

# 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.

## Copyright Notice

Copyright © 1998–2001 Symantec Corporation.

All Rights Reserved.

Documentation version 7.0

PN: 07-30-00455

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, Norton 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

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

## LICENSE AND WARRANTY:

The software which accompanies this license (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. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

- (i) use Symantec Ghost to clone a hard drive from another disk, partition, or image file onto that number of hard drives equal to the number of Symantec Ghost licenses granted by Symantec under this license;
- (ii) reapply, upgrade, refresh, or recover a hard drive an unlimited number of times provided that the hard drive is part of the original Symantec Ghost licenses granted by Symantec under this license;
- (iii) reuse a Symantec Ghost license to apply an image file to a replacement hard drive provided the replaced hard drive has been permanently decommissioned.

You may not:

- (i) copy the documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software; or
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, create derivative works from the Software, reuse the license as a reseller of systems containing the hard drive, or redistribute Symantec Ghost for disaster recovery or any other purposes.

## Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

## 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. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

## Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC 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.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

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

## 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. §27.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §27.7202 through 27.7202-4, 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 Boulevard, Cupertino, CA 95014.

## General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

---

# C O N T E N T S

## Section 1 Getting started

### Chapter 1 Introducing Symantec Ghost

About Symantec Ghost .....	17
New features in Symantec Ghost .....	18
How Symantec Ghost works .....	18
What you can do with Symantec Ghost .....	20
PC management using Symantec Ghost .....	20
Using Symantec Ghost without the Console .....	21
Quick reference guide .....	23

### Chapter 2 Understanding Symantec Ghost basics

Choosing a method to create an image file .....	25
Symantec Ghost components .....	27
Symantec Ghost Console .....	27
Symantec Ghost Console client .....	28
Symantec Ghost Multicast Server .....	28
Ghost Boot Wizard .....	29
Symantec Ghost AutoInstall .....	30
Symantec Ghost executable .....	30
Ghost Walker .....	31
Ghost Explorer .....	32
GDisk .....	32
License Audit Utility .....	33

### Chapter 3 Installing Symantec Ghost

Preparing for installation .....	36
System requirements .....	36
What to install .....	37
Installing the Symantec Ghost Enterprise Console .....	38
Installing the Console client .....	38
Installing Symantec Ghost Standard Tools .....	39
Installing the Symantec Ghost Console client for the first time .....	39
Updating Symantec Ghost .....	43
Updating the Symantec Console client .....	43
Uninstalling Symantec Ghost .....	44

---

## Section 2 Creating image files and managing tasks from the Console

### Chapter 4 Managing image files, configuration resources, and computers

Using the Symantec Ghost Console .....	47
Creating and executing a Symantec Ghost Console task .....	48
Starting the Symantec Ghost Console .....	49
Grouping Console client computers .....	50
Adding or moving a computer to a group .....	51
Storing the Console client computer details .....	52
Checking client software and status .....	53
Removing a computer from a group .....	53
Renaming a computer .....	54
Viewing and changing the Console client computer properties .....	55
Editing and applying new default configuration settings .....	55
About the Configuration Resources folder .....	57
Creating and viewing image definitions .....	58
Creating and viewing configuration sets .....	59
Creating and viewing AI package definitions .....	64

### Chapter 5 Creating and executing tasks

Task overview .....	67
Creating image dump tasks .....	68
Setting image dump task properties .....	69
Creating tasks .....	71
Setting task properties .....	72
Reviewing tasks .....	80
Scheduling and executing tasks .....	81

### Chapter 6 Incremental backups and rollbacks

Introducing incremental backups and backup regimes .....	83
Creating a backup regime .....	84
Setting backup regime properties, task, and schedule details .....	85
Creating a backup manually .....	87
Viewing computer backups .....	88
Viewing a backup regime .....	88

Restoring a computer .....	88
----------------------------	----

## **Chapter 7      Move the User**

Introducing Move the User .....	91
Creating a data template .....	92
Viewing a data template .....	94
Creating a User Profile .....	95
Viewing a User Profile .....	96
Capturing and restoring user data .....	97
Variables for directory locations .....	99
Variables for use with Move the User .....	99

## **Chapter 8      Sysprep**

Introducing Sysprep .....	101
Setting up Sysprep .....	102
Cloning with Sysprep .....	103
Editing Sysprep.inf .....	104
How Sysprep works with cloning and the Console	
post-configuration process .....	104
Configuring Sysprep.inf .....	106

## **Chapter 9      Creating boot images and disks with the Ghost Boot Wizard**

Introducing the Ghost Boot Wizard .....	107
Creating boot disks and boot images .....	108
Creating boot disks with network support .....	108
Standard boot disks with the option of LPT and	
USB support .....	110
Creating boot disks that support mapping	
network drives .....	112
Creating boot disks with CD-ROM support .....	113
Creating a boot image containing the Console	
boot partition .....	114
Boot packages that support RIS .....	115
Bootting client computers from the network .....	117
Adding drivers to the multcard template .....	118
Adding network drivers to the Ghost Boot Wizard .....	119
Adding a file to the multcard template .....	119
Adding packet drivers to the Ghost Boot Wizard .....	120
Adding NDIS2 drivers to the Ghost Boot Wizard .....	121
Adding command-line parameters to a boot package .....	122

---

## **Chapter 10 Additional Console options**

Adding users to the user list .....	125
Monitoring the Symantec Ghost Console activity .....	126
Launching the Configuration Server .....	128
Setting the Symantec Ghost Console options .....	128
Symantec Ghost Console security .....	130
Updating the boot partition certificates .....	131
Generating new certificates .....	132
Configuration server password .....	132

## **Chapter 11 Image file options**

About Symantec Ghost image files .....	133
Image files and compression .....	134
Performance expectations on a network .....	134
Image files and CRC32 .....	135
Image files and volume spanning .....	135
Standard image files .....	135
Size-limited, multisegment image files .....	136
Spanned image files .....	136
Spanning across multiple volumes and limiting span sizes ....	136
Loading from a spanned image .....	137
Image files and tape drives .....	138
Image files and CD writers .....	139

# **Section 3 Multicasting image files in a networked environment**

## **Chapter 12 Using multicasting to create and load images**

About Symantec Ghost multicasting .....	143
Preparing for multicasting .....	144
Creating the source computer .....	145
Creating a Multicast Server .....	145
Starting a multicast session .....	146
Controlling the multicast session from the server .....	151
Setting Auto Start parameters .....	154
Viewing and recording Ghost Multicast Server session options .....	155
Running the Symantec Ghost executable .....	155



---

## Chapter 13 Multicasting from the command line

Running the Multicast Server for Windows from the command line .....	157
Running the DOS-based Ghost Multicast Server .....	158
Running the NetWare-based Ghost Multicast Server .....	159
NetWare configuration and software requirements .....	159
Starting the multicast session .....	160
Multicast Server command-line options .....	160
Examples using Multicast Server command-line options .....	161
Creating a DOS boot disk manually .....	164
Setting up packet drivers .....	165

## Chapter 14 Multicasting and IP addresses

Introducing IP addresses for multicasting .....	169
Locally specified IP addresses .....	170
Examples of Wattcp.cfg client configuration files .....	170
Using BOOTP/DHCP to assign IP addresses .....	172
BOOTP/DHCP automatically defined IP address .....	172
Examples of BOOTP/DHCP defined addresses .....	173

## Section 4 Cloning image files locally

### Chapter 15 Symantec Ghost as a standalone program

Starting the Symantec Ghost executable .....	177
Navigating without a mouse .....	178
Using Ghost.exe on a standalone computer .....	179
Cloning disks .....	179
Cloning disk to disk .....	180
Cloning a disk to an image file .....	181
Cloning a disk from an image file .....	183
Cloning partitions .....	185
Cloning from partition to partition .....	185
Cloning a partition to an image file .....	187
Cloning a partition from an image file .....	189
Adding switches to your cloning task .....	191
Cloning dynamic disks in Windows 2000 .....	191
Creating a DOS boot disk .....	192

---

## Section 5 Creating executables to roll out applications

### Chapter 16 Getting started with AutoInstall

How AutoInstall works .....	197
Using AutoInstall .....	198
Installing AI Builder on the distribution server .....	199
Installing AI Snapshot and AI Builder on the model computer .....	199
Setting up target computers .....	200

### Chapter 17 Creating AI packages

Creating an installation script for a software installation .....	201
Capturing existing system information .....	201
Installing the software that you would like to package .....	202
Capturing system information again to determine changes ....	204
Customizing and building AI packages .....	205
Customizing installation scripts .....	207
Building AI packages .....	210
Modifying installation scripts and AI packages .....	210
Executing and rolling out AI packages .....	211

## Section 6 Symantec Ghost utilities

### Chapter 18 Using Ghost Explorer to modify image file contents

About Ghost Explorer .....	215
Viewing image files .....	216
Restoring a file or directory from an image file .....	217
Modifying image files in Ghost Explorer .....	217
Adding, moving, and deleting files .....	218
Saving a list of contents of an image file .....	218
Setting span file sizes .....	219
Compiling a file .....	219
Determining Symantec Ghost image file version .....	219
Using Ghost Explorer from the command line .....	220

---

## **Chapter 19    Managing partitions using GDisk**

Introducing GDisk .....	223
Overview of main command-line switches .....	224
Online Help for command-line switches .....	225
Switches common to all GDisk commands .....	225
Creating a partition .....	226
Reinitializing the Master Boot Record .....	227
Showing information about disks .....	228
Performing multiple GDisk operations using batch mode .....	228
FAT16 partitions in Windows NT .....	230
Deleting and wiping your disk .....	230
Activate or deactivate a partition .....	231
Hide or unhide a partition .....	232
Support for large hard disks .....	232

## **Chapter 20    Tracking Symantec Ghost license numbers**

Setting up the License Audit Utility .....	235
Running the License Audit Utility .....	236
Viewing the database file .....	237
Removing the License Audit Utility .....	237

## **Chapter 21    Updating Security Identifiers (SIDs) and computer names**

Making SID changes with Sysprep and Ghost Walker .....	239
Symantec Ghost Walker capabilities .....	240
Symantec Ghost Walker shortcomings .....	240
Microsoft Sysprep capabilities .....	240
Microsoft Sysprep shortcomings .....	241
Problems with SID changing .....	241
Using Ghost Walker .....	242
Running Ghost Walker from the command line .....	244
Loss of access to external data objects .....	248
Identical user names and passwords across workstations .....	248

---

## Section 7 Appendices

### Appendix A Command-line switches

Symantec Ghost command-line switches .....	251
--	-----

### Appendix B Setting up the hardware and transfer methods

Hardware and transfer requirements .....	277
Peer-to-peer connections .....	277
SCSI tape driver .....	279
Multicasting .....	279
Removable media .....	279
CD-ROM usage .....	279
Mapped network volume .....	280
Internal drives .....	280
Third party device .....	280

### Appendix C USB and DirectParallel Cables

Parallel Technologies cables .....	281
Other USB cables .....	282

### Appendix D The Wattcp.cfg network configuration file

The Wattcp.cfg configuration file .....	283
---	-----

### Appendix E Cloning with Linux

Supported configurations .....	285
Position of disk .....	286
Boot configuration .....	286
Symantec Ghost utility support .....	287

### Appendix F Customizing Symantec Ghost functionality

Limiting functionality from the environment file .....	289
Examples of customized functionality .....	291
Image file restoration only .....	291
Backup tool only .....	291
Saving switches from the Options menu .....	292
OEM version of Symantec Ghost .....	292

---

## **Appendix G Troubleshooting**

Symantec Ghost error message .....	293
Symantec Ghost multicast errors .....	295
Symantec Ghost and multicast DOS errors .....	297
Running command-line or scheduled tasks .....	297

## **Appendix H Diagnostics**

Hard drive detection and diagnostic information .....	299
Symantec Ghost abort error file (Ghosterr.txt) .....	299
Listing hard disk geometry diagnostics .....	300
Creating a full diagnostic statistics dump summary .....	300
Elementary network testing techniques .....	300
Testing TCP/IP functionality .....	300
Generating a multicast log file .....	302

## **Appendix I Installing Symantec Ghost from the command line**

Choosing an interface type for installation .....	305
Choosing an installation mode .....	306
Installing from the command line .....	307
Installing from the command line in Windows 9x or NT .....	308
Uninstalling from the command line .....	309

## **Service and support solutions**

## **CD Replacement Form**

## **Glossary**

## **Index**

---

# 1

## G e t t i n g   s t a r t e d

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

---



# Introducing Symantec Ghost

This chapter contains the following:

- [About Symantec Ghost](#)
- [New features in Symantec Ghost](#)
- [How Symantec Ghost works](#)
- [What you can do with Symantec Ghost](#)
- [Quick reference guide](#)

## About Symantec Ghost

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. New functionality, including computer configuration management, computer/user migration, incremental backup, and compliance with new labor-saving technologies makes Ghost the solution for removing the problems associated with PC management.

## New features in Symantec Ghost

With Symantec Ghost 7.0, you can preserve user setups when loading images onto computers, schedule backups and restore when required, prepare a system prior to cloning using Microsoft Sysprep, and quickly install software applications onto client computers. New features include:

- The Move the User addition to the Symantec Ghost Console lets you save and restore a user's files and personal setup after a cloning operation. This makes moving users to another computer, or updating the operating system on their current computers, a simple task.
- You can create automatic backups of client computers. A time and frequency for backing up a computer are defined. Backups can also be created manually and rolled back as required.
- You can use the Microsoft Sysprep utility when creating an image file of a model computer. Sysprep lets you load images onto computers with different hardware setups.
- The Deploy AI Package feature lets you quickly install software applications onto client computers. This lets you customize networked computers to either an individual's or a group of users' requirements. The packages are created using the Ghost AutoInstall components, AI Snapshot and AI Builder, and are installed, or uninstalled in a simple Symantec Ghost Console task.
- A Getting Started with the Console Guide walks you through the initial installation of the Console. It is a detailed step-by-step guide to installing the Console, setting up client computers, and cloning clients with an image file.

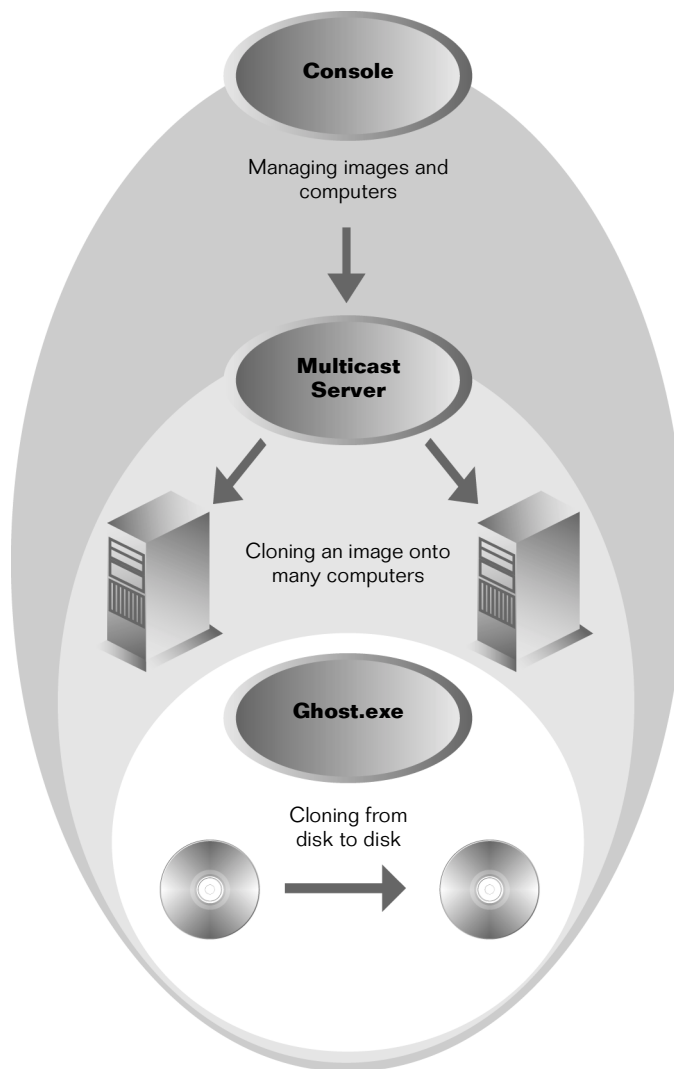
## How Symantec Ghost works

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 (a computer 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.

Multicasting 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 multicasting 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 Multicast Server, and Ghost.exe.



## What you can do with Symantec Ghost

There are many ways in which to use Symantec Ghost and exploit its full functionality to reduce time and cost in maintaining your computers on a network. You can use Symantec Ghost as a PC management tool, and for disk cloning only.

### PC management using Symantec Ghost

Using Symantec Ghost as a PC management tool lets you remotely control client computers, clone image files, migrate users, and perform backups.

#### **Managing computers and image files centrally from the Console**

Cloning a source workstation onto many computers can be time-consuming. One-to-one connections with a small number of computers is fast, but as the number of computers increases, network degradation and the duration of the task increases. Using the Symantec Ghost Console reduces this time with the multicasting functionality. Once you have used the Ghost Boot Wizard to create boot disks to install a boot partition on the client computers, you can remotely control them from the Console.

When the Symantec Ghost Console client is installed on a computer, an icon representing that computer appears in the Console. Icons for any number of computers can be grouped into folders. Then you can create a Console task for an individual computer or a group of computers.

Tasks specify a series of steps to be performed on all selected computers, including cloning, post-cloning configuration, file transfer, and executing a command on the client. The Console can also use Wake on Lan technology to start computers at the beginning of a task and shut them down at the end.

Tasks can be scheduled to execute at any time or on demand, and a complete log of all activities is stored.

## **Migrating a user from one operating system to another**

If you are upgrading a user from one operating system to another, or upgrading a user to a new computer, you can use the Move the User functionality from the Console. Move the User lets you capture configuration and desktop settings and data and transfer them. Once a computer has been installed with the Console client this is done remotely from the Console server computer.

## **Implementing a backup regime**

Part of managing a user's computer is creating a backup plan that lets you quickly and efficiently restore end-user data. Using Backup Regime from the Console, you can create a baseline image of any client computer and subsequently create incremental images of any changes since the last backup. This lets you restore the baseline image and then apply any required subsequent images.

## **Customizing computers**

Using the Console server, you can roll out a base image, often only an operating system, to client computers and then add the appropriate AutoInstall packages containing applications to update computers with required software.

## **Refreshing networked workstations**

Symantec Ghost can refresh computers to a known state at any specified time. For example, in a classroom, you may want to refresh computers to a known state at the beginning of each day, or at the beginning of a class to provide a software environment specific to each subject being taught.

The Console lets you group and view computers and refresh the group on a regular basis.

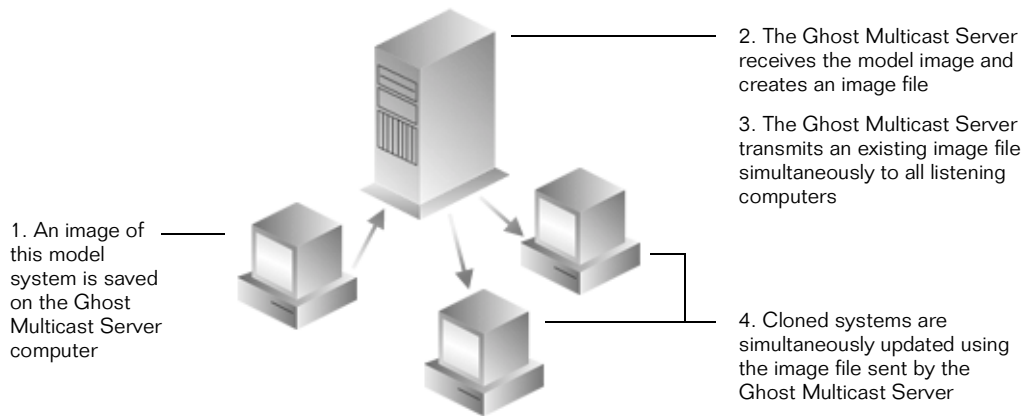
## **Using Symantec Ghost without the Console**

You can use Symantec Ghost as a standalone tool if you do not need remote control of the client computers. Using the Multicast Server and the executable, Ghost.exe, provides cloning capabilities locally and across a network. The standalone version of Symantec Ghost includes all components except for the Console.

### Multicasting an image file to or from a group of computers

A multicasting session consists of a server, an image file, and a group of clients that are to be cloned with the image file. The server and clients join a common session. The client computers are started from a boot disk containing Ghost.exe that has been created using the Ghost Boot Wizard.

IP multicasting is used in conjunction with a reliable session protocol to provide one-to-many communication. Symantec Ghost multicasting supports both ethernet and token ring networks, and removes the bottleneck that occurs when multiple copies of data pass through the network. Symantec Ghost multicasting also includes support for the creation of image files from one workstation at a time.



### Cloning or restoring nonnetworked workstations

The standalone Symantec Ghost executable can create an image file for use as a source image or as a backup.

Create a model computer system. Then use Ghost.exe to create an image file on removable media, such as CD-R/RW, ZIP disks, JAZ disks, or on a hard drive. Once the image is created, use Ghost.exe to create duplicates of the model computer. You can also use an LPT or USB port connection to connect to another computer and clone a disk or partition, or create an image file.

## Installing clean systems from CD-ROMs

Use the Symantec Ghost executable, Ghost.exe, to install a complete Windows 9x system (or other operating system) from an image file on a CD-ROM. For example, a university might issue students a CD-ROM containing an image file and Symantec Ghost. Students can reload their computers from the CD-ROM at any stage, just by starting from the CD. No further user input is required.

Ghost.exe can burn an image file directly onto a CD-ROM and make the CD bootable. The copy of Symantec Ghost included on the CD-ROM can be configured to limit the functionality it provides to the end user, for example, to restore.

For more information, see [“Customizing Symantec Ghost functionality”](#) on page 289.

## Cloning disks at optimum speed using Ghost.exe

Ghost.exe saves you time when:

- Copying one hard drive onto another
- Copying an image file from one hard drive to another when both drives are installed in the same computer

Many computers can transfer data at speeds of 1 gigabyte (GB) per minute. This is an astounding speed especially considering that a compressed image of a drive containing a Windows 98 operating system is a few hundred megabytes in size. Using Ghost.exe to install Windows 98 may take seconds.

# 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 a cross-reference to the associated procedure.

- Create an image of a source computer from a standalone computer.  
For more information, see [“Cloning disks”](#) on page 179.
- Create an image of a networked computer.

- Use the Console if the Enterprise Tools are installed.  
For more information, see [“Creating image dump tasks”](#) on page 68.
- Use multicasting if the Standard Tools are installed.  
For more information, see [“Starting a multicast session”](#) on page 146.
- Create a boot disk for use with a cloning job.  
For more information, see [“Creating boot disks with network support”](#) on page 108.
- 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 242.
  - Use the Console to alter configuration settings.  
For more information, see [“Creating and viewing configuration sets”](#) on page 59.
- Clone a group of computers with one task.  
For more information, see [“Creating tasks”](#) on page 71.
- Clone one or more computers using multicasting.  
For more information, see [“Loading an image file onto client computers”](#) on page 149.
- Clone a computer that is not networked.  
For more information, see [“Cloning disks”](#) on page 179.
- Create an image file containing the boot package needed to start a client computer for multicasting and control from the Console.  
For more information, see [“Creating boot disks with network support”](#) on page 108.
- Create an executable to install an application.  
For more information, see [“Getting started with AutoInstall”](#) on page 197.
- Create a backup regime.  
For more information, see [“Incremental backups and rollbacks”](#) on page 83.
- Migrate a user to a new operating system.  
For more information, see [“Move the User”](#) on page 91.



# Understanding Symantec Ghost basics

This chapter contains the following:

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

## Choosing a method to create an image file

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

- Standalone
- Multicasting
- 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 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 multicasting	<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	<p>The Console draws on the functionality of standalone and multicasting 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.</p> <p>The Symantec Ghost boot partition is installed on every client computer, allowing the existing configuration settings to be captured by the Console. A task is run to clone the client computer with an image file and restore the original configuration settings, or apply new settings.</p> <p>More documentation about the Console can be found in the <i>Getting Started with the Console Guide</i>. It is a detailed step-by-step guide to installing the Console, setting up client computers, and cloning clients with an image file.</p>

# 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 and post-cloning configuration. The installation CD is required to perform a one-time installation of the Console client software, but it is not required on subsequent cloning operations.

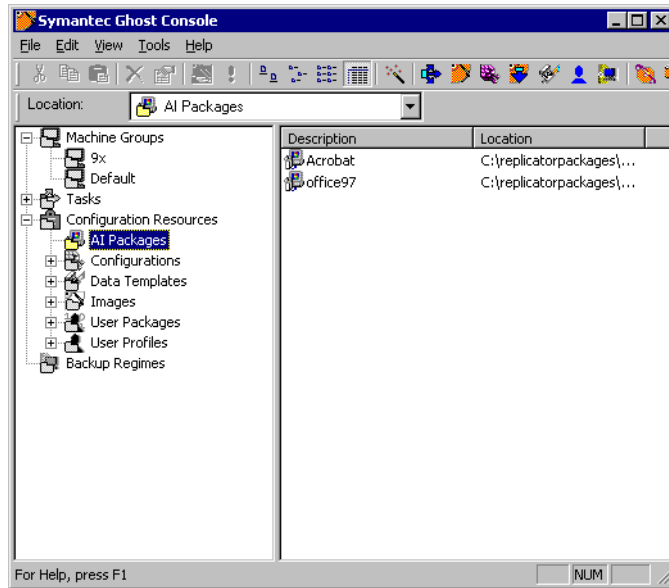
Using the Symantec Ghost Console, IT managers can group targeted computers for a cloning task and initiate the process from the Console.

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

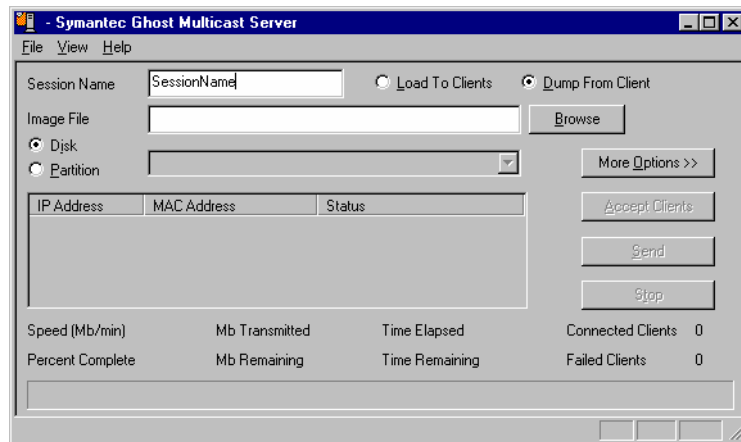
The Console client is comprised of a Windows agent and a Ghost boot partition. The client is installed on all Windows 9x, NT, and 2000 computers, enabling remote control from the Symantec Ghost Console. The Windows agent is an unobtrusive application with no Start menu entry that lets the computer start from the Ghost boot partition when required by the Console. The Ghost boot partition is a hidden DOS partition created using the Ghost Boot Wizard. It is installed on the computer letting the Symantec Ghost executable perform cloning operations.

## Symantec Ghost Multicast Server

The Multicast Server simultaneously delivers an image file to multiple computers using a single IP multicast transmission. It minimizes the impact on network bandwidth by eliminating multiple transmissions of the same image. The Multicast Server sends or receives images to or from one or

more computers rather than accessing a mapped network drive, which is slower than multicasting.

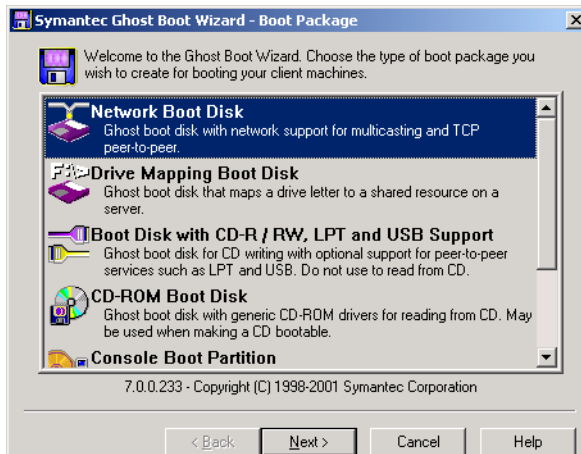
Symantec Ghost  
Multicast Server  
main window



## 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 multicasting, 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.

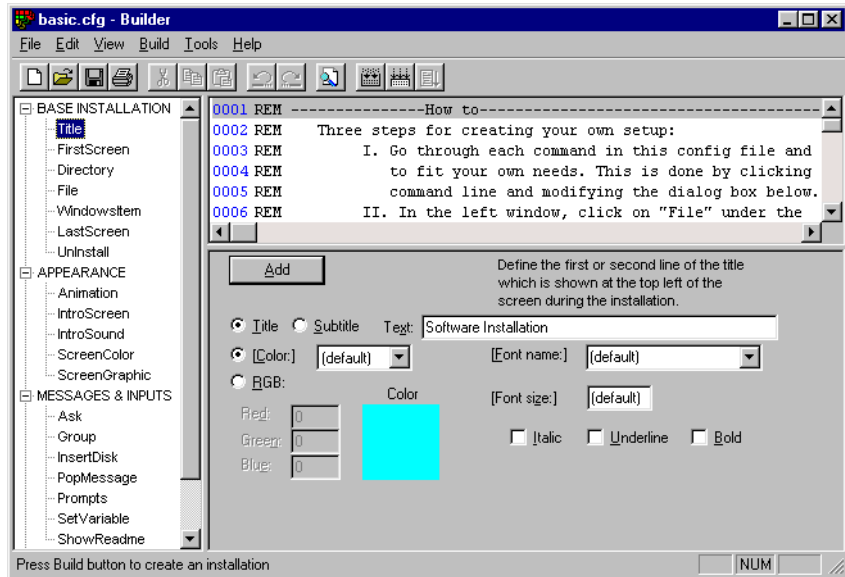
Symantec Ghost  
Boot Wizard  
main window



## Symantec Ghost AutoInstall

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

AI builder main window

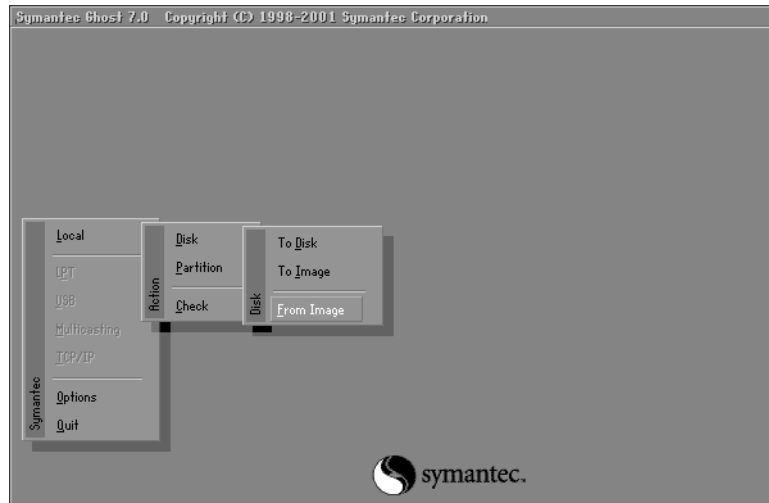


## Symantec Ghost executable

The Symantec Ghost executable makes disk cloning possible. Because the executable is small with minimal conventional memory requirements, it can be run 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 about seven minutes.

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



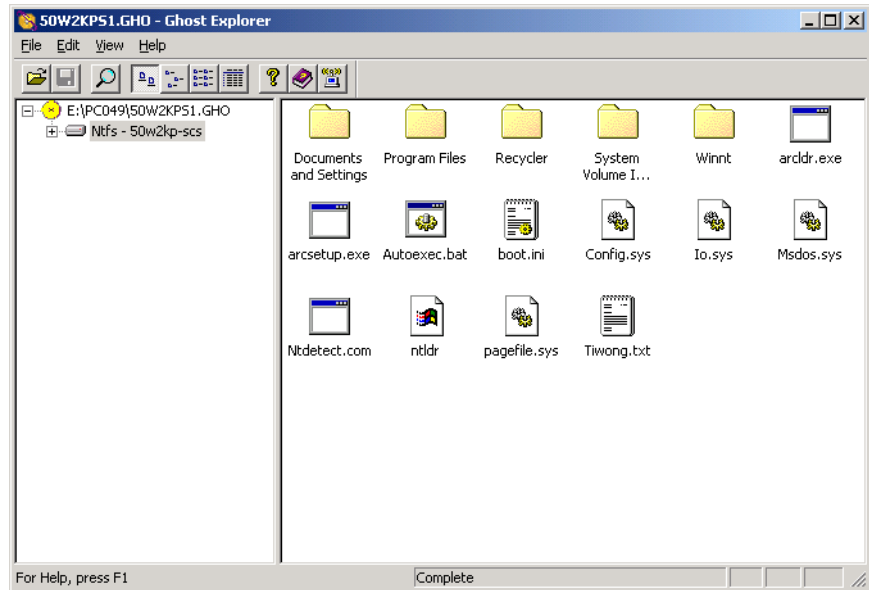
## Ghost Walker

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

## Ghost Explorer

Ghost Explorer lists all image files. It lets you view directories and files in an image file, and then add, recover, and delete individual directories and files 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
- Better disk space utilization
- 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.



## 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 in the file.



# Installing Symantec Ghost

This chapter contains the following:

- [Preparing for installation](#)
- [Installing the Symantec Ghost Enterprise Console](#)
- [Installing the Console client](#)
- [Installing Symantec Ghost Standard Tools](#)
- [Installing the Symantec Ghost Console client for the first time](#)
- [Updating Symantec Ghost](#)
- [Uninstalling Symantec Ghost](#)

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

How to install Symantec Ghost AutoInstall is covered separately.

For more information, see [“Installing AI Builder on the distribution server”](#) on page 199.

## Preparing for installation

The minimum hardware and software requirements to run Symantec Ghost vary according to what you are installing.

### System requirements

To install the Symantec Ghost Console the minimum requirements are:

- For Windows 98: 32 MB RAM (64 MB recommended)
- For Windows NT/2000: 48 MB RAM (96 MB recommended)
- Pentium processor
- VGA monitor
- One of the following:
  - Windows 2000 SP1 with Internet Explorer 4.0 installed
  - Windows NT 4.0 SP6A or above with Internet Explorer 5.0 installed
  - Windows 98 with Internet Explorer 4.0 installed

---

**Note:** If you have Windows 98 installed, you cannot add or remove client computers to or from NT domains.

---

To run Ghost.exe the minimum requirements are:

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

To support the Symantec Ghost Console remote control:

- Networked computer with Windows 95/98/2000, or Windows NT 4.0 SP3
- 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 107.

To support CD writing:

- An additional 6.5 MB above standard Symantec Ghost requirements

File systems supported for standalone cloning are:

- All FAT
- All NTFS
- EXT2

For more information, see [“Cloning with Linux”](#) on page 285.

## What to install

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

Component	Description
Symantec Ghost Enterprise 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.
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 or deploy packages to install applications.  For more information, see <a href="#">“Getting started with AutoInstall”</a> on page 197.

# Installing the Symantec Ghost Enterprise Console

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

## To install the Symantec Ghost Enterprise Console

- 1 Insert the Symantec Ghost CD into the CD-ROM drive.
- 2 In the Symantec Ghost installation window, click **Install Symantec Ghost Enterprise**.
- 3 Click **Enterprise Console (including Standard Tools)**.
- 4 Click **Next**.
- 5 Follow the on-screen instructions.

The Console Service Account Name and Console Service Account Password appear during the installation. Change the password to increase security.

# Installing the Console client

Manually install the Console client on a workstation to enable communication between the workstation and the Symantec Ghost Console. To set up client computers for a cloning task, a number of steps must be completed.

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

Further documentation about the Console can be found in the *Getting Started with the Console Guide*. It is a detailed step-by-step guide to installing the Console, setting up client computers, and cloning clients using an image file.

## To install the Symantec Ghost Console client on a workstation

- 1 Insert the Symantec Ghost CD into the CD-ROM drive.
- 2 In the Symantec Ghost install window, click **Install Symantec Ghost Enterprise**.
- 3 Click **Console Client**.

- 4 Click **Next**.
- 5 Follow the on-screen instructions.
- 6 Confirm that the client appears in the Symantec Ghost Console.  
For more information, see [“Storing the Console client computer details”](#) on page 52.

## Installing Symantec Ghost Standard Tools

Install Standard Tools to use the Ghost executable and Multicast Server.

### To install Symantec Ghost Standard Tools

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

## Installing the Symantec Ghost Console client for the first time

This process guides you through installing Symantec Ghost client software on a client computer for the first time. Once the installation is complete, the client computer can be controlled from the Console.

You can also preserve the original client setup and perform a post configuration to reapply the configuration settings.

For more information, see *Getting Started with the Console Guide*.

Note the following as you complete the installation:

- The Symantec Ghost boot partition must exist on a client computer for it to be fully controlled by the Symantec Ghost Console.
- It is possible to take an image of a computer that includes both the Symantec Ghost boot partition and a Windows partition. However, this is not recommended.

- The Symantec Ghost boot partition must have network drivers that match the network card. Create the boot partition using the Ghost Boot Wizard to ensure that they match.

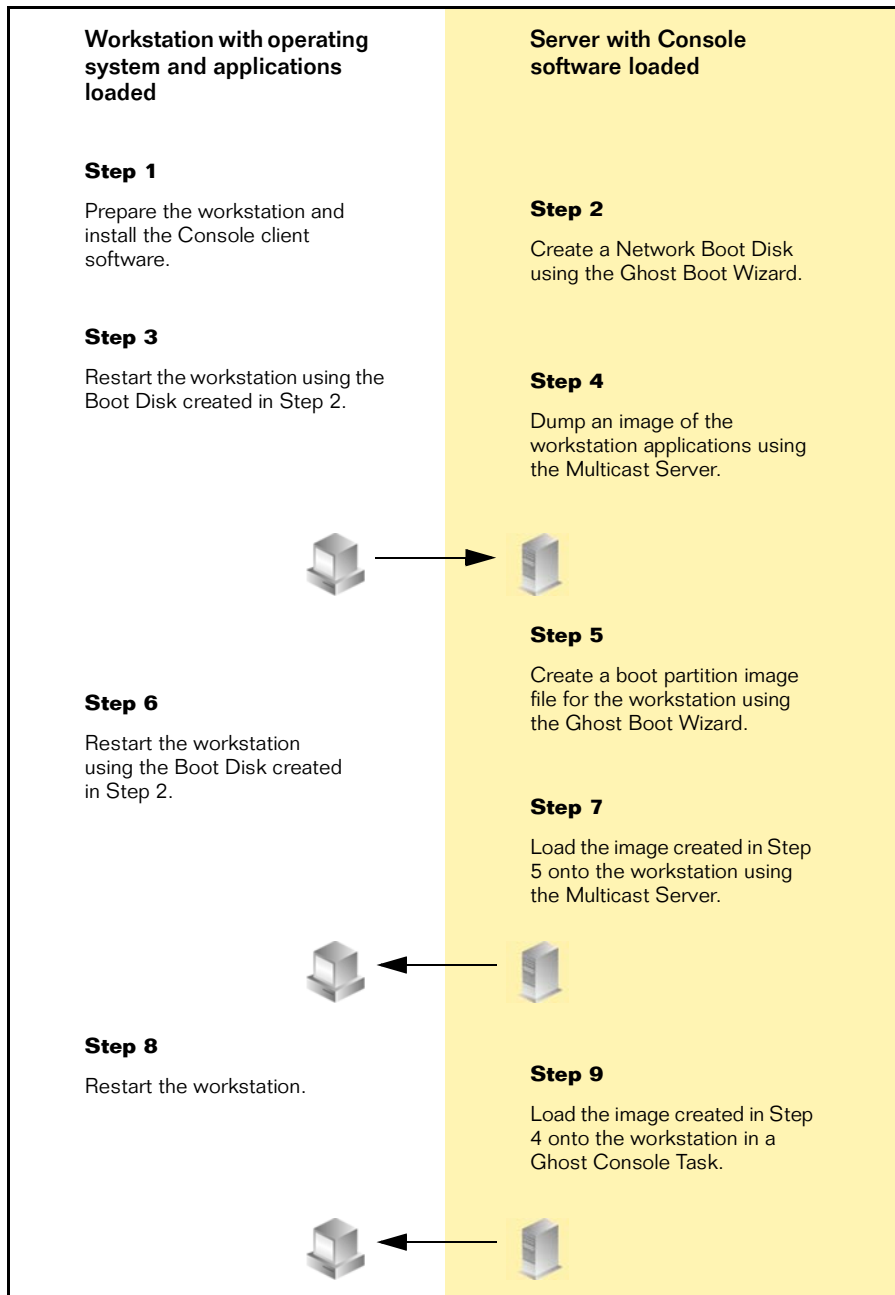
### To install the Symantec Ghost Console client for the first time

- 1 Install the Console client on the client computer.  
For more information, see [“Installing the Console client”](#) on page 38.
- 2 On the Console server, use the Ghost Boot Wizard to create a boot disk.  
This lets the Symantec Ghost Multicast Server take an image of the client computer.  
For more information, see [“Creating boot disks with network support”](#) on page 108.
- 3 Insert the Ghost boot disk into the client computer and restart it.
- 4 On the Console server, use the Ghost Multicast Server to create an image file of the client computer.  
For more information, see [“To create an image file using the Multicast Server”](#) on page 147.
- 5 On the Console server, create a boot partition image using the Ghost Boot Wizard.  
The boot partition contains the necessary Symantec Ghost utilities, including the Console client and drivers for your network card.  
Use the same network card template that you used to create the boot disk. Save the image along with the image you created in step 4. Both images are used on your client computer.  
For more information, see [“Creating a boot image containing the Console boot partition”](#) on page 114.
- 6 Install the boot partition on the client computer.  
This erases the hard disk on the client computer. The disk contains only the Symantec Ghost boot partition, which is very small. Do not perform this step unless you are sure that you have copied all data off of the computer and that it is safe to proceed.
  - a Insert the boot disk into the client computer's floppy disk drive.
  - b Use the Symantec Ghost Multicast Server to load the boot partition onto the client.  
For more information, see [“To load an image onto client computers using the Multicast Server”](#) on page 149.



- 7 Remove the boot disk and restart the client computer.  
The client computer is ready to be managed from the Console server.
- 8 On the Console Server, do the following:
  - a Create a location for the image file that you created in step 4.  
For more information, see [“To create a new image definition”](#) on page 58.
  - b Create a task to clone your client computer.  
For more information, see [“Setting task properties”](#) on page 72.
- 9 Execute the task to load the image file back onto your client computer.  
For more information, see [“Scheduling and executing tasks”](#) on page 81.

This diagram illustrates the installation of the Console client.



# 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 Do one of the following:
  - On the Windows taskbar, click **Start > Programs > Symantec Ghost > Enterprise 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

To update client computers with the latest Symantec Ghost software, you must first update the Ghost Console software on the server using the Symantec Ghost Console LiveUpdate option.

For more information, see [“Updating Symantec Ghost”](#) on page 43.

## To update client computers with a new version of the Console client

- 1 In the left pane of the Symantec Ghost Console, do one of the following:
  - Select the computer or Machine Group that you want to update.
  - Select the top folder to update all computers.
- 2 Do one of the following:
  - On the File menu, click **Client Update**.
  - Right-click the computer or group and then click **Client Update**.

- 3 Select the version of the Console client software that you want to install on the client computers.
- 4 Click **OK**.  
The software is updated when the computers are next included in a task.

---

**Note:** The default software version, defined in the console options, may not be the latest version. If there is a red cross on the left side of the client icon after you update the Console, then the client software is no longer the same version as the default version.

---

## Uninstalling Symantec Ghost

The Console is uninstalled from the Control Panel in Windows.

### To uninstall the Symantec Ghost Console

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

Ghost.exe is uninstalled either from the Control Panel in Windows, or manually.

### To uninstall Symantec Ghost

- Do one of the following:
  - If you installed Symantec Ghost using the install program, in the Control Panel, double-click **Add/Remove Programs**.
  - If you manually copied the Symantec Ghost files, delete **Ghost.exe** and associated files.

# 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:

- [Using the Symantec Ghost Console](#)
- [Grouping Console client computers](#)
- [About the Configuration Resources folder](#)

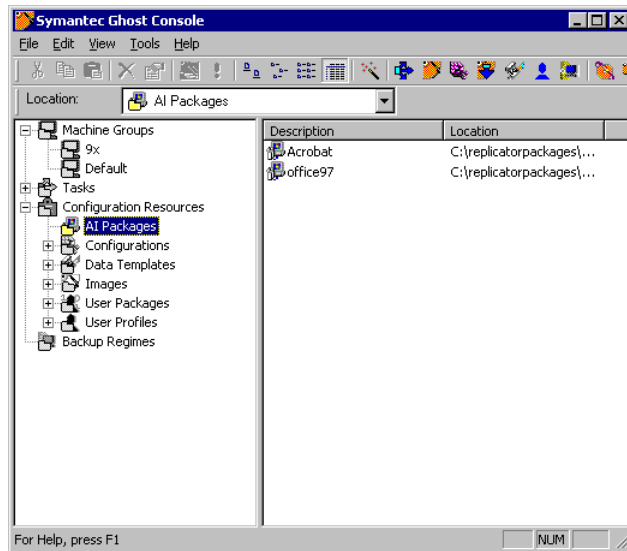
## Using the Symantec Ghost Console

The Symantec Ghost Console lets you:

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

- 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 and Ghost boot partition must be installed on each client computer.

---

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

### To create and execute a Symantec Ghost Console task

- 1 Install the Symantec Ghost client software and boot partition on all Console client computers.

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

- 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 50.

- 3 Define a task, which may include one or both of the following:

- A configuration set, including IP address and NT/2000 domain logon.

For more information, see [“Creating and viewing configuration sets”](#) on page 59.

- An image file for a cloning task.

For more information, see [“Creating image dump tasks”](#) on page 68.

For more information see [“About the Configuration Resources folder”](#) on page 57.

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

For more information, see [“Scheduling and executing tasks”](#) on page 81.

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

For more information, see [“To view the Task Log”](#) on page 126.

## 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.

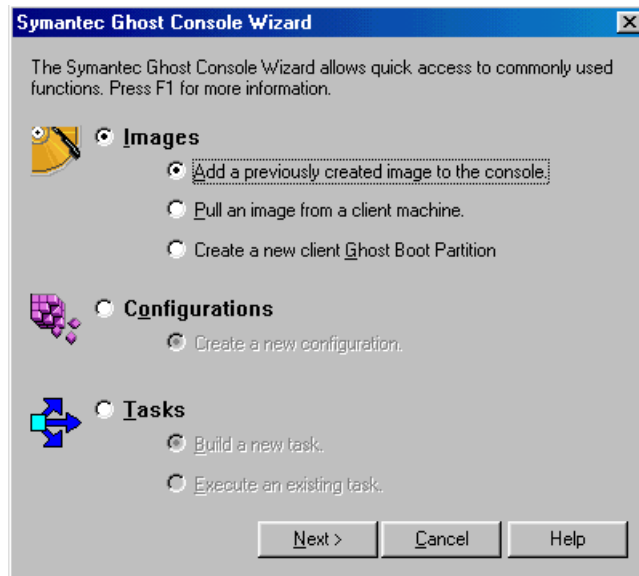
### To start the Symantec Ghost Console

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Enterprise Console**.
- 2 Click **OK** and read the Readme document.
- 3 Click **OK** when the logon parameters appear.

For more information, see [“Adding users to the user list”](#) on page 125.

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 on Windows 98, Windows Me, Windows NT, and Windows 2000. It does not run on Windows 95.

---

## 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's computers, and then run another task to clone another image file onto the teacher's 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 On the File menu, click **Rename**.
- 4 Type a new name for the Machine Group.
- 5 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 and restart the 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.

## 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, or Windows NT/2000 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 71.

- 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 53.

## 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 installed client software is the default version selected in the Console options. A tick means that the default version is installed.
- The right side of the icon shows the computer status. The red X means that the computer is offline or unavailable.



— The computer is online and the client software is the default



— The computer is offline, and the client software is the default



— The computer is online but the client software is not the default



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

The default version may not be the latest version.

For more information, see [“To set the client version option”](#) on page 130 and [“Updating the Symantec Console client”](#) on page 43.

## 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, the Symantec Ghost DOS boot partition must be overwritten and the client software removed from the computer.

### To remove a computer from a group permanently

- 1 Create an image file of the computer.  
For more information, see [“Creating tasks”](#) on page 71.
- 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 71.
- 3 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 4 Double-click **Add/Remove Programs**.
- 5 Click **Symantec Ghost**.
- 6 Click **OK**.

## 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**.

## Viewing and changing the 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
- Version of the Symantec Ghost Console client software on the computer
- Details of the backups created for this computer

### To view 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**.

## 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 72.

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 75.

### 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 59.

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 update the Console client software installed on a client computer.

### To update the client computer software

- On the Version tab, click **Update**.  
The software is updated when the computer is next included in a task.

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

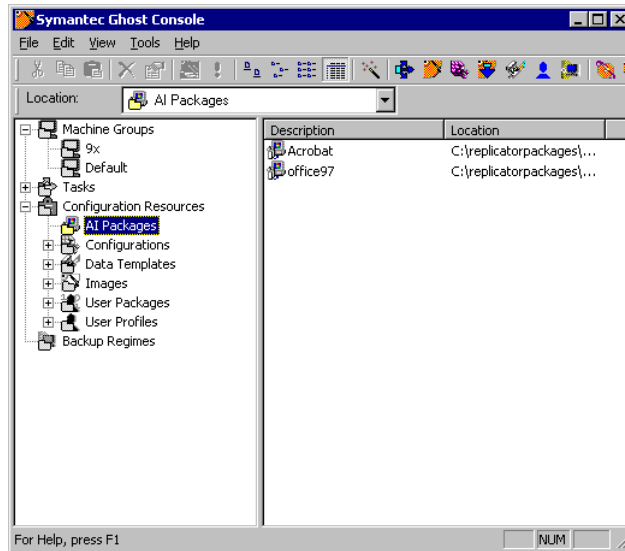
### To view backups created for a computer

- 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 <a href="#">“Creating a data template”</a> on page 92.
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 <a href="#">“Capturing and restoring user data”</a> on page 97.</p>
User Profiles	<p>Stores user profiles used to define Move the User tasks.</p> <p>For more information, see <a href="#">“Creating a User Profile”</a> on page 95.</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 of the image
- Name and location of the image file
- Image file status
- Details of the image:
  - Partition number
  - Type
  - Original size of the partition
  - 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 Definition**.
- 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 [“About Ghost Explorer”](#) on page 215.

## Creating and viewing configuration sets

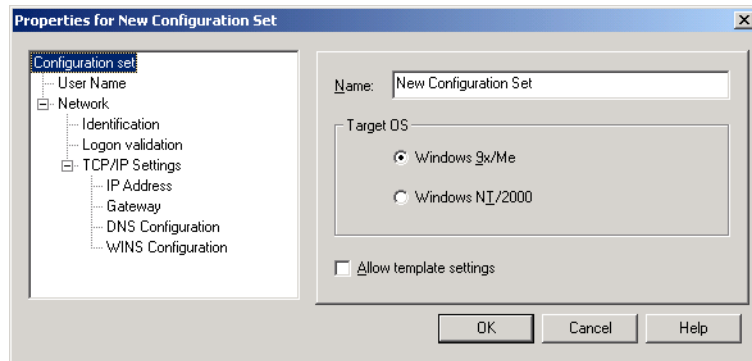
A configuration set is a number of registry settings that are saved and applied as part of a cloning task. The settings can be saved as a template and applied to a group of computers, or saved and applied to individual computers. You can create tasks that apply configuration settings after an image file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

#### To create a configuration set

- 1 In the left pane of the Symantec Ghost Console, 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.
- 2 On the File menu, click **New > Configuration**.

- 3 In the Properties For New Configuration Set window, type a name for your new configuration set.



- 4 Select a target operating system: Windows NT/2000 or Windows 9x/Me.
- 5 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.
- 6 In the left hand window, click **User Name** to specify a user name.
- 7 Click **Identification** to specify identification parameters.
- 8 Click **Logon validation** to specify logon validation parameters.  
This option is not available for Windows NT and Windows 2000 computers.
- 9 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.  
This name can be changed after cloning so that there is a unique user name.
- 4 Click **Apply Workgroup** to specify a workgroup.
- 5 In the space provided, type the name of a workgroup for this Console client to join.
- 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 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 type the name of a domain 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 domain** if you want Windows 9x or Me computers to log on to an NT/2000 domain.
- 3 In the Windows NT/2000 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 for either Windows 9x or Me or Windows NT/2000

- 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 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 **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 **Default Gateway Address**.
- 2 Type the default gateway address.

### To specify DNS configuration information

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

## 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 for Windows 9x or Me or Windows NT/2000 computers.
- 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

## 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.

- 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 205.



# Creating and executing tasks

This chapter contains the following:

- [Task overview](#)
- [Creating image dump tasks](#)
- [Creating tasks](#)
- [Scheduling and executing tasks](#)

## Task overview

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

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

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

### Creating the source computer

A source computer is created 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 the computers are to be controlled from the Symantec Ghost Console, install the Console client executable on the source computer.

If you are creating a source 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 source computer for each unique hardware setup. For example, if you have some computers with SCSI disks and some with IDE disks, you must have separate images for them. However, on Windows 2000 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.
Wake On Lan	An instruction to include all computers in the target group that are currently shut down and have this feature installed.
Sysprep	Facilitates restoring of image files on computers that have different hardware configurations.  For more information, see <a href="#">“To clone with Sysprep”</a> on page 103.

### To begin creating an image dump task

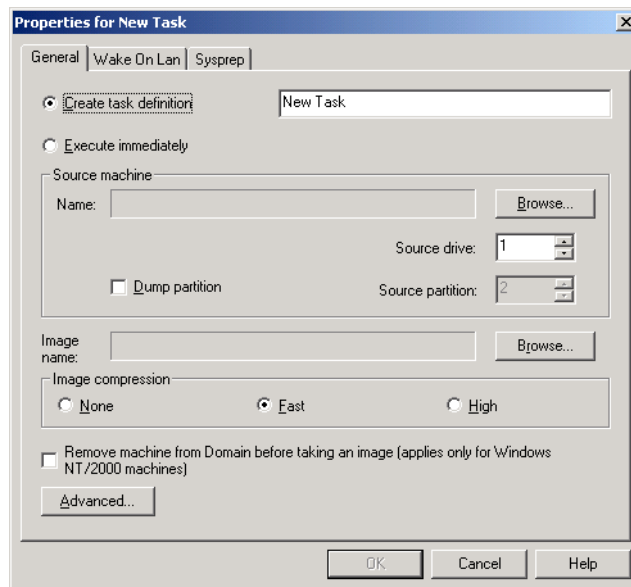
- 1 In the left pane of the Symantec Ghost Console, expand the Tasks folder. Open the folder in which you want to add the new task.  
If you do not select a task folder, the task is stored in the Tasks root directory.
- 2 On the File menu, click **New > Image Dump**.
- 3 Set the image dump task properties.

## Setting image dump task properties

An image dump task includes details of the image file to be created and optionally the Wake on Lan and Sysprep components. The General tab lets you select the computer to dump from 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, 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 58.

- 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 create an image file of a Windows NT/2000 operating system.  
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 134.
- 12 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 75.
- 13 Click **OK** to save the image dump task.

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.

### To set Wake on Lan properties

- 1 In the Properties for New Task window, on the Wake on Lan 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.
Wake on Lan	Lets you include all computers in the target group that are currently turned off and have Wake on Lan installed.
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

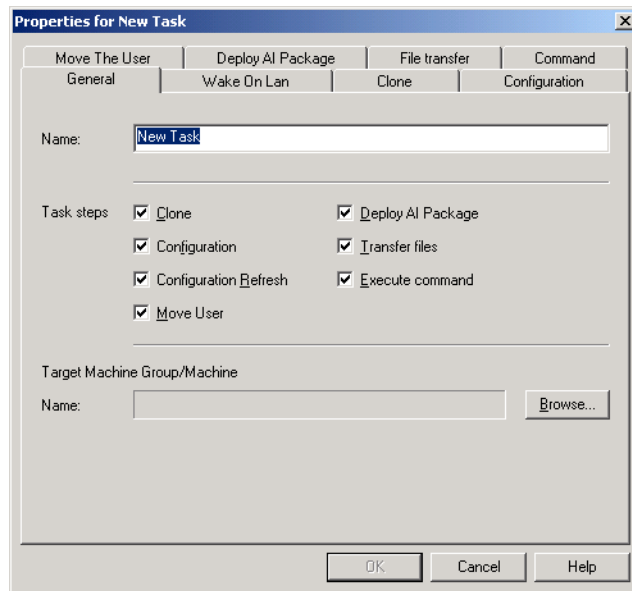
A task always includes General properties and Wake on Lan properties. The other components depend on the steps required for the task being completed.

### 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 of the following options:
  - Click **Clone** to create a task that loads an image file onto client computers.
  - Click **Configuration** to create a task that configures client computers.



- Click **Configuration Refresh** to update the client computer's default configuration settings to the computer's current configuration settings.  
For more information, see [“Editing and applying new default configuration settings”](#) on page 55.
  - Click **Move User** to capture or restore user details from or on the target computers.
  - Click **Deploy AI Package** to install or uninstall AutoInstall packages on the target computers.
  - Click **Transfer files** to transfer a file from the server to a client computer.
  - Click **Execute Command** to execute a command on all of the target computers.
- 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.

## Setting Wake on Lan properties

Wake on Lan properties let you run a task on a computer that is turned off.

For more information, see [“To set Wake on Lan properties”](#) on page 70.

## Setting Clone properties

The Clone properties specify the details of the cloning task. This includes 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 58.

- 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 operating system.

For more information, see [“Using Ghost Walker”](#) on page 242.
- 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 251.
- 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 it does not, you can select it.
- 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	Restores the current default settings to the target computers.  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.  For more information, see <a href="#">“Editing and applying new default configuration settings”</a> on page 55.
Template	Applies a template configuration set to the computers in your group.
Custom	Applies an individual template configuration set to 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 72.

### 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 Template or Custom 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 Template or Custom 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 are 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 97.

## 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.

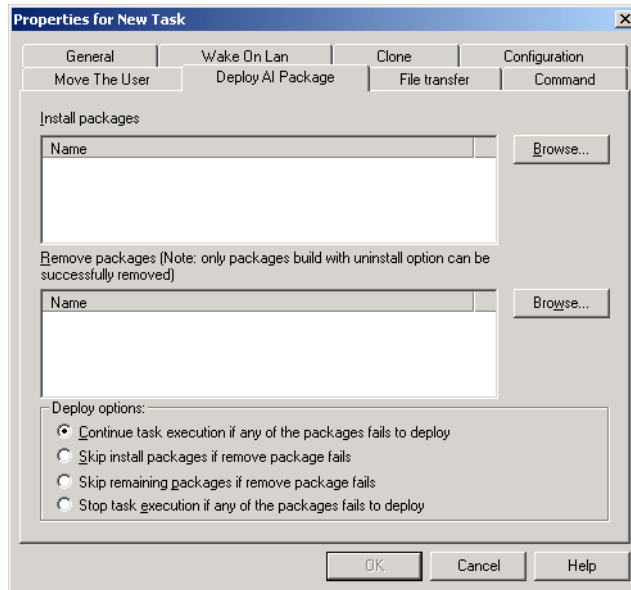
You cannot uninstall all packages. You can uninstall a package if it was created with an uninstall command included. If you are unsure, open the package with AI Builder to see if there is an uninstall command.

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 the 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 the 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 WindowsNT and Windows2000 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

Files can be transferred to the operating system or the Ghost boot partition. The target is selected on a file-by-file basis.

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 Boot Partition** to transfer files to the Ghost boot 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 boot partition. The target is selected on a command-by-command basis.

### 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.
  - Click **In Ghost Boot Partition** to execute a command in the Ghost boot partition.
- 2 Type the command in the space provided to add a command to the Command list.
- 3 Click **Add**.
- 4 Repeat steps 1 through 4 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 a specific date and time, or they can be executed at any time. You can execute tasks once, or more than once on a regular basis.

**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.
- 5 On the Schedule tab, set the date, time, and frequency with which to execute the task.

For more information, see [“To set up schedule properties”](#) on page 87.

A task can be executed manually at any time.

**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 filename
```

# 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

Create a backup regime by completing fields on the Properties, Task and Schedule tabs.

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 130.

### To create a backup regime

- 1 In the left pane of the Symantec Ghost Console, expand the Backup Regime folder.
- 2 Expand the folders until you open the parent folder to place your new regime beneath an existing folder.
- 3 On the File menu, click **New > Backup**.
- 4 On the Properties tab, enter the properties.  
For more information, see [“To set backup regime properties”](#) on page 85.
- 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 86.
- 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 87.
- 7 Click **OK**.

## Setting backup regime properties, task, and schedule details

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

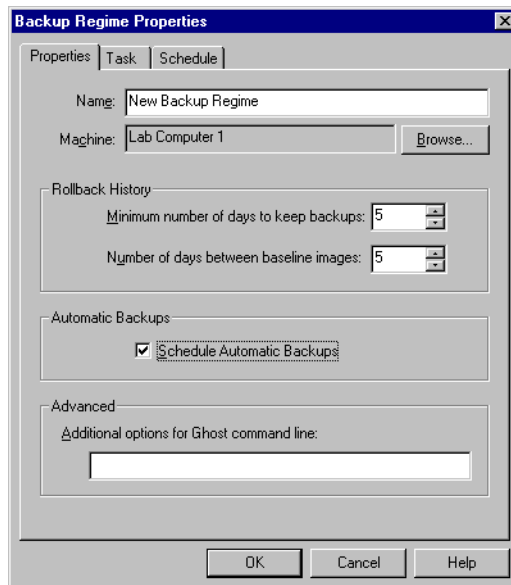
- Properties: The name of, and computers included in the regime.
- Task: Details on the backup task.
- Schedule: Scheduling of the backup task.

### 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.
- 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 251.

---

**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.

The deletion occurs as follows:

- Neither the incremental images nor the baseline image is deleted.
- Once the last incremental image is older than the specified number of days, then 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

- On the Task tab, in the Comments field, type identifying comments for the scheduled backup regime.

You must enter a user name and password for a Win NT/2000 backup task to run.

### To set backup regime task properties for Windows NT/2000 systems

- 1 On the Task tab, in the Name field, type the user name of the person who is running the backup task.

The default is the logged on user.

- 2 Click **Password** to type your password.

A password must be entered to run the backup task.

- 3 In the Password field, type your password.  
The password is confirmed when the backup task runs.
- 4 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.

The Console must be turned off when a scheduled backup task runs.

## Creating a backup manually

Computers are backed up manually as defined by a backup regime. Once selected, a computer is backed up.

**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 backup.
- 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 under the properties.

For more information, see [“To view computer properties”](#) on page 55.

## 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 > Enterprise 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 backup.



- 7 In the bottom pane, you can view the status of the backup.  
The status for the computer is as follows:
  - OK: This computer was successfully backed up.
  - Unfinished: This computer did not complete the backup, or is currently running the backup.
- 8 Click **Restore user 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](#)

## 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 a User Profile is created, it can be used 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 to place the data template beneath an existing folder.
- 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 92.
- 6 On the Advanced tab, complete the fields to allow relative paths.  
For more information, see [“To enable relative paths”](#) on page 94.

### 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 Select the path and files to include or exclude.  
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.
  - Click **During the previous** to select files from a previous number of months.
  - Click **During the previous** to select files from a previous number of days.
- 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 1 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 Select the path and files to be included or excluded.  
The path and files can be relative to the reference path or specifically defined. For example, HKEY\_LOCAL\_MACHINE
- 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 directory locations”](#) on page 99.

- 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

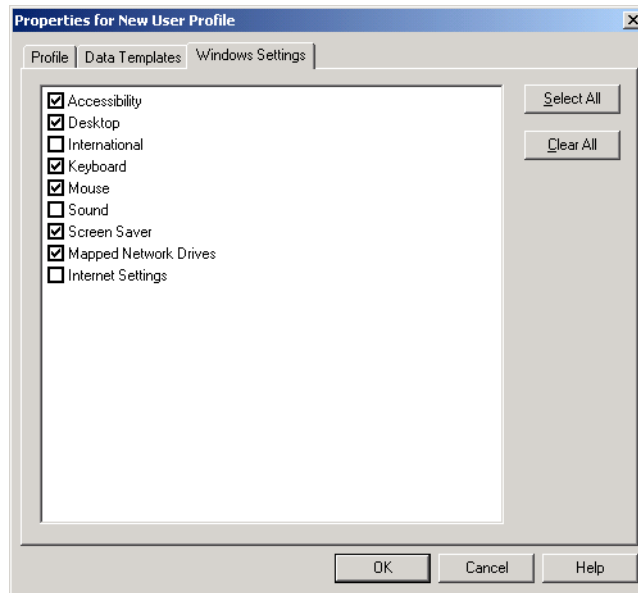
You define what to include in the capture and for whom in the User Profile. You also give the package a name. You define the data files and registry keys by selecting the appropriate templates. You can select as many as you want to use. Specify the user and Windows settings by making the appropriate 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.
- 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 C:\WINDOWS\All Users\Application Data\Symantec\Ghost\MoveTheUser folder. You can restore packages as often as needed.

Move the User tasks can be completed with only the Console client installed. They do not require the boot partition.

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 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 95.
- 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 Check **Restore User Package(s)** to restore user data on a client computer.
- 5 To specify which package that you want to be restored on which 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 97.
  - 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 directory locations

The location of some directories is determined by the operating system and is represented by variables.

<b>Variable</b>	<b>Automatically assigns the directory path for..</b>
\$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

## Variables for use with Move the User

Other variables take on specific values depending on certain factors.

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



# 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 restore Windows 2000 image files on computers that have different hardware setups. You can download it from the Microsoft Web site.

Sysprep changes the settings on source and target computers to make cloning among computers with different hardware setups possible. It 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.

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 also ensures that the Security Identifiers (SID) on the destination computers are unique.

Get information on how to deploy Microsoft Windows 2000 using Sysprep at:

<http://www.microsoft.com/TechNet/win2000/sysprep.asp>

Get a general guide to deployment at:

<http://www.microsoft.com/technet/win2000/dguide/home.asp>

Read these documents, even if you are familiar with Sysprep.

## Setting up Sysprep

Use the Symantec Ghost Console to automatically install and configure Sysprep on your Console and the Console client computers.

The Symantec Ghost Console only supports Sysprep v1.1. The version that is included with Windows 2000 is Sysprep v1.0 and contains reduced functionality.

Download Sysprep v1.1 from the Microsoft Web site:

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

and decompress to a temporary directory on your Console computer. For example, c:\Temp.

### To set up Sysprep

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Enterprise Console**.
- 2 Do one of the following to move the Sysprep files to the Symantec Ghost Console's data directory:
  - On the Tools menu, click **Update Sysprep**.
  - On the File menu, click **New >Image Dump** and then click **Update Sysprep**.

If you do not move the Sysprep files using one of the Update Sysprep options, you are prompted to install them after creating an image dump task that uses Sysprep. If you do not install them, your Sysprep tasks fail to execute.

- 3 In the Browse For Folder window, click the **Sysprep** folder.
- 4 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's local data area. When you load a Sysprep image, all folders and files from that location are copied to the Console client computer.

## 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 > Enterprise Console**.
- 2 On the File menu, click **New > Image Dump**.
- 3 Complete the Wake on Lan and the General image dump details.  
For more information, see [“Setting image dump task properties”](#) on page 69.
- 4 On the Sysprep tab, click **Run Microsoft Sysprep on this machine before dumping the image**.
- 5 Edit the Sysprep.inf file to make changes to the Sysprep.inf file for this task.  
For more information, see [“Editing Sysprep.inf”](#) on page 104.
- 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 page 239.

## Editing Sysprep.inf

You can edit the Sysprep template file. 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 106.

### To edit the Sysprep.inf file

- 1 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 106.
- 3 Click **OK** to save your changes.

### To restore the template Sysprep.inf file

- 1 On the Sysprep tab, click **Reload Template**.
- 2 Click **Restore** to restore previous settings.

## 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 source computer before you dump an image.
- It then starts the computer and the image dump task executes.
- The client remains in DOS and therefore does not process the Mini-Setup Wizard.



### 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 is finished.
- Sysprep uses the Mini-Setup Wizard along with information specified in Sysprep.inf to gather configuration parameters and 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 106.

---

- 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 page 239.

- 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

The Sysprep.inf file that is copied by the Console when you choose to update Sysprep, becomes the template for all of your Sysprep tasks. 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 that you downloaded from the Web site, and complete one of the Update Sysprep options again.

Sysprep can be configured in many ways. Information on how to configure Sysprep.inf is available at:

<http://www.microsoft.com/technet/win2000/dguide/home.asp>

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 page 239.



# 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](#)
- [Adding drivers to the multcard template](#)
- [Adding network drivers to the Ghost Boot Wizard](#)
- [Adding command-line parameters to a boot package](#)

## Introducing the Ghost Boot Wizard

For the Symantec Ghost Console to execute dumping and cloning tasks, a boot package must be installed on the client computers. You create boot packages using the Ghost Boot Wizard, a utility designed to easily create boot disks and images. Boot packages let you complete a number of different cloning tasks. For any given task, the Ghost Boot Wizard guides you through the different steps to select the settings and drivers for the task.

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:

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

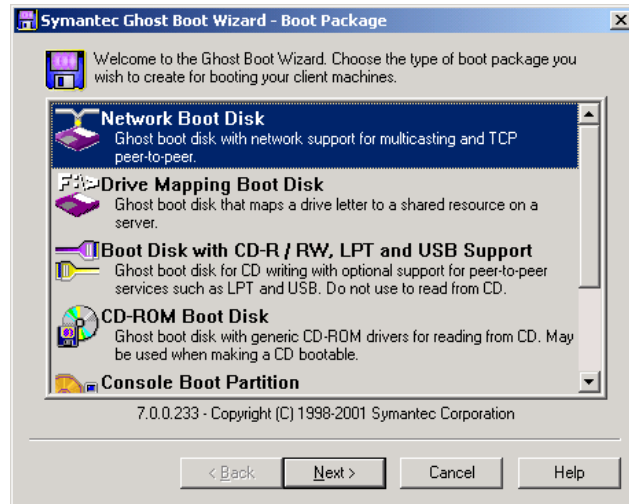
## Creating boot disks with network support

The Ghost Boot Wizard helps you create boot disks that provide network support for multicasting 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 119 and [“Adding drivers to the multicard template”](#) on page 118.

- 4 Click **Next**.
- 5 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 Multicast Server to transfer image files to and from the client.
  - Click **Symantec Ghost Multicast Server for DOS** to create a boot package that loads the DOS version of the Multicast Server.

For more information, see [“Running the DOS-based Ghost Multicast Server”](#) on page 158.

- 6 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 is in the Ghost.exe field.

- 7 In the Parameters field, type any required command-line parameters.  
For more information, see [“Adding command-line parameters to a boot package”](#) on page 122.
- 8 Click **Next**.
- 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. Your network administrator can provide the values for these fields.
- 10 Click **Next**.
- 11 In the Floppy Disk Drive field, type the appropriate drive letter.
- 12 In the Number of disks to create field, type the number of disks that you want to create.
- 13 Click **Format disk(s) first** to format the disks before disk creation.
- 14 Click **Quick Format** to perform a quick format.
- 15 Click **Next**.

## Standard boot disks with the option of LPT and USB support

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

- Lets you write Ghost images to a CD-R/RW
- Runs Ghost.exe on computers with LPT and USB support
- Contains Ghost.exe only

---

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

---

The default mode 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 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. If you cannot get a connection with the default LPT port, you can connect to a specific port.

**To create a boot disk for use on a single computer, 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.
- 4** Click **Advanced** to change the LPT mode or port.
- 5** Click **Next**.
- 6** Type the correct path in the Ghost.exe field, 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.
- 7** In the Parameters field, type any required command-line parameters.

For more information, see [“Adding command-line parameters to a boot package”](#) on page 122.
- 8** Click **Next**.
- 9** In the Floppy Disk Drive field, type the appropriate drive letter.
- 10** In the Number of disks to create field, type the number of disks that you want to create.
- 11** Click **Format disk(s) first** to format the disks before disk creation.
- 12** Click **Quick Format** to perform a quick format.
- 13** 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 119.

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

For more information, see [“Adding drivers to the multicard template”](#) on page 118.

- 4 Click **Next**.

- 5 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.

- 6 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.

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

- 8 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.

- 9 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.



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

## Creating 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 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.
- 4 In the Parameters field, type any required command-line parameters.  
  
For more information, see [“Adding command-line parameters to a boot package”](#) on page 122.
- 5 Click **Next**.

- 6 In the Floppy Disk Drive field, type the appropriate drive letter.
- 7 In the Number of disks to create field, type the number of disks that you want to create.
- 8 Click **Format disk(s) first** to format the disks before disk creation.
- 9 Click **Quick Format** to perform a quick format.
- 10 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 Symantec Ghost Console client for the first time”](#) 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 119.

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

For more information, see [“Adding drivers to the multcard template”](#) on page 118.

- 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 Config Folder field, 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. Your network administrator can provide the values for these fields.
- 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, including Windows 2000. 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 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 network driver for the particular make and model of the network card installed on the client computer.

Use the generic PXE packet driver template. 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 119.

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

For more information, see [“Adding drivers to the multicard template”](#) on page 118.

- 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 Multicast Server to transfer image files to and from the client.
  - Click **Symantec Ghost Multicast Server for DOS** to create a boot package that loads the DOS version of the Multicast Server.
- 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 In the Parameters field, type any required command-line parameters.

For more information, see [“Adding command-line parameters to a boot package”](#) on page 122.
- 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**.

## Booting 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 boot client computers from the network

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

Use the generic PXE packet driver template. 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 119.

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

For more information, see [“Adding drivers to the multicard template”](#) on page 118.
- 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 Ghost Multicast Server for DOS** to include the Ghost Multicast Server for DOS in the boot package.

The default path to the Multicast 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 122.
- 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**.

## Adding drivers to the multiscard template

You can use multiscard templates to create a boot package containing several NDIS2 drivers. When the computer starts, a special multiscard driver checks the computer's hardware to see if any of the NDIS2 drivers can be used to access the installed network card.

Multiscard 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 add a driver to a multiscard template

- 1 In the Ghost Boot Wizard window, select the type of boot package that you want to create.
- 2 Click **Multiscard Template**.
- 3 Click **Next**.
- 4 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.
- 5 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 Ghost Boot Wizard 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 Driver

Many manufacturers ship both drivers with their network cards so you have a choice of which one to use.

- 5 Click **OK**.
- 6 On the Advanced tab, click **Options**.

You may require additional drivers and programs in order to use the network device attached to your computer. For example, many USB network devices need to load an extra driver for the USB port before the driver for the network device.

## Adding a file to the multiscard template

You can add files to the template and customize the Autoexec.bat and Config.sys files of the resulting boot package. These are either DOS drivers or executable programs, but any type of file can be added. Files added to the template appear in the list to the right of the button.

If this template is a multiscard template then any additional files or modifications are overridden by the settings in the multiscard template.

### To add a file to 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.  
Type lines before any network-related commands, such as Nethbind.com or the packet driver executable.
- 4 In the Config.sys field, type any additional Config.sys entries for the driver.  
Type lines 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 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 multicasting. NDIS2 drivers are DOS drivers that load from the DOS Config.sys file. Symantec Ghost does not communicate with NDIS2 directly, but uses a shim (supplied by the Ghost Boot Wizard) to access the network card.

### 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.

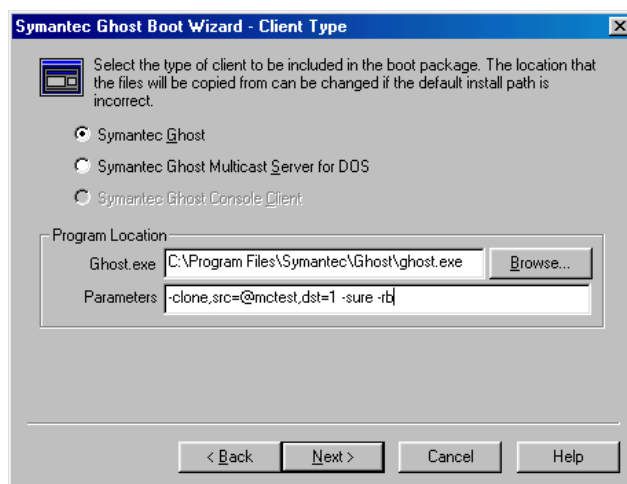
If you use Setup to automatically fill in this page, you will see the parameters that you need to adjust. For the majority of plug-and-play cards, all of the parameters are optional, so you can either accept the defaults or leave this field empty.

## 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 251.

In the following example, the parameters instruct Symantec Ghost to connect to the multicast 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 multicast 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 multicast `sessionname` parameters on each client computer.

For more information, see [“Controlling the multicast session from the server”](#) on page 151.



## Additional Console options

This chapter contains the following:

- [Adding users to the user list](#)
- [Monitoring the Symantec Ghost Console activity](#)
- [Launching the Configuration Server](#)
- [Setting the Symantec Ghost Console options](#)
- [Symantec Ghost Console security](#)

### Adding users to the user list

All users of the Symantec Ghost Console appear on the user list. A user must be added to the user list to access the Symantec Ghost Console. It is important to limit access to the Symantec Ghost Console to the appropriate staff.

When the Symantec Ghost Console is installed, a default user is created:

- Default name: Admin
- Default password: Password

Change the default user password immediately in the user list after install.

#### To add a user to the user list

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Enterprise Console**.
- 2 On the View menu, click **User list**.
- 3 In the Users window, click **Add User**.

- 4 Type the user name and password.  
You must use standard English characters.
- 5 Click **OK**.
- 6 Click **Close**.

## 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.
Console Log	A log of all problems occurring during execution of tasks from the command line or scheduler.
Client Summary	A summary of all executions for a client computer.
Event Log	The history of all events for all computers for a task.
Ghost error file	The error file that is created on the client computer if the task fails.
Event Details	The details for an item in the client summary or event log.
Active Tasks	A list of tasks that are currently executing.

### To view the Task Log

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Enterprise 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
  - 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 > Enterprise 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 297.

### To view a Client Summary

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Enterprise Console**.
- 2 In the Task Log window, on the View menu, click **Client Summary**.
- 3 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 > Enterprise Console**.
- 2 In the Task Log window, on the View menu, click **Event Log**.
- 3 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
- 4 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 > Enterprise 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 > Enterprise Console**.
- 2 On the View menu, click **Active Tasks**.

## 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

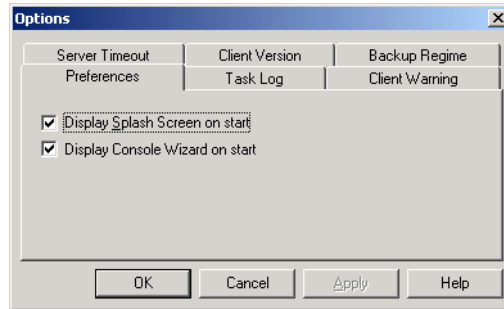
You can set several user options in the Symantec Ghost Console:

- Optional splash screen and wizard when the user opens the Console.
- The number of days that you want tasks held in the log.
- Warn a client that you are about to run a task and let the user abort the task.
- The number of minutes the Configuration Server waits for a client to connect.
- The default version of the Console client to be loaded on client computers.
- The folder in which to store incremental backups.



### To set the splash screen and wizard options

- 1 On the View 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 set the Task Log option

- 1 On the View menu, click **Options**.
- 2 On the Task Log 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 Task Log** to clear the Task Log immediately.
- 4 Click **Apply**.

### To warn the client about a task

- 1 On the View menu, click **Options**.
- 2 On the Client Warning tab, in the Warn client field, type the number of seconds.

This causes a warning message to appear on the client computer a specified number of seconds before a task runs.

- 3 Click **User can abort an operation** to let the user abort the task.
- 4 Click **Proceed with operation if no user intervention** to let the task continue if the user does not respond to the warning message.
- 5 Click **Apply**.

### To set the configuration server timeout option

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

### To set the client version option

- 1 On the View menu, click **Options**.
- 2 On the Client Version tab, select the Console client software release that you want to be the default.
- 3 Click **Set Default**.

The client default determines whether the computers have a cross or tick to the left of their icons when viewed in the Console.
- 4 Click **Apply**.

### To set the location for incremental backups

- 1 On the View menu, click **Options**.
- 2 On the Backup Regime tab, type the location in which you want to store the backups.

This can be changed, as required.
- 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 132.

When a client communicates with the server, it uses a challenge-response protocol. The client must have the server's public certificate to perform this operation. Therefore, the server's public certificate must be distributed to all clients.

When clients are first installed, a boot disk and a boot partition image file can be generated with 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.

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.

## 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, you must change the public certificate on 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.

### To update the boot partition certificate

- 1 On the new Console Server generate a new boot partition image.  
For more information, see [“Creating boot images and disks with the Ghost Boot Wizard”](#) on page 107.
- 2 Use a console task to distribute the new image to the client.  
For more information, see [“Managing image files, configuration resources, and computers”](#) on page 47.
- 3 Click **Partition Load**.
- 4 In the Destination partition number field, type **1**.
- 5 In the Properties for New Task window, on the Clone tab, click **Advanced**.
- 6 Click **Overwrite Hidden Partition**.

## 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**.
- 4 Click **Run**.
- 5 Use the Ghost Boot Wizard to generate a new boot partition image that includes the public certificate.  
For more information, see [“Creating boot images and disks with the Ghost Boot Wizard”](#) on page 107.
- 6 Distribute the boot partition to the clients.  
For more information, see [“Updating the boot partition certificates”](#) on page 131.

## Configuration server password

On Windows NT/2000 systems, an NT/2000 service is installed called ngserver. This service is responsible for task execution and client communication. One of its roles is to create computer accounts in NT/2000 domains if computers are added to domains during the execution of a task. To perform this role, a user is created during installation. The user name and password are set as the Console Service Account during installation. The ngserver service logs on as this user. The ngserver user does not have interactive logon rights, is not a member of any groups, and only has the privilege to manage computer accounts.

Although it is unlikely to be a security risk, you might want to use Windows NT/2000 administration tools to change the password for this user. If you do this, you must inform the ngserver service of the new password by setting the registry value password under the key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Ngserver  
\Params
```

## 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](#)

### About Symantec Ghost image files

You can create image files using the Symantec Ghost executable, multicasting, 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, individual files from these image files are recovered 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 251.

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 multicasting.

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 in the image file. 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 image files are 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 251.

## 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 multicasting), 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 251.



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. The loading procedure is the reverse of the saving procedure. However, during the loading of the spanned image file, you are prompted for the location 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.

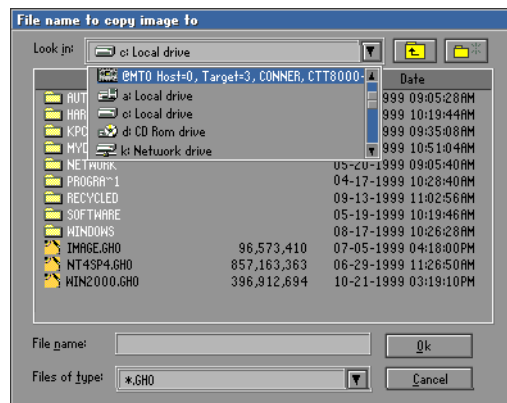
To load spanned images without prompting, you can set the AutoName switch on the Ghost main menu under Options.

For more information, see [“Adding switches to your cloning task”](#) on page 191.

## 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 277.

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 251.

---

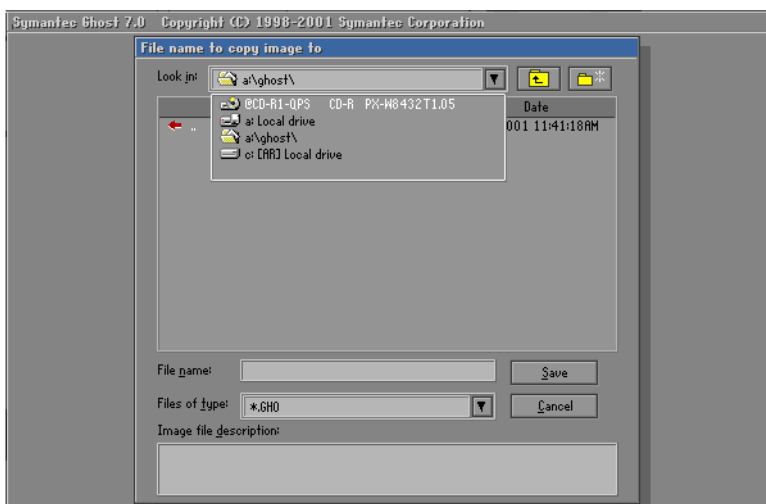
**Note:** Ghost Explorer cannot access an image stored on tape.

---

## 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 or CD-RW disks. The CDs can be read by any modern CD reader.

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 [“Creating boot disks with CD-ROM support”](#) on page 113.

Symantec Ghost should work with most SCSI and IDE writers produced in 2000. It may or may not work with older models. Use the latest firmware available for your CD writer. Symantec Ghost has been tested with the following:

- Acer CRW4432A, Acer 8432A, use firmware 5.FV or newer
- Creative Labs 4224, Creative Labs Blaster 8432
- HP 8200, 9110, 9210e

- Imation IMW0802201S
- Iomega ZipCD/Phillips PCRW404
- Lacie 8424 external, Lacie 8/2/20 SCSI external (sensitive to media used)
- LG CED-8080B
- Pacific Digital (Mitsumi) CR-480TE
- Plextor PX-8432, PX-R412, PX-R820, PX-W124, PX-W4220, PX-W8220
- Que PX-W8432Ti
- Ricoh MP9060A
- Smart and Friendly 8220, Smart and Friendly 2224 (sensitive to media used)
- Sony CRX140E, CRX145
- TDK VeloCD
- TEAC CDR-58S (8/24)
- Yamaha 6416S, 8424SZ, CRW8424E

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. However, a bootable CD created with the Ghost Boot Wizard contains PC DOS, and may not start on all computers. It is recommended that you replace PC DOS with MS DOS.

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.

# 3

## M u l t i 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 multicasting to create and load images
- Multicasting from the command line
- Multicasting and IP addresses

---

# Using multicasting to create and load images

This chapter contains the following:

- [About Symantec Ghost multicasting](#)
- [Preparing for multicasting](#)
- [Creating a Multicast Server](#)

## About Symantec Ghost multicasting

Multicasting lets multiple computers running Symantec Ghost receive the same information over a computer network, using a single transmission. The Symantec Ghost Multicast 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.

Symantec Ghost multicasting makes workstation migration and rollouts more efficient by eliminating 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 multicasting: one on the network server and another on every client workstation to be cloned.

- The Multicast 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 multicasting 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 multicasting
- Multiple, simultaneous sessions, or one session per server

## Preparing for multicasting

Before multicasting, set up the required software and hardware.

### To prepare for multicasting

- 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 [“Multicasting and IP addresses”](#) on page 169.



- 3 Select the executable that matches the platform.

The Multicast Server can be run on three platforms: Windows, DOS, and NetWare. There is a separate server executable for each platform.

Platform	Multicast server executable
Windows	Ghostsrv.exe
DOS	Dosghsrv.exe
NetWare	Nwghsrv.nlm

## Creating the source computer

A source computer is created 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 source 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 source 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 computers, Microsoft Sysprep can help you create a generic template image for different hardware setups.

## Creating a Multicast Server

The Symantec Ghost Multicast 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 Multicast Server

- 1 Do one of the following:
  - For Windows (Ghostsrv.exe): Install Ghost Multicast Server on the computer.  
For more information, see [“Installing Symantec Ghost Standard Tools”](#) on page 39.
  - For DOS (Dosghsrv.exe): Create a DOS packet driver boot disk containing Dosghsrv.exe.  
For more information, see [“Creating boot disks with network support”](#) on page 108.
  - For NetWare (Nwghsrv.nlm): Copy Nwghsrv.nlm onto the NetWare server.
- 2 Create a boot disk for the client computers that contains Ghost.exe.  
For more information, see [“Creating boot disks with network support”](#) on page 108.

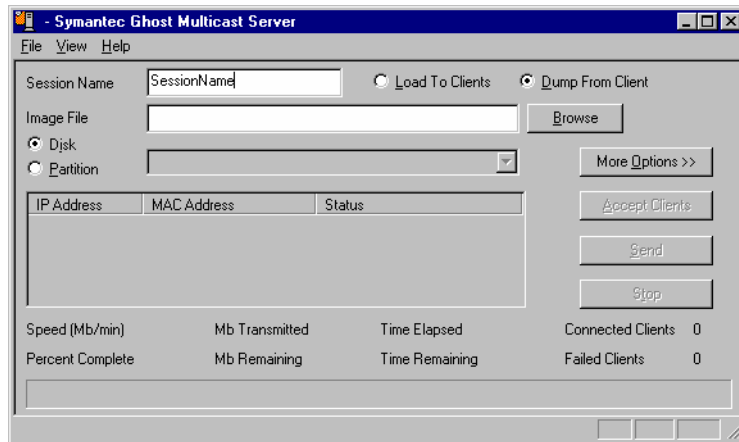
## Starting a multicast session

After setting up the server and preparing the boot disk for the client computers, you can run a multicast session.

### To start a multicast session

- 1 On the Windows taskbar, click **Start > Programs > Symantec Ghost > Multicast Server**.
- 2 In the Symantec Ghost Multicast Server window, in the Session Name field type a session name.  
A multicast session name can be any alphanumeric sequence of characters and must be unique. 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 multicast session from the Multicast Server. Once you create a session on the server, join the multicast session from the source computer.

### To create an image file using the Multicast Server

- 1 In the Symantec Ghost Multicast 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 multicast session.

For more information, see [“To connect a source computer to a multicast session”](#) on page 148.

- 6 Restart the cloned computers when the session is completed.

Once the multicast 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 multicast session

- 1 Create a multicast session on the Multicast Server.

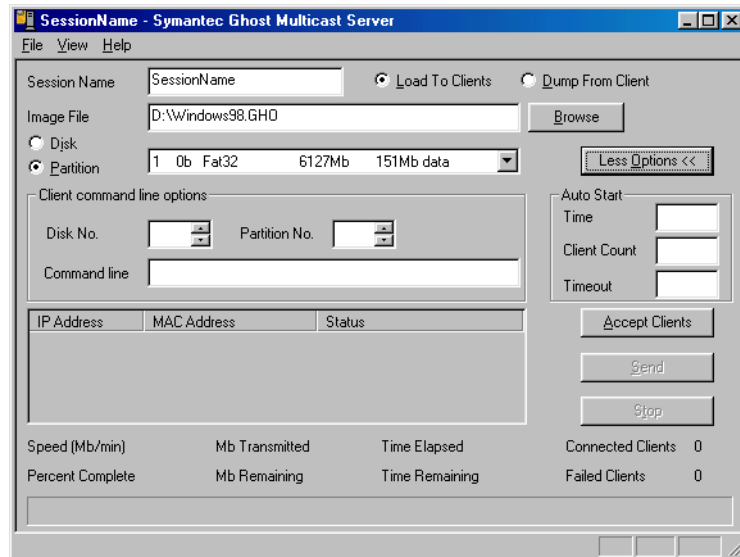
For more information, see [“To create an image file using the Multicast Server”](#) on page 147.

- 2 Using the Ghost network boot disk, start Ghost.exe on the client computer.
- 3 On the Ghost menu, click **Multicasting**.
- 4 In the Multicast 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 155.

## Loading an image file onto client computers

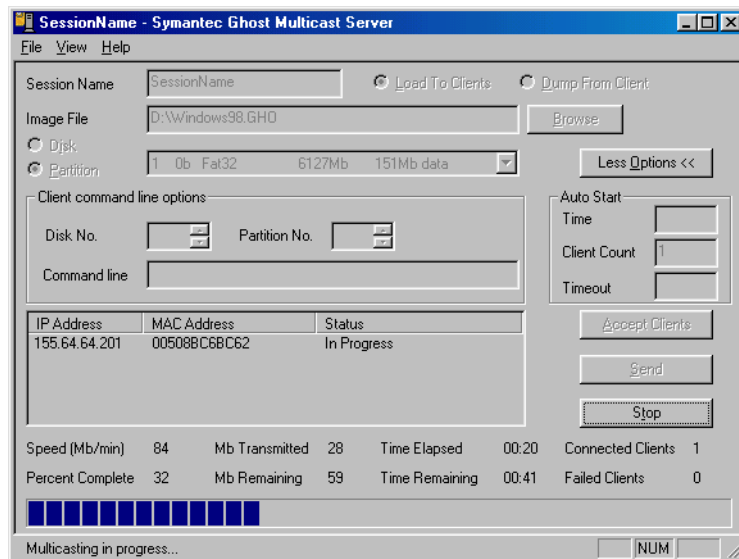
To load an image file, you must first start a multicast session on the Multicast Server. Once you create a session, connect the client computers to the multicast session.



### To load an image onto client computers using the Multicast 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 multicast session.  
For more information, see [“To join a multicast session to load an image file to client computers”](#) on page 151.
- 7 Click **Send** to start the image load and the multicast session when all of the required clients have joined the session.



The progress indicator shows the status of the multicast 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 Multicast Server or turn off the computer once a multicast session has started, the multicast session stops and a warning message appears.

**To join a multicast 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 Symantec Ghost main menu, click **Multicasting**.
- 3 In the Multicast 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 155.

The IP and MAC addresses of the client computers that are connected and waiting for the multicast session to start appear in the Connected Clients list along with their statuses.

## Controlling the multicast session from the server

In your multicast 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 Multicast Server and command-line options**

- 1 Start a multicast session to create an image file from the Multicast Server.

For more information, see [“To create an image file using the Multicast Server”](#) on page 147.

- 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.

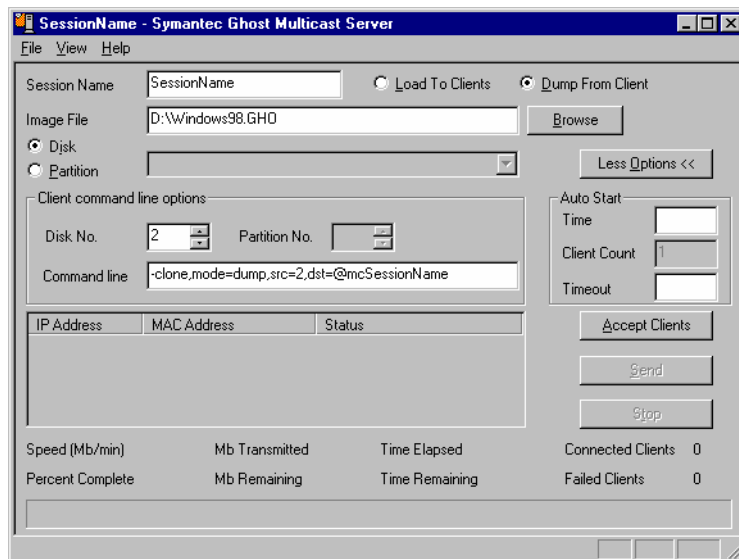
For example, if the initial command is:

```
-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 multicast session from the command line:  

```
ghost.exe -ja=SessionNm
```
- 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 155.



### To load an image to client computers using the Multicast Server

- 1 Create a multicast session to load an image from the Multicast Server.  
For more information, see [“To load an image to client computers using the Multicast Server”](#) on page 153.
- 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.

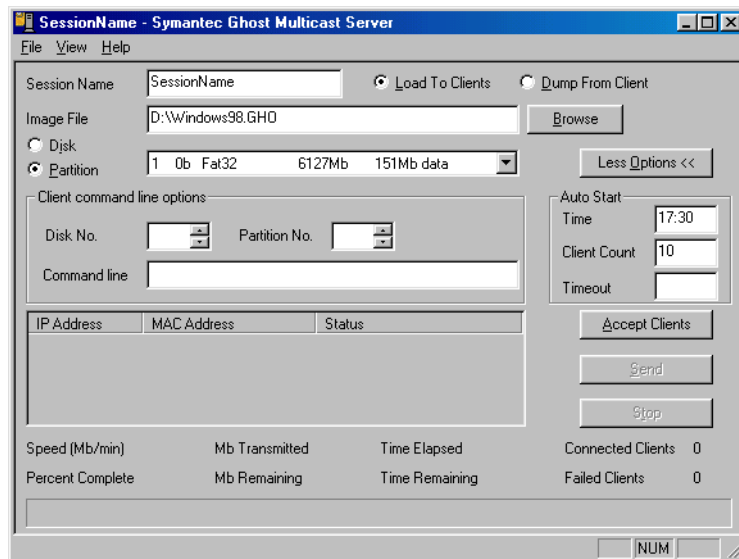
For example, if the initial command is:

```
-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 multicast 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 155.

## Setting Auto Start parameters

When your multicast 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 On the Symantec Ghost Multicast 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.

## Viewing and recording Ghost Multicast Server session options

Details of Ghost Multicast Server sessions are recorded and can be viewed in the Options dialog box. You can also specify session parameters.

### To view or record Ghost Multicast Server options

- 1 On the File menu, click **Options**.
- 2 In the Log Level field, select a log level to set a level of diagnostic multicast logging.  
For more information, see [“Generating a multicast log file”](#) on page 302.
- 3 In the Log File field, type a destination log file location.
- 4 Do one of the following:
  - Click **Restart On Completion** to restart the Multicast Server, accepting clients and using the same Auto Start parameters.
  - Click **Close Ghostsrv On Completion** to close Ghost Multicast Server once the session is completed.
- 5 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.
- 6 Click **Log clients** to create a log that lists multicasting 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.

## Running the Symantec Ghost executable

When using multicasting, the client executable, Ghost.exe, loads multicast copies of an image file onto the client computer and dumps image files to the Multicast 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 277.

Use the Symantec Ghost multicast client command-line switches to run Ghost from the command line or in the multicast session.

For more information, see [“Command-line switches”](#) on page 251.

For a multicasting 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 179 and [“Cloning partitions”](#) on page 185.

For any multicasting session, the session name on the entry screen of Ghost running on the client should match the multicast server session name.

## Multicasting from the command line

This chapter contains the following:

- [Running the Multicast Server for Windows from the command line](#)
- [Running the DOS-based Ghost Multicast Server](#)
- [Running the NetWare-based Ghost Multicast Server](#)
- [Starting the multicast session](#)
- [Multicast Server command-line options](#)
- [Creating a DOS boot disk manually](#)

You can run the Symantec Ghost Multicast Server from the command line by including the appropriate switches with the Windows, PC-DOS, or Netware versions of the application.

### Running the Multicast Server for Windows from the command line

You can run the Windows-based Ghost Multicast 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 [“Multicast Server command-line options”](#) on page 160.

## Running the DOS-based Ghost Multicast Server

The DOS-based Ghost Multicast Server offers a DOS command-line alternative to the Windows-based Ghost Multicast Server. It uses identical files to those on the DOS application disk. However, the file Ghost.exe is replaced by Dosghsrv.exe.

For more information, see [“Creating a DOS boot disk manually”](#) on page 164.

Dosghsrv.exe provides a command-line view interface and uses the same packet driver setup as the Ghost Multicast Client.

For more information, see [“Setting up packet drivers”](#) on page 165.

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 [“Multicast Server command-line options”](#) on page 160.

# Running the NetWare-based Ghost Multicast Server

Nwghsrv.nlm is the NetWare version of the Ghost Multicast Server. It allows multicasting of images to or from a NetWare server. An image can therefore be multicast directly from the file server on which it is stored.

NetWare Symantec Ghost Multicast Server has the same functionality as the DOS Ghost Multicast Server.

## Syntax

**nwghsrv.nlm filename session [options]**

filename            Specifies the path and name of an image file.

session            Specifies the session name.

For more information, see “[Multicast Server command-line options](#)” on page 160.

## NetWare configuration and software requirements

Nwghsrv.nlm requires the configuration of NetWare 5 with support pack 1 or 2 installed. Nwghsrv.nlm does not support NetWare versions prior to version 5.

The server must also have an IP address, which means that Symantec Ghost multicasting is not available on an IPX only based server.

You can get NetWare support packs from Novell. See the following Web page for details: <http://support.novell.com/misc/patlst.htm>

Nwghsrv.nlm multicasts using the TCP/IP protocol. However, if you do not start the Winsock2 TCP/IP service, it starts automatically as Nwghsrv.nlm loads.

## Starting the multicast session

Once you have created a multicast 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 on DOS or NetWare systems.

## Multicast Server command-line options

The Multicast Server command-line switches are listed below.

Switch	Description
-Ncount	Starts the multicast transmission after “count” clients have joined the session.
-Ttime	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 multicast session completion (Windows only).
-D	Uses dump from client mode (load to client is the default).
-R	Restarts the multicast session on completion.  Waits for client connections again after multicasting 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.



Switch	Description
-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.

## Examples using Multicast Server command-line options

Examples are for Ghost Multicast Server for Windows, but they also apply to the DOS-based and NetWare-based Ghost Multicast Server applications. Replace `ghostsrv` with `dosghsrv` or `nwghsrv` when using the DOS server or NetWare 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 multicast 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 multicast 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 multicast 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 multicast session”](#) on page 160.

### Loading a specific partition from an image file onto client computers

```
ghostsrv c:\test123.gho TestSession -p2
```

Starts a multicast session called TestSession, and uses the second partition in the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen.

### Multicasting 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 multicast 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 multicast transmission.

For more information, see [“Starting the multicast session”](#) on page 160.

### Specifying the number of clients to Auto Start

```
ghostsrv c:\test123.gho TestSession -n10
```

Starts a multicast 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 multicast 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 multicast 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 multicast session is completed, ghostsrv closes down as requested.

## Isolating problems

```
ghostsrv c:\test123.gho TestSession -la -ferlog.txt -n10
```

Starts a multicast 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 multicast transmission.

## Creating a DOS boot disk manually

There are times when you want to create boot disks manually. For example, if your network driver is not compatible with IBM DOS.

### 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 165.

- 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 277.

- 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 251.

## Setting up packet drivers

The DOS-based Ghost multicast client and server require an ethernet-based or token ring-based packet driver prior to running. The Windows and NetWare versions do not as they use 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 166.

- NDIS version 2.01 driver with supplied packet driver shim.

For more information, see [“To set up an NDIS 2.01 network adapter driver with supplied packet driver shim”](#) on page 166.

NDIS version 3 or greater drivers do not work with the Ghost multicast client.

- Third-party network adapter driver and packet driver shim. These have not been tested or documented with the Symantec Ghost multicasting 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 multicast 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 multicasting 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.



# Multicasting and IP addresses

This chapter contains the following:

- [Introducing IP addresses for multicasting](#)
- [Locally specified IP addresses](#)
- [Using BOOTP/DHCP to assign IP addresses](#)

## Introducing IP addresses for multicasting

For multicasting 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 Multicast Server and NetWare Symantec Ghost Multicast Server receive their 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 Ghost Multicast 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 a DOS boot disk is used to start multicasting with locally specified IP addresses, each computer requires a different Wattcp.cfg file to be specified to ensure that every boot disk for the workstations is unique.

## Examples of Wattcp.cfg client configuration files

### **Windows 95 computer #1 running the Windows Ghost Multicast 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 to 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 multicasting.

If you are multicasting 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.

For more information, see [“BOOTP/DHCP automatically defined IP address”](#) on page 172.

### BOOTP/DHCP automatically defined IP address

Specifying a local configuration for every computer on an IP network can be inconvenient or impractical. Symantec Ghost multicasting 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 Ghost Multicast 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 multicasting 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 multicasting 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

---



## 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](#)
- [Adding switches to your cloning task](#)
- [Cloning dynamic disks in Windows 2000](#)
- [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, 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 95/98 is installed must not be overwritten.
- If you overwrite a drive or partition, the system must be restarted.
- Symantec Ghost client multicast operation 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, 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.
  - Start your computer in DOS using the Symantec Ghost installation CD if your computer is configured to start from the CD-ROM drive. Consult your computer documentation for instructions.

## 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.
- 2 Add command-line switches, if necessary.  
For more information, see [“Command-line switches”](#) on page 251.
- 3 Select the transfer method.
- 4 Select the Symantec Ghost operation.
- 5 Do one of the following:
  - Select the source hard drive and partitions.
  - Select the image file.
- 6 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.

- 7 Follow the on-screen prompts to proceed with the clone.
- 8 Restart the computer.

## 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:

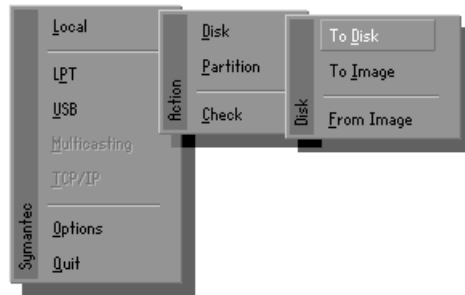
- You can change the size of any destination FAT, NTFS, or Linux Ext2 partition by entering the new size in megabytes.
- You cannot enter a value that exceeds the available space, is beyond the file system's limitations, or that is not large enough to contain the data held in the source partition.

## 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 when the disk clone is complete.
  - 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

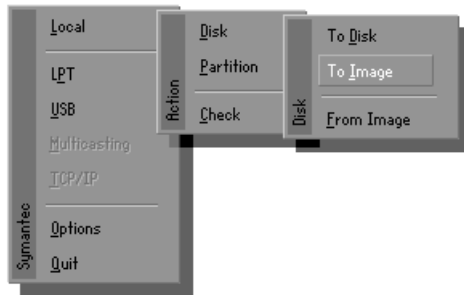
You can copy an image file to another disk or use the image file as a backup file.

When using peer-to-peer connections, the image file is created on the slave computer.

If you write the image file to a CD, write to a bootable CD. 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 134.
- 7 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 135.

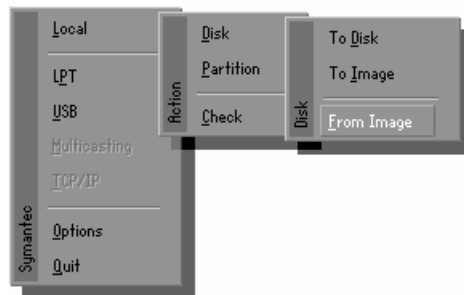
- 8 When the “Proceed with Image File Creation?” question appears, check the details and ensure that the correct options have been selected.
- 9 Do one of the following:
  - Click **Yes** to proceed with the image file creation.  
The system performs an integrity check of the file structure on the source 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.
- 10 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, do one of the following:
  - Type the path and file name of the image file.
  - Click **Browse** to locate 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 When the final "Proceed with disk load?" question appears, ensure that the correct options have been selected.

10 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.

---

**Note:** 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.



- 11 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.
- 12 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:

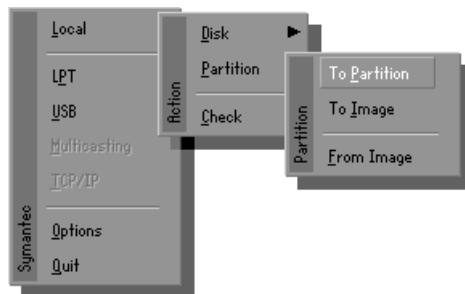
- Local
- LPT > Master
- USB > Master
- TCP/IP > Master

## 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.
- 
- Note:** 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.
  - 10 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 a partition to use as a backup, or to clone onto another partition.

The image file may reside on a mapped network drive or a local drive with a FAT filesystem (but not the one that is being copied from). Local drives include writable CD, tape, ZIP, JAZ, and LS120 Superdisk drives.

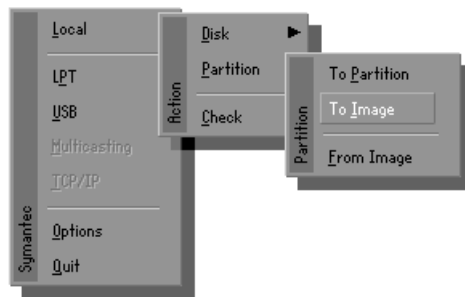
When using peer-to-peer connections, the image file is created on the slave computer.

If you write the image file to a CD, write to a bootable CD. 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 135.
- 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**.

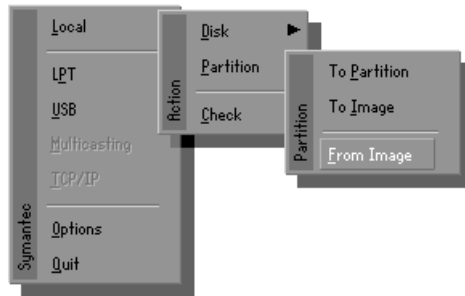
After the image file has been created, Symantec Ghost can verify the integrity of the image file.

## Cloning a partition from an image file

Once you have created an image file from a partition, you can clone a partition onto a partition on another computer with 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.
  - 11 Run Symantec Disk Doctor, ScanDisk, or a similar utility to verify the integrity of the destination partition.

## 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 tabs, select the options to include in your current cloning task:

Tab	Command-line options
Span/CRC	-span, -auto, -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

For more information, see “[Command-line switches](#)” on page 251.

- 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.

## 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 from a partition to a dynamic disk. You can restore this image to a basic disk, but not to a dynamic disk.

You can only 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 backup of an image. 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 an 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

## 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 multicasting, 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 the A drive of a Windows 9x computer.
- 2 Copy the system files onto the disk.
- 3 Double-click **My Computer**.
- 4 Right-click the floppy disk drive, and click **Format**.
- 5 Click **Copy System Files**.
- 6 Copy **Ghostpe.exe** onto the boot disk.

For example:

```
C:\> copy c:\progra~1\symantec\ghost\ghost.exe a:\
```

- 7 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 the A drive 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\ghostghost.exe a:\**

- 5 Set up any drivers required for the transfer method.



# 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](#)

### 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.

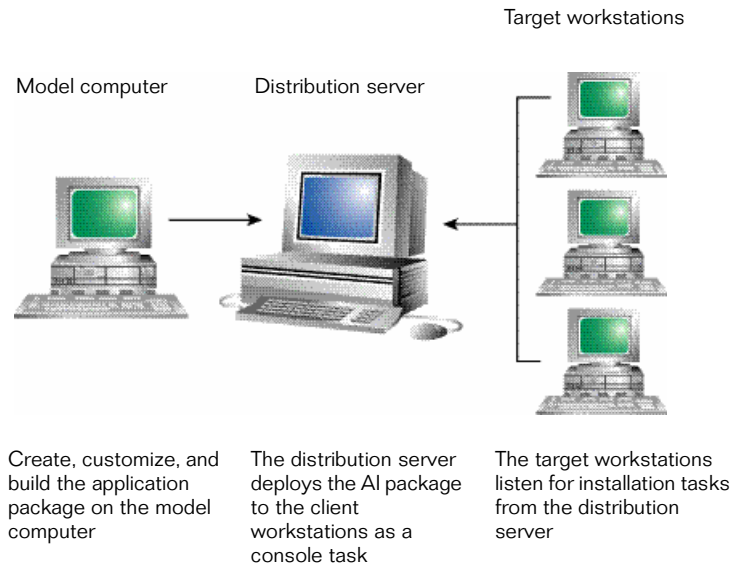
Symantec Ghost AutoInstall has two components to help you create and customize AI packages. AI Snapshot creates an installation script that records the changes to a model computer when software is installed. AI Builder uses the installation script to create a package that duplicates the changes made 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 distribution server.
- 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 201.



## Installing AI Builder on the distribution server

The AI Builder application is installed on the distribution server as part of the Symantec Ghost Enterprise Console software.

### To install AI Builder on the distribution server

- 1 Insert the Symantec Ghost CD into the CD-ROM drive.
- 2 Click **Install Symantec Ghost Enterprise**.
- 3 On the list of options, click **Enterprise Console (including Standard Tools)**.
- 4 Click **Next** to start the install.
- 5 Follow the on-screen instructions.

Make sure the AI Builder application is selected for installation on the Custom Setup screen.

## 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 distribution server.

### To set up a 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 38.

Once installed, the client program runs in the background on client computers, ready to launch installation tasks when they are deployed from the server.



## 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

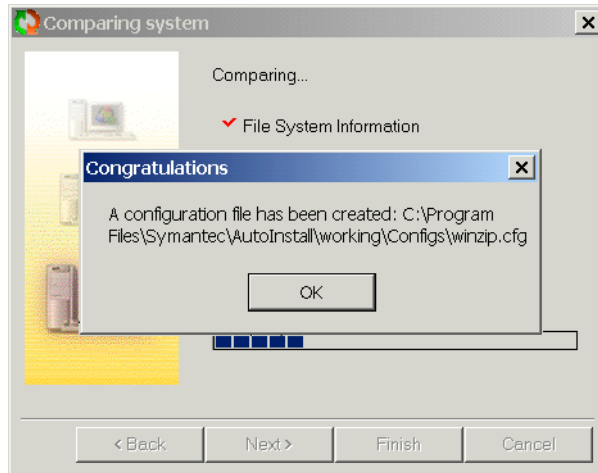
The next step in the installation script process is to take another snapshot of the model computer.

### To take another snapshot of the model computer

- 1 On 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 205.  
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.

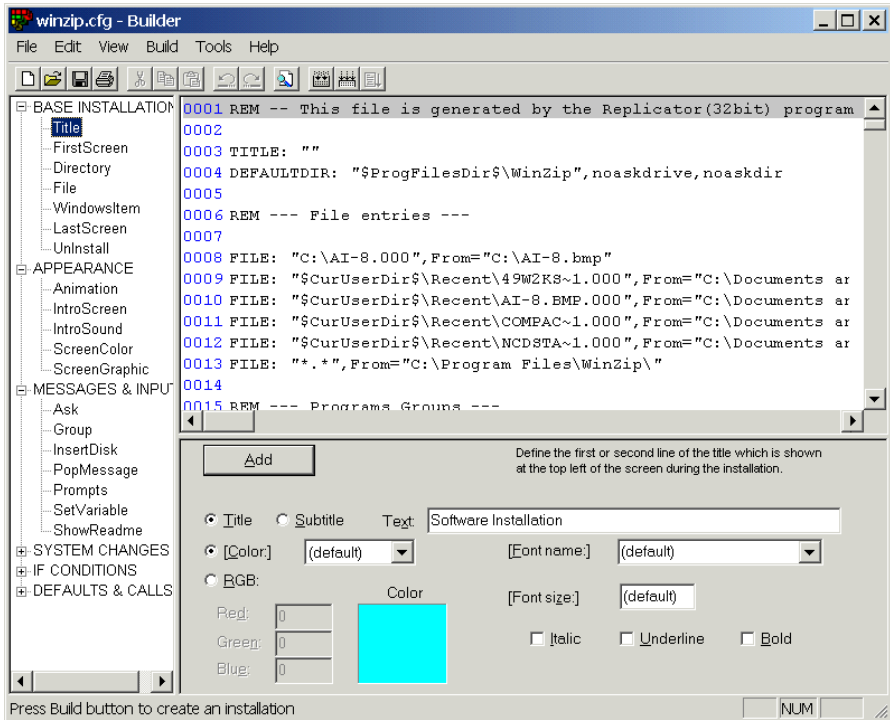
For more information, see [“To include an uninstall command in a build package”](#) on page 209.

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 on 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 210.

## 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.

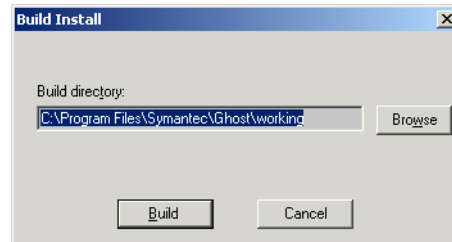
The package is saved as a single file that requires a large storage medium, such as a hard drive, network file server, or CD-ROM.

### 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 78.

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:

- [About 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](#)

### About 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
- Linux Ext2
- FAT16
- NTFS (read only)
- FAT32

### 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 219.

#### To view an image file

- 1 Open Ghost Explorer.  
For more information, see [“To open Ghost Explorer”](#) on page 216.
- 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 219.

## 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 multicasting. 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 219.

---

## 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 **Properties**.
- 2 On the File menu, click **Compile** if compilation is recommended.
- 3 Type a new name for the compiled file.
- 4 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 218.

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.

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](#)
- [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.

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.

### To run GDisk

- 1 Start your computer in DOS mode.
- 2 At the DOS prompt, type **GDisk** followed by the required disk and switches.

## Overview of main command-line switches

GDisk has eight 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)
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



## Online Help for command-line switches

You can get an overview of the eight modes of operation and their switches by using the Help switch:

```
C:\progra~1\symantec\ghost\gdisk /?
```

---

**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 eight main modes of operation.

For example, to view the detailed Help file for Hide, type the following command line:

```
C:\progra~1\symantec\ghost\gdisk /hide /?
```

## Switches common to all GDisk commands

You can use the following switches for any of the eight main 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.

The syntax for this command is as follows:

```
gdisk disk /cre {/pri | /ext | /log} [/sz: {MB | pcent{p | %}}]  
[ /for [/q] [/v[:label]] ] [/32] [/ntfat16]
```

Switch	Explanation
disk	Represents the physical fixed disk, 1 to 8.
/cre	Creates a DOS partition or logical DOS drive.
/pri	Creates a primary DOS partition.
/ext	Creates an extended DOS partition.
/log	Creates a logical DOS drive in the extended DOS partition.
/sz:MB	Specifies the size of the partition in megabytes (MB). This is rounded up to the nearest cylinder.
/sz:pcent{p   %}	Specifies the size of the partition as a percentage of the total disk size, not the available disk space.
/for	Formats the new partition once it has been created. Unless the /ntfat16 or /-32 switches are used, the partition type is determined by the following: <ul style="list-style-type: none"><li>■ If the partition is less than 16MB: FAT12</li><li>■ If the partition is between 16MB and 512MB: FAT16</li><li>■ If the partition is greater than 512MB: FAT32</li></ul>
/q	Performs a quick format if used in combination with the /for switch. If you do not use this switch, then GDisk performs a surface scan of the partition and marks any bad sectors.
/v[:label]	Gives the new formatted partition the specified label when used in combination with the /for switch.

Switch	Explanation
<code>/-32</code>	Indicates that the partition is not formatted as FAT32. Limits primary and logical partitions to 204 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:** This switch must be used when deleting Linux partitions if LILO resides in the MBR.

---

The syntax for this command is as follows:

```
gdisk 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.

The syntax for this command is as follows:

```
gdisk [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.

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
/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 spaces.

The syntax for the delete switch command is as follows:

```
gdisk disk /del [/pri[:nth]] [/ext[:nth]] [/log:nth] [/p:partn-no] [/all]
[/qwipe] [/dodwipe] [/customwipe:n]
```

The syntax for the diskwipe switch is as follows:

```
gdisk disk /diskwipe [dodwipe] [/customwipe:n]
```

Switch	Explanation
disk	Represents the physical fixed disk, 1 to 8.
/del	Deletes a DOS partition or logical DOS drive.
/pri[:nth]	Deletes the nth primary DOS partition. The default is 1.
/ext[:nth]	Deletes the nth extended DOS partition. The default is 1. Also deletes any logical partitions in the extended partition.

Switch	Explanation
/log:nth	Deletes the nth logical DOS drive from the extended DOS partition.
/p:partn-no	Indicates the partition to delete. Use the number reported by GDisk in standard display mode (not using /lba or /raw) for partn-no.
/all	Deletes all partitions.
/qwipe	Overwrites the partition's data area before deleting the partition. Makes one pass of the disk.
/dodwipe	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.
/customwipe: n	Overwrites the partition's data area n times before deleting the partition. n can be set from 1 to 100. /customwipe:7 is equivalent to /dodwipe.

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 boots to an active partition. Using this switch you can choose the partition to which the computer boots.

The syntax for this command is as follows:

```
gdisk disk [/l]act /p:partn-no
```

Switch	Explanation
disk	Represents the physical fixed disk, 1 to 8.
/act	Activates a partition.

Switch	Explanation
<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.

The syntax for this command is as follows:

```
gdisk disk /[-]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> .

## 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 systems 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 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 Lsclient.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 server        \winnt\SYSVOL\sysvol\<servername>.com\scripts

### 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](#)
- [Using Ghost Walker](#)

### Making SID changes with Sysprep and Ghost Walker

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.

You can use either Sysprep or Ghost Walker to make SID changes after a cloning task. However, because the data that a SID changer operates on is continually evolving, you should use Sysprep for the following reasons:

- Sysprep is supported, maintained, and endorsed by Microsoft.
- Since Sysprep was developed by Microsoft, the Sysprep development groups have advanced knowledge of new operating system features, which enables them to provide an accurate and timely solution to Windows NT and Windows 2000 product changes.

However, there are times when it is more appropriate to use Ghost Walker than Sysprep. Use the following sections to help you decide which application to use.

### 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, and 2000 operating systems.

### 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 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 NTFS File Encryption, Windows NT, and Windows 2000 Protected Storage make use of a SID as a unique token. 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 computers following a clone operation. Each Windows 95, 98, or Me computer can be assigned a unique name. Each Windows NT or 2000 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, 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 is located in its normal location.

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 or Windows 2000 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=<new_computer_name>	<p>Specifies a new computer name.</p> <p>The new name must be the same length as the original name, and cannot contain any of the following characters: / \ [ ] : ;   &lt; &gt; + = , ? * To include spaces in the computer name, enclose the computer name in quotes, for example; /CN="EW PC 123"</p>
/CN="<random_computer_name_format>"	<p>Replaces the original computer name with a randomly generated name using the &lt;random_computer_name_format&gt; template. The &lt;random_computer_name_format&gt; template specifies which sections of the new name will be randomly generated and the type of random value to place in that location.</p> <p>Only one instance of the following keywords is permitted in a format:</p> <p>&lt;RANDOM_NUMERIC&gt; - Generate random numbers &lt;RANDOM_ALPHA&gt;- Generate random letters &lt;RANDOM_HEX&gt; - Generate random hex digits (0-9,A-F)</p> <p><b>Examples:</b></p> <p>/CN="PC&lt;RANDOM_NUMERIC&gt;" replaces the computer name with a name that starts with PC, followed by a series of random digits between 0 and 9.</p> <p>/CN="ID&lt;RANDOM_ALPHA&gt;X" replaces the computer name with a name that starts with ID followed by a series of random letters ending with the character X.</p> <p>/CN="&lt;RANDOM_ALPHA&gt;" replaces the computer name with a name that is randomly generated using letters.</p> <p>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.</p>
/BV=<drv:part>	<p>Specifies the drive number and partition number of the bootable operating system installation to update.</p>
/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"><li>■ More than one volume may be specified by repeating the argument for each additional volume.</li><li>■ This switch cannot be combined with /AV=ALL.</li></ul>

Switch	Description
/AV=ALL	Specifies that all other volumes are to be included as additional volumes.  /AV=ALL cannot be combined with the /AV=<drv>:<part> switch.
/SURE	Specifies that the update should start without user confirmation.
/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.
/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.

Switch	Description
/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, 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 SIDs 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](#)

### 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
```

### **-#e=filename**

Standalone switch to bind and activate Symantec Ghost using the license details included in the environment file. Useful when installing or upgrading Symantec Ghost to a newer version. If the file name is not given, it defaults to Ghost.env. The environment file is created when Symantec Ghost is first licensed.

### **-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=x**

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. The x value indicates the maximum number of bad sectors allowed by Symantec Ghost. The default value is 500. Symantec Ghost aborts when a bad sector is encountered in a nonFAT partition after the maximum number of bad sectors is exceeded. 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.

**-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.

The syntax for this switch is:

-clone,MODE={operation},SRC={source},DST={destination},  
[SIZE{size},SIZE{size},.....]

MODE={copy | load | dump | pcopy | pload | pdump}

MODE defines the type of clone command:

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

---

SRC={disk | file | multicast | tape}

SRC defines the source for the operation selected by the clone mode option:

---

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.
multicast	@MCsessionname	The session name for the multicast session that is executing the operation. For example, SRC=@MCdumpdisk  The mode is defined on the multicast server. If written in the command line, the mode must match.
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

---

DST={disk | file | multicast | tape | cdwriter}

DST defines the destination location for the operation:

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	<p>The destination image file name. For example, DST= g:\destination.gho</p>
multicast	@MCsessionname	<p>The session name for the multicast session that is executing the operation. For example, DST=@MCdumpdisk</p> <p>The mode is defined on the Multicast Server. If written in the command line, the mode must match.</p>
tape	@MTx	<p>The tape drive number. Numbers start at 0. For example, DST=@MT0</p>
cdwriter	@CDx	<p>The CD writer drive number. Numbers start at 1. For example, DST=@CD1</p>

## Cloning combination options

Mode	Source	Destination
copy	disk	disk
load	file Multicast Server tape	disk
dump	disk	file Multicast Server tape CD writer
pcopy	disk:partition	disk:partition
pload	file:partition Multicast Server (no partition specified) tape:partition	disk:partition
pdump	disk:partition:partition:partition  More than one partition can be specified	file Multicast Server tape CD writer

**SZE**[E | F | L | n={nnnnM | nnP | F | V}]

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.

Available options:

- n=xxxxM** Indicates that the nth destination partition is to have a size of xxxxMB (for example, SZE2=800M indicates partition two is to have 800 MB).
- n=mmP** Indicates that the nth destination partition is to have a size of mm percent of the target disk. Due to partition size rounding and alignment issues, 100% physical use of disk space may not be possible.
- n=F** Indicates that the nth destination partition is to remain the same size on the destination as it was on the source. This is referred to as 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.

---

**Note:** Some cloning switches for use in Ghost can be specified on the Multicast Server.

---

## 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  The slave machine can be started with ghost.exe -lps	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
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.
ghost.exe -clone,mode=load,src=E:\savedsk.gho,dst=1 -sure  This example is typical of a command line included in a batch file to automate workstation installations from a network file server.	Load the disk image file Savedsk.gho that is held on the server drive which is mapped locally to drive E onto local disk one. Performed without the final warning prompt.

---

<b>Switch</b>	<b>Function</b>
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=2 size1=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 Multicast Server with the session name "sessionname" without the final warning prompt.
ghost.exe -clone,src=1,dst=@MCsessionname -sure	Create an image file of disk one to an image file being created by the Multicast Server with the session name "sessionname" without the final warning prompt.

Switch	Function
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:\part 146.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 Multicast 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 be 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 be run if Symantec Ghost
REM fails here **
:FINISH
ECHO Batch File Finished
```

## **-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. 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 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:

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,crc file=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
<code>ghost.exe</code> <code>-CRC32,action=verify,src=1,crcfile=myfile.txt</code> <code>,vlist=myfile.out</code>	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.	
<code>ghost.exe</code> <code>-CRC32,action=verify,src=1,crcfile=myfile.txt</code> <code>,vlist=myfile.out,vexcept=myfile.exc</code>	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 \*. Thus, 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 an extension. To match all files with or without an extension, `WINDOWS\COOKIES\*` should be used.

Short file names should be used 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, wildcards should be used for files, not for directories.

#### **-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.

#### **-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.

#### **-di**

Shows diagnostics. This is useful for Technical Support purposes. For each disk present on the computer, the physical attributes such as drive number, cylinders, heads, sectors per track, and total sectors appear. The diagnostics may be redirected to a file and given to Technical Support to assist with problem solving.

Example:

```
ghost.exe -di > diag.txt
```

outputs disk diagnostics to the file `Diag.txt`.

### **-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 260.

### **-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.

### **-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 95/98.



**-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 271.

### **-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 (imageboot), 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 Multicast Server using the specified session name. The disk and possibly partition to be cloned should be set at the Multicast Server.

**-jl:x=filename**

Creates a multicast log file to assist in diagnosing multicasting 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.

### **-js=n**

Sets to n the maximum number of router hops Symantec Ghost is allowed to cross in an attempt to find the Multicast Server. (Default is 10.)

### **-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	Compaq
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 machine.

### **-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 277.

**-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 277.

**-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.

**-ntchkdsk**

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. Avoid using this switch.

### **-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.

### **-pmbr**

Specifies that the master boot record of the destination disk be preserved when performing a disk-to-disk or image-to-disk cloning operation.

**-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 266.

**-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  
-chking,c:\drv2.gho  
-clone,mode=dump,src=2,dst=c:\part2.gho  
-chking,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.



**-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**

Specifies the tape block size in units of 512 bytes.

**-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 277.

### **-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 277.

### **-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 277.

### **-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 277.

### **-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)



## Setting up the hardware and transfer methods

This appendix contains the following:

- [Hardware and transfer requirements](#)

### 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 281.

### 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.

## Multicasting

For multicasting transfers, the following hardware and software is 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 media are required.

For more information, see [“Image files and CD writers”](#) on page 139.

## 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 107.

## 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	<a href="http://www.lpt.com">http://www.lpt.com</a>
Via telephone	800.789.4784 (U.S.) 425.869.1119 (International)
Via fax	253.813.8730
Via email	<a href="mailto:sales@lpt.com">sales@lpt.com</a>

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 Ghost Multicast Server. The Wattcp.cfg file is not required for the Windows and NetWare Symantec Ghost Multicast Servers, Ghostsrv.exe, and Nwghsrv.exe.

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 251.

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. It does not support files greater than 2 GB within an ext2 file system. 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](#)
- [Saving switches from the Options menu](#)
- [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"><li>■ Process used to create the drive or partition</li><li>■ Time the operation was performed</li><li>■ Date the operation was performed</li><li>■ Disk number</li></ul>
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 their 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

## Saving switches from the Options menu

Symantec Ghost switches set from the Symantec Ghost Options menu can be saved to the Ghost.ini file.

### To save switches set from Options menu

- 1 On the main menu, click **Options**.
- 2 On the Save Settings tab, click **Save Settings**.  
All currently selected active settings appear.
- 3 Click **Yes** to confirm that the active settings are saved to the Ghost.ini file.

## 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 311.



# Troubleshooting

This appendix contains the following:

- [Symantec Ghost error message](#)
- [Symantec Ghost multicast errors](#)
- [Symantec Ghost and multicast 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 299.

Further information is available on the Symantec Ghost Technical Support Web site.

For more information, see [“Service and support solutions”](#) on page 311.

Error code	Description
8006, 8008	The trial period of the evaluation has expired. Visit the Symantec Web site at <a href="http://www.symantec.com">http://www.symantec.com</a> for details on how to purchase Symantec Ghost.
10030	Symantec Ghost was unable to communicate with the Ghost Multicast Server. Check that the multicast session name is correct, and the Multicast Server is ready to accept clients.

Error code	Description
10098	<p>The partition number must be included in the command-line switches.</p> <p>For more information, see <a href="#">“Command-line switches”</a> on page 251.</p>
10010,10014, 11000	<p>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 on the network.</p>
14030	<p>An unregistered version of Symantec Ghost has encountered a file with a date beyond its expiration date. Scan your system for files beyond this date and temporarily remove them from the system to let Symantec Ghost continue. You can locate the offender by looking at the drive:\path\file name at the bottom of the Symantec Ghost window when this error occurs. Visit the Symantec Web site at <a href="http://www.symantec.com">www.symantec.com</a> for details on how to purchase Symantec Ghost.</p>
15170	<p>There is an unformatted or invalid partition on the source hard drive. Ensure that the source drive is completely allocated as Symantec Ghost looks for 100% viable media.</p>
19906	<p>Symantec Ghost was unable to establish a connection with the Multicast Server. You may need to add the line RECEIVE_MODE = 6 to Wattcp.cfg.</p> <p>For more information, see <a href="#">“The Wattcp.cfg network configuration file”</a> on page 283.</p>
19910, 20070	<p>No packet driver was found.</p> <p>For more information, see <a href="#">“When I launch Symantec Ghost, I am unable to select multicasting because it is grayed out”</a> on page 295.</p>
19913	<p>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.</p>
19916	<p>Duplicate IP address detected. An IP address has been allocated that is already in use.</p>

Error code	Description
19900	The multicast 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 multicast errors

If you are having problems using Symantec Ghost or the Symantec Ghost Multicast Server ensure that:

- You have the latest version of Symantec Ghost and the latest version of the Symantec Ghost Multicast Server.

The latest versions of Symantec Ghost, the Symantec Ghost Multicast 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 multicasting because it is grayed out**

Symantec Ghost uses a packet driver to perform multicasting. If Symantec Ghost does not detect a packet driver in memory, or if the packet driver is inappropriate for your network card, the multicasting option is not available. You must have a boot disk that loads the appropriate packet driver for your network card.

Use the Ghost Boot Wizard to create a packet driver boot disk.

For more information, see [“Creating boot disks with network support”](#) on page 108.

### 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 Multicast 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 multicasting enabled.
- Check the Wattcp.cfg file for a valid IP address and subnet mask.

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 **Multicast**.
- 3 Do not enter a session name, to initialize the IP address.
- 4 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 multicasting, 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 283.

If you are multicasting across routers or switches, a multicasting protocol must be enabled on these devices.

For more information on multicast protocols, refer to your router or switch documentation.



**When I try to launch the Symantec Ghost Multicast Server on a Windows 95 system, 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 multicast DOS errors

Windows 95 and 98 are plug-and-play operating systems. They reconfigure most network cards if they find an IRQ conflict. Because multicasting 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 126.

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 84.

# 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 293.

### Listing hard disk geometry diagnostics

A list of all detected hard drives on the system and their associated geometry values can be shown on-screen using the command-line switch `-di`. To generate a file containing the details, use the following DOS redirect output:

```
c:\>ghost-di>drives.txt
```

### 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 multicast 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. An example of two Windows 95 TCP/IP utilities, `Ping.exe` and `Winipcfg.exe`, is 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 multicast connections, Symantec Ghost only responds to a ping request sent from another computer if it is in multicast 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 multicast 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.

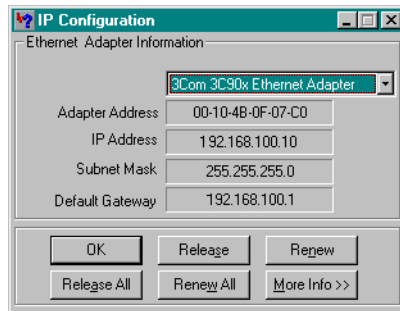
### **Pinging a Symantec Ghost multicast client**

On the Ghost Multicast 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 multicast log file

A multicast log file can be generated for Technical Support diagnostic purposes. Logging can slow down the multicasting 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 multicast 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 multicast session performance.

## The Windows Symantec Ghost Multicast Server log file

You can generate a log file while running the Windows Symantec Ghost Multicast Server.

### To generate a log file

- 1 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 Multicast Server as required.

The Symantec Ghost Multicast Server can be used for normal operation and the log file can be inspected upon completion.

## The DOS Symantec Ghost Multicast Server log file

You can generate a log file while running the DOS Symantec Ghost Multicast Server.

For example:

```
dosghsrv.exe c:\test123.gho TestSession -la -n10
```

starts a multicasting 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 multicast 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 Multicast Server application.
- 3 Use other command-line options as required.

### The Symantec Ghost Multicast Client log file

You can generate a log file while running Ghost.exe on a client computer.

### To generate a multicast 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 multicast log file, d:\logs\multi.log, to log all information while using multicasting in interactive mode:

`ghost.exe -jl:a=d:\logs\multi.log`

- 3 Use the Symantec Ghost multicasting 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 308.

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.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. The syntax for this installation is:

```
msiexec /i "c:\temp\Symantec Ghost.msi" /q
```

## 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.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.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.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.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
GHOSTINSTALLTYPE	Server	Determines the type of installation: server = enterprise console server tools = tools only client = Console client
EMAILADDRESS	(empty string)	User email address

Property	Default value	Description
GHOSTNGSERVERUSERNAME	GHOST_XXXXXXX where XXXXXXX is the computer name	Configuration server user name (applies only to Console installations)
GHOSTNGSERVERPASSWORD	GHOST_XXXXXXX where XXXXXXX is the computer name	Configuration server password (applies only to Console installations)
GHOSTCONSOLESERVERNAME	(empty string)	Console server computer name (applies only to Console client installations)
LICENSECERTIFICATE	(empty string)	Certificate number received from Symantec

## 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\"  
GHOSTINSTALLTYPE=\"Client\"  
GHOSTCONSOLESERVERNAME=\"ntServer\" /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.msi" [/q or /qb]**

The switches /q and /qb are optional.

For more information, see [“Installing from the command line”](#) on page 307.



## 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:

- StandardCare support

Connect to the Symantec Service & Support Web site at <http://service.symantec.com>, then select your product and version. This gives you access to product knowledge bases, interactive troubleshooter, Frequently Asked Questions (FAQ), and more.

- PriorityCare, GoldCare, and PlatinumCare support

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.

For telephone support information, connect to <http://service.symantec.com>, select your product and version, and then click Go! On the Service & Support page for your product, click Contact Options.

- 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) 984-2490.

## Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for six months after the release of the new version. Technical information may still be available through the Service & 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 Service & Support Web site only.

## Customer service

Visit Symantec Customer Service online at <http://service.symantec.com> for 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.symantec.com/upgrades/> or call the Customer Service Order Desk at (800) 568-9501.

## 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://www.symantec.com>, select the country you want information about, and click Go!



---

## Service and support offices

### North America

Symantec Corporation  
175 W. Broadway  
Eugene, OR 97401  
U.S.A.

<http://www.symantec.com/>  
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403  
(541) 984-2490

### Argentina and Uruguay

Symantec Region Sur  
Cerrito 1054 - Piso 9  
1010 Buenos Aires  
Argentina

<http://www.symantec-sur.com.ar>  
+54 (11) 5382-3802  
Fax: +54 (11) 5382-3888

### Asia/Pacific Rim

Symantec Australia Pty. Ltd.  
408 Victoria Road  
Gladesville, NSW 2111  
Australia

[http://www.symantec.com/region/reg\\_ap/](http://www.symantec.com/region/reg_ap/)  
+61 (2) 9850-1000  
Fax: +61 (2) 9817-4550

### Brazil

Symantec Brasil  
Market Place Tower  
Av. Dr. Chucuri Zaidan, 920  
12º andar  
São Paulo - SP  
CEP: 04583-904  
Brasil, SA

<http://www.symantec.com/region/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/](http://www.symantec.com/region/reg_eu/)  
+353 (1) 811 8032  
Fax: +353 (1) 811 8033

Automated Fax Retrieval

+31 (71) 408-3782

## **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.symantec.com/region/mx/>  
+52 (5) 481-2600  
Fax: + 52 (5) 481-2626

## **Other Latin America**

Symantec Corporation  
175 W. Broadway  
Eugene, OR 97401  
U.S.A.

<http://www.symantec.com/region/mx/>  
+1 (541) 334-6054 (U.S.A.)  
Fax: +1 (541) 984-8020 (U.S.A.)

# **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.

February 14, 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)	
Shipping & Handling	\$ 9.95
TOTAL DUE	<input type="text"/>

**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, Symantec Ghost, and Norton 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

<b>Autoinstall package</b>	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.
<b>backup regime</b>	A group of settings that determine which computer to include in a backup task and other details, for example, scheduling.
<b>boot package</b>	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 Multicast Server, or the Console.
<b>boot partition</b>	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.
<b>cloning</b>	Creating one or more replicas of a source computer.
<b>configuration settings</b>	Registry settings for client computers that can be set during the execution of a Console task.
<b>Console client</b>	Client of the Symantec Ghost Console that allows remote control of the client computer.
<b>data template</b>	A template that defines files or registry entries to include in a backup.
<b>image file definition</b>	A description of the properties of an image file, including the image file name, location, and status.
<b>image file</b>	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.
<b>multicasting</b>	A method of cloning to a group of computers simultaneously across a network.
<b>package definition</b>	A link from the Console to an AI package, either on an attached drive or on a Web server.

---

<b>snapshot</b>	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.
<b>source computer</b>	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.
<b>Creating an image file</b>	<p>Specifies a series of steps to be performed on all selected computers including:</p> <ul style="list-style-type: none"><li>■ Cloning of an image file</li><li>■ Applying configuration settings</li><li>■ Loading software applications</li><li>■ Loading user settings</li><li>■ Loading a file</li><li>■ Creating a backup</li><li>■ Restoring a computer from a backup</li></ul>
<b>user package</b>	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.
<b>user profile</b>	A definition of the data that you want to capture during a Move the User operation.

# I N D E X

## Symbols

#e=filename switch 252  
? switch 266  
@filename switch 252

## A

Abort log 252, 299  
Active tasks 127  
Adding  
    Data Template information 94  
Advanced options 70, 75  
afile=filename switch 252  
AI package definition 64  
Application image files 198  
ASPI driver 279  
Auto Start 154  
auto switch 252  
Autoexec.bat, multicast  
    NDIS driver 168  
    Packet driver 164  
AutoInstall  
    Builder 198, 205-210  
    Overview 197  
    Package definition 317  
    Snapshot 198, 201, 205  
    Using 201  
Automation  
    Batch switch 252  
    Clone switch and examples 253, 257-259  
    Close on completion 266  
    Quiet mode 271  
    Remove confirmation 272  
    Restart on completion 271  
    Switches 251-275  
    Version checking 274

## B

Backup 18, 21, 317  
    Creating a regime 84  
    Manual 87  
    Regime 83  
batch switch 252  
bfc=x switch 253  
Boot disk 40, 178  
    Creating 107  
    Creating manually 164  
    Setup 107, 192  
Boot package 317  
    Creating 107  
Boot partition 39, 75, 317  
    Certificate 131  
    Image 40  
bootcd switch 253  
BOOTP 172, 172-173  
Bootstrap Protocol. *See* BOOTP  
Builder 198, 205-210

## C

Cables 281  
Capturing  
    User Data 97  
CD writers 139  
CD-ROM 23, 279  
Certificate files, generating 131  
chkimg,filename switch 253  
Client summary 127  
clone switch 253  
Clone task properties 74  
Cloning 317  
    Windows 2000 191  
Close Ghostsrv on completion 155  
Command line 70, 75, 191  
    Examples 257-262  
    Ghost 251-275  
Command task properties 80  
Computer identification 243

---

- Computer, renaming 54
- Computers, viewing properties 55
- Config.sys multicast 168
- Configuration
  - Default settings 76
  - Files 198
  - Server 128
    - Timeout 130
  - Settings 317
    - Creating 59
    - Custom 76
    - Template 76
  - Task properties 75
- Console
  - Changing servers 131
  - Default client 130
  - Security 130
  - Wizard 129
- Console client 28, 52, 317
  - Installation 42
  - Status 53
  - Updating 43
- Console options
  - Splash screen 129
  - Task log 129
  - Warn client 129
- Copy command 253
- crc32 switch 135, 260, 260-263, 264
- crcignore switch 263
- Creating
  - Backup regime 84
  - Data Template 92
  - Machine Groups 51
  - Tasks 57
- Custom settings 76

## D

- Data Template 91, 317
  - Adding information 94
  - Creating 92
  - Specifying files 92
  - Specifying registry keys 93
  - Viewing 94
- dd switch 263
- Decompression 134
- Default settings 76

- Deploy AI package, task properties 77
- Details 127, 243
- dfile=filename switch 263
- DHCP 172, 172-173
- di switch 263
- Diagnostics 299-304
- Directory location variables 99
- dl=number switch 264
- Domain
  - Removing a computer from 70
- DOS, command-line, Multicast server 160
- dst switch 254
- Dump 147
  - Command 253
  - Task 68
- Dynamic Host Control Protocol. *See* DHCP

## E

- Enterprise 38
- Environment file 290
- Ethernet 22
- Event 127
- Execute task 81

## F

- f32 switch 264
- f64 switch 264
- fatlimit switch 264
- fcr switch 264
- fdsp switch 264
- fdsz switch 264
- ffi switch 264
- ffs switch 265
- ffx switch 265
- File system
  - FAT12 216
  - FAT16 216
    - Windows NT 230, 264
  - FAT32 216
    - Conversion from FAT16 264
  - Linux Ext2 216, 227
  - NTFS, switches 269
- File transfer task properties 79



---

## Files

- skipping 271
- To specify Data Template 92
- finger switch 265
- Fingerprint. *See* Ghost
- fis switch 265
- fni switch 265
- fns switch 265
- fnx switch 265
- fro switch 265
- fx switch 266

## G

- Gateway. *See* TCP/IP settings
- GDisk 32, 223, 224
  - Batch mode 228
  - Command line switches 225
- General task properties 72
- Ghost
  - Environment file 252
  - Fingerprint 265
  - Introduction 17-33
  - OEM version 292
  - Scenarios 20-23
  - Updating 43
  - See also* Uninstalling
  - See also* Procedures
- Ghost Boot Wizard 29
- Ghost Console 27, 131
  - Components 48, 67
  - User options 128
  - Using 132
- Ghost Explorer 32, 215-221
  - Command line 220
- Ghost Multicast Server 28
- Ghost operation, operating system 178
- Ghost Walker 31, 242-248
  - Command line 244
- Ghost.exe 23, 30, 143, 155, 179
- Ghosterr.txt. *See* Abort log

## H

- h switch 266
- Hard disk
  - Active 224
  - Batch 224
  - Creating 224
  - Deleting 224, 230
  - Hiding partitions 224
  - Large drives 232
  - MBR 224
  - Status 224
  - Wiping 230

## I

- ia switch 266
- ial switch 266
- ib switch 266
- id switch 267
- Image 149
- Image definitions 58, 317
- Image files 317
  - Add definition 58, 64
  - Applications 197
  - CD-ROM 23
  - Compression 134, 182, 275
  - crc. *See* crc32
  - Creating 136, 179
    - Insufficient space 136
  - File list 218
  - Loading 137
  - Modification 217
  - Multisegment 136, 252, 272
  - Password 270
  - Restoring 217
  - Size limited. *See* Image files multisegment
  - Spanned 136-137, 219, 252, 272
  - Split. *See* Image files, multisegment
  - Standard 135
  - Viewing contents 217
- Internal drives 280
- IP address. *See* TCP/IP settings

---

## J

ja=sessionname switch 267  
jl x=filename switch 267  
js=n switch 268

## L

License Audit Utility 33, 235-237  
Linux 178, 180, 216, 227, 266  
LiveUpdate 43  
Load 149

- Command 253

lockinfo switch 268  
locktype=type switch 268  
Log 127

- Clients 155
- Level and File 155

lpm switch 268  
lps switch 269  
LPT port 278

- Support 108

## M

Machine Groups 50

- Adding a computer to 52
- Creating 51
- Removing computers 53
- Renaming a computer 54
- Restrictions 51
- Viewing properties 55

Manual

- Backup 87

Mapped drive setup 280  
Master 277  
MBR, reinitializing 225  
memcheck switch 269  
Migrating a user 21  
Mode switch 253  
Move the User 77, 91

Multicast 20, 22, 143, 156, 279, 317

- Address 155
- Automating 153
- Command line 151
- Dump from client 146, 147
- From the server 151
- Load to clients 146, 149
- Session 146
- Setup 145
  - Boot disk 165
  - Quick guide 144-148
  - See also* Packet driver
  - See also* TCP/IP settings

Multicast server

- Automating 155
- Buffer 155
- Command line 160
- DOS 158
- Log 155
- NetWare 155
- Options 155
- Windows 143, 157

Multicast setup. *See* Packet driver

## N

NDIS driver 168

- Protocol manager files 166

Netmask. *See* TCP/IP settings  
Network 280

- Performance 134
- Routers, IP multicast 268

NGServer 132  
NIC packet driver 165  
nofile switch 269  
nolilo switch 269  
noscsi switch 269  
ntc switch 269  
ntchkdsk switch 269  
ntd switch 269  
ntic switch 269  
ntiid switch 270  
ntil switch 270  
Nwghsrv.nlm 159

---

## O

OEM version 292  
Operations. *See also* Procedures  
Options 70, 75  
or switch 270

## P

Packet driver 165  
    NIC 166  
Parallel port transfer  
    Automation 268, 274  
    Setup 277  
Partitions 223  
    Cloning 185  
Password 38, 242, 248, 270  
PC management 20  
pcopy command 253  
pdump command 253  
Peer-to-peer connections 277  
Performance network 134  
ping utility 300  
pload command 253  
pmbr switch 270  
Private certificate files 131  
Procedures  
    Disk cloning 179  
        From image file 185  
        To disk 180  
        To image file 182  
    Multicasting 143-156  
    Partition cloning 185  
        From image file 189  
        To image file 187  
        To partition 185  
Profile, user 92  
Properties  
    Backup regime 85  
    Clone 74  
    Command 80  
    Configuration task 75  
    File transfer 79  
    General 72  
Protocol.ini, NDIS driver for multicasting 167  
Public certificate files 131  
pwd, -pwd=x switch 270  
PXE 115, 117

## Q

quiet switch 271

## R

rb switch 271  
Regime  
    Incremental 83  
Removing  
    Computer from a domain 70  
    Computer from a group 53  
Renaming computers 54  
Restart on completion 155  
Restoring  
    Backup 88  
    User Data 97  
RIS 108, 115

## S

Schedule  
    Backup regime 87  
Scheduling tasks 81  
script switch 271  
SCSI tape  
    drives 138  
    Setup 279  
    Switches 273  
Sector, bad 253, 265, 274  
Sector-by-sector copy 266  
Security 130  
Service and Support 311  
Session name 145  
Setting task properties 72-80  
Setup 164, 165, 280  
    NDIS driver and shim 166  
    NIC packet driver 165  
    ODI driver and shim 165  
    *See also* Multicast  
    *See also* Network mapped drive  
    *See also* SCSI Tape  
SID 102, 105  
skip=x switch 271  
Slave 277  
Snapshot 198, 201, 205, 318  
Source computer 68, 145, 318  
span switch 272

---

- Spanning 136-137, 191
- split=x switch 272
- src switch 254
- Standalone Ghost. *See* Ghost.exe
- Subnet mask. *See* TCP/IP settings
- sure switch 272
- Switches 191
- Symantec Ghost
  - Updating 43
- Sysprep 101
  - .inf 106
- size switch 256

## T

- Tape drives 138
- tapebuffered switch 273
- tapeeject switch 273
- tapesafe switch 273
- tapesize switch 273
- tapespeed=x switch 273
- tapeunbuffered switch 273
- Task 71
  - Backup regime 86
  - Clone properties 74
  - Command properties 80
  - Configuration properties 75
  - Creating 48, 57
  - Deploy AI package properties 77
  - Dumping 68
  - Executing 48, 81
  - File transfer properties 79
  - General 68
  - General properties 72
  - Log 126
  - Move the User 97
  - Scheduling 81
  - Sysprep 68
  - Viewing 81
  - Wake On Lan 68
- TCP/IP 278
  - Settings 22, 169-173
    - See also* BOOTP
    - See also* DHCP
    - See also* Wattcp.cfg
- tcpm switch 274
- tcps switch 274

- Technical Support 311
- Template settings 76
- Template, data 91
- templates 91
- Token ring 22

## U

- Uninstalling 44
- Updating
  - Computer name 243
  - Console client 43
  - SID 243
  - Symantec Ghost 43
- USB port 278
  - Support 108
- usb switch 274
- User
  - Capturing Data 97
  - Migration 18, 21
  - Move the 91
  - Package 318
  - Profile 92, 318
  - Restore Data 97
  - Viewing a Profile 96
- Using
  - AI Builder 205-210
  - AI Snapshot 201, 205
  - AutoInstall 201
  - Console 132
  - Ghost Explorer 215-221

## V

- Variables
  - Directory location 99
  - Move the User 97, 99
- vdw switch 274
- ver switch 274
- ver=value switch 275
- vexcept switch 262
- View
  - Backup regime 88
  - User Profile 96
- Viewing
  - Data Template 94
  - tasks 81

---

## **W**

Wake on Lan 68, 70

Wattcp.cfg 164, 170, 171

*See also* TCP/IP settings

Windows, running Ghost inside 178

## **Z**

z switch 275

