for the boot package.

This text appears as a help message when the menu option is selected.
- 10 Select a language if there is more than one.
- 11 Click **Next**.

Starting client computers from the network

You can create an image file that lets you start client computers from the network without using a floppy disk.

To create an image file to start client computers from the network

- 1 In the Ghost Boot Wizard window, click **TCP/IP Network Boot Image**.
- 2 Click **Next**.
- 3 Select the generic PXE packet driver template.
- 4 Click **Next**.
- 5 Do one of the following:
 - Click **Symantec Ghost** to include the Ghost client in the boot package.

The default path to the Ghost executable is entered in the Ghost.exe field. If the executable has been moved, or you want to use a different version of Ghost, type the correct path.
 - Click **Symantec GhostCast Server for DOS** to include the GhostCast Server for DOS in the boot package.

The default path to the GhostCast Server for DOS is entered in the Dosghsrv.exe field. If the executable has moved, or you want to use a different version of the server, type the correct path.
- 6 In the Parameters field, type any required command-line parameters.

For more information, see [“Adding command-line parameters to a boot package”](#) on page 148.
- 7 Click **Next**.
- 8 Do one of the following:
 - Click **DHCP will assign the IP settings** if your network contains a DHCP server.
 - Click **The IP settings will be statically defined** and complete the fields below this option if your network does not contain a DHCP server. Your network administrator can provide the values for these fields.
- 9 Click **Next**.
- 10 In the Image File field, type a file name for the image file.

This image can be used with any BOOTP/TFTP server.
- 11 Click **Next**.

Multicard templates and the boot disk

You can use multicard templates to create a boot package containing several NDIS2 drivers. When the computer starts, 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 client computers without modification.

Refer to the Software License Agreement for use restrictions.

To create a multicard template

- 1 In the Network Interface Card window, click **Multicard Template**.
- 2 Click **Next**.
- 3 Select the required drivers from the list of NDIS2 drivers.
If you are creating a floppy disk from the boot package, select no more than four or five drivers, as space is limited on a floppy disk.
- 4 Click **Next**.

Adding network drivers to the Ghost Boot Wizard

The Ghost Boot Wizard includes drivers to over 80 network interface cards. If your driver isn't in the list, you can add it to the wizard so that it's set up the next time you need it.

To begin adding a network driver to the Ghost Boot Wizard

- 1 In the Boot Package window, select the type of boot package that you want to create.
- 2 Click **Next**.
- 3 Click **Add**.
- 4 Select one of the following:
 - Packet Driver
 - NDIS2 DriverMany manufacturers ship both drivers with their network cards so you have a choice of which one to use.
- 5 Click **OK**.

Adding packet drivers to the Ghost Boot Wizard

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.

To add a packet driver to the Ghost Boot Wizard

- 1 In the Template Properties window, on the Packet Driver tab, in the Driver Executable field, type the packet driver location so that the Ghost Boot Wizard can copy the file to the current template.

Packet drivers are usually included on the driver disk supplied with the network card. If you are installing the packet driver from the original disks that came with your network interface card, the packet driver should be in a directory called Packet or Pktdrv.

- 2 In the Parameters field, type the command-line parameters if the network card requires them.

These parameters vary from driver to driver and are usually optional with plug-and-play network cards. Consult the documentation that came with the network card. This is often in the form of a Readme.txt file in the same directory as the driver itself.

- 3 Click **Select Automatically** to let Ghost determine the best multicasting mode based on the information in the packet driver.

If the Select Automatically mode does not work, try Receive Mode 5. If that doesn't work, try Receive Mode 6.

Adding NDIS2 drivers to the Ghost Boot Wizard

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.

To add an NDIS2 driver to the Ghost Boot Wizard

- 1 In the Template Properties window, on the NDIS Driver tab, click **Setup**.
- 2 Locate the 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.
- 3 Type the DOS file name for the NDIS2 driver.
- 4 In the Driver Name field, 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. If the Setup did not fill in this field for you, read the sample Protocol.ini file in the same directory as the driver itself to find the driver name.
- 5 In the Parameters field, 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.

Customizing the 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 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. Files added to the template appear in the list to the right of the button.

If this template is used as a multicard template, then any additional files or modifications are overridden by its settings.

To add or delete a file to or from a template

- 1 In the Template Properties window, on the Advanced tab, click **New**.
- 2 Click **Delete** to delete the selected file from the list.
- 3 In the Autoexec.bat field, 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.

- 4 In the Config.sys field, type any additional Config.sys entries for the driver.

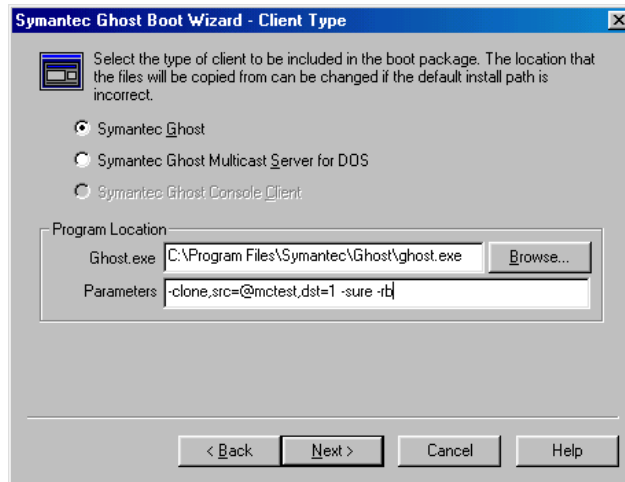
The entries appear before any driver-related devices load to ensure that enabling drivers load before the main network device drivers specified on the network driver page.

Adding command-line parameters to a boot package

You can enter command-line parameters to a boot package to instruct Symantec Ghost to perform certain actions.

For more information, see [“Command-line switches”](#) on page 297.

In the following example, the parameters instruct Symantec Ghost to connect to the GhostCast session called test and load the disk image to the first drive.



Switch	Description
-sure	Removes the need to confirm the specified details.
-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=dump,src=1,dst=d:\backups\maindrv.gho
```

Clone Parameters	Description
mode=dump	Dumps an image.
src=1	Specifies drive 1 as the source drive.
dst=D:\Backups\Maindrv.gho	Saves the image to the file D:\Backups\Maindrv.gho

The `-ja = sessionname` switch lets you avoid having to specify the GhostCast session name parameters on each client computer.

For more information, see [“Controlling the GhostCast session from the server”](#) on page 183.

Selecting a version of DOS

The Ghost Boot Wizard includes IBM DOS on boot disks. However, a boot disk that includes IBM DOS might not start all computers. When creating a boot disk, you can include MS-DOS instead of IBM DOS.

If you use MS-DOS, then you must install MS-DOS files on the computer on which you are creating the boot disk. Using a floppy disk that was formatted on a Windows 9x computer, you can install the MS-DOS files during the creation of the boot disk.

To install MS-DOS files on your computer

- 1 Insert a blank floppy disk into drive A of a Windows 9x computer.
- 2 Double-click the **My Computer** icon.
- 3 Right-click drive A then click **Format**.
- 4 Click **Copy System Files**.
- 5 Insert the formatted floppy disk into drive A of the computer on which the Ghost Boot Wizard is running.

Additional Console options

This chapter contains the following:

- [Monitoring the Symantec Ghost Console activity](#)
- [Launching the Configuration Server](#)
- [Setting the Symantec Ghost Console options](#)
- [Symantec Ghost Console security](#)

Monitoring the Symantec Ghost Console activity

To review the history of a task or client computer you can view various logs or summaries.

Logs/summaries	Description
Task Log	The history of execution for all tasks. For more information, see “To view the Task Log” on page 152.
Console Log	A log of all steps occurring during the execution of tasks from the command line or scheduler. For more information, see “To view the Console Log” on page 153.
Client Summary	A summary of all executions for a client computer. For more information, see “To view a Client Summary” on page 153.

Logs/summaries	Description
Event Log	The history of all events for all computers for a task. For more information, see “To view the Event Log” on page 153.
Ghost error file	The error file that is created on the client computer if the task fails. For more information, see “To view the Event Log” on page 153.
Event Details	The details for an item in the client summary or event log. For more information, see “To view Event Details” on page 153.
Active Tasks	A second window that lists tasks that are currently executing. For more information, see “To view Active Tasks” on page 154.

To view the Task Log

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the View menu, click **Task Log**.
- 3 In the Task Log window, on the View menu, select a sort option:
 - Time: Time and date of execution
 - User: User name from the logon window
 - Name: Task title

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 the Console Log

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the View menu, click **Task Log**.
- 3 In the Task Log window, on the View menu, click **Console Log**.
For more information, see [“Running command-line or scheduled tasks”](#) on page 344.

To view a Client Summary

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the View menu, click **Task 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 Event Log.

To view the Event Log

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the View menu, click **Task 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 Event Details

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 In the Event Log window, on the View menu, click **Event Details**.

To view Active Tasks

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Corporate Console**.
- 2 On the View menu, click **Active Task Pane**.

Launching the Configuration Server

The Configuration Server manages task executions and communication with clients. Usually it 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 it down by mistake.

To launch the Configuration Server

- On the Symantec Ghost Console, on the File menu, click **Launch Server**.
This item is unavailable if the Configuration Server is already running.

Setting the Symantec Ghost Console options

You can set several user options in the Symantec Ghost Console:

- Optional splash screen and wizard when the user opens the Console.
- Turn off Ghost watermark.

For more information, see [“Accessibility features in Symantec Ghost”](#) on page 32.

- The number of days that you want tasks held in the log.
- 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.

- Warn a client that you are about to run a task and let the user abort the task.

- Set the 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 not indicated on the Console.

For more information, see [“Setting properties for computers in a subnet”](#) on page 61 and [“Setting the client computer heartbeat interval”](#) on page 65.

- 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 are transferred over your network. You can alter these settings globally, for a task, and for a single execution of a task.

For more information, see [“Setting the data transfer mode”](#) on page 187, [“Controlling the amount of network bandwidth used”](#) on page 188, and [“Optimizing data transfer over the network”](#) on page 85.

- Control the amount of network bandwidth used.

Symantec Ghost lets you control how much network bandwidth is used when transferring image files while cloning. By using this functionality, you can avoid overloading the network with GhostCasting traffic.

For more information, see [“Controlling the amount of network bandwidth used”](#) on page 188.

- Set the size of the virtual partition.

You can alter the size of the virtual partition if you require. For example, if you need to transfer a large executable to the virtual partition.

- The number of minutes the Configuration Server waits for a client to connect.

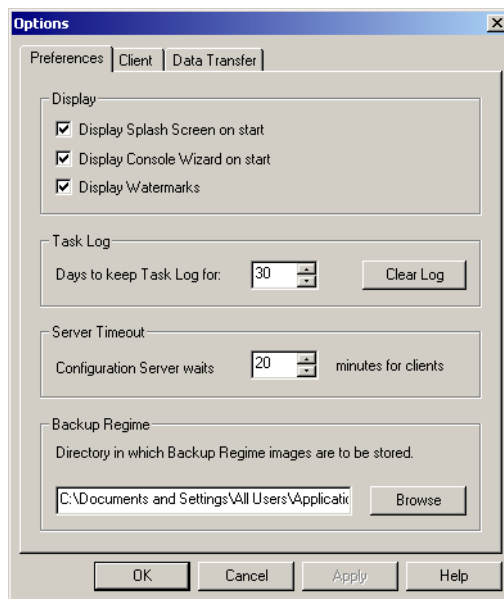
- The folder in which to store incremental backups.
- Set the default DOS version for the virtual partition.

You can select a default version of DOS that is installed when the virtual partition is created on a client. The client computer runs under the selected version of DOS. You can select MS-DOS only if it is installed on your computer.

For more information, see [“Selecting a version of DOS”](#) on page 150.

To set the splash screen and wizard options

- 1 On the Tools menu, click **Options**.



- 2 On the Preferences tab, click **Display Splash Screen on start** to see the splash screen.
- 3 Click **Display Console Wizard on start** to see the wizard screen.
- 4 Click **Apply**.

To turn off the Ghost watermark in the Symantec Ghost Console

- 1 On the Tools menu, click **Options**.
- 2 On the Preferences tab, click **Display Watermarks**.
- 3 Click **Apply**.

To allow client initiated tasks

- 1 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**.

To set the Task Log option

- 1 On the Tools menu, click **Options**.
- 2 On the Preferences tab, 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 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 a client heartbeat

- 1 On the Tools menu, click **Options**.
- 2 On the Client tab, in the Interval field, type the number of seconds to set the rate at which status reports are sent from client computers to the Console.
- 3 Click **Apply**.

To set the data transfer mode

- 1 On the Tools menu, click **Options**.
- 2 On the Data Transfer tab, select one of the following:
 - Multicast: Set the data transfer mode to Multicast.
 - Directed Broadcast: Set the data transfer mode to Directed Broadcast.
 - Unicast: Set the data transfer mode to Unicast.
- 3 Click **Apply**.

To set the amount of network bandwidth used

- 1 On the Tools menu, click **Options**.
- 2 On the Data Transfer tab, do one or both of the following:
 - Check **Load**, then type the maximum MB per minute to set a limit for loading an image.
 - Check **Dump**, then type the maximum MB per minute to set a limit for dumping an image.
- 3 Click **Apply**.

To set the virtual partition size

- 1 On the Tools menu, click **Options**.
- 2 On the Client tab, in the Size field, type a size for the virtual partition.
The maximum size that you can set this field to is 2000 MB.
- 3 Click **Apply**.

To set the configuration server timeout option

- 1 On the Tools menu, click **Options**.
- 2 On the Preferences tab, in the Configuration Server waits field, type the number of minutes that you want the configuration server to wait for clients.
- 3 Click **Apply**.

To set the location for incremental backups

- 1 On the Tools menu, click **Options**.
- 2 On the Preferences tab, type the location in which you want to store the backups.
This can be changed, as required.
- 3 Click **Apply**.

To set the default version of DOS

- 1 On the Tools menu, click **Options**.
- 2 On the Client tab, select one of the following:
 - PC-DOS: Set the default DOS version to PC-DOS
 - MS-DOS: Set the default DOS version to MS-DOS
MS-DOS is only available if you have it installed on the Console server.
- 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, 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.

The private certificate must be safeguarded. If an unauthorized user copies it, security is compromised. If you accidentally delete your private certificate and have no other copy, generate a new certificated pair and distribute the public certificate to all clients.

For more information, see [“Generating new certificates”](#) on page 160.

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.

The Windows client needs the public certificate to communicate with the Console. 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 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 boot partition 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. This is done automatically when a task is executed for a client.

For NT based computers you must perform a remote client install for the client computer.

For 9x computers you must uninstall and then reinstall the client.

There are two certificates for the Console Server on each client, one in the Symantec Ghost boot partition, and one with the Windows client in the Symantec Ghost directory.

Generating new certificates

If you lose your private certificate, or if you think security has been compromised, generate a new certificate pair and distribute the public certificate to all clients.

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**.

Image file options

This chapter contains the following:

- [About Symantec Ghost image files](#)
- [Image files and compression](#)
- [Image files and CRC32](#)
- [Image files and volume spanning](#)
- [Image files and tape drives](#)
- [Image files and CD writers](#)
- [Cloning dynamic disks in Windows 2000](#)
- [Hibernation and swap files](#)

About Symantec Ghost image files

You can create image files using the Symantec Ghost executable, GhostCasting, or the Symantec Ghost Console.

The image files created with Symantec Ghost have a .gho extension by default. They contain the entire disk or partitions of the disk. Image files support:

- 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 smaller if you use compression.

If you also use the Ghost Explorer application, an image file companion utility, you can recover individual files from these image files selectively without having to restore the complete partition or disk.

Image files and compression

Image files created in Symantec Ghost support several levels of data compression. When using Symantec Ghost in interactive mode, three compression options are provided: none, fast, and high. The Symantec Ghost command-line switch, `-z`, provides access to nine levels of compression.

For more information, see [“Command-line switches”](#) on page 297.

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 own individual requirements.

Performance expectations on a network

One advantage of Symantec Ghost is speed. It takes minutes to install an operating system such as Windows 98, whether onto 10 or 100 computers. Many factors affect performance. There are ways to gauge whether Symantec Ghost is running optimally.

When using Symantec Ghost on a network, use the fast compression option. If disk space is at a premium, you can use higher compression, but it affects speed. The fastest performance over a network is usually achieved with GhostCasting.

Using a 10 MB/s ethernet network, a 25-60 MB/minute server speed is common. Factors influencing this range are:

- Using up-to-date drivers
- LAN traffic
- Choice of network hubs or switches, including brand and model
- Compression

On a 100 MB/s 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 state-of-the-art 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. The 32 value in CRC32 indicates that the CRC technique uses a 32-bit value to store error checking information. The use of CRC32 increases detection of errors in the image file.

When an image file is created, CRC32 details are embedded into the file to ensure that image file corruption is detected when it is being loaded to disk. CRC32 is currently included on a file-by-file basis with FAT and Linux Ext2 partitions, and on an MFT table 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 detection method against bad sector writes and other drive anomalies that may be missed during normal imaging checks.

A text file containing CRC values and associated file attributes can be generated using the `-CRC32` command-line switch.

For more information, see [“Command-line switches”](#) on page 297.

Image files and volume spanning

Images can be contained in a single file or spanned across a number of files.

Standard image files

Standard image files consist of a single file containing 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.

Size-limited, multisegment 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 550 MB for later transfer onto CD-ROM. The default (and maximum) file size is 2 GB.

Spanned image files

Spanned image files are similar to size-limited, multisegment 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 sort out 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.

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.

Spanning across multiple volumes and limiting span sizes

When creating 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 determining whether the image will fit. Alternatively, you can use the `-span` and `-split` command-line switches to configure Symantec Ghost to use image file splitting.

For more information, see [“Command-line switches”](#) on page 297.

Before saving the disk contents to the image file, Symantec Ghost shows the source and destination details and offers a chance to back out. The default is to back out.

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 an option to span onto a different location.

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 loading from an image.

Loading from a spanned image

When loading a disk or partition from a spanned image file, the process is the same as loading from an unspanned image file. However, during the loading 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.

To load spanned images without prompting, you can set the AutoName switch on the Ghost main menu under Options.

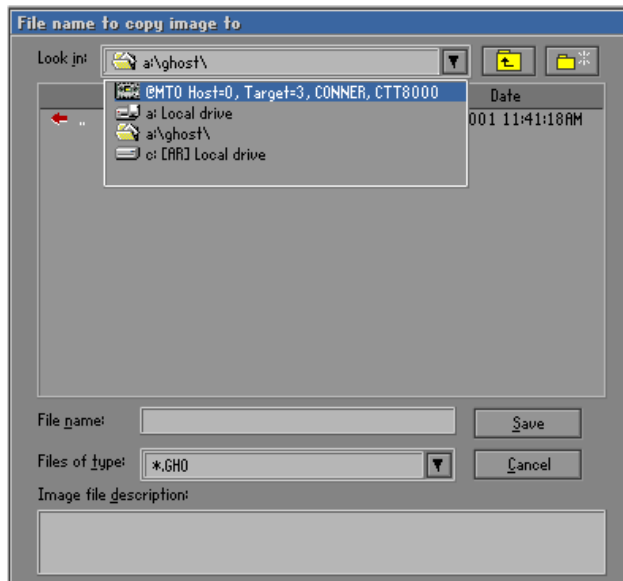
For more information, see [“Adding switches to your cloning task”](#) on page 227.

Image files and tape drives

Symantec Ghost support of SCSI tape drives allows the storage of a single image file onto a tape. When written onto the tape, there is no associated file system used, which means that you are unable to access the tape from a drive letter as if it were another storage drive. SCSI tapes do not support spanning to multiple tapes.

When using tape drives with Symantec Ghost, the tape drive can be selected as the source or destination device in the File Locator window. Each SCSI tape device is shown as MTx, where x is a number starting at 0

and increasing incrementally for each drive present. For example, the following screen shows a tape drive MT0 available for use.



For Symantec Ghost to access SCSI tape drives, a DOS ASPI driver must be installed prior to use.

For more information, see [“Setting up the hardware and transfer methods”](#) on page 325.

Symantec Ghost in its default mode performs well with most SCSI tape devices. In some situations with older SCSI tape devices and possibly with unreliable tapes, Symantec Ghost may need to be configured to slow down or alter the way it uses the tape device.

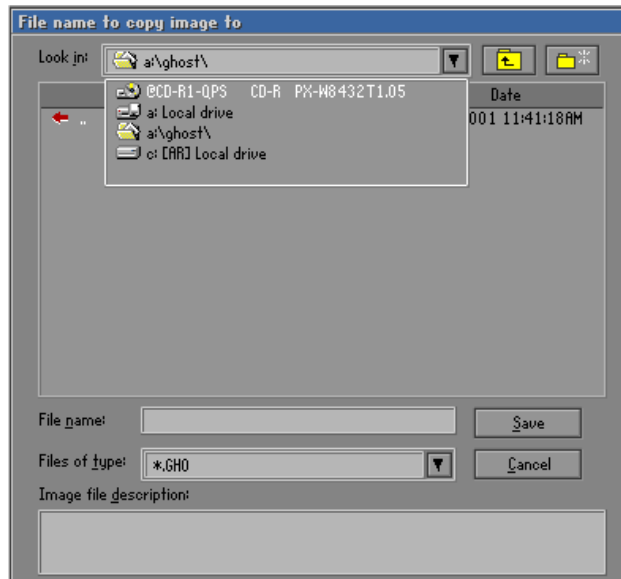
For more information, see [“Command-line switches”](#) on page 297.

Note: Ghost Explorer cannot access an image stored on tape.

Image files and CD writers

Symantec Ghost support of SCSI and IDE CD writers allows the storage of a single image file onto one or more CD-R/RW. The CDs can be read by any modern CD reader. USB CD writers are not supported by Symantec Ghost.

When using CD writers with Symantec Ghost, a writer can be selected 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 example, the following screen shows a CD writer available for use.



For Symantec Ghost to access SCSI CD writers, a DOS ASPI driver must be installed prior to use.

For more information, see [“Boot disks with CD-ROM support”](#) on page 140.

Symantec Ghost should work with most SCSI and IDE writers produced in 2000 or later. It may or may not work with older models. Use the latest firmware available for your CD writer. An IDE CD writer performs best if it is mounted on the secondary IDE controller.

A list of CD writers that Symantec Ghost has been tested with is available on the Symantec Service and Support Web site:

<http://service.symantec.com>

Use blank CD-R or unformatted CD-RW media with Symantec Ghost.

When creating an image on CD, you can make the CD bootable. You need an appropriate boot disk with CD drivers and MSCDEX loaded for this option. The Ghost Boot Wizard can create a suitable boot disk for you.

Start from a disk with appropriate drivers and MSCDEX loaded. Symantec Ghost restores images from CD as it does from other media, so the CD-reader must have a CD-drive letter.

For more information, see “[Saving an image file to a CD-R/RW](#)” on page 226.

Cloning dynamic disks in Windows 2000

Symantec Ghost supports the cloning of simple or mirrored volumes on dynamic disks. Cloning of spanned, striped, and RAID-5 volumes is not supported by Symantec Ghost. You can dump an image of a partition on a disk in a dynamic disk set to an image file. If you dump a disk, then all of the partitions that Ghost supports on the disk are dumped 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 to a basic disk only, 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. However, this method destroys all data on the disk.

For more information, see [“Reinitializing the Master Boot Record”](#) on page 268.

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 loaded must be identical to the source disk in every way. This function is only useful for creating a back up. If you load an image created using -ia onto a drive with different geometry, Windows 2000 does not understand the dynamic disk.

If you load an -ia disk image of a dynamic disk onto a SCSI hard drive and you get the error Destination drive too small, you must load the ASPI driver for the SCSI card. Without an ASPI driver, Symantec Ghost does not always have the correct size of the SCSI drive and cannot distinguish if the drive is large enough to hold the image.

Note: You should not take an image all of a dynamic disk as the method is slow and the image file would be very big.

Hibernation and swap files

When creating image files or cloning, Symantec Ghost does not clone 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 type of file system:

- 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 cloned.

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.bin
- Win386.swp

3

G h o s t C a s t i n g i m a g e f i l e s i n a n e t w o r k e d e n v i r o n m e n t

- Using GhostCasting to create and load images
- GhostCasting from the command line
- GhostCasting and IP addresses

Using GhostCasting to create and load images

This chapter contains the following:

- [About Symantec Ghost GhostCasting](#)
- [Preparing for GhostCasting](#)
- [Creating a GhostCast Server](#)

About Symantec Ghost GhostCasting

GhostCasting lets multiple computers running Symantec Ghost receive the same information over a computer network simultaneously. The Symantec Ghost GhostCast Server works with the Symantec Ghost executable (Ghost.exe) to create an image file of a model computer, or load an image file onto a number of client computers.

The GhostCast Server supports three forms of data transfer for transferring image files during cloning tasks:

- Unicasting
- Direct Broadcasting
- Multicasting

Symantec Ghost GhostCasting makes workstation migration and rollouts more efficient and may eliminate most replicated network traffic. You can use it through the Windows interface, command-line switches, batch files, or in a combination of the three.

Two applications are used in Symantec Ghost GhostCasting: one on the network server and another on every client workstation to be cloned.

- The GhostCast Server loads image files to multiple clients or creates an image file from a single connected client.
- On a client workstation, the DOS Symantec Ghost application (Ghost.exe) receives and writes the image file to the local disk.

Symantec Ghost GhostCasting supports:

- 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

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

For more information, see [“GhostCasting and IP addresses”](#) on page 205.

- 3 Select the executable that matches the platform.

You can run the GhostCast Server on two platforms: Windows and DOS. There is a separate server executable for each platform.

Platform	GhostCast Server executable
Windows	Ghostsrv.exe
DOS	Dosghsrv.exe

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.

If you are creating a model computer for Windows NT computers, see the Online Knowledge Base article “How to clone an NT system” under the General Information section.

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.

Ensure that Windows NT/2000/XP computers are not domain members before taking an image.

Creating a GhostCast Server

The Symantec Ghost 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 client or a group of similar clients. The session name acts as a key. It identifies the session, and is used by clients to indicate the session that they are to join.

To create a GhostCast Server

- 1 Do one of the following:
 - For Windows (Ghostsrv.exe): Install GhostCast Server on the computer.
For more information, see [“Installing Symantec Ghost Standard Tools”](#) on page 42.
 - For DOS (Dosghsrv.exe): Create a network boot disk in the Ghost Boot Wizard containing Dosghsrv.exe.
For more information, see [“Boot disks with network support”](#) on page 136.
- 2 Create a boot disk for the client computers that contains Ghost.exe.
For more information, see [“Boot disks with network support”](#) on page 136.

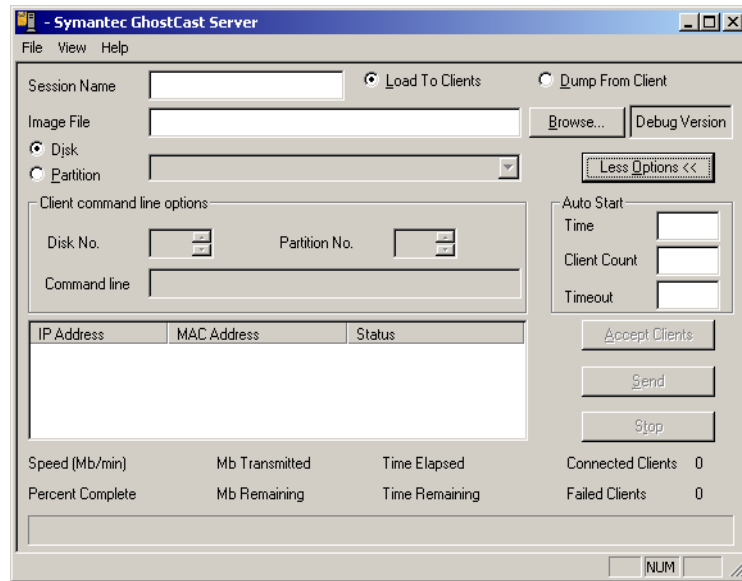
Starting a GhostCast session

After setting up the server and preparing the boot disk 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**.
- 2 In the Symantec Ghost GhostCast Server window, in the Session Name field, 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

in graphical mode 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 Symantec Ghost GhostCast Server window, click **Dump From Client** to dump and create an image file.
- 2 Do one of the following:
 - In the Image File field, 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:
 - Click **Disk** to create an image of an entire disk.
 - Click **Partition** to create an image of a selected partition.

- 4 Click **Accept Clients** to accept the client computer into the session.
The Accept Clients button becomes active when all fields are completed.
- 5 Start Symantec Ghost on the destination client computers and begin a GhostCast session.
For more information, see [“To connect a source computer to a GhostCast session”](#) on page 180.

Once the GhostCast session is started on the server, you can start the client computers from a boot disk and have them join the session.

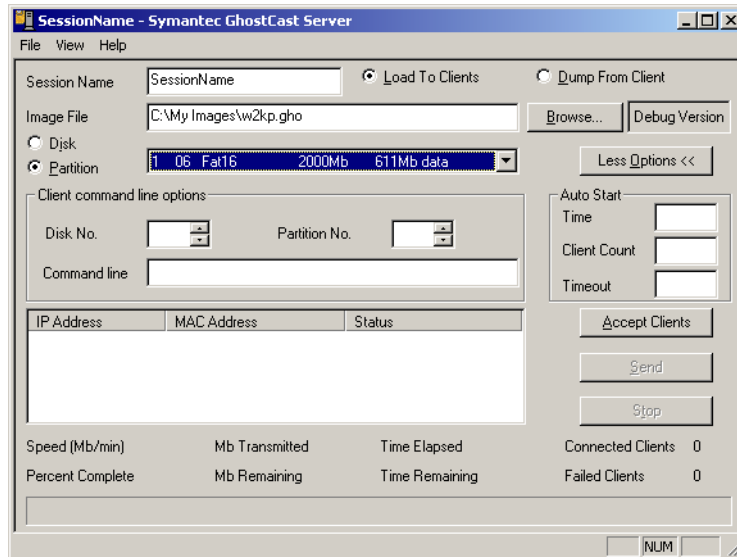
To connect a source computer to a GhostCast session

- 1 Create a GhostCast session on the GhostCast Server.
For more information, see [“To create an image file using the GhostCast Server”](#) on page 179.
- 2 Using the Ghost network boot disk, start Ghost.exe on the client computer.
- 3 On the Ghost 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 to dump.
- 7 Click **OK**.
- 8 Select the partition to dump, if required.
- 9 Click **OK**.
- 10 Select the level of compression that you require.
- 11 Click **Yes** to begin the image dump.

For more information, see [“Running the Symantec Ghost executable”](#) on page 190.

Loading an image file onto client computers

To load 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.



To load an image onto client computers using the GhostCast Server

- 1 Click **Load To Clients** to send an image file to all connecting clients.
 - 2 Do one of the following:
 - In the Image File field, 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:
 - Click **Disk** to load an image of an entire disk.
 - Click **Partition** to load an image of a partition and select the partition from the image file.

- 5 Click **Accept Clients** to accept the client computer into the session.
The Accept Clients button becomes active when all required fields are completed.
- 6 Log the client computers on to the GhostCast session.
For more information, see [“To join a GhostCast session to load an image file to client computers”](#) on page 182.
- 7 Click **Send** to start the image load 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.

To join a GhostCast session to load an image file to client computers

- 1 On the client computers, use the Ghost Boot Disk to start Ghost.exe.
- 2 On the Ghost 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 load.
- 6 Click **OK**.
- 7 Select the partition to load, if required.

- 8 Click **OK**.
- 9 Click **Yes** to indicate that the computer is ready for the image load to begin.

For more information, see [“Running the Symantec Ghost executable”](#) on page 190.

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 statuses.

Controlling the GhostCast session from the server

In your GhostCast session, you can specify the client disk or partition to clone from the server. You can also define command-line options to execute 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.
For more information, see [“To create an image file using the GhostCast Server”](#) on page 179.

- 2 Click **More Options**.

- 3 In the Disk No. field, type the disk number.

- 4 In the Partition No. field, type the partition number if you are dumping an image of a partition.

The client clone command appears in the Command line field.

- 5 Add other switches to the command line to execute specific command-line options on the client computer, if required.

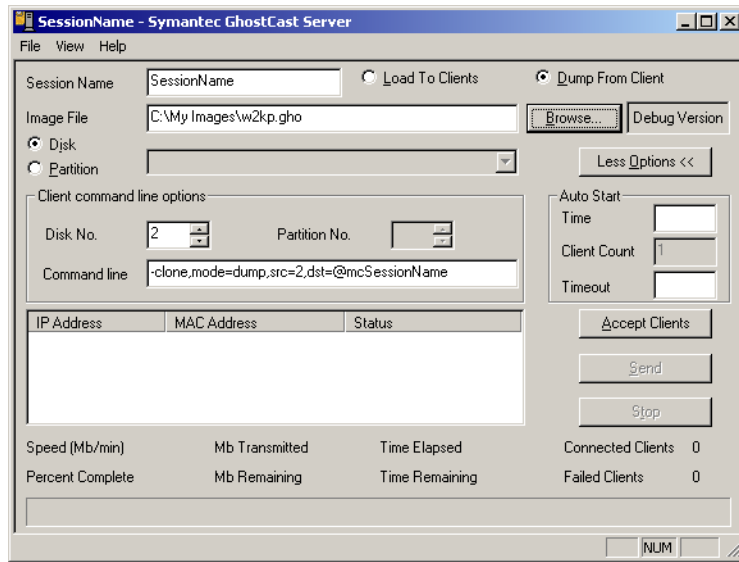
For example, if the initial command is:

```
-clone,mode=pdump,src=2,dst=@mcSessionNm
```

Add the following switches to avoid prompts and restart the client computer after the image has been extracted:

```
-clone,mode=pdump,src=2,dst=@mcSessionNm -sure -rb
```


Only use the -sure switch when you are sure that you are writing from the intended disk or partition.



- 6 Click **Accept Clients** to accept the client computer into the session.
- 7 Start the client computers in DOS.
- 8 Run Ghost using the -ja switch to log on to the GhostCast session from the command line:
ghost.exe -ja=SessionName
- 9 Confirm your choices on the client computers if the -sure switch was not used.

For more information, see [“Running the Symantec Ghost executable”](#) on page 190.

To load an image onto client computers using the GhostCast Server

- 1 Create a GhostCast session to load an image from the GhostCast Server.
- 2 Click **More Options**.
- 3 In the Disk No. field, type the disk number.
- 4 In the Partition No. field, type the partition number, if required.
- 5 In the Command line field, type the client clone command.

- 6 Add other switches to the command line to execute specific commands on the client computer.

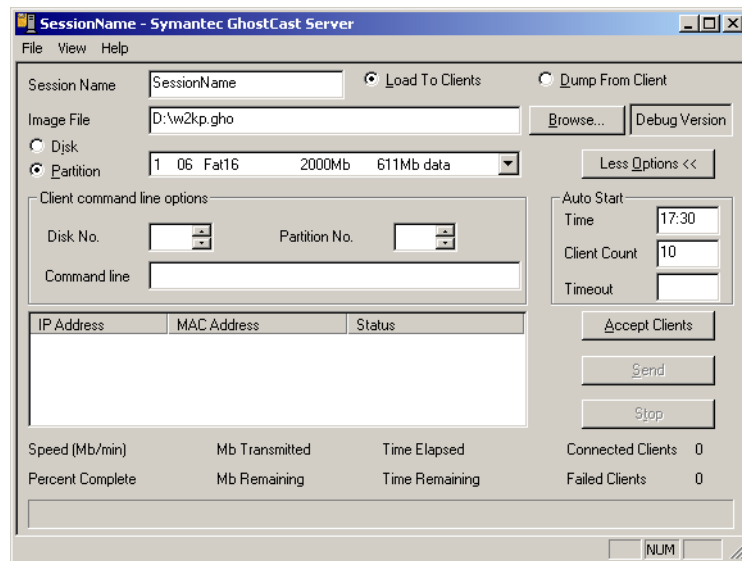
For example, if the initial command is:

```
-clone,mode=pload,dst=1.1,dst=@mcSessionNm
```

Add the following switches to avoid prompts and restart the client computer after the image has loaded:

```
-clone,mode=pload,dst=1.1,dst=@mcSessionNm -sure -rb
```

Only use the `-sure` switch when you are sure that you are writing to the intended disk or partition.



- 7 Click **Accept Clients** to accept the client computer into the session.
- 8 Start the client computers in DOS.
- 9 Run Ghost using the `-ja` switch to log on to the GhostCast session from the command line:

```
ghost.exe -ja=SessionNm
```

- 10 Confirm your choices on the client computers if the `-sure` switch was not used.

For more information, see [“Running the Symantec Ghost executable”](#) on page 190.

Setting Auto Start parameters

When your GhostCast session includes loading an image file to client computers, you can set the server to start the session automatically. The start time can be based on one parameter or a combination of parameters.

To set Auto Start parameters

- 1 In the Symantec Ghost GhostCast Server window, click **More Options** to access Auto Start options.
- 2 Do one or more of the following:
 - To use the time parameter, type a specified time 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 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.

If you specify more than one Auto Start parameter, the session starts when one of the conditions is fulfilled.

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 the network bandwidth limits, you can optimize the way in which data files are transferred over your network.

Note: Cloning tasks support all three transfer options. Any transfer of data during a Symantec Ghost Console task that is not a transfer task is via Unicast.

You can choose from one of the following 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 sent to all computers on a specified subnet. If clients are on more than one network, one stream is sent to each network.	Your network hardware does not support Multicasting.
Multicast	Data sent to all computers on the network that have requested the data.	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 to client computers that have requested data from the GhostCast Server. Only computers that have requested this data receive it.

Note: This requires the support of appropriately configured routers and switches.

You can alter these settings globally, for a GhostCast session, and for a task.

For more information, see [“Optimizing data transfer over the network”](#) on page 85 and [“Setting the Symantec Ghost Console options”](#) on page 154.

To set the data transfer mode

- 1 In the Symantec Ghost GhostCast Server window, on the File menu, click **Options**.
- 2 Click **Force Mode**.
- 3 Select one of the following:
 - Multicast: Set the data transfer mode to Multicast.
 - Directed Broadcast: Set the data transfer mode to Directed Broadcast.
 - Unicast: Set the data transfer mode to 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 loading an image, dumping 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.

Limiting network bandwidth is useful in some circumstances. When deciding whether or not to use it, consider the following:

- How do you want to treat other users on the network?
By limiting network bandwidth, you can increase performance on the network for users who are not the intended recipients of image files.
- Does your network hardware support multicasting?
If your network hardware does not support multicasting, then limiting bandwidth is helpful in many situations.

The following table provides a guide to network hardware setups and when you may or may not want to limit 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 the situations in which you should 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 Ghost GhostCast Server window, on the File menu, click **Options**.
- 2 Check **Limit data throughput for**.
If this option is not enabled, then no limit is set.
- 3 In the Loading field, type the maximum MB per minute to set a limit for loading an image.
- 4 In the Dumping field, type the maximum MB per minute to set a limit for dumping an image.

The ideal maximum usage to expect is:

- 100 BaseT: 300 MB per minute
- 10 BaseT: 60 MB per minute

You can also set a limit from the command line.

For more information, see [“GhostCast Server command-line options”](#) on page 195.

Viewing and changing GhostCast Server session options

Details of GhostCast Server sessions are recorded and can be viewed in the Options dialog box. You can also specify session parameters.

To view or record GhostCast Server options

- 1 On the File menu, click **Options**.
- 2 Click **Use a Fixed Multicast Address** to use the multicast address specified.

Addresses in the following range are valid: 224.77.2.0–224.77.255.155. This option should be used by advanced users only.
- 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 Ghost GhostCast Server once the session is completed.
- 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 field, select a log level to set a level of diagnostic GhostCast logging.

For more information, see [“Generating a GhostCast log file”](#) on page 348.
- 7 In the Log File field, type a destination log file location.

Running the Symantec Ghost executable

When using GhostCasting, the client executable, Ghost.exe, loads a GhostCast copy of an image file onto the client computer or dumps an image file onto the GhostCast Server.

The Symantec Ghost client executable runs under DOS and uses a packet driver interface to the network card. The TCP/IP settings are stored in a configuration file named Wattcp.cfg that is located in the directory in which Ghost.exe runs.

As with all Symantec Ghost applications, DHCP, BOOTP, and manual setting of IP addresses are supported.

For more information, see [“Setting up the hardware and transfer methods”](#) on page 325.

Use the Symantec Ghost GhostCast client command-line switches to run Symantec Ghost from the command line or in the GhostCast session.

For more information, see [“Command-line switches”](#) on page 297.

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. Follow the on-screen prompts.

For more information, see [“Cloning disks”](#) on page 215 and [“Cloning partitions”](#) on page 221.

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 contains the following:

- [Running the GhostCast Server for Windows from the command line](#)
- [Running the DOS-based GhostCast Server](#)
- [Starting the GhostCast session](#)
- [GhostCast Server command-line options](#)
- [Creating a DOS boot disk manually](#)

You can run the Symantec Ghost GhostCast Server from the command line by including the appropriate switches with the Windows or PC-DOS versions of the application.

Running the GhostCast Server for Windows from the command line

You can run the Windows-based GhostCast Server from the command line. Use a batch file or third-party scheduler application to start the server.

Syntax

ghostsrv filename session [options]

filename Specifies the path and file name of a disk image file

session Specifies the session name

For more information, see [“GhostCast Server command-line options”](#) on page 195.

Running the DOS-based GhostCast Server

The DOS-based GhostCast Server offers a DOS command-line alternative to the Windows-based GhostCast Server. A DOS boot disk with the DOS GhostCast Server can be created for you using the Ghost Boot Wizard network boot disk option. You can also create a boot disk manually.

For more information, see [“Boot disks with network support”](#) on page 136 and [“Creating a DOS boot disk manually”](#) on page 198.

Dosghsrv.exe provides a command-line interface and uses the same packet driver setup as the GhostCast Client.

For more information, see [“Setting up packet drivers”](#) on page 199.

The TCP/IP settings are configured in Wattcp.cfg (located in the Symantec Ghost directory).

Syntax

DOSGHSRV filename session [options]

filename Specifies the path and name of an image file

session Specifies the session name

For more information, see [“GhostCast Server command-line options”](#) on page 195.

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

- Do one of the following:
 - Click **Start** when all clients have connected.
 - Press any key.

GhostCast Server command-line options

The GhostCast Server command-line switches are listed below.

Switch	Description
-Ncount	Starts the GhostCast transmission after count clients have joined the session.
-Time	Starts sending to session automatically after a specified time (24 hour hh:mm format).
-Ominutes	Starts transmission minutes after last client connection.
-Llevel	Creates a log file specifying log level (E, S, W, I, or A).
-Ffilename	Specifies log file name for the -L option (by default, Ghostlog.txt).
-C	Closes ghostsrv application after GhostCast session completion (Windows only).
-D	Uses dump from client mode (load to client is the default).
-R	Restarts the GhostCast session on completion. Waits for client connections again after GhostCasting is complete.
-P	Specifies partition mode operation. If loading to clients, the partition number must be given. If dumping from client, no partition number is required.
-Ma	Sets the multicast address to a. Addresses between 224.77.2.0–224.77.255.255 are valid.
-DISKnumber	Specifies the client disk number to which to load or create the image file.
-PARTnumber	Specifies the client partition number to which to load 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 loading an image, where xxx is the number of megabytes per minute (Windows only).

Switch	Description
-HDxxx	Sets the maximum amount of bandwidth consumed while dumping an image, where xxx is the number of megabytes per minute (Windows only).
-TTLxxx	Sets the multicasting time to live (Windows only).
-Sxxx	DOS version of -TTL.

Examples using GhostCast Server command-line options

Examples are for GhostCast Server for Windows, but they also apply to the DOS-based GhostCast Server application. Replace ghostsrv with dosghsrv when using the DOS server.

Dumping 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.

Dumping partitions 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.

Loading 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.

For more information, see [“Starting the GhostCast session”](#) on page 194.

Loading 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.

For more information, see [“Starting the GhostCast session”](#) on page 194.

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 ten 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 (Windows only)

```
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 -ferlog.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.

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 client boot disk manually

- 1 If the operating system is DOS/Win9x, 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:\
```

For more information, see [“Setting up packet drivers”](#) on page 199.

- 4 Copy Ghost.exe and Wattcp.cfg to the floppy disk:

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.

For more information, see [“Setting up the hardware and transfer methods”](#) on page 325.

- 6 Edit the Autoexec.bat startup file.

For example:

3c5x9pd.com 0x60

ghost.exe

Add the command line for the packet drive to the Autoexec.bat file.

For more information, see the packet driver documentation.

You can add additional command-line switches to the Ghost.exe command to automate the cloning process.

For more information, see [“Command-line switches”](#) on page 297.

Setting up packet drivers

The DOS-based GhostCast client and server require an ethernet-based or token ring-based packet driver prior to running. The Windows version does not as it uses the host operating system TCP/IP support.

There are several packet driver interface options:

- Network interface card-dependent packet driver.

For more information, see [“To set up a network interface card-dependent packet driver”](#) on page 200.

- 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 GhostCast client.

For more information, see [“To set up an NDIS 2.01 network adapter driver with supplied packet driver shim”](#) on page 201.

- Third-party network adapter driver and packet driver shim. These have not been tested or documented with the Symantec Ghost 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).

Do not use the Network Client Administrator from Windows NT 4 or the Microsoft Network Client Installation program to create a GhostCast boot disk 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.

The command-line arguments vary slightly from driver to driver.

- 3Com 590 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 Symantec Ghost GhostCasting installation files. Extract these configuration files and edit as shown.
- 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.

Your directory or floppy disk should contain the following 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
Drvspace.bin (hidden)		Protman.exe
		*.dos

- Delete drvspace.bin to provide more space on the boot disk.
- 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).

Sample protocol.ini file

```
[PROTMAN]
drivename = PROTMAN$
[PKTDRV]
drivename = PKTDRV$
bindings = PC_CARD
intvec = 0x60
chainvec = 0x66
[PC_CARD]
drivename = 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 3Com 509 card then change the driver name to:

```
drivename = 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 3Com 509 card lets you optionally specify the IO Base address:

```
[PC_CARD]
drivename = ELNK3$
IOADDRESS = 0x300
```

Sample Config.sys file

```
device=protman.dos /I:\
device=dis_pkt.dos
device=pnwnd.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
```


Sample Autoexec.bat file

```
prompt $p$g  
netbind
```

NETBIND binds the NDIS drivers together and installs the packet driver interface.

GhostCasting and IP addresses

This chapter contains the following:

- [Introducing IP addresses for GhostCasting](#)
- [Locally specified IP addresses](#)
- [Using BOOTP/DHCP to assign IP addresses](#)

Introducing IP addresses for GhostCasting

For GhostCasting to make initial contact with a computer, the computer must have a unique IP address. Associated with an IP address is a subnet mask. The subnet mask indicates the range of IP addresses that are accessible by the computer. Each of these accessible computers becomes a member of the local subnet. If the address of another computer is outside the range of IP addresses specified by the subnet mask, then this computer is on a different subnet.

To communicate with a computer on a different subnet, the local computer sends the information to the default gateway. The default gateway forwards information to the correct receiver. The default gateway of a computer must be on the same subnet as that computer.

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 system

Locally specified IP addresses

An IP network using locally specified addresses requires each manually setup computer to have:

- A unique IP address
- The correct subnet mask
- The default gateway (optional)

The Windows Symantec Ghost 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.

The DOS-based GhostCast Server and clients receive their IP addresses, subnet masks, and default gateways from the configuration file named `Wattcp.cfg` that is usually located in the Symantec Ghost directory.

If you use a DOS boot disk to start GhostCasting with locally specified IP addresses, each computer requires a different `Wattcp.cfg` file to be specified to ensure that every boot disk for each workstation is unique.

Examples of `Wattcp.cfg` client configuration files

Windows 95 computer #1 running the Windows GhostCast Server application, `Ghostsrv.exe`

IP address: 192.168.100.10

Subnet mask: 255.255.255.0

Default gateway: 192.168.100.1

Uses Windows TCP/IP stack configuration so there is no need for a `Wattcp.cfg` file.

DOS computer #2 running Ghost.exe

IP address: 192.168.100.3

Subnet mask: 255.255.255.0

Default gateway: 192.168.100.1

DOS computer #2 Wattcp.cfg file includes

IP = 192.168.100.3

NETMASK = 255.255.255.0

GATEWAY = 192.168.100.1

DOS computer #3 running Ghost.exe

IP address: 192.168.100.44

Subnet mask: 255.255.255.0

Default gateway: 192.168.100.1

DOS computer #3 Wattcp.cfg file includes

IP = 192.168.100.44

NETMASK = 255.255.255.0

GATEWAY = 192.168.100.1

Any address other than 192.168.100.0–192.168.100.255 is on another subnet and must be passed on to the default gateway (192.168.100.1 in this example).

If the server and client are within the same subnet, a default gateway is not required.

Using BOOTP/DHCP to assign IP addresses

If a BOOTP or DHCP server is installed on the network, you may take advantage of Dynamic Host Configuration Protocol (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 Symantec Ghost 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. Symantec Ghost GhostCasting supports the automatic, or remote, definition of IP addresses and network parameters using BOOTP and DHCP systems.

You must run the BOOTP or DHCP server on the network to use BOOTP or DHCP to specify a computer's IP address. This 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.

Examples of BOOTP/DHCP defined addresses

Windows NT 4.0 server #1 running GhostCast Server, Ghostsrv.exe, and DHCP server

IP address: 172.16.5.10
Subnet mask: 255.255.255.0
Default gateway: 172.16.5.1

DOS computer #2 running Ghost.exe

IP address: supplied via DHCP
Subnet mask: supplied via DHCP
Default gateway: supplied via DHCP

The Wattcp.cfg file for DOS computer #2 is empty or does not exist because Symantec Ghost GhostCasting defaults to using BOOTP and DHCP if no locally specified network TCP/IP parameters are supplied.

DOS computer #3 running Ghost.exe

IP address: supplied via DHCP
Subnet mask: supplied via DHCP
Default gateway: supplied via DHCP

The Wattcp.cfg file for DOS computer #3 is empty or does not exist because Symantec Ghost GhostCasting defaults to using BOOTP and DHCP if no locally specified network parameters are supplied.

The controlling element for DHCP is the DHCP server that serves the requests of clients and ensures that no duplicate IP addresses exist on the network. Since many DHCP servers can be placed on a network, avoid duplicate address generation and its problems. This is equally true for BOOTP servers.

4

C l o n i n g i m a g e f i l e s l o c a l l y

- Symantec Ghost as a standalone program
- Standalone configuration

Symantec Ghost as a standalone program

This chapter contains the following information:

- [Starting the Symantec Ghost executable](#)
- [Navigating without a mouse](#)
- [Cloning disks](#)
- [Cloning partitions](#)
- [Saving an image file to a CD-R/RW](#)
- [Adding switches to your cloning task](#)
- [Creating a DOS boot disk](#)

You can run the Symantec Ghost executable as a standalone program to copy disks or partitions from one computer to another. Images can be dumped to an image file, which is loaded back onto a computer at any time.

Starting the Symantec Ghost executable

The Symantec Ghost executable is a DOS-based application and should run in DOS mode outside of Windows, if possible. If you run the Symantec Ghost executable (Ghost.exe) within Windows 95/98/Me, note the following:

- Files may be in an open or changing state. If these files are cloned, the resulting destination files are left in an inconsistent state.
- The partition on which Windows is installed must not be overwritten.
- If you overwrite a drive or partition, the system must be restarted.
- GhostCasting is not available.

- Ghost.exe does not automatically restart the system.
- Hard disk sizes may appear smaller than their actual sizes. The Symantec Ghost executable can only access the shown destination size. The remaining space is not used.
- The Symantec Ghost executable fails if you try to overwrite any of the following:
 - Windows swap files
 - Registry files
 - Open files

You cannot run Symantec Ghost within Windows NT, Windows 2000/XP, Linux, OS/2, or other nonDOS operating systems. To run Symantec Ghost on a computer running a nonDOS operating system, use a Ghost boot disk.

To start the Symantec Ghost executable

- Do one of the following:
 - At the DOS prompt, type:
C:> \progra~1\symantec \ghost\ghost.exe
 - Start the computer using a DOS boot disk.

You can create a DOS boot disk on a computer running Windows or DOS. Running Symantec Ghost in DOS may require additional DOS drivers to let Symantec Ghost access and use some hardware.

For more information, see [“Creating boot disks and boot images”](#) on page 134.

Navigating without a mouse

If you have mouse drivers loaded, you can use the mouse to navigate in Symantec Ghost. You can also use the keyboard.

- Use arrow keys to navigate the menu.
- Press Tab to move from button to button.
- Press Enter to activate the selected button.
- Press Enter to select an item in a list.

Using Ghost.exe on a standalone computer

You can use Ghost.exe to clone disks and partitions, and to load image files. This is an overview of the process of using Ghost.exe.

To use Ghost.exe on a standalone computer

- 1 Start the Symantec Ghost executable.
Add command-line switches, if necessary.
For more information, see [“Command-line switches”](#) on page 297.
- 2 Select the transfer method.
- 3 Select the Symantec Ghost operation.
- 4 Do one of the following:
 - Select the source hard drive and partitions.
 - Select the image file.
- 5 Do one of the following:
 - Select the destination hard drive and partition.
 - Select the image file.

Make sure that you select the correct destination to overwrite. In most cases, you cannot recover data from an incorrectly selected destination drive.
- 6 Complete the cloning operation.

Cloning disks

You access disk cloning procedures from the main menu. You can specify one of the following transfer methods:

- Local
- LPT > Master
- USB > Master
- TCP/IP > Master

By default Symantec Ghost tries to maintain the same size ratio between the new disk partitions. However, you should note the following:

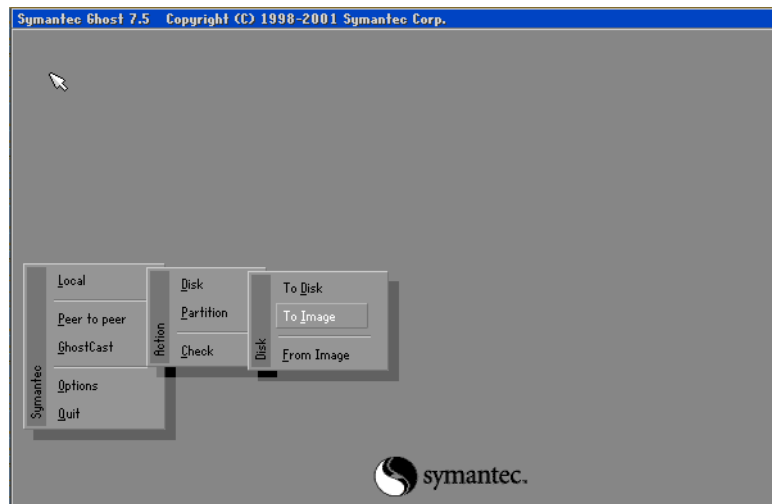
- You can change the size of any destination FAT, NTFS, or Linux Ext2 partition by entering the new size in megabytes.
- You cannot enter a value that exceeds the available space, is beyond the file system's limitations, or that is not large enough to contain the data held in the source partition.

Cloning disk to disk

When you clone disk to disk, Symantec Ghost copies the contents of one hard disk onto another.

To clone disk to disk

- 1 On the Symantec Ghost main menu, click **Local > Disk > To Disk**.



- 2 In the Source Drive dialog box, select the source drive.
The Source Drive dialog box shows the details of every disk that Symantec Ghost finds on the local computer.
- 3 In the Destination Drive dialog box, select the destination drive.
Choose carefully as this is the disk that will be overwritten.
If a peer-to-peer connection method is used, the destination drive will 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 or change the destination drive partition layout.
The Destination Drive Details dialog box shows a suggested partition layout for the destination drive.
- 5 Click **OK**.
- 6 When the “Proceed with Disk Clone?” question appears, check the details and ensure that the correct options are selected.
- 7 Do one of the following:
 - Click **Yes** to proceed with the disk cloning.
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.

Warning: Only click **Yes** if you are sure that you want to proceed. The destination drive is overwritten with no chance of recovering any data.

- Click **No** to return to the menu.
- 8 Restart the computer.

Warning: You should remove the second hard drive before you restart your computer. If you leave the second drive in the computer, damage can occur to both of the bootable operating systems.

- 9 Run Symantec Disk Doctor, ScanDisk, or a similar utility to verify the integrity of the destination disk.

Cloning a disk to an image file

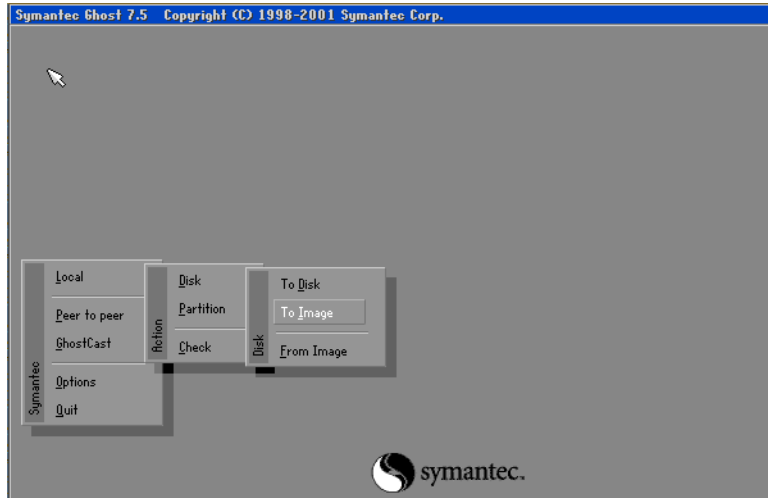
You can copy an image file to another disk or use the image file as a backup file.

When using peer-to-peer connections, the image file is created on the slave computer.

If you write the image file to a CD, you can make the CD bootable. If a boot disk is placed in the floppy drive before the cloning session begins, Symantec Ghost copies the system files from the boot disk onto the CD.

To clone a disk to an image file

- 1 On the Symantec Ghost main menu, click **Local** > **Disk** > **To Image**.



- 2 In the Source Drive dialog box, select the source drive.
The Source Drive dialog box shows details of every disk that Symantec Ghost finds on the local computer.
- 3 In the File Locator dialog box, type the image file destination and name.
The image file may reside on either a locally mapped network file server or a local drive (but not the one from which it is being copied). Local drives include writable CD, tape, ZIP, JAZ, and LS120 Superdisk drives.
- 4 In the Image file description dialog box, type a description of the image file.
You can modify this description on the Symantec Ghost Console or in Ghost Explorer.
- 5 Click **Save**.
- 6 When the "Compress Image File?" question appears, do one of the following:
 - Click **No** for no compression (high speed).
 - Click **Fast** for low compression (medium speed).
 - Click **High** for high compression (slower speed).

For more information, see ["Image files and compression"](#) on page 162.

- 7 When the “Proceed with Image File Creation?” question appears, check the details and ensure that the correct options have been selected.
- 8 Do one of the following:
 - Click **Yes** to proceed with the image file creation.

The system performs an integrity check of the file structure on the source disk and then copies the source disk to the destination image file. If you need to abort the process, press **Ctrl-C**, but be aware that this leaves the destination image file in an unknown state.
 - Click **No** to return to the menu.
- 9 On the main menu, click **Check > Image File** to verify the integrity of the image file.

Cloning a disk from an image file

You can load a copy of one disk to another disk using a previously created image file.

To clone a disk from an image file

- 1 On the main menu, click **Local > Disk > From Image**.
- 2 In the File Locator dialog box, type the path and file name of the image file.
- 3 Select the drive or device.
- 4 Select the full path name.

The image file may reside on either a locally mapped network file server or a local drive (but not the one to which it is being copied). When using peer-to-peer connections, the file is located on the slave computer.

- 5 Press **Enter**.
- 6 In the Destination Drive dialog box, select the destination drive.

Choose carefully as this is the disk that will be overwritten.

The Destination Drive dialog box shows the details of every drive that Symantec Ghost finds on the local computer. If you are copying from the local computer, the disk containing the source image file is not available for selection.

- 7 In the Destination Drive Details dialog box, confirm or change the destination drive partition layout.

The Destination Drive Details dialog box shows a suggested partition layout for the destination drive. By default, Symantec Ghost tries to maintain the same size ratio between the new disk partitions.

However, you should note the following:

- You can change the size of any target FAT, NTFS, or Linux Ext2 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 partition.

- 8 Click **OK**.

- 9 Do one of the following:

- Click **Yes** to proceed with the disk cloning.

Symantec Ghost creates the destination drive using the source image file drive details. If you need to abort the process, press **Ctrl-C**, but be aware that this leaves the destination drive in an unknown state.

Warning: Only click **Yes** if you are sure that you want to proceed. The destination drive is completely overwritten with no chance of recovering any data.

- Click **No** to return to the menu.

- 10 If spanning is enabled, do one of the following:

- Click **OK** to continue on the same form of media.
- Click **Filename** to restore from a different location, then type the location and file name of the image file span.

- 11 Restart the computer when the disk image load is complete.

Run Symantec Disk Doctor, ScanDisk, or a similar utility to verify the integrity of the destination drive.

Cloning partitions

You access partition cloning procedures from the main menu. You can select to transfer with one of the following methods:

- Local
- LPT > Master
- USB > Master
- TCP/IP > Master

Cloning from partition to partition

You can directly clone from one partition to another.

To clone from partition to partition

- 1 On the main menu, click **Local > Partition > To Partition**.
- 2 In the Source Drive dialog box, select the source drive.
The Source Drive dialog box shows details of every drive that Symantec Ghost 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 drive.
- 4 In the Destination Drive dialog box, select the destination drive.
The Destination Drive dialog box shows the details of every disk that Symantec Ghost 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 drive. 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?” question appears, ensure that the correct options have been selected.

This is the last chance to back out.

- 8 Do one of the following:

- Click **Yes** to proceed with the partition copy.

If you need to abort the process, press **Ctrl-C**, but be aware that this leaves the destination drive in an unknown state.

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.

- Click **No** to return to the menu.

- 9 Restart the destination computer when the partition copy is complete. Run Symantec Disk Doctor, ScanDisk, or a similar utility to verify the integrity of the destination partition.

Cloning 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.

The image file may reside on a mapped network drive or a local drive with a FAT filesystem (but not the one from which it is being copied). Local drives include writable CD, tape, ZIP, JAZ, and LS120 Superdisk drives.

When using peer-to-peer connections, the image file is created on the slave computer.

If you write the image file to a CD, you can make it bootable. If a boot disk is placed in the floppy drive before the cloning session begins, Symantec Ghost copies the system files from the boot disk onto the CD.

Compression may affect the speed of operations. When you select a compression level, Symantec Ghost estimates the amount of space available for the destination image file. If there is insufficient space, Symantec Ghost prompts you to enable spanning of image files.

To clone a partition to an image file

- 1 On the main menu, click **Local > 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 Symantec Ghost 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 drive. Multiple partitions may be selected.
- 4 Click **OK**.
- 5 In the File Locator dialog box, select the image file.
- 6 Do one of the following:
 - Type the path and file name for the disk image file.
 - Click **Browse** to locate the image file.
- 7 Press **Enter**.
- 8 In the Compress Image? dialog box, do one of the following:
 - Click **No** for no compression (high speed).
 - Click **Fast** for low compression (medium speed).
 - Click **High** for high compression (slower speed).
- 9 If spanning is enabled, click **Yes** and type the location of the next span of the image file.

For more information, see [“Image files and volume spanning”](#) on page 164.
- 10 In the Proceed with Partition Dump? dialog box, ensure that the correct options have been selected.

11 Do one of the following:

- Click **Yes** to proceed with the image file creation.

The system performs a quick integrity check of the file structure on the source partitions and then copies the source partitions to the destination image file. If you need to abort the process, press **Ctrl-C**, but be aware that this leaves the destination image file in an unknown state.

- Click **No** to return to the menu.

12 On the main menu, click **Check > Image File**.

After the image file has been created, Symantec Ghost can verify the integrity of the image file.

Cloning a partition from an image file

Once you have created an image file, you can clone the partition onto another partition on another computer using the image file.

To clone a partition from an image file

1 On the main menu, click **Local > 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 either a locally mapped network file server volume or a local drive. When using peer-to-peer connections, the image file is located on the slave computer.

3 Press **Enter**.

4 In the Source Partition dialog box, select the source partition for 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 drive.

The Destination Drive dialog box contains the details of every disk that Symantec Ghost 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 drive. 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.

- 7 In the Proceed with Partition Load? dialog box, ensure that the correct options have been selected.
- 8 Do one of the following:

- Click **Yes** to proceed with the partition cloning.

Symantec Ghost 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.

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.

- Click **No** to return to the menu.

- 9 If spanning is enabled do one of the following:

- Click **OK** to continue on the same form of media.
- Click **Filename** to restore from a different location, then type the location and file name of the image file span.

- 10 Restart the destination computer when the partition copy is complete. Run Symantec Disk Doctor, ScanDisk, or a similar utility to verify the integrity of the destination partition.

Saving an image file to a CD-R/RW

You can save an image file directly to a CD-R or CD-RW. You can also make the CD bootable.

For more information, see [“Image files and CD writers”](#) on page 168.

To save an image file to a bootable CD-R/RW, you must do the following:

- Create Ghost boot disks.
- Start your computer.
- Create and save the image file.

When writing an image file directly to a CD-R/RW, note the following:

- The CD-R/RW drive must be compatible with Symantec Ghost.
For more information, see [“Image files and CD writers”](#) on page 168.
- Symantec Ghost automatically spans CD-R/RW disks if necessary. You do not need to use a spanning switch on the command-line.

Create Ghost boot disks

To write an image file directly to a CD, you must have a boot disk with which to start the computer. In the Ghost Boot Wizard, create a boot disk, using the Boot Disk with CD-R/RW, LPT and USB Support option. This creates a boot disk that contains the Ghost executable and DOS system files.

For more information, see [“Standard boot disks with the option of LPT and USB support”](#) on page 135.

To make the CD bootable, you must have a second boot disk. This boot disk is created in the Ghost Boot Wizard, using the CD-ROM Boot Disk option. This option creates a boot disk that contains the CD-R/RW driver files.

For more information, see [“Boot disks with CD-ROM support”](#) on page 140.

Start your computer

Insert the first boot disk you created into the computer's floppy disk drive and restart the computer.

Create and save the image file

Create an image of the computer, choosing the CD-R/RW drive as the destination drive.

For more information, see [“Cloning a disk to an image file”](#) on page 217.

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. When prompted for the required files, insert the second boot disk that you created using the Ghost Boot Wizard into the computer's floppy disk drive.

Adding switches to your cloning task

When defining a cloning task, you can include a number of options (or switches) that are usually entered via the command-line.

To add switches to your cloning task

- 1 On the main menu, click **Options**.
- 2 On the following tabs, select the options to include in your current cloning task:

Tab	Command-line options
Span/CRC	-span, -auto, -cns, -crcignore, -fcr
FAT 32/64	-f32, -f64, -fatlimit, -fnw
Misc	-sure, -fro, -rb, -fx
Image/Tape	-ia, -ib, -id -tapebuffered, plus options to: make safe, unbuffer, and eject the tape
HDD access	-ffx, -fnx, -ffi, -fni, -ffs, -fns
Security	-pwd, -locktype=type

For more information, see [“Command-line switches”](#) on page 297.

- 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.

Creating a DOS boot disk

Symantec Ghost is a DOS-based application that should run in DOS mode outside of Windows. On some systems, such as Windows NT, Windows 2000, and other nonDOS operating systems, a DOS boot disk must be used to start the system to let Symantec Ghost operate. Additional DOS drivers may be required to let Symantec Ghost access local or network hardware. The configuration files on a DOS boot disk can be altered to load these drivers.

You only need to create a DOS boot disk if you are using Symantec Ghost without GhostCasting, TCP/IP, or peer-to-peer connections.

To create a DOS boot disk for Symantec Ghost within Windows 95/98

- 1 Insert a blank floppy disk into drive A of a Windows 95/98 computer.
- 2 Double-click **My Computer**.
- 3 Right-click the floppy disk drive, then click **Format**.
- 4 Click **Copy System Files**.
- 5 Copy **Ghost.exe** onto the boot disk.

For example:

```
C:\> copy c:\progra~1\symantec\ghost\ghost.exe a:\
```

- 6 Set up any drivers required for the transfer method.

To create a DOS boot disk for Symantec Ghost in DOS

- 1 Insert a blank floppy disk into drive A of a DOS (Windows 9x) computer.
- 2 Format the floppy disk.
- 3 At the DOS command prompt, type the following:

```
C:\> sys c: a:
```

This copies the system files onto the floppy disk.

- 4 Copy **Ghost.exe** onto the boot disk.

For example:

```
C:\> copy c:\progra~1\symantec\ghost\ghost.exe a:\
```

- 5 Set up any drivers required for the transfer method.

Standalone configuration

This chapter contains the following:

- [Introducing the standalone configuration](#)
- [Generating the configuration data file](#)
- [Running the standalone configuration](#)

Introducing the standalone configuration

Use the standalone configuration feature to apply configuration settings to a computer directly. This lets you run a post clone configuration without the Symantec Ghost Console.

There are some differences between the standalone configuration and the post clone configuration from the Console. The differences are as follows:

- Standalone configuration allows the addition of Microsoft Windows NT/XP/2000 computers to a domain. However, you must create the computer account on the domain before using the standalone configuration. For the computer account to work, you must first add security permissions for Windows 2000 and Windows XP native mode Active Directory domain controllers.
- Standalone configuration supports an extra option to disable itself after running. This works on standalone client installations only, and disables the standalone configuration from running on that computer after it is run the first time. To use the standalone configuration again on that computer, you must uninstall and reinstall the standalone configuration client.

The steps involved in the process of standalone configuration are as follows:

- 1 Install the Symantec Ghost standalone or Console client on the target computer.
For more information, see [“Installing the standalone configuration client”](#) on page 41.
- 2 Write a program to generate the configuration data file.
For more information, see [“Generating the configuration data file”](#) on page 230.
- 3 Run the program to generate the configuration data file.
- 4 Apply the configuration data file to the target computer.
For more information, see [“Running the standalone configuration”](#) on page 231.

Generating the configuration data file

To generate the configuration data file, you must write a program that calls MachConf.dll, the .dll file supplied by Symantec Ghost. MachConf.h lists the settings and values required for creating a configuration data file.

The following example files on which to base your program are included:

- Genghostfile.cpp
- Genghostfile.dsp
- Genghostfile.dsw
- StdAfx.cpp
- Stdafx.h
- MachConf.h

All of the example program files, .dll files, and Help files are on the Symantec Ghost CD in the following directory:

`\Extras\Source\Genghostfile`

Running the standalone configuration

If you are using Ghost.exe to clone a computer, you can use the -replace switch to run the configuration data as you perform the clone. The image file must include either the standalone or Console client.

To run a standalone configuration using Ghost.exe

- 1 Ensure that the data configuration file is available on the target computer.
For example, on a floppy disk.
- 2 Clone the computer using the -replace switch to replace the existing configuration file with the one that you generated.

For example:

```
ghost -replace:gvpcfg.bin=a:\gvpcfg.bin
```

When the computer is restarted, the configuration data file is processed and the configuration data is applied to the computer.

You can also run the standalone configuration without using Ghost.exe.

To run a standalone configuration without using Ghost.exe

- 1 Copy the data configuration file into the root directory of the system drive as follows, overwriting the existing data file:
 - For Microsoft Windows 9x computers: c:\
 - For Microsoft Windows NT/2000/XP computers: %systemdrive%\
- 2 Restart the computer.

The configuration data file is processed and the configuration data is applied to the computer.

Errors logged during a standalone configuration

Any errors generated during the standalone configuration are logged as follows:

- Microsoft Windows NT/XP/2000: Event log
- Microsoft Windows 9x/Me: Error file, c:\lastpostconfigurationstaus.txt

5

C r e a t i n g e x e c u t a b l e s t o r o l l o u t a p p l i c a t i o n s

- [Getting started with AutoInstall](#)
- [Creating AI packages](#)

Getting started with AutoInstall

This chapter contains the following:

- [How AutoInstall works](#)
- [Using AutoInstall](#)
- [Installing Microsoft products using AutoInstall](#)

How AutoInstall works

Symantec Ghost AutoInstall (AI) reduces the time and cost of managing software distribution across a network by providing an efficient means of installing application packages and updates. Once installed, these packages can be removed quickly using the AutoInstall applications.

AutoInstall captures changes to a single Windows computer that you can then deploy across a network. For example, you can capture changes to files, registry entries, or entire application suites and deploy the changes using the Symantec Ghost Console software.

AutoInstall, in conjunction with the Symantec Ghost Console, simplifies and streamlines the process of implementing workstation updates. AutoInstall lets you create a comprehensive software install AI package that you can deploy to workstations via the Symantec Ghost Console.

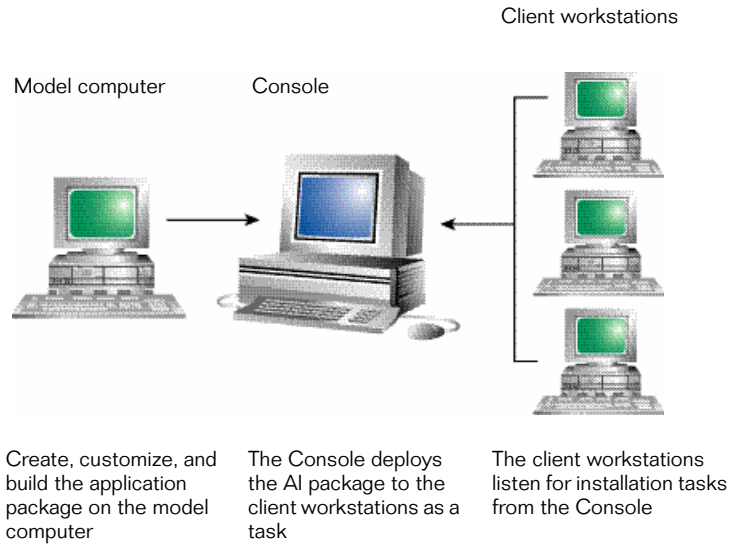
Symantec Ghost AutoInstall has two components to help you create and customize AI packages. AI Snapshot creates an installation script that records the changes to a model computer when software is installed. AI Builder uses the installation script to create a package that duplicates the changes made by the software installation. AI Builder also lets you customize the package to meet your needs. Once created, packages can be modified using AI Builder.

Using AutoInstall

To use AutoInstall you must perform the following procedures:

- 1 Install AI Builder on the Console server.
AI Builder is included in the Corporate Console installation.
- 2 Install AI Snapshot and AI Builder on the model computer.
- 3 Capture existing system information.
- 4 Install the software that you would like to deploy.
- 5 Capture system information again to determine changes.
- 6 Use AI Builder to build and save the file created by AI Snapshot as an executable AI package. You can also use AI Builder to customize the installation script, prior to building, or after building the executable, if necessary.
- 7 Use the Symantec Ghost Console to deploy the AI package to target workstations.

For more information, see [“Creating AI packages”](#) on page 241.



Installing AI Snapshot and AI Builder on the model computer

Before you can create an AI package, you must set up a model computer with AI Builder and AI Snapshot installed.

Choose a computer that has a similar configuration to those that will receive the finished AI package. Ideally, this computer should have only the operating system installed and have network support to connect to the Console.

To install AI Snapshot and AI Builder on the model computer

- 1 Insert the Symantec Ghost installation CD-ROM into the CD-ROM drive.
- 2 In the list of options, click **Install AI Snapshot**.
- 3 Click **Next**.
- 4 Type the location in which you would like to install AutoInstall.
- 5 Click **OK**.

Setting up target computers

The AutoInstall client program is installed as part of the Symantec Ghost client software.

For more information see [“Installing the Console client”](#) on page 39.

Once installed, the client program runs in the background on client computers, ready to launch installation tasks when they are deployed from the server.

Installing Microsoft products using AutoInstall

There are some issues you may need to consider when using AutoInstall to install Microsoft software.

Letting the model computer restart

If you use AI Snapshot to create an installation script to include in an AI package executable, you must capture system information and build the executable AI package before letting the computer restart. If you are installing software that is not Microsoft, then you can allow restarts and configure the application before performing the comparison scans and building the AI package.

Adding uninstall commands

You can add an AutoInstall uninstall command to an AI package if you are deploying software that is not Microsoft software. You must add the uninstall to the AI package by modifying the installation script before building the AI package executable. This feature does not work with Microsoft products due to limitations of having to build the AI package before any restarts.

Using AutoInstall to clone Office XP

Due to the new Product Activation feature in Microsoft Office XP, you must stop Office XP from locking to the model computer before cloning. By using Microsoft Office Installer commands, you can prevent the hardware detection and activation process from occurring until Office XP is deployed to the client computers and launched for the first time.

To install Office XP using AutoInstall, you must complete the following process:

- 1 Download 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>

- 2 Install AI Snapshot.
- 3 Start AI Snapshot and perform the first system scan.
- 4 Run Office XP setup using the following command line:
driveletter:\Setup.exe enterprise_image="1" nusername="1"
pidkey="[Enter your Volume License key here]"/qb
- 5 Apply the Microsoft patch for enterprise deployments specified in the Microsoft Knowledge Base article number Q304226.
- 6 Perform a system compare and build the package.
Do not let the computer restart after installing Microsoft Office XP and the patch.

Note: You must have a Volume License Key from Microsoft to perform this installation.

Microsoft system file protection (SFP) limitations on deploying AI packages

There are some issues to consider when you are rolling out software that contains files used by Windows Me/2000/XP. Do not turn off the system file protection as it may cause corruption or the loss of necessary operating

system files. Do not clone or deploy software containing operating system updates.

Operating system	Software that contains operating system updates
Windows Me	<ul style="list-style-type: none">■ An Internet Explorer version that is later than the one that came with the operating system■ Any application that installs a later version of Internet Explorer
Windows 2000	<ul style="list-style-type: none">■ Service packs■ Operating system hot fixes■ An Internet Explorer version that is later than the one that came with the operating system■ Any application that installs a later version of Internet Explorer
Windows XP	<ul style="list-style-type: none">■ An Internet Explorer version that is later than the one that came with the operating system■ Any application that installs a later version of Internet Explorer

Creating AI packages

This chapter contains the following:

- [Creating an installation script for a software installation](#)
- [Customizing and building AI packages](#)
- [Executing and rolling out AI packages](#)

Creating an installation script for a software installation

Creating the installation script, `Install.cfg`, involves a number of steps. First, AI Snapshot captures computer information before the software is installed. Then you install the software, and AI Snapshot captures the computer information again. Finally, AI Snapshot creates the `Install.cfg` file that notes the differences.

Note: If you are going to install the software on the model computer using Microsoft Installer, make sure that Microsoft Installer is not installed before the first snapshot is taken.

Capturing existing system information

The first step in creating an installation script is to prepare the model computer and run AI Snapshot to capture existing system information.

When installing software, the model computer should have only the operating system installed.

To take a snapshot of the model system

- 1 Disable any programs that are running in the background.
- 2 If the installation process includes a restart, disable any programs that execute during the restarting process.
- 3 On the Windows taskbar, click **Start > Programs > Symantec Ghost > AI Snapshot**.
- 4 Click **Options**.

You can restrict the disks and directories that are monitored on the target platform. If you monitor only the disks affected by the installation, the monitor process goes faster. For example, if the installation affects the C drive, you don't need to monitor drive D.

You can also change the default working directory at this time. AI Snapshot automatically purges the working directory at regular intervals, except for the resulting installation packages.

- 5 Change the Search Path or Temporary Work Directory, if desired.
- 6 Click **OK**.
- 7 Click **Next** to let AI Snapshot start analyzing the system.

When AI Snapshot finishes analyzing your system, the Start Your Installation screen appears.

The next step is to install the software that you would like to package.

Installing the software that you would like to package

After you take a snapshot of the model system, install the software that you would like to package while AI Snapshot is still running.

Warning: For a Microsoft installation, it is important that you let AI snapshot perform a complete scan of the computer by cancelling all restarts until the build is completed.

To monitor the software installation

- 1 On the Start Your Installation screen, do one of the following:
 - Type the path to the software's installation program (usually named Setup.exe).
 - Click **Browse** and navigate to the file.
- 2 Click **Monitor**.



- 3 During the installation, select the options that you want to install on the target workstations.

Some installation programs launch slowly and have long pauses between screens.
- 4 Do one of the following:
 - For a Microsoft installation, cancel all restarts by clicking **No** or pressing **Ctrl-Esc** to regain control of the computer until the build is completed.
 - For all other installations, restart the computer if the installation requires it.
- 5 Click **AI Snapshot**.

- 6 Click **Yes** when prompted to build the setup program.
- 7 Type a name for the installation package when the software installation is complete.

The default name is INSTALL.

If you are installing the software from an autorun CD, the initial installation steps are automatically performed.

To monitor the software installation from an autorun CD

- 1 On the Start Your Installation screen, click **Next**.
- 2 Insert the autorun CD into the CD-ROM drive.
- 3 Click **Yes** when prompted to build the setup program.
- 4 Type a name for the installation package when the software installation is complete.

The default name is INSTALL.

Capturing system information again to determine changes

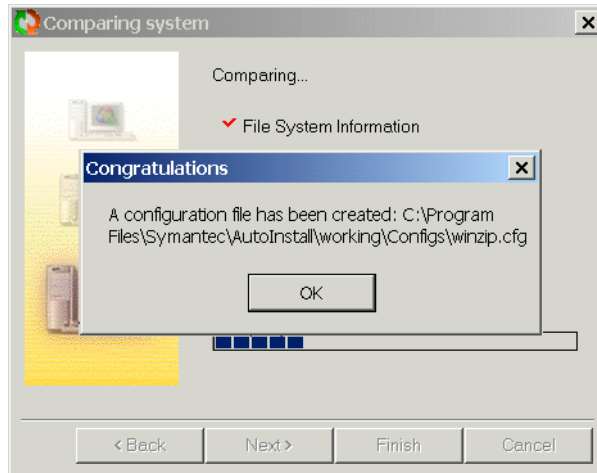
The next step in the installation script process is to take another snapshot of the model computer.

To take another snapshot of the model computer

- 1 In the Is Software Installation Complete window, click **Compare** for AI Snapshot to check the new configuration against the original configuration.

AI Snapshot places references to the differences, such as new files and directories, groups and icons, and modifications to the System Registry, in the installation script. When the comparison is complete, the location of the installation script appears.

- 2 Click **OK** when the installation script file name appears.



- 3 Do one of the following:
 - Click **Build** to let AI Builder make an AI package from the installation script as it stands.
A message appears showing the package progress and file location.
 - Click **Modify** to customize the installation script.
For more information, see [“Customizing and building AI packages”](#) on page 245.
Once the installation script has been modified, the package should be built before any changes are made to the model computer.
- 4 Click **Finish**.

Customizing and building AI packages

AI Builder uses the installation script created by AI Snapshot to build an AI package that can be customized to meet your needs. For example, you can add a specialized splash screen to the package, or customize a lengthy installation process to run automatically without user interaction. Once a package has been created, you can use AI Builder to modify and rebuild the package.

The installation script is an ASCII text file that can be read by AI Builder, a text editor. The commands in the installation script dictate how the software is installed.

AI Builder integrates graphics, sound, and animation so that your installations look professional. It includes messages and questions and allows .ini file and registry editing.

The checklist interface guides you through the required steps. Installations can test for CPU, RAM, and video configurations. You can use If statements to adapt to individual configurations. AI Builder creates a wizard interface for AI packages that can be run by the client. It cannot be deployed by the console.

Extra lines are ignored, so you can add them for readability. However, extra spaces and carriage returns should not be added as they cause syntax errors. You can use the REM command to add remarks to any line. The text on that line is ignored by AI Builder even if it is a valid command. This is useful for documenting your installation script.

AI Snapshot does not automatically add the uninstall command to a replicated application. You can include this option by selecting the Uninstall command in AI Builder.

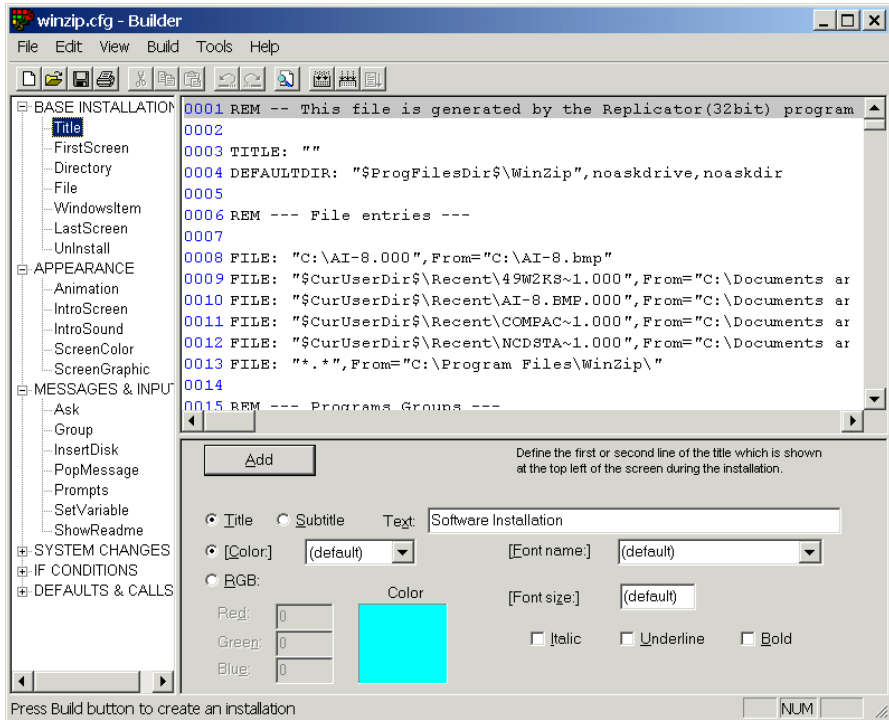
For more information, see [“To include an uninstall command in a build package”](#) on page 249.

For troubleshooting purposes, AI Builder uses error messages for invalid commands in the installation script. AI Builder gives you the line number of the invalid command, along with the contents of the line. For example, if you use a BEGIN command and forget to include the END command, an error message appears with the last line of the .cfg file.

Use AI Snapshot or AI Builder to generate the AI package to avoid any syntax errors that may result from using other text editors. Once a package has been generated, you can use the Run option on the Build menu to test the installations that you created.

Customizing installation scripts

Installation scripts can be modified as soon as they have been created. They can also be modified after the AI package has been built by opening the package in AI Builder. In both cases the following screen appears.



The customizing options appear in the left pane, and details of the selected option appear in the bottom right pane. The installation script is in the top right pane.

This table outlines the command types that are available in AI Builder.

Command type	Description
Base Installation	<p>Defines how the installation begins.</p> <p>For example, select WindowItem to add, remove, or replace items within a program group.</p>
Appearance	<p>Defines how the installation appears to the user.</p> <p>For example, select IntroScreen to display a graphic when the installation begins.</p>
Messages & Input	<p>Adds messages that require user input.</p> <p>For example, select Prompts to change the messages that display during the installation.</p>
System Changes	<p>Makes changes to Windows during the installation.</p> <p>For example, select Registry/BeginRegistry to insert or delete items in the Windows registry.</p>
If Conditions	<p>Lets you include If statements for unattended installations.</p> <p>For example, select MemoryO to check a memory value during the installation.</p>
Defaults & Calls	<p>Set up defaults and include calls to external programs.</p> <p>For example, select RunAtExit to run an external program at the end of the installation.</p>

To customize an installation script

- Do one of the following:
 - In AI Snapshot click **Modify** if you have just created an installation script.
 - In AI Builder select an AI package that you want to modify.
- In the left pane of the AI Builder window, expand a command type.

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.
- Select a command.

- 4 In the right pane of the AI Builder window, enter the parameters for the selected command.

For more information about AI Builder commands, consult the online Help file.
- 5 Do one of the following:
 - Click **Add** to add a command.
 - Click **Remove** to remove a command.
- 6 Repeat steps 1 through 5 until the installation script is completed.
- 7 Build the AI package.

For more information, see [“Building AI packages”](#) on page 250.

Adding an uninstall command to the installation script

The uninstall program is placed in the default directory and a hidden file, Uninstall.cfg, is created that captures the changes made during the installation. Successive installations modify the Uninstall.cfg file so that the uninstall program returns the system to the state before the first installation.

To include an uninstall command in a build package

- 1 In the left pane of the builder options, expand **BASE INSTALLATION** and then click **UnInstall** to include an uninstall package.
- 2 Click **Create Uninstall icon** to create an uninstall icon.

The icon is added to the group that is selected in the first WinItem command.
- 3 Check **Remove Groups During Uninstall** to remove any program groups that were created during the installation.

Use this option carefully as some users might select an existing group for the installation, or add files to the group after installation.
- 4 Type the name for the uninstall in the space provided.

This name appears on-screen when the uninstall runs.
- 5 Click **Add** to record the options that you have chosen.

Building AI packages

When you have made all of the changes to your installation script that you require, you can build the AI package.

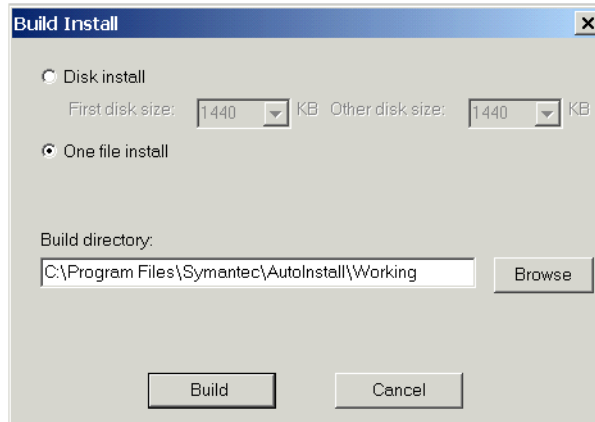
The package is saved as a single file that requires a large storage medium, such as a hard drive, network file server, or CD-ROM.

To build an AI package

- 1 On the Build menu, click **Build**.
- 2 Type the build directory if it is not already listed.

The default directory is:

C:\Program Files\Symantec\Ghost\Working



- 3 Click **Build**.
- 4 Close AI Builder.

AI Builder automatically creates an entry in the task log with a status of Hold.

Modifying installation scripts and AI packages

Installation scripts can be modified before a package has been created if the model computer is the same as it was when the installation script was created. Once created AI packages can be modified at any time on any computer.

To modify an installation script

- 1 Open AI Builder on the model system.
- 2 On the File menu, click **Open**.
- 3 Navigate to the installation script (Install.cfg).

The default location is:

C:\Program Files\Symantec\AutoInstall\Working\Configs\

- 4 Double-click the file to open it.

To modify an AI package

- 1 Open AI Builder.
- 2 On the File menu, click **Open**.
- 3 Navigate to the package (an .exe file).

The default location is:

C:\Program Files\Symantec\AutoInstall\Working\Onefile\

- 4 Double-click the file to open it.

The installation script is extracted from the file.

Executing and rolling out AI packages

AI Builder creates executable files that can be run on individual workstations to install the packaged software. You can deploy the package to a number of workstations via the Symantec Ghost Console.

The Symantec Ghost Console creates an installation task that rolls out AI packages to client computers. The Console task provides the path to the AI package to be run, as well as the parameters that dictate which target workstations receive the package.

For more information, see [“To set Deploy AI Package properties”](#) on page 93.

When the distribution server tells the target workstation that an AI package is available for installation, the Symantec Ghost client runs the executable.

6

S y m a n t e c G h o s t u t i l i t i e s

- Using Ghost Explorer to modify image file contents
- Managing partitions using GDisk
- Tracking Symantec Ghost license numbers
- Updating Security Identifiers (SIDs) and computer names

Using Ghost Explorer to modify image file contents

This chapter contains the following:

- [Understanding Ghost Explorer](#)
- [Viewing image files](#)
- [Restoring a file or directory from an image file](#)
- [Modifying image files in Ghost Explorer](#)
- [Saving a list of contents of an image file](#)
- [Setting span file sizes](#)
- [Compiling a file](#)
- [Determining Symantec Ghost image file version](#)
- [Using Ghost Explorer from the command line](#)

Understanding Ghost Explorer

The image files that are created when a computer's hard disk or partition is dumped contain data, applications, and registry settings. These image files can be loaded onto client computers as part of a cloning task. However, the Ghost Explorer utility also lets you view, alter, add, and extract files from an image file. This means that you can add extra files to the image file, rearrange the files within the image file, and extract files from the image file to copy onto client computers.

Ghost Explorer lets you quickly and easily restore files or directories from an image file. Using Ghost Explorer you can:

- View image file contents and save a list of files within an image file.
- Restore 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.

Note: Right-click a file or directory in Ghost Explorer to access a list of file commands.

Ghost Explorer supports the following partition types:

- FAT12
- FAT16
- FAT32
- NTFS (read only)
- Linux Ext2

To open Ghost Explorer

- On the Windows taskbar, click **Start > Programs > Symantec Ghost > Ghost Explorer**.

Viewing image files

You can view the contents of an image file, including details of the partitions, directories, and files.

There may be some degradation of performance when viewing image files created with Symantec Ghost V3. Ghost Explorer cannot view:

- Image files created with a version earlier than version 3.0
- NTFS partitions in image files created by Symantec Ghost V3 with compression

You can check the Symantec Ghost version in which your image file was created in Ghost Explorer.

For more information, see [“Determining Symantec Ghost image file version”](#) on page 260.

To view an image file

- 1 Open Ghost Explorer.
For more information, see [“To open Ghost Explorer”](#) on page 256.
- 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.

Restoring a file or directory from an image file

You can restore a file or directory directly from an image file using Ghost Explorer.

To restore a file or directory from an image file

- 1 In Ghost Explorer, open the image file.
- 2 Select the file or directory to be restored.
- 3 On the File menu, click **Restore**.
- 4 Select the location to which you want to restore the file or directory.
- 5 Click **Restore** to restore the file or directory to the chosen location.

Note: You can also drag and drop a file from Ghost Explorer to Windows Explorer to restore it.

Modifying image files in Ghost Explorer

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 greater and is not NTFS. You can also delete files from any image file that was created in Symantec Ghost v5.1c or a later version and is not NTFS.

You can check the version of Symantec Ghost used to create your image file in Ghost Explorer.

For more information, see [“Determining Symantec Ghost image file version”](#) on page 260.

Adding, moving, and deleting files

Within image files, Ghost Explorer supports Windows cut-and-paste operations, including copying, pasting, moving, deleting, and adding files to images. You can also drag and drop from Windows Explorer to Ghost Explorer.

Warning: If you use Ghost Explorer to add files to an image file, there may be some performance degradation when you clone the file using GhostCasting. Symantec Explorer calculates whether compilation is recommended. If it is, you can compile the file to improve performance. For more information, see [“Compiling a file”](#) on page 259.

Saving a list of contents of an image file

You can save a text file that contains a list of the directories (and optionally, files and their details) that are in the current image file.

To save a list of the contents of an image file

- 1 In Ghost Explorer, open the image file.
- 2 On the File menu, click **Save Contents**.
- 3 Do one of the following:
 - Click **Directories only** to include directories only.
 - Click **Include Files** to include files.
 - Click **Include Details** to include file details.

- 4 Select a directory to which to save the text file.
- 5 Type a file name.
- 6 Click **Save**.

Setting span file sizes

Symantec Ghost lets you split an image file into smaller files called spans. The Span Split Point function in Ghost Explorer lets you set the size of each span so that when you add files or directories, each span file does not get bigger than the specified size.

To set a span file size

- 1 On the View menu, click **Options**.
- 2 In the Span Split Point (MB) field, type the required size.
- 3 Click **Autoname Spans** if you want Ghost Explorer to choose a default name for additional span files that it creates.

Compiling a file

If you add or delete files from within an image file, the image file becomes fragmented. Symantec Ghost takes longer to restore a fragmented image than a compiled file. Compiling a file defragments it, which improves performance when restoring.

Check the properties of the image file to see whether compilation is recommended.

To compile a file

- 1 On the File menu, click **Compile** if compilation is recommended.
- 2 Type a new name for the compiled file.
- 3 Click **Save**.

Determining Symantec Ghost image file version

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. Ghost Explorer cannot open a file created with a version of Symantec Ghost earlier than 3.0. If the image file was created in Symantec Ghost 3.0 or greater, you can determine the version by looking at its properties in Ghost Explorer.

To determine the version of Symantec Ghost used to create an image file

- 1 In Ghost Explorer, open the image file.
- 2 On the File menu, click **Properties**.

The Properties window appears. The version of Symantec Ghost used to create the image file appears next to Produced by Ghost version.

Using Ghost Explorer from the command line

You can start Ghost Explorer from an MS-DOS prompt by typing its path and file name. For example:

```
C:\Progra~1\Symantec\Ghost\Ghostexp
```

Note: If Ghost Explorer is in the current directory, or in a directory on your path, you do not need to type the path name.

You can also provide a Ghost image file as an argument for Ghost Explorer to open. For example:

```
Ghostexp n:\Images\Myimage.gho
```

If Ghost Explorer reports a corruption in your image file, you may be able to get further details of the nature of the corruption. Normally, you would only use these options when asked to do so by Ghost Explorer Technical Support. Start the program with one of the following arguments:

- | | |
|-----|--|
| -d1 | Reports on corruptions or significant events in FAT file systems. |
| -d2 | Reports on corruptions or significant events in NTFS file systems. |
| -d4 | Reports on corruptions or significant events in Ext2 files. |

The reports are presented to you as dialog boxes. You can use all switches, or use `-d7` to turn on all options.

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. To use this mode, specify one of the following switches:

- `-t` Save 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` Save a list of directories and files.
- `-tv` Save a verbose listing of directories and files.
- `-t[vf]=filename` Save the list to the file specified.

For more information, see [“Saving a list of contents of an image file”](#) on page 258.

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.

For more information, see [“Setting span file sizes”](#) on page 259.

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 loading of the image is much slower. Use the switch `-ignoreindex` to force this behavior.

Managing partitions using GDisk

This chapter contains the following:

- [Introducing GDisk](#)
- [Overview of main command-line switches](#)
- [Creating a partition](#)
- [Reinitializing the Master Boot Record](#)
- [Showing information about disks](#)
- [Performing multiple GDisk operations using batch mode](#)
- [FAT16 partitions in Windows NT](#)
- [Deleting and wiping your disk](#)
- [Activate or deactivate a partition](#)
- [Hide or unhide a partition](#)
- [Modify the Windows NT/2000/XP boot menu](#)
- [Support for large hard disks](#)

Introducing GDisk

GDisk lets you create partitions, reinitialize Master Boot Records, and delete and wipe your disks in many different ways.

Two versions of GDisk are supplied with Symantec Ghost:

- GDisk: Runs in DOS
 - GDisk32: Runs from the command-line in a Windows operating system
- All GDisk command-line switches can be run with GDisk32.

GDisk is a complete replacement for the Fdisk and Format utilities that offers:

- On-the-fly formatting.
- Extensive partition reporting.
- High security disk wiping.
- The ability to hide a partition or make a hidden partition visible.

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.

Run either GDisk in DOS or GDisk32 in Windows.

To run GDisk

- 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 GDisk32

- 1 On the Windows taskbar, click **Start > Programs > MS-DOS Prompt**.
- 2 At the DOS prompt, type **progra~1\symantec \ghost\GDisk32** followed by the required disk and switches.

Overview of main command-line switches

GDisk has nine main modes of operation. The first four correspond to the menu options on the Fdisk main menu. The mode in which GDisk operates is selected by one of the following switches:

Mode	Switch	Explanation
Create	/cre	Create partitions: primary DOS partitions, extended DOS partitions.
Delete	/del	Delete partitions of any type, including nonDOS partitions.
Status (default)	/status	List information on the specified fixed disk and its partitions.
Activate	/act	Activate and deactivate a partition (specifying it as the bootable partition).

Mode	Switch	Explanation
Hide	/hide	Hide an existing partition or unhide a hidden partition.
Reinitialize MBR	/mbr	Reinitialize the Master Boot Record.
Batch	/batch	Use batch-mode command execution.
Disk wipe	/diskwipe	Wipe the contents of the whole disk.
Boot.ini	/bootini	Makes a modification to the Windows NT/2000/XP boot menu. This switch functions with GDisk32 only.

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:

- GDisk: C:\progra~1\symantec\ghost\gdisk /?
- GDisk32: C:\progra~1\symantec\ghost\gdisk32 /?

Note: An additional switch not shown in Help is the /VERSION switch. This switch shows the version information for the GDisk 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: C:\progra~1\symantec\ghost\gdisk /hide /?
- GDisk32: C:\progra~1\symantec\ghost\gdisk32 /hide /?

Switches common to all GDisk commands

You can use the following switches for any of the nine main GDisk operations:

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. Same functionality as /y.
/r	Causes GDisk to restart the computer if the operation is successful.

Creating a partition

The create switch creates a partition of the specified type using the largest block of unused disk space. The partition is not formatted during the operation unless the /for switch is used. You cannot create a dynamic disk partition.

Note: When GDisk loads a FAT32 partition, it aligns the first data sector to a 4 KB boundary from the start of the partition.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

- GDisk: `gdisk disk /cre {/pri | /ext | /log} [/sz: {MB | pcent{p | %}}] [/end] [/for [/q] [/v[:label]]] [/-32] [/ntfat16]`
- GDisk32: `gdisk32 disk / cre {/pri | /ext | /log} [/sz: {MB | pcent{p | %}}] [/end] [/for [/q] [/v[:label]]] [/-32] [/ntfat16]`

Switch	Explanation
<code>disk</code>	Represents the physical fixed disk, 1 to 8.
<code>/cre</code>	Creates a DOS partition or logical DOS drive.
<code>/pri</code>	Creates a primary DOS partition.
<code>/ext</code>	Creates an extended DOS partition.
<code>/log</code>	Creates a logical DOS drive in the extended DOS partition.
<code>/sz:MB</code>	Specifies the size of the partition in megabytes (MB). This is rounded up to the nearest cylinder.
<code>/sz:pcent{p %}</code>	Specifies the size of the partition as a percentage of the total disk size, not the available disk space.
<code>/end</code>	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 <code>/end</code> switch is ignored.
<code>/for</code>	Formats the new partition once it has been created. Unless the <code>/ntfat16</code> or <code>/-32</code> switches are used, the partition type is determined by the following: <ul style="list-style-type: none"> ■ 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
<code>/q</code>	Performs a quick format if used in combination with the <code>/for</code> switch. If you do not use this switch, then GDisk performs a surface scan of the partition and marks any bad sectors.
<code>/v[:label]</code>	Gives the new formatted partition the specified label when used in combination with the <code>/for</code> switch.

Switch	Explanation
<code>/-32</code>	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 (for example, Windows NT4).
<code>/ntfat16</code>	Indicates that the partition is not formatted as FAT32, but 64 KB, cluster FAT16 is allowed. This limits primary and logical partitions to 4097 MB. Partitions over 16 MB are formatted as FAT16. Windows 9x and DOS systems are unable to access partitions created with this switch and that are over 2048 MB.

Reinitializing the Master Boot Record

Use the `/mbr` switch to rewrite the boot code in the Master Boot Record (MBR). You may need to reinitialize the MBR to eliminate a boot sector virus residing there. You can also use the `/mbr` switch with the `/wipe` option to delete a dynamic disk.

Note: The switch must be used when deleting Linux partitions if LILO resides in the MBR.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

- GDisk: `gdisk disk /mbr [/wipe]`
- GDisk32: `gdisk32 disk /mbr [/wipe]`

Switch	Explanation
<code>disk</code>	Represents the physical fixed disk, 1 to 8.
<code>/mbr</code>	Reinitializes the boot code in the Master Boot Record.
<code>/wipe</code>	Deletes the partition on the disk.

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: `gdisk [disk] [/status] [/raw] [/lba] [/ser]`
- GDisk32: `gdisk32 [disk] [/status] [/raw] [/lba] [/ser]`

Switch	Explanation
disk	Represents the physical fixed disk, 1 to 8.
/raw	Shows the contents of the partition table in CHS 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 pre-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.

Note: To use the Windows version of GDisk in the example commands, replace `gdisk` with `gdisk32`.

For example:

```
C:\> gdisk /batch:cmds.gg
```


If the batch mode switch is supplied without a file name, GDisk prompts for the commands to execute.

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 an example batch command file called Two-new.gg. Blank lines and lines starting with the hash symbol are considered comments. These lines are ignored. (In this 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.gg
```

The 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, so if a second file called Std_init.gg contained the following lines:

```
1 /batch:two-new.gg
2 /batch:two-new.gg
```

then this command performs the actions of Two-new.gg on both fixed disks:

```
gdisk /batch:std-init.gg
```


FAT16 partitions in Windows NT

FAT16 partitions can be up to 4 GB in size using 64 K clusters in Windows NT. GDisk can create a FAT16 partition using 64 K clusters when the /Ntfat16 switch is added to the create partition command line. This switch disables the creation of FAT32 partitions and allows the creation of FAT16 partitions up to 4 GB.

Note: DOS and Windows 9x do not support FAT16 partitions using 64 K clusters and are limited to 2 GB FAT16 partitions.

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.

Depending on the version of GDisk that you require, the syntax for the delete switch is one of the following:

- GDisk: gdisk disk /del {/pri[:nth] | /ext[:nth] | /log:nth | /p:partn-no | /all} [/qwipe | /dodwipe | /customwipe:n]
- GDisk32: gdisk32 disk /del {/pri[:nth] | /ext[:nth] | /log:nth | /p:partn-no | /all} [/qwipe | /dodwipe | /customwipe:n]

Depending on the version of GDisk that you require, the syntax for the diskwipe switch is one of the following:

- GDisk: `gdisk disk /diskwipe [dodwipe | /customwipe:n]`
- GDisk32: `gdisk32 disk /diskwipe [dodwipe | /customwipe:n]`

Switch	Explanation
<code>disk</code>	Represents the physical fixed disk, 1 to 8.
<code>/del</code>	Deletes a DOS partition or logical DOS drive.
<code>/pri[:nth]</code>	Deletes the nth primary DOS partition. The default is 1.
<code>/ext[:nth]</code>	Deletes the nth extended DOS partition. The default is 1. Also deletes any logical partitions in the extended partition.
<code>/log:nth</code>	Deletes the nth logical DOS drive from the extended DOS partition.
<code>/p:partn-no</code>	Indicates the partition to delete. Use the number reported by GDisk in standard display mode (not using <code>/lba</code> or <code>/raw</code>) for <code>partn-no</code> .
<code>/all</code>	Deletes all partitions.
<code>/qwipe</code>	Overwrites the partition's data area before deleting the partition. Makes one pass of the disk.
<code>/dodwipe</code>	Overwrites the partition's data area before deleting the partition. Makes seven passes of the disk. This is the security standard for the U.S. Department of Defense.
<code>/customwipe:n</code>	Overwrites the partition's data area n times before deleting the partition. n can be set from 1 to 100. <code>/customwipe:7</code> is equivalent to <code>/dodwipe</code> .

For example:

- `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.

Activate or deactivate 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: `gdisk disk [-l]act /p:partn-no`
- GDisk32: `gdisk32 disk [-l]act /p:partn-no`

Switch	Explanation
<code>disk</code>	Represents the physical fixed disk, 1 to 8.
<code>/act</code>	Activates a partition.
<code>/-act</code>	Deactivates a partition.
<code>/p:partn-no</code>	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 <code>/lba</code> or <code>/raw</code>) for <code>partn-no</code> .

Hide or unhide 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: `gdisk disk [-l]hide /p:partn-no`
- GDisk32: `gdisk32 disk [-l]hide /p:partn-no`

Switch	Explanation
<code>disk</code>	Represents the physical fixed disk, 1 to 8.
<code>/hide</code>	Hides a partition.
<code>/-hide</code>	Unhides a partition.
<code>/p:partn-no</code>	Indicates the partition to hide or unhide. Use the number reported by GDisk in standard display mode (not using <code>/lba</code> or <code>/raw</code>) for <code>partn-no</code> .

Modify the Windows NT/2000/XP boot menu

The `/bootini` switch lets you make a modification to a Windows NT/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 is operational with GDisk32 only.

When GDisk changes the state of `Boot.ini`, a copy of the current `Boot.ini` is created. The copy is named either `C:\boot_gdisk32_copy.ini` or `C:\boot.ini_gdisk32_copy`.

Specifying the boot.ini path and file name

The `/inifile` switch is common to all operations performed with the `/bootini` switch.

`/inifile` lets you specify the full path and file name of the current Windows NT/2000/XP `Boot.ini` file. This lets you locate `Boot.ini` if it is not on the C drive.

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 NT/2000/XP operating system.

The syntax for this command is as follows:

```
gdisk32 /bootini [/inifile:filename]
```


Adding an entry to Boot.ini

There are two types of entries that you can add to a Boot.ini file:

- Start another installation of Windows NT/2000/XP that resides on a different partition.
- Start a nonWindows NT/2000/XP operating system that resides on a different partition.

GDisk does not add an entry to Boot.ini if:

- An entry with the description already exists in Boot.ini (case insensitive).
- The referenced partition is of type Extended.
- The referenced partition is hidden.

The following table describes the function of each switch for both types of entries.

Switch	Explanation
/bootini	Modifies Boot.ini.
/add	Creates a new entry in Boot.ini.
/d:diskno	Physical fixed disk, from 1 through 8.
/p:partno	Number of the partition from which to boot.
/desc:description	Description to appear in the NT boot loader menu.
/inifile:filename	The full path and file name for Boot.ini. The default value is C:\boot.ini.
/bsectfile:filename	Boot sector file to create. For example, C:\bsect.dat.
/winnt	Adds an entry to start a Windows NT/2000/XP operating system.
/sysfolder:folder	System folder on the Windows NT/2000/XP operating system from which to start. The default value is Winnt.
/r	Restart after the execution of the command.

Adding an entry for starting Windows NT/2000/XP

The syntax for this command is as follows:

```
gdisk32 /bootini /add /d:diskno/p:partno /desc:description /winnt [/sysfolder:folder] [/infile: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 NT/2000/XP. If this switch is not used, then GDisk32 creates an entry as if the target operating system is not Windows NT/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 for starting a nonWindows NT/2000/XP operating system

The syntax for this command is as follows:

```
gdisk32 /bootini /add /d:diskno/p:partno /desc:description [/infile:filename] [/bsectfile:filename] [/r]
```

This entry to Boot.ini references a boot sector file used to continue the starting 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 lets you specify the full path and file name for the boot sector file that is created.

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 ***"

produces a boot sector file C:\bootos2.dat.

Removing an entry from Boot.ini

The syntax to remove an entry from Boot.ini as follows:

gdisk32 /bootini /remove /entry:no [/infile:filename] [/r]

Switch	Explanation
/remove	Removes the entry from Boot.ini.
/entry:no	Removes the ID of the entry from Boot.ini.

If the entry to be removed is the default boot option, 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:no] [/timeout:sec] [/infile:filename] [/r]
```

Switch	Explanation
<code>/default</code>	Sets the default boot option and timeout.
<code>/entry:no</code>	Sets the ID of entry as the default boot option.
<code>/timeout:sec</code>	Sets the number of seconds before the default boot option is selected.

Support for large hard disks

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.

Remember the following information when creating partitions for use in Windows 95/98:

- On a system with a PC BIOS that does not support interrupt 13h extended disk services, take care to ensure that the partitions created can be used as intended. When a primary partition or extended partition starts or ends past the 7.8 GB limit of the hard drive, it is not accessible on such systems in Windows or in DOS-only mode. This affects all logical partitions contained within an extended partition starting or ending past the limit.

Remember the following information when you create partitions for use in Windows NT:

- According to the Microsoft Support Knowledgebase, Windows NT NTFS bootable partitions cannot exceed 7.8 GB (8,455,716,864 bytes). This information is detailed in the Windows Knowledgebase Article “Windows NT Boot Process and Hard Disk Constraints,” Article ID: Q114841.

Nonbootable NTFS partitions do not have this size limitation.

- NT cannot start from partitions that start or end over the 1024-cylinder boundary. If this condition exists, NT reports a “Boot Record Signature AA55 Not Found” error message.

Windows NT does not support drives larger than 7.8 GB unless you install Service Pack 4 or apply the ATAPI hot fix to Service Pack 3. This information is included in the Windows Knowledgebase Article “IBM DTTA-351010 10.1 GB Drive Capacity Is Inaccurate,” Article ID: Q183654.

Tracking Symantec Ghost license numbers

This chapter contains the following:

- [Setting up the License Audit Utility](#)
- [Running the License Audit Utility](#)
- [Viewing the database file](#)
- [Removing the License Audit Utility](#)

The License Audit Utility (LAU) runs as a part of user logon scripts. When a user logs on to a computer with a cloned disk, the disk's details are recorded in a database file that can be viewed by the administrator.

Setting up the License Audit Utility

The License Audit Utility tracks the number of licenses that a copy of Symantec Ghost uses by recording the number of cloned disks that it finds in a particular domain. The utility only runs on Windows NT/2000/XP operating systems and is part of the Standard Tools for Symantec Ghost.

To set up the License Audit Utility, you need administrator privileges on the PDC (Primary Domain Controller). This gives you the necessary rights to execute the LAU setup.

The files required for LAU setup are included in the Symantec Ghost Console and Standard Tools installation packages.

The LAU installation program does the following:

- Checks that you have administrator user rights on the PDC
- Creates a share on the License directory called ghostlau, or ghlauxxx if ghostlau is already used as a share name for another directory
- Queries all users on the PDC and finds the users' logon script files
- Creates a logon script named Ghostlog.bat that runs the Laclient.exe program and places it in the NETLOGON directory on the PDC
- Adds a reference to the Ghostlog.bat file in all found user scripts

NETLOGON is a share name for:

WinNT systems \winnt\system32\repl\import\scripts

Win2000 active directory \winnt\SYSTEM\sysvol\<servername>.com\scripts
server

To set up the License Audit Utility

- 1 Install the Symantec Ghost Console or Standard Tools on a system running Windows NT or Windows 2000.
For more information, see [“Installing Symantec Ghost”](#) on page 35.
- 2 On the Windows taskbar, click **Start > Programs > Symantec Ghost > License Audit Utility**.
- 3 In the License Audit Utility window, click **Setup**.

Running the License Audit Utility

After installation, LAU runs in the background looking for fingerprint information on client hard drives as users log on.

If LAU finds a cloned disk, it updates the database file on the server. The next time a user logs on to a computer, LAU looks for fingerprint information. If it detects any changes, it updates the database file on the server.

LAU retrieves Ghost fingerprint information on Windows 9x systems, regardless of the user's privileges. On Windows NT or Windows 2000 systems, however, it can only retrieve Ghost fingerprint information if the user has domain administrator privileges.

Viewing the database file

You can view the database file to check the number of licenses in use.

To view the database file

- On the Windows taskbar, click **Start > Programs > Symantec Ghost > License Audit Utility**.

The following domain information appears:

- Total number of cloned disks
- MAC address of the computer to which cloned drives belong
- The user that cloned the disks (Ghost 6.5 only)
- Disk model and serial number of each cloned disk (Ghost 6.5 only)

Note: If a SCSI disk is cloned with Symantec Ghost version 6.5, the database file includes the disk model number and serial number information only if the ASPI drivers were loaded when cloning was performed.

Removing the License Audit Utility

The Uninstall program:

- Checks that you have administrator user rights on the PDC
- Removes all references to the Ghostlog.bat file from the user scripts that contain them
- Deletes Ghostlog.bat from the NETLOGON directory on the PDC

To remove the License Audit Utility

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > License Audit Utility**.
- 2 In the License Audit Utility window, click **Remove**.

Updating Security Identifiers (SIDs) and computer names

This chapter contains the following:

- [Making SID changes with Sysprep and Ghost Walker on NT based clients](#)
- [Using Ghost Walker](#)

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 computer name. When loading an image onto a number of client computers, unique identifiers must be assigned as part of the task. There are a number of tools available to do this. Symantec Ghost supports two of them: the Microsoft application Sysprep, and the Symantec utility Ghost Walker.

Symantec Ghost Walker capabilities

- Runs in native DOS, allowing the SID to be changed without an additional restart following a clone operation.
- 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 so that local users retain user profiles and access rights.
- Alters computer names for Windows 95, 98, Me, NT, XP and 2000 operating systems.

Note: This does not change the computer name within the Symantec Ghost Console.

Symantec Ghost Walker shortcomings

- Computer name change functionality is limited. New name must contain the same number of characters as the original.
- Not officially endorsed by Microsoft.

Microsoft Sysprep capabilities

- Invokes the Windows 2000 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 2000/XP 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 shortcomings

- 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.
- The version of Sysprep that runs on Windows NT 4.0 is limited in its functionality. Not supported by Symantec Ghost.
- No equivalent exists for Windows 95, 98, and Me for computer name changes.

Problems with SID changing

SID changing is an approximate technology, as you can only change SIDs in known locations.

Problems arise because:

- 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.
- Microsoft technologies such as Windows 2000/XP NTFS File Encryption, Windows NT, and Windows 2000/XP 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. Microsoft does not address changing local workstation user SIDs.

For these reasons you are strongly advised to test computer environments and the applications on them before mass rollouts or upgrades.

Using Ghost Walker

Ghost Walker lets you alter identification details of Windows 95, Windows 98, Windows Me, Windows NT, and Windows 2000/XP computers following a clone operation. Each Windows 95, 98, or Me computer can be assigned a unique name. Each Windows NT or 2000/XP computer can be assigned a unique computer name and a Machine Security Identifier (SID).

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 graphical user interface or from the command line. Ghost Walker does not run from:

- A Windows NT or 2000 DOS shell
- A Windows 95, 98, or Me DOS shell if you are also updating a Windows 95, 98, or Me operating system

The Ghost Walker window lists all bootable 95, 98, Me, NT, XP, and 2000 systems on the computer hard drives. 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 NT/2000/XP workstations that are members of a server domain.
You must add the workstation to the Domain using the new SID and Computer Name once you have completed the update.
- 2 Run DOS.
- 3 In the command line, type **Ghstwalk.exe**.
- 4 Press **Enter**.

Ghost Walker lists all interpretable volumes on the computer.

- If there is one operating system on the computer, 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, details of all existing operating systems appear in the top pane.

- 5 If there is more than one operating system on the computer:
 - a In the Select a System ID field, type an ID for the operating system to appear.
 - b Click **V -Change Additional Vols** to add or remove nonbootable volumes to be updated.
 You must include any additional nonbootable volumes that may have security information or shortcuts containing the computer name from the bootable operating system embedded in them. Failure to do so results in mismatched data and a loss of security access.
- 6 To change the computer name, type **N**, then press **Enter**.
 The new name must be the same length as the previous name. The field you type the name into is the correct length of the name.
 The name cannot contain any of the following characters:
 ^[]";|<>+=,?*
- 7 Press **Enter** to update.
 This lists the new name, and for NT and 2000 computers, a new SID.
 The computer name and SID updates occur in:
 - The registry of the selected operating system
 - The file system on which the operating system resides
 - Any additional volumes selected for the update
- 8 If you removed an NT or 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.

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|/?]
```



```
[/LOGGING]
[/SAFE_LOGGING]
[/#E=<environment file>]
[/H|/HELP|/?]
[/SID=<replacement SID>]
[IGNORE_ENCRYPTFILES]
```

The following table describes the command-line options.

Switch	Description
/CN=	Specifies a new computer name.
<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 will be randomly generated and the type of random value to place in that location. Only one instance of the following keywords is permitted in a format: <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.

Switch	Description
/BV=<drv:part>	Specifies the drive number and partition number of the bootable operating system installation to update.
/AV=<drv:part>	<p>Specifies the drive number and partition number of an additional volume containing a file system to update.</p> <ul style="list-style-type: none">■ 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	<p>Specifies that all other volumes are to be included as additional volumes.</p> <p>/AV=ALL cannot be combined with the /AV=<drv>:<part> switch.</p>
/SURE	Specifies that the update should start without user confirmation.
/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 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 file Gwalklog.txt. 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.
/#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.

Switch	Description
/IGNORE_ENCRYPTFILES	Disables the warning generated by Ghost Walker when it encounters Windows 2000 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 wholly 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.
/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
```

The above command line does the following:

- Updates the Windows 95, 98, Me, NT, XP, or 2000 installation 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.

Loss of 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 accessed by a peer-to-peer connection, security information is created for those data objects that is 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.

Identical 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.

It appears that the accessing user is given the rights that the accessed user has by proxy. For example, the access is performed on behalf of the accessing user by the accessed user, just because there is a user name/password match. This can best be seen when specific access rights are granted remotely by the accessing user to a resource on the accessed computer. The Access Control List shows that the accessed user is the user who has rights to the resource.

Updating the SID on a workstation does not stop this situation from occurring. You must change the password of one of the users.

7

A p p e n d i c e s

- [Command-line switches](#)
- [Setting up the hardware and transfer methods](#)
- [USB and DirectParallel Cables](#)
- [The Wattcp.cfg network configuration file](#)
- [Cloning with Linux](#)
- [Customizing Symantec Ghost functionality](#)
- [Troubleshooting](#)
- [Diagnostics](#)
- [Installing Symantec Ghost from the command line](#)



Command-line switches

This appendix contains the following:

- [Symantec Ghost command-line switches](#)
- [Clone switch syntax](#)
- [CRC32 switch usage](#)

Symantec Ghost command-line switches

Symantec Ghost can be run:

- 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.

To list Symantec Ghost command-line switches

- In the Ghost directory, type one of the following:
 - `ghost.exe -h`
 - `ghost.exe -?`

A hyphen (-) or a slash (/) must precede all switches except @. Switches are not case sensitive. They can be entered in upper, lower, or mixed case.

@filename

Specifies a file containing additional command-line switches that should be 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, except for -afile and -dfile. The Symantec Ghost command-line switch file must be a text file with each switch on a new line. This feature lets you exceed the DOS command-line limit of 150 characters.

For example, for the following command line:

```
ghost.exe @ghswitch.txt
```

The file Ghswitch.txt would read:

```
-clone,mode=pdump,src=1:2,dst=g:\part2.gho  
-fcr  
-sure
```

-afile=filename

Overrides the default abort error log file (Ghosterr.txt) to the directory and file given in filename.

-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 loaded.

-batch

Batch mode switch. Prevents abort messages waiting for user acknowledgment, and removes user interaction prompts. The return value of Ghost.exe must be checked to identify if the operation was successful. Symantec Ghost returns 0 on success and 1 or higher on failure or error. See Example 14 of the Clone switch.

-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. This option may slow Symantec Ghost operation substantially.

-bootcd

When writing an image directly to a CD writer, make the CD bootable. You need a bootable floppy disk in drive A. If this switch is untitled and -sure is used, a nonbootable CD is created.

-buffersize=x

Where x = number of KB. Ghost creates an image file using a small buffer. The 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

Clone operation switch. This switch allows automation of Symantec Ghost operations and has a series of arguments that define the operation parameters. No spaces are allowed in the command line. The number of size switches depends on the number of partition sizes that you want to specify. There may be none.

Note: Some cloning switches for use in Ghost can be specified on the GhostCast Server.

For more information, see [“Clone switch syntax”](#) on page 314.

-cns

Reverts the naming of spanned files to the system used by versions of Symantec Ghost previous 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. For example:

With -cns	Without -cns
Filename.gho	Filename.gho
Filename.001	Filen001.ghs
Filename.002	Filen002.ghs

-CRC32

The -CRC32 switch lets you make a list of the files on a disk or partition, or create an image file with CRC values, and to verify the list against the original or a clone. 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.

For more information, see “[CRC32 switch usage](#)” on page 320.

-crcignore

Ignores CRC errors. CRC errors indicate data corruption. This switch overrides the CRC error detection and may let a corrupted image file be used. Using this switch leaves the corrupted files in an unknown state.

-cvtarea

Creates a cvtarea file when copying or loading FAT32 partitions. 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 <http://www.microsoft.com/hwdev/storage/ntfs-preinstall.htm>

The file is created in the root directory of the partition during a partition or disk load 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:

```
-cvtarea,filename=xxx,size=yyy{%disk,%free,KB,MB,GB},firstcluster=zzz{%disk,%free,KB,MB,GB}
```

The default settings are:

filename	cvtarea.tmp
size	12%disk
firstcluster	1 3 GB 33%disk

Defaults to:

- 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.dmp. 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. This switch cannot be included in the @ Ghost switch text file.

-dl=number

Specifies the number of hard drives present. Valid numbers are between 1 and 8. This may help when the BIOS does not report the number of drives correctly.

-f32

Lets Symantec Ghost convert all FAT16 volumes to FAT32 volumes when the destination partition is larger than 256 MB in size. Ensure that the installed operating systems requiring access to the volumes that will be converted support FAT32.

-f64

Lets Symantec Ghost resize FAT16 partitions to be greater than 2047 MB using 64 K clusters. This is only supported by Windows NT and Windows 2000. Do not use on computers with other operating systems.

-fatlimit

Limits the size of FAT16 partitions to 2047 MB. Useful when Windows NT FAT16 partitions are present on the disk, and 64 K clusters are not wanted.

-fcr

Creates a CRC32 file (called Ghost.crc) while creating an image file.

For more information, see [“-CRC32”](#) on page 300.

-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 when performing a disk-to-disk or image-to-disk cloning operation.

-femax

When an extended partition is created in a disk-to-disk or image-to-disk operation, the extended partition takes up all free space.

-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. This switch does not have any effect when running Symantec Ghost in Windows 98.

-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.

-fis

Use 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 5 MB free even when -fis is specified.

-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.

-fro

Forces Symantec Ghost to continue cloning even if the source contains bad clusters.

-fx

Flag exit. Causes Symantec Ghost to exit to DOS after operation completion. 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 may be processed.

For more information, see “-rb” on page 309.

-h or -?

Shows the Symantec Ghost command-line switch Help page.

-ia

Image all. The image all switch forces Symantec Ghost to perform a sector-by-sector copy of all partitions. 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 loaded to a disk with identical geometry.

-ial

Forces a sector-by-sector copy of Linux partitions. Other partitions are copied as normal.

-ib

Image boot. 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 boot track. You cannot perform partition-to-partition or partition-to-image functions with the -ib switch.

-id

Image disk. 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.

-ir

Image raw. 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 on restore and you need an identical or larger disk.

-ja=sessionname

Connects to the GhostCast Server using the specified session name. Set the disk and possibly partition to be cloned on the GhostCast Server.

-jaddr=<id_address>

Use the IP address for the GhostCast Server.

-jl:x=filename

Creates a GhostCast log file to assist in diagnosing GhostCasting 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.)

-lockinfo

Shows the type code and information stored in the BIOS, or the Pentium III Processor ID.

For example:

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.

-lpm

LPT master mode. This switch causes Symantec Ghost to automatically go into LPT master mode, and is the equivalent of selecting LPT Master from the main menu.

For more information, see [“Peer-to-peer connections”](#) on page 325.

-lps

LPT slave mode. This switch causes Symantec Ghost to automatically go into LPT slave mode, and is the equivalent of selecting LPT Slave from the main menu.

For more information, see [“Peer-to-peer connections”](#) on page 325.

-memcheck

Activates internal memory usage checking for Technical Support.

-nofile

Disables the Image File Selection dialog box. Useful when opening directories with large numbers of files and slow links.

-nolilo

Does not attempt to patch the LILO boot loader after a clone. If you use the -nolilo switch, you need to start from a floppy disk after the clone, and then run /sbin/lilo as the root user to reinstall LILO.

-noscsi

Disables access to SCSI devices via ASPI.

-ntc-

Disables NTFS contiguous run allocation.

-ntchkdisk

Cloned NTFS volume will have the CHKDSK bit set. This causes Windows NT to check the integrity of the volume when it is started.

-ntd

Enables NTFS internal diagnostic checking.

-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, run CHKDSK on the volume to ensure that the disk is in a sound state before cloning.

-ntiid

By default, Symantec Ghost copies partitions participating in an NT volume set, stripe set, or mirror set using image all sector-by-sector copying. This switch forces Symantec Ghost to ignore the Windows NT volume set partition status and clone the partition as if it were an NTFS partition to let it be intelligently cloned on a file-by-file basis. 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 NT software RAID partitions)

- 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 a 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

Override. Allows the override of internal space and integrity checks. 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.

-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 cloning operation.

-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

Quiet mode. Disables status updates and user intervention.

-rb

Restarts after finishing a load or copy. After completing a load or copy operation, the target computer must be restarted so that the operating system can load the new disk/partition information. Normally, Symantec Ghost prompts the user to restart or exit. -rb tells Symantec Ghost to automatically restart after completing the clone and is useful when automating Symantec Ghost in a batch command file.

For more information, see “-fx” on page 303.

-script

Allows you to specify a series of commands (one per line) and Symantec Ghost will execute them in a sequential order.

Example:

```
ghost -script=script.txt
```

Following is an example of script.txt:

```
-clone,mode=dump,src=2,dst=c:\drv2.gho  
-chkimg,c:\drv2.gho  
-clone,mode=dump,src=2,dst=c:\part2.gho  
-chkimg,c:\part2.gho
```


-skip=x

Skip file. Causes Symantec Ghost to exclude the indicated files during a create or load operation. A skip entry can specify a single file, 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.

Examples:

- -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, Skipfile.txt contains:

```
*\*.tmt  
[partition:1]  
\windows\  
*\*.exe  
[Partition:2]  
*\*me.txt
```

This would skip all *.tmt files on any partition, the Windows directory and any *.exe files on the first partition, and any file that ends with me.txt on the second partition.

-span

Enables spanning of image files across volumes.

-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
```

divides the image into 200 MB segments.

-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.

-size

Sets the size for the destination partitions for either a disk load or disk copy operation. When numbering partitions in the -size switch, do not include the hidden Ghost partition.

For more information, see [“Setting a destination size for the clone switch”](#) on page 316.

-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.

-tapesafe

Sets the ASPI driver to report a read/write as successful only when the data has been transferred to the physical medium. Useful when using older or unreliable tape devices or sequential media.

-tapebsize=x

Specifies the tape block size in units of 512 bytes, where x is 1 to 128.

-tapespeed=x

Allows control of tape speed. Where x equals 0 to F. 0 is the default. 1-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. (It is possible that this occurs before the data is physically written to the medium.)

-tcpml:slave IP address]

TCP/IP master mode. This switch causes Symantec Ghost to automatically go into TCP/IP master mode, and is the equivalent of selecting TCP/IP Master from the main menu. The IP address of the slave computer may be specified.

For more information, see [“Peer-to-peer connections”](#) on page 325.

-tcps

TCP/IP slave mode. This switch causes Symantec Ghost to automatically go into TCP/IP slave mode, and is the equivalent of selecting TCP/IP Slave from the main menu.

For more information, see [“Peer-to-peer connections”](#) on page 325.

-usbm

USB master mode. This switch causes Symantec Ghost to automatically go into USB master mode, and is the equivalent of selecting USB Master from the main menu.

For more information, see [“Peer-to-peer connections”](#) on page 325.

-usbs

USB slave mode. This switch causes Symantec Ghost to automatically go into USB slave mode, and is the equivalent of selecting USB Slave from the main menu.

For more information, see [“Peer-to-peer connections”](#) on page 325.

-vdw

If this 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.

-ver=value

Tests the version of Symantec Ghost. If Symantec Ghost is older than the specified version, it aborts and exits, otherwise it proceeds as normal. This is designed for use in batch files. The version number should be specified without the period. For example, Symantec Ghost 6.5 is `-ver=650`.

-z

Compresses when saving a disk or partition to an image file. The greater the compression, the slower the transmission.

- `-z` or `-z1`: Low compression (fast transmission)
- `-z2`: High compression (medium transmission)
- `-z3` through `-z9`: Higher compression (slower transmission)

For more information, see [“Image files and compression”](#) on page 162.

Clone switch syntax

The syntax for the clone switch is:

```
-clone,MODE={operation},SRC={source},DST={destination},  
[SIZE{size},SIZE{size}.....]
```

Defining the type of clone command

MODE defines the type of clone command.

MODE={copy | load | dump | pcopy | pload | pdump}

Switch	Action
copy	Disk-to-disk copy
load	File-to-disk load
dump	Disk-to-file dump
pcopy	Partition-to-partition copy
pload	File-to-partition load
pdump	Partition-to-file dump, allows multipart Ghost dump selection for file

Cloning combination options

This table illustrates the possible cloning operations that you can perform.

Mode	Source	Destination
copy	disk	disk
load	file GhostCast Server tape	disk
dump	disk	file GhostCast Server tape CD writer
pcopy	disk:partition	disk:partition

Mode	Source	Destination
pload	file:partition GhostCast Server (no partition specified) tape:partition	disk:partition
pdump	disk:partition:partition:partition You can specify more than one partition.	file GhostCast Server tape CD writer

Setting a source for the clone switch

SRC defines the source for the operation selected by the clone mode option.

SRC={disk | file | multicast | tape}

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.
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

Setting a destination for the clone switch

DST defines the destination location for the operation.

DST={disk | file | multicast | tape | cdwriter}

Switch	Destination	Explanation
disk	drive	<p>The destination disk drive number. For example, DST=2</p> <p>A partition on a drive can also be specified. For example, DST=2:1</p> <p>To create a new partition, type a destination partition one greater than the existing number of partitions, if there is enough free space.</p>
file	filename	The destination image file name. For example, DST= g:\destination.gho
tape	@MTx	The tape drive number. Numbers start at 0. For example, DST=@MT0
cdwriter	@CDx	The CD writer drive number. Numbers start at 1. For example, DST=@CD1

Setting a destination size for the clone switch

SZE sets the size of the destination partitions for either a disk load or disk copy operation. This is optional. Multiple partition size switches are supported.

SZE{E | F | L | n={xxxxM | mmP | F | V}}

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.

Switch	Explanation
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 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	The sizes of all partitions remain fixed.
F	The sizes of all partitions except the first remain fixed. The first partition uses the remaining space.
L	The sizes of all partitions except the last remain fixed. The last partition uses the remaining space.

Examples of clone switch usage

The following table describes clone switches and their functions.

Switch	Function
ghost.exe -clone,mode=copy,src=1,dst=2	Copy local disk one to local disk two.
ghost.exe -clone,mode=dump,src=2,dst=c:\drive2.gho -lpm	Connect a master computer using LPT to another computer running Symantec Ghost in slave mode, and save 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	Copy the second partition of local disk one to the first partition of local disk two, without the final warning prompt.

Switch	Function
ghost.exe -clone,mode=load,src=E:\savedsk.gho,dst=1 -sure	Load 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.
ghost.exe -clone,mode=pdump,src=1:2,dst=g:\part2.gho	Save the second partition of disk one to an image file on mapped network drive G.
ghost -clone,mode=pload,src=g:\part2.gho:2,dst=1:2	Load partition two from a two-partition image file on mapped drive G onto the second partition of the local disk.
ghost.exe -clone,mode=load,src=g:\2prtdisk.gho,dst=2size1=60P,size2=40P	Load disk two from an image file and resize the destination partitions into a 60:40 allocation.
ghost.exe -clone,mode=copy,src=1,dst=2,size2=F	Clone a two partition disk and keep the second partition on the destination disk the same size as on the source disk, and let the first partition use the remaining space, leaving no unallocated space.
ghost.exe-clone,mode=load,src=g:\3prtdisk.gho,dst=1,size1=450M,size2=1599M,size3=2047M	Load disk one from an image file and resize the first partition to 450 MB, the second to 1599 MB, and the third to 2047 MB.
ghost.exe -clone,mode=load,src=g:\2prtdisk.gho,dst=1,sizeL	Load a disk from an image file and resize the last partition to fill the remaining space.
ghost.exe -clone,src=@MCsessionname,dst=1 -sure	Load disk one from an image file being sent from the GhostCast Server with the session name "sessionname" without the final warning prompt.

Switch	Function
ghost.exe -clone,src=1,dst=@MCsessionname -sure	Create 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=copy,src=2:2,dst=@MT0	Create an image file of the second partition on disk 2 onto the first tape drive.
ghost.exe -clone,mode=pdump,src=2:1:4:6,dst=d:\part146.gho	Create an image file with only the selected partitions. This is an example of selecting partitions 1, 4, and 6 from disk 2.

Batch file example

This example loads 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 alter depending on the success or failure of the Symantec Ghost operation.

Batch file contents:

```
@ECHO OFF
ghost.exe
-clone,src=@mcSN,dst=1,size1=450M,size2=1599,size3=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
```


CRC32 switch usage

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:

```
-CRC32,action={create|verify|pcreate|pverify|dcreate|dverify},src={{DiskSpec}|{PartSpec}|{File}},crcfile={File},vlist={File},vexcept={File}
```

The following parameters can be used with the -CRC32 switch:

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

Switch	Function
ghost.exe -fcr	Create a CRC32 file (called Ghost.crc) while making an image file.
ghost.exe -fcr=d:\test.crc	Create a CRC32 file while making an image file with a different name.
ghost.exe -CRC32,action=create,src=1,crcfile=ghost.crc	Create a list of files and CRC32 values for a disk.
ghost.exe -crc32,action=dverify,src=x:dumpfile.gho,crcfile=ghost.crc	Verify the list against an image file.
ghost.exe -crc32,action=pverify,src=1:2,crcfile=filename.crc:2	Verify a partition in an image file 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	Create 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	Create an ASCII CRC32 file. Same as previous except that you specify the disk and ASCII CRC32 file. This example uses disk 2 as the source drive and the output file as Myfile.txt.
ghost.exe -CRC32,action=verify	Verify the contents of the primary disk against a CRC32 file. The default disk is the primary drive and the default ASCII CRC32 file is Ghost.crc (in the current directory). In addition, the default verification list file is Ghost.ls.

Switch	Function
ghost.exe -CRC32,action=verify,src=1,crcfile=myfile.txt,vlist=myfile.out	Verify the contents of the primary disk against a CRC32 file. Same as previous 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	Verify 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.

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 upper case. The * wildcard follows UNIX rules, it is more powerful than the MS-DOS *. In particular it matches the . as well as any other character, but other characters can follow the *. Therefore a wildcard of *br* matches any files containing the letters br, for example, Brxyz.txt, Abr.txt, and Abc.dbr.

The specification of `\WINDOWS\COOKIES*.*` in the example above means match all files in the subdirectory `\WINDOWS\COOKIES` 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 above 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.

Setting up the hardware and transfer methods

This appendix contains the following:

- [Hardware and transfer requirements](#)
- [Removable media](#)

Hardware and transfer requirements

Before using Symantec Ghost, consider the hardware and transfer 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, transferring drives and partitions and using image files between them.

The following table describes different cloning situations, and the master/slave relationship.

Action	Master	Slave
Disk-to-disk copy	Computer containing source disk	Computer containing destination disk
Disk-to-image file copy	Computer containing source disk	Computer receiving destination image file
Image file-to-disk copy	Computer containing destination disk	Computer containing source image file

Action	Master	Slave
Partition-to-partition copy	Computer containing source partition	Computer containing destination partition
Partition-to-image file copy	Computer containing source partition	Computer receiving destination image file
Image file-to-partition copy	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.

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/min, Symantec Ghost provides support for the Parallel Technologies universal DirectParallel cable. For peer-to-peer USB port connections, use a USB cable that supports a host-to-host connection and a data transfer of approximately 20-30 MB/min.

ECP is the best option for LPT connections. Symantec Ghost must be running under DOS on both computers.

For more information, see [“USB and DirectParallel Cables”](#) on page 329.

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 ethernet cable (pins 1236 > 3612)
- Coaxial cable
- Standard cables with hub or MAU

Install a network interface card (NIC).

SCSI tape driver

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 example below:

```
device=C:\scsitape\aspi4dos.sys
```

Refer to the documentation included with the SCSI tape device for more information.

GhostCasting

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-ROM usage

A CD writer and blank CD-R/RW media are required.

For more information, see [“Image files and CD writers”](#) on page 168.

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 attaching to a Microsoft network volume or an IBM LAN server.

For more information, see [“Creating boot images and disks with the Ghost Boot Wizard”](#) on page 133.

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, 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.

Third party device

Install the DOS driver as outlined in the device documentation.



USB and DirectParallel Cables

This appendix contains the following:

- [Parallel Technologies cables](#)
- [Other USB cables](#)

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.

Via Web site	http://www.lpt.com
Via telephone	800.789.4784 (U.S.) 425.869.1119 (International)
Via fax	253.813.8730
Via email	sales@lpt.com

The USB and DirectParallel connection cables can also be used for high-speed computer-to-computer file transfer and networking in Windows 9x and 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 9x and 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

The Wattcp.cfg network configuration file

This appendix contains the following:

- [The Wattcp.cfg configuration file](#)

The Wattcp.cfg configuration file

The Wattcp.cfg configuration file contains the TCP/IP networking configuration details for Symantec Ghost and DOS GhostCast Server. The Wattcp.cfg file is not required for the Windows GhostCast Server, Ghostsrv.exe.

Wattcp.cfg is created automatically 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 when 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
```


The keywords in the Wattcp.cfg configuration file are as follows:

Keyword	Description
IP	<p>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.</p> <p>Example: IP=192.168.100.10</p>
Netmask	<p>Specifies the network IP subnet mask.</p> <p>Example: NETMASK=255.255.255.0</p>
Gateway (optional)	<p>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.</p> <p>Example: GATEWAY=192.168.100.1</p>
Bootpto (optional)	<p>Overrides the time-out value (in seconds) for BOOTP/DHCP.</p> <p>Example: BOOTPTO=60</p>
Receive_Mode (Ethernet only)	<p>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.</p> <p>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 provide all packets being sent on the network.</p> <p>Example: RECEIVE_MODE=6</p>

Cloning with Linux

This appendix contains the following:

- [Supported configurations](#)
- [Position of disk](#)
- [Boot configuration](#)
- [Symantec Ghost utility support](#)

Supported configurations

Symantec Ghost can clone many different Linux distributions successfully. However, Symantec Ghost is sensitive to any possible changes in ext2 file system and LILO specifications. If changes are made to these specifications, Symantec Ghost may no longer support the Linux distribution. Symantec attempts to release new builds of Ghost promptly to address such changes.

Symantec Ghost is not sensitive to kernel versions. Use the `-nolinux` and `-nolilo` command-line switches to resolve problems with any incompatibilities.

For more information, see [“Command-line switches”](#) on page 297.

Symantec Ghost clones any x86-based Linux system with full support for ext2 file systems (type 0x83) containing 1 KB, 2 KB, or 4 KB block sizes. Other file systems, for example, reiserfs, are cloned on a sector-by-sector basis and cannot be resized during cloning.

Linux systems that use LILO as their boot loader in the MBR or in the active ext2 partition are supported with some exceptions. 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. `/boot` can be a directory within the root file system.

Symantec Ghost supports type 0 and type 1 Linux swap file systems (type 0x82).

Symantec Ghost partially supports Linux extended partitions (type 0x85). It clones 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.

Position of disk

Linux is sensitive to the position of the disk in hardware. A system running on the primary master disk does not run if the disk is mounted as the primary slave or as the secondary master. Symantec Ghost does not resolve this issue.

Boot configuration

Symantec Ghost uses the file `/etc/lilo.conf` to determine the boot configuration. If this file does not match the boot configuration, Symantec Ghost may be unable to patch LILO during cloning. It does not support the default keyword in `Lilo.conf`, so the first target specified should be the default target.

If a different boot loader is used, for example, `grub`, or the above conditions are not met, Symantec Ghost clones the system but the new disk probably won't boot afterwards. It should be started from a floppy disk or CD, and the boot loader should be reinstalled by running `/sbin/lilo` or an equivalent. Always have a boot disk available in case of problems starting a Linux system after cloning.

Symantec Ghost utility support

Ghost Explorer substantially supports ext2 file systems within image files, including the restoration, deletion, and addition of files within these file systems. Problems arise when files are manipulated that have names that are illegal on Windows. Ghost Explorer cannot manipulate device files or symbolic links. Sparse files are expanded on restoration, and hard links are broken.

GDisk does not create any Linux file systems, or recognize any partitions within a Linux extended partition.

Customizing Symantec Ghost functionality

This appendix contains the following:

- [Limiting functionality from the environment file](#)
- [Examples of customized functionality](#)
- [OEM version of Symantec Ghost](#)

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 licensed user's details
- The maximum number of licensed concurrent users
- Additional product licensing information
- Functionality switches

The following switches are available:

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	Perform Disk-to-disk and partition-to-partition actions
PEER	Connect via LPT, USB, TCP/IP peer-to-peer
FPRNT	Creates fingerprint. A fingerprint is a hidden mark on a cloned drive or partition that includes the following: <ul style="list-style-type: none">■ 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

To tailor Symantec Ghost functionality

- 1 Manually edit the environment file, Ghost.env.
The file should be located in the same directory in which Ghost.exe is started unless otherwise configured.
- 2 Add a switches parameter line as the first line of the environment file.
Each feature except IMGTMO can be activated with switchname=y or deactivated 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 line:

```
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
```


Examples of customized functionality

Following are examples of how system administrators can customize functionality for end users of Symantec Ghost.

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.

Enabling image file restoration only

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 1024

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.

Using Symantec Ghost as a backup tool

Switches: load=n,dump=y,disk=n,peer=n

OEM version of Symantec Ghost

Symantec Ghost can be further customized for OEM customers. Contact Symantec for more information about this version.

For more information, see [“Service and support solutions”](#) on page 357.

Troubleshooting

This appendix contains the following:

- [Symantec Ghost error message](#)
- [Symantec Ghost Console errors](#)
- [Symantec Ghost GhostCast errors](#)
- [Symantec Ghost and GhostCast DOS errors](#)
- [Running command-line or scheduled tasks](#)

Symantec Ghost error message

A Symantec Ghost error message consists of an error number, a description, and possibly a suggestion to remedy the problem. Make sure that you are running the latest version of Ghost as many errors have been fixed.

A Ghosterr.txt file is generated when an abort error occurs.

For more information, see [“Diagnostics”](#) on page 345.

Further information is available on the Symantec Ghost Technical Support Web site.

For more information, see [“Service and support solutions”](#) on page 357.

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. For more information, see “Command-line switches” on page 297.
10010,10014, 11000	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. You may need to add the line RECEIVE_MODE = 6 to Wattcp.cfg. For more information, see “The Wattcp.cfg network configuration file” on page 331.
19910, 20070	No packet driver was found. For more information, see “When I launch Symantec Ghost, I am unable to select GhostCasting” on page 341.
19913	Can't 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.
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.

Symantec Ghost Console errors

If a task to restore a back up fails and your back ups are stored in a mapped network location, ensure that the network connection is still available.

Symantec Ghost GhostCast errors

If you are having problems using Symantec Ghost or the Symantec Ghost GhostCast Server ensure that:

- You have the latest version of Symantec Ghost and the latest version of the Symantec Ghost GhostCast Server.

The latest versions of Symantec Ghost, the Symantec Ghost GhostCast Server, and all Symantec Ghost-related utilities are available at:

<http://www.symantec.com/techsupp/files/ghost/ghost.html>

- 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.

Following are specific answers to certain situations. Use the solution most closely related to the problem that you are experiencing.

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.

For more information, see [“Boot disks with network support”](#) on page 136 and [“Setting up packet drivers”](#) on page 199.

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:

- 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.

You can also try pinging the IP address of the client computer from the server computer.

To ping the IP address of the client computer

- 1 Start the client computer.
- 2 On the Symantec Ghost main menu, click **GhostCast** and select one of the following:
 - Unicast
 - Direct Broadcast
 - Multicast

Do not enter a session name. This will initialize the IP address.

- 3 Ping the client from the server.

If you are not able to ping the client, there is a communication problem and IP packets are not being passed between these computers.

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.

For more information, see [“The Wattcp.cfg network configuration file”](#) on page 331.

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.

When I try to launch the Symantec Ghost GhostCast Server on a Windows 95 computer, I get the error message “A required DLL file, WS_32.DLL, was not found” or “RMLstartup failed: host not found”

Obtain and install the Winsock2 update available from Microsoft. A document containing the current location of this file is located at:

<http://service1.symantec.com/SUPPORT/ghost.nsf/docid/1998101316275025>

Symantec Ghost and GhostCast DOS errors

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. The DOS configuration utility lets you set these explicitly.

Running command-line or scheduled tasks

Normal task logging can be viewed from the Console task log.

For more information, see [“Monitoring the Symantec Ghost Console activity”](#) on page 151.

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.

For more information, see [“Creating a backup regime”](#) on page 102.

Diagnostics

This appendix contains the following:

- [Hard drive detection and diagnostic information](#)
- [Elementary network testing techniques](#)

Hard drive detection and diagnostic information

Symantec Ghost can generate several diagnostic reports outlining the hard drive devices detected, other system-related information, and error conditions when they are detected.

Symantec Ghost 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 an erroneous condition is detected by the software 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 generated by Symantec Ghost during an abort can be altered using the -afile=drive:\path\file name command-line switch.

For more information, see [“Troubleshooting”](#) on page 339.

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`. The location and file name of a file generated by Symantec Ghost can be altered by adding the `-dfile=drive:\path\filename` command-line switch.

Elementary network testing techniques

There are two 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 of two Windows 95 TCP/IP utilities, `Ping.exe` and `Winipcfg.exe`, are included below. On Windows NT, the equivalent utilities are `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.

Ping utilities that do not indicate multicast packets can traverse between two points on a network. 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. The address used in the following example identifies the local host on the network.

Pinging a local host

In a Windows DOS prompt dialog box on a Windows 95 computer with a computer name Win95PC1, the following command is entered:

```
c:\> ping LocalHost
Pinging Win95PC1 [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
```

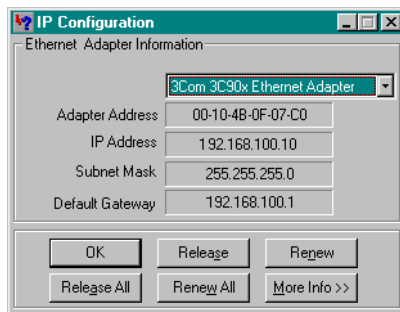
This test indicates that the TCP/IP stack is installed and operating.

Pinging a Symantec Ghost multicast client

On the GhostCast Server, a Windows 95 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
C:\>winipcfg
```

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. Winipcfg then verifies that the Windows 95 computer's IP configuration parameters are as follows:



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:

- **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.
- **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.

The Windows Symantec Ghost GhostCast Server log file

You can generate a log file while running the Windows Symantec Ghost GhostCast Server.

To generate a log file

- 1 On the GhostCast Server, on the File menu, click **Options**.
- 2 Select the desired logging level:
 - Error
 - Statistics
 - Warning
 - Information
 - All
- 3 Do one of the following:
 - In the Options dialog box, in the Log File field type the log file location and name.
 - Click **Browse** to select a location for the file.
- 4 Use the Symantec Ghost GhostCast Server as required.

The Symantec Ghost GhostCast Server can be used for normal operation and the log file can be inspected upon completion.

The DOS Symantec Ghost GhostCast Server log file

You can generate a log file while running the DOS Symantec Ghost GhostCast Server.

For example:

```
dosghsrv.exe c:\test123.gho TestSession -la -n10
```

starts a GhostCasting session called TestSession and uses the file c:\test123.gho. The connecting client's IP address appears on-screen. The session transmission starts when 10 clients have connected. A log file, Ghostlog.txt, is created for debugging purposes. Using a log file reduces the performance of the GhostCast transmission.

To generate a log file while using dosghsrv

- 1 Add the logging switch -l<loglevel>, where loglevel specifies the diagnostic reporting level (E, S, W, I, or A).
- 2 Use the DOS Symantec Ghost GhostCast Server application.
- 3 Use other command-line options as required.

The Symantec Ghost GhostCast Client log file

You can generate a log file while running Ghost.exe on a client computer.

To generate a GhostCast log file in Symantec Ghost

- 1 Add the logging switch -jl:loglevel = filename, where loglevel specifies the diagnostic reporting level. (E, S, W, I, or A.)

ghost.exe -jl:a=d:\filename

- 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 Use the Symantec Ghost GhostCasting application.

On completion, the log is written to the selected location.



Installing Symantec Ghost from the command line

This appendix contains the following:

- [Choosing an interface type for installation](#)
- [Choosing an installation mode](#)
- [Installing from the command line](#)
- [Uninstalling from the command line](#)

Choosing an interface type for installation

Microsoft Windows Installer lets you choose the interface that you'll see during installation. If you are installing in Basic or Silent mode, you must run the installation from the command line. If you are using a Windows 9x or Windows NT computer, then you must run the installation from a setup file.

For more information, see [“Installing from the command line in Windows 9x or NT”](#) on page 354.

The interface modes are as follows:

- The Full interface mode guides you through a series of dialog boxes to install Symantec Ghost, letting you change settings, such as selecting components and changing directories. This mode does not require passing parameters in the command line.
- The Basic interface mode shows a progress bar and any system level error messages. If you alter any default settings, you must pass this information through as parameters from the command line. The syntax for this installation is:

```
msiexec /i "c:\temp\Symantec Ghost 2002.msi" /qb
```


- 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 the Symantec Ghost Console, the syntax is:

```
msiexec /i "c:\temp\Symantec Ghost 2002.msi" /q
```

To install any other component, the syntax is:

```
msiexec /i "c:\temp\Symantec Ghost.msi" /q  
ghostinstalltype="xxxxxx"emailaddress="zzzzzz"
```

where xxxxxx is any of the following:

- Server = Symantec Ghost Console
- Server Tools = Standard Tools only
- Client = Console client
- AutoInstall = AutoInstall

Choosing an installation mode

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. The installation modes are as follows:

- 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.
- 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 clicks the shortcut or opens one of the associated files, the component is installed. Therefore only those components that the user needs are installed. The syntax for this installation is:

```
msiexec /j "c:\temp\Symantec Ghost 2002.msi"
```

- 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 installation requires administrative privileges. The syntax for this installation is:

```
msiexec /a "c:\temp\Symantec Ghost 2002.msi"
```


- 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 clicking Add/Remove Programs in the Control Panel and clicking Ghost. You can also run this mode from the command line. The syntax is as follows:

```
msiexec /f "c:\temp\Symantec Ghost 2002.msi"
```

The switch /fa reinstalls all files, /fu rewrites all required user registry entries, and /fs overwrites any existing shortcuts.

- The Modify installation mode lets you change the user's current configuration. To do this, click Add/Remove Programs in the Control Panel, then click Symantec Ghost.

Installing from the command line

You can specify parameters when installing Symantec Ghost from the command line by setting installer packages. The syntax for these packages is:

```
msiexec /i "c:\temp\Symantec Ghost 2002.msi" /q PROPERTY = VALUE
```

The property name must be in uppercase, and the value is case-sensitive.

On Windows 2000 computers, Msiexec.exe is in the path by default, so it can be called from any directory. However, on Windows 9x and Windows NT systems that have Windows Installer installed, Msiexec.exe is not in the path. It is always located in the Windows\System directory on Windows 9x systems, and in Winnt\System32 on Windows NT systems.

If you are installing in Administration mode, you don't need to set these properties as you are copying the installation package to a location on the network. Set these properties once you run the installation from the network location.

You must set a user name, company name, and email address in the command line, or the installation fails. An error file, Ghmsierr.txt, is generated in the Windows System folder if the installation fails.

The following table shows the package properties that can be set from the command line.

Property	Default value	Description
INSTALLDIR	Program files\Symantec\Ghost	Destination directory
USERNAME	Registered user	User name
COMPANYNAME	Registered company	Company name

Installing from the command line in Windows 9x or NT

If you are running Windows 9x or Windows NT and you do not have Windows Installer installed, then the installation must be performed through a setup file. Setup.exe is located in the same directory as Symantec Ghost.msi. The following table contains the switches that can be used with Setup.exe.

Switch	Description
/s	Runs installation in Silent installation mode
/a	Runs installation in Administrative installation mode
/j	Runs installation in Advertise installation mode
/s	Runs installation in Silent installation mode
/x	Uninstalls the application
/f	Runs installation in Repair installation mode
/v	Passes the parameters to Msiexe.exe

The /v switch is used to pass 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 with a backslash.

The following command line installs the client in a specified destination folder, changes the default user name, specifies the console server computer name, and runs the installation in the Silent installation 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.

To uninstall Symantec Ghost from the command line

- In DOS type the following command:
**Msiexec /x "<path to msi package> \Symantec Ghost 2002.msi"
[/q or /qb]**

The switches /q and /qb are optional.

For more information, see [“Installing from the command line”](#) on page 353.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- Online Service and Support

Connect to the Symantec Service & Support Web site at <http://service.symantec.com>, select your user type, and then select your product and version. This gives you access to current hot topics, knowledge bases, file download pages, multimedia tutorials, contact options, and more.

- PriorityCare telephone support

PriorityCare fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

You can also access the PriorityCare number for your product through the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options available for your product and version.

- Automated fax retrieval

Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 726-9410.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information by mail. Telephone support will be provided for the old version for at least 6 months after the release of the new version. Technical information may still be available through the Service and Support Web site (<http://service.symantec.com>).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Services and Support Web site only.

Customer service

Access customer service options through the Service & Support Web site at <http://service.symantec.com>. From this site, you can receive assistance with non-technical questions, and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at:
<http://www.symantecstore.com>

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to <http://service.symantec.com> and select your region under the Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

<http://www.symantec.com/>
Fax: (541) 335-5020

Automated Fax Retrieval

(800) 554-4403
(541) 726-9410

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

<http://www.service.symantec.com/mx>
+54 (11) 5382-3802

Asia/Pacific Rim

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

<http://www.service.symantec.com/br>
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

<http://www.service.symantec.com/mx>
+52 (5) 661-6120

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

<http://www.service.symantec.com/mx>

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

July 13, 2001

Symantec Ghost™

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ☐ CD Replacement

Name

Company Name

Street Address (No P.O. Boxes, Please)

City State Zip/Postal Code

Country* Daytime Phone

Software Purchase Date

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem:

CD Replacement Price \$ 10.00
Sales Tax (See Table) \$ 9.95
Shipping & Handling
TOTAL DUE

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

☐ Check (Payable to Symantec) Amount Enclosed \$ ☐ Visa ☐ Mastercard ☐ American Express

Credit Card Number Expires

Name on Card (please print) Signature

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.

Symantec and Symantec Ghost are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2001 Symantec Corporation. All rights reserved. Printed in the U.S.A.



G L O S S A R Y

AutoInstall package	An executable, created by AI Snapshot and AI Builder, containing one or more applications that can be distributed to client computers using the Symantec Ghost Console.
backup regime	A group of settings that determine which computer to include in a backup task and other details, for example, scheduling.
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. 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	Creating one or more replicas of a source computer.
configuration settings	Registry settings for client computers that can be set during the execution of a Console task.
Console client	Client of the Symantec Ghost Console that allows remote control of the client computer.
data template	A template that defines files or registry entries to include in a backup.
dump	Create an image of a computer.
image file definition	A description of the properties of an image file, including the image file name, location, and status.
image file	A file created using Symantec Ghost. An image file of a disk or partition is created and is used to create exact duplicates of the original disk or partition.
GhostCasting	A method of cloning to one or a group of computers simultaneously across a network.
load	Overwrite all existing data on a computer with an image file, or directly with a copy of another computer.

package definition	A link from the Console to an AI package, either on an attached drive or on a Web server.
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 cloned onto other client computers.
Creating an image file	<p>Specifies a series of steps to be performed on all selected computers including:</p> <ul style="list-style-type: none">■ Cloning of an image file■ Applying configuration settings■ Loading software applications■ Loading user settings■ Loading a file■ Creating a backup■ Restoring a computer from a backup
user package	The data captured in a Move the User operation. These packages can be used to restore a user's data and settings to another computer.
user profile	A definition of the data that you want to capture during a Move the User operation.

I N D E X

Symbols

? switch 303
@filename switch 298

A

Abort log 298, 345
Accessibility 32
Active tasks 154
Adding, Data Template information 110
Advanced options 85, 90
afile=filename switch 298
AI package definition 78
Application image files 236
ASPI driver 327
Auto Start 186
auto switch 298
Autoexec.bat, multicast
 NDIS driver 203
 Packet driver 199
AutoInstall
 Builder 236, 245-250
 Installing Microsoft products 238
 Limitations 239
 Office XP 238
 Overview 235
 Package definition 364
 Snapshot 236, 241, 245
 Uninstall command 238
 Using 241
Automation
 Batch switch 298
 Clone switch and examples 314, 317-319
 Close on completion 303
 Quiet mode 309
 Remove confirmation 311
 Restart on completion 309
 Switches 297-313
 Version checking 312, 313

B

Backup 363
 Creating a regime 102
 Manual 105
 Regime 101
batch switch 298
bfc=x switch 298
Boot disk 214
 Creating manually 198
 Setup 228
Boot menu 274
Boot package 134, 363
 Creating 133, 134
 Setup 133
Boot partition 17, 24, 64, 90, 363
bootcd switch 299
BOOTP 208, 208-209
Bootstrap Protocol. *See* BOOTP
bufferize switch 299
Builder 236, 245-250

C

Cables 329
Capturing, User Data 113
CD bootable disk 168, 217, 222, 226
CD writers 168, 226
CD-R/RW
 Cloning to 226
 Write to 135
CD-ROM 327
 Support 140
Certificate files, generating 160
chkimg,filename switch 299
Client heartbeat 61
Client initiated tasks 82, 154
Client summary 153
clone switch 299, 314
Clone task properties 89

- Cloning 24, 363
 - Compression 162
 - Speed 162
 - To a CD-R/RW 226
 - Windows 2000 169
- Close Ghostsrv on completion 190
- cns switch 299
- Command line 85, 90
 - Examples 317-322
 - Symantec Ghost 297-313
- Command task properties 96
- Compression 162, 222
- Computer identification
 - Details 288
- Computer, renaming 61
- Computers, viewing properties 64
- Config.sys 202
- Configuration
 - Default settings 91
 - Files 236
 - Server 49, 154
 - Timeout 158
 - Settings 64, 363
 - Creating 71
 - Custom 92
 - Novell NetWare 76
 - Standalone 229
 - Template 91
 - Standalone 19
 - Task properties 91
- Configuration data file 230
- Console
 - Changing servers 160
 - cloning 24
 - Heartbeat 18, 154
 - Security 159
 - Wizard 156
- Console client 24, 27, 63, 141, 363
 - Remote installation 17
 - Status 63
 - Updating 47
 - Version 64
- Console options
 - Splash screen 156
 - Task log 157
 - Warn client 157
 - Watermark 154

- Copy command 314
- crc32 switch 163, 300, 301, 319
- crcignore switch 300
- Creating
 - Backup regime 102
 - Data Template 108
 - Machine Groups 59
 - Partition 266
 - Tasks 69
- Custom settings 92
- cvtarea switch 300

D

- Data checking 163
- Data compression 162
- Data Template 363
 - Adding information 110
 - Creating 108
 - Specifying files 108
 - Specifying registry keys 110
 - View 111
- Data throughput limits 61
- Data transfer mode 61, 85, 154, 187
- dd switch 301
- Decompression 162
- Default settings 91
- Deleting, Partitions 271
- Deploy AI package, task properties 92
- dfile=filename switch 301
- DHCP 208, 208-209
- Diagnostics 345-350
- Direct broadcast 18, 61, 175, 189
- Directory location variables 115
- Disk
 - Dynamic 169
 - Large 278
 - Status 269
- dl=number switch 301
- Documentation 33
- Domain
 - Accounts 49
 - Removing a computer from 85
- DOS
 - IBM DOS 133
 - MS-DOS 25, 68, 150, 156
 - PC-DOS 68, 150, 156

dst switch 316
Dump 179
 Command 314
 Task 83
Dynamic disks 18, 169
Dynamic Host Control Protocol. *See* DHCP

E

Environment file 336
error message 339
Errors
 GhostCast 341
 Task 344
Event 153
 Details 153
Execute task 97

F

f32 switch 301
f64 switch 301
fatlimit switch 301
fcr switch 301
fdsp switch 301
fdsz switch 302
femax switch 302
ffi switch 302
ffs switch 302
ffx switch 302
File system
 FAT12 256
 FAT16 256
 Windows NT 271, 301
 FAT32 256
 Conversion from FAT16 301
 Linux Ext2 256, 268
 NTFS, switches 307
File transfer task properties 95
Files
 Skipping 310
 To specify Data Template 108
finger switch 302
Fingerprint. *See* Symantec Ghost
fis switch 303
fni switch 303
fns switch 303

fnx switch 303
fro switch 303
fx switch 303

G

Gateway. *See* TCP/IP settings
GDisk 31, 264
 Batch mode 269
 Command line switches 265
 Large hard disks 278
 Switches 264-277, 278
GDisk32 18, 263
 Modifying boot menu 274
General task properties 88
Ghost
 OEM version 338
Symantec Ghost
 See also Procedures
Ghost Boot Wizard 28
 Bootable CD 168
 Starting 134
 Writing to a CD 168, 226
Ghost Console 26, 159
 Components 56
 User options 154
 Using 50
Ghost Explorer 31
 Command line 260
 Switches 260
Ghost operation, operating system 214
Ghost partition 24, 27
Ghost Walker 30, 287-293
 Command line 289
 Switches 289
Ghost. *See* Symantec Ghost
Ghost.exe 22, 24, 30, 176, 190, 215
GhostCast 61, 176, 191, 363
 Address 190
 Automating 184
 Command line 183
 Dump from client 178, 179
 From the server 183
 Load to clients 178, 181
 Network bandwidth 188
 Session 178
 Setup 177

GhostCast *(continued)*
 Boot disk 199
 Quick guide 176-177
 See also Packet driver
 See also TCP/IP settings
GhostCast Server 18, 24, 28, 187
 Automating 190
 Buffer 190
 Direct broadcast 18, 187
 DOS 194
 Log 190
 Multicast 18, 187
 NetWare 190
 Options 190
 Reducing network traffic 18
 Switches 198
 Unicast 18, 187
 Windows 176, 193
GhostCast setup. *See* Packet driver
Ghosterr.txt. *See* Abort log
Grouping computers 58
 By subnet 61

H

h switch 303
Hard disk
 Active 264
 Batch 264
 Creating 264
 Deleting 265, 271
 Hiding partitions 264
 Large drives 278
 MBR 264
 Status 265
 Wiping 271
Heartbeat interval 18, 64
Hibernation files 170
Hiding Partitions 273

I

ia switch 304
ial switch 304
ib switch 304
id switch 304
Image definitions 70, 363

Image files 363
 Add definition 70, 78
 Applications 235
 CD writers 168
 Compression 162, 218, 313
 crc. *See* crc32
 Creating 24, 165, 215
 Insufficient space 165
 File list 258
 Loading 166
 Modification 258
 Multisegment 164, 298, 311
 Password 309
 Restoring 257
 Size limited. *See* Image files multisegment
 Spanned 164-166, 259, 298, 310
 Spanning 164
 Split. *See* Image files, multisegment
 Standard 164
 Tape drives 166
 Viewing contents 257
Internal drives 328
IP address. *See* TCP/IP settings
ir switch 305

J

ja=sessionname switch 305
jl x=filename switch 305
js=n switch 305

L

License Audit Utility 32, 281-283
Linux 214, 217, 256, 268, 304
LiveUpdate 47
Load
 Command 314
 Image 181
lockinfo switch 306
locktype=type switch 306
Log 153
 Clients 190
 Level and File 190
lpm switch 306
lps switch 306
LPT port 136, 326

M

- Machine Groups 58
 - Adding a computer to 60
 - Creating 59
 - Removing computers from 60
 - Renaming a computer 61
 - Restrictions 59
 - Viewing properties 64
- Manual Backup 105
- Mapped drive setup 328
- Mapping network drives 138
- Master 325
- MBR 308
 - Reinitializing 265
- memcheck switch 307
- Microsoft system file protection (SFP) 239
- Mode switch 314
- Model computer 82, 177
- Move the User 92, 107
 - Relative paths 116
 - Settings 117
- MS-DOS 150
- Multicast 18, 61, 136, 175, 189, 327

N

- NDIS driver 202
 - Protocol manager files 201
- Netmask. *See* TCP/IP settings
- Network 85, 328
 - Bandwidth 85, 154, 188
 - Performance 162
 - Routers, IP multicast 305
- Network drives
 - Mapping 138
- NIC packet driver 199
- nofile switch 307
- nolilo switch 307
- noscsi switch 307
- Novell NetWare 18, 76
- ntc switch 307
- ntchkdsk switch 307
- ntd switch 307
- ntic switch 307
- ntiid switch 308
- ntil switch 308

O

- OEM version 338
- Operations of Symantec Ghost. *See also* Procedures
- Optimizing data transfer 85
- Options 85, 90
- or switch 308

P

- Packet driver 199, 200
 - NIC 200
- Parallel port transfer
 - Automation 306, 312
 - Setup 325
- Partition 264
 - Boot 17, 24
 - Cloning 221
 - Creating 266
 - FAT id 302
 - Hiding 273
 - Status 269
 - Virtual 17, 24
- Password 287, 293, 309
- PC-DOS 150
- pcopy command 314
- pdump command 314
- Peer-to-peer connections 325
- Performance network 162
- ping utility 346
- pload command 314
- pmbd switch 308
- Private certificate files 159
- Procedures
 - Disk cloning 215
 - From image file 220
 - To disk 216
 - To image file 218
 - GhostCasting 176-191
 - Partition cloning 221
 - From image file 224
 - To image file 223
 - To partition 221
- Profile, user 108

Properties

- Backup regime 103
- Clone 89
- Command 96
- Configuration task 91
- File transfer 95
- General 88
- Protocol.ini, NDIS driver for multicasting 202
- Public certificate files 159
- pwd, -pwd=x switch 309
- PXE 142, 144

Q

- quiet switch 309

R

- RAID 169, 308
- rb switch 309
- Regime, Incremental 101
- Remote installation, Template 67
- Removing
 - Computer from a domain 85
 - Computer from a group 60
- Renaming computers 61
- Restart on completion 190
- Restoring
 - Backup 106
 - User Data 113
- RIS 135, 142

S

- Schedule, Backup regime 104
- Scheduling tasks 97
- script switch 309
- SCSI drivers, Adaptec 135
- SCSI tape
 - drives 167
 - Setup 327
 - Switches 311-312
- Sector, bad 298, 303, 313
- Sector-by-sector copy 304
- Security 18, 159
- Service and Support 357
- Session name 178

- Setting task properties 88-96

- Setup 198, 199, 328
 - NDIS driver and shim 201
 - NIC packet driver 200
 - ODI driver and shim 199
 - See also* GhostCast
 - See also* Network mapped drive
 - See also* SCSI Tape

- SID 126, 132
- skip=x switch 310
- Skipping files 170
- Slave 325
- Snapshot 236, 241, 245, 364
- Source computer 364
- span switch 310
- Spanning 164-166, 169
 - Override 308
 - To a CD-R/RW 226
- split=x switch 311
- src switch 315
- Standalone configuration 19, 229
 - Running 231
- Subnet
 - Grouping computers 61
- Subnet mask. *See* TCP/IP settings
- sure switch 311
- Swap files 170
- Symantec Ghost
 - Fingerprint 302
 - Switches 297-322
 - Updating 47
- Sysprep 125
 - .inf 132
- size switch 316

T

- Tape drives 166
- tapebsize switch 312
- tapebuffered switch 311
- tap eject switch 311
- tapesafe switch 311
- tapespeed=x switch 312
- tapeunbuffered switch 312

Task 87

- Backup regime 104
 - Client initiated 18, 82, 154
 - Clone properties 89
 - Command properties 96
 - Configuration properties 91
 - Creating 57, 69
 - Deploy AI package properties 92
 - Dumping 83
 - Executing 57, 97
 - File transfer properties 95
 - General properties 83, 88
 - Log 152
 - Move the User 113
 - Scheduling 97
 - Sysprep 83
 - View 96
 - Wake On Lan 83
- TCP/IP 136, 144, 326
- Settings 205-209
 - See also* BOOTP
 - See also* DHCP
 - See also* Wattcp.cfg
- tcpm switch 312
- tcps switch 312
- Technical Support 357
- Template settings 91
- Terminal Services 18
- troubleshooting 339

U

- Unicast 18, 61, 175, 189
- Updating
- Computer name 288
 - Console client 47
 - SID 288
 - Symantec Ghost 47
- USB port 326
- Support 136
- usb switch 313
- usbm switch 312
- usbs switch 313

User

- Capturing Data 113
- Move the 107
- Package 364
- Profile 108, 364
- Restore Data 113
- Viewing a Profile 113

Using

- AI Builder 245-250
- AI Snapshot 241, 245
- AutoInstall 241
- Console 50

V

Variables

- Directory location 115
- Move the User 113, 116

vdw switch 313

ver switch 313

ver=value switch 313

vexcept switch 322

View

- Backup regime 105
- Data Template 111
- Tasks 96
- User Profile 113

Virtual partition 17, 24, 64, 68

W

Wake on Lan 83, 86

Watermark 32, 154

Wattcp.cfg 199, 206, 207

See also TCP/IP settings

Windows

2000 169

Boot menu 274

Running Ghost 214

Wiping

Disks 271

Partitions 271

Writing to a CD-R/RW 168, 226

Z

z switch 313