Symantec Ghost™ Reference Guide

Symantec Ghost™ Reference Guide

Documentation version 8.2
PN: 10287427

Copyright Notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
Symantec Ghost Solution Suite

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

1. License:

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

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate

subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) 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.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

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

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. You agree to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. You agree not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, You agree not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will You sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that 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 to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland , or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

Notwithstanding any of the terms and conditions contained in this Symantec Software License Agreement, the following additional terms apply to the Software you have purchased:

A. The Software may contain multiple components. For each copy of the Software, such components, whether used individually or collectively, may be used on only one computer.

B. You may:

(i)use the Software only in accordance with its documentation;

(ii)use the Software on one computer to clone, or apply an image of a hard drive on that computer, or to another hard drive on the same computer. If a License Module accompanies, precedes, or follows this license, You may make and use the number of copies of the Software set forth in Your License Module on an equal number of individual computers pursuant to the terms of this License Agreement. Your License Module shall constitute proof of Your right to make and use such copies;

(iii)use the Software on a single computer to create an image file of a hard drive on that computer and store the image file on removable media for disaster recovery purposes;

(iv)use the Software to create a boot disk as described in the documentation for reapplying the hard drive image that was created for disaster recovery purposes to the hard drive on the original computer; or

(v)use the Software to clone a hard drive from a computer to a replacement computer in the manner described in the software documentation, and to use the Software on the replacement computer provided that the Software has been removed from the original computer and the original computer has been permanently decommissioned.

C. Scripting Documentation:

Any scripting documentation provided in conjunction with the Software may be used only in conjunction with the Software. You may not copy, distribute, license or sublicense the scripting documentation.

D. If Your Software includes the Symantec Client Migration, the following uses and restrictions apply to the Software:

(i)You may use a single copy of the Software to copy and deploy data and settings on a single computer. Such copy may be used an unlimited number of times for such single computer;

(ii)You may use a single copy of the Software to copy and transfer data and settings from one computer to a replacement computer, provided that the original computer is permanently decommissioned or destroyed; and

(iii)In order to deploy data and settings to multiple computers, You must have a copy of the Software for each computer that is the recipient of such data and settings.

Contents

Section 2 GhostCasting image files

Chapter 3 Using GhostCasting to create and restore images

Chapter 4 GhostCasting from the command line

Chapter 5 GhostCasting and IP addresses

Section 3 Creating executables to roll out applications

Chapter 6 Getting started with AutoInstall

Appendix B AI Builder variables, commands and conditions

Appendix C Transfer methods and hardware setup

Appendix D USB and DirectParallel cables

Appendix E Wattcp.cfg network configuration file

Appendix F Cloning with Linux

Appendix G Customizing Symantec Ghost functionality

Appendix H Adding DOS drivers to the Ghost Boot Wizard

Appendix I Installing Symantec Ghost from the command line

Appendix J Troubleshooting

Section 1

Using Symantec Ghost locally

Chapter 1

Using Symantec Ghost as a stand-alone program

This chapter includes the following topics:

About Ghost.exe

Ghost.exe is a stand-alone program you can use to copy disks or partitions from one computer to another. Image files can be created and then restored back onto a computer at any time.

Ghost.exe is run within DOS.

Using Ghost.exe on a stand-alone computer

The following is an overview of how to start and run Ghost.exe.

To use Ghost.exe on a stand-alone computer

1. Start Ghost.exe.
   Add command-line switches, if necessary.
   See "Command-line switches" on page 148.
2. If necessary establish a peer-to-peer connection.
   See "Establishing a peer-to-peer connection with Ghost.exe" on page 21.
3. Select the Ghost.exe operation:
   - Disk or partition to image file
   - Disk or partition from image file
   - Disk to disk
   - Partition to partition
   - Check image or disk
4. Do one of the following:
   - Select the source hard disk or partitions.
   - Select the image file.
5. Do one of the following for operations other than checking an image:
   - Select the destination hard disk or partition.
   - Select the image file.

   Warning: Make sure that you select the correct destination. The destination disk is completely overwritten with no chance of recovering any data.
6. Complete the Ghost.exe operation.

Starting Ghost.exe

Ghost.exe is a DOS-based application and runs in DOS mode outside of Windows. You cannot run Ghost.exe within Windows NT/2000/XP/9x/Me, Linux, OS/2, or other non-DOS operating systems. To run Ghost.exe on a computer that runs a non-DOS operating system, start the computer in DOS using a Ghost boot disk created with the Ghost Boot Wizard.

To start Ghost.exe

- 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. Once the computer has started, insert the second Ghost boot disk, and at the DOS prompt, type:
    A:\>\ghost\ghost.exe
    You can create a DOS boot disk on a computer running Windows or DOS. Running Ghost.exe may require additional DOS drivers. If you cannot access some hardware or network resources, such as a CD-R/RW drive, then create a boot disk using the Ghost Boot Wizard that contains the necessary drivers.
    For more information on creating boot disks and boot images, see the *Symantec Ghost Implementation Guide*.

Establishing a peer-to-peer connection with Ghost.exe

If you are using an LPT, USB, or TCP peer-to-peer connection, then you must set up the connection between computers before a clone, backup or restore operation.

The computers must be physically connected using one of the following:

LPT	A parallel connection cable
USB	A USB 1.1 cable
See "USB and DirectParallel cables" on page 215.	
TCP peer-to-peer	A network connection
See "TCP/IP connections" on page 210.	

In a peer-to-peer operation, one computer is designated the master computer, and the other is designated the slave computer. Table 1-1 describes the possible Ghost.exe processes and the master/slave relationships that exist within these processes.

Table 1-1 Master and slave computers

Action	Master	Slave
Disk-to-disk clone	Computer containing source disk	Computer containing destination disk
Back up disk to image file	Computer containing source disk	Computer receiving destination image file
Restore disk from image file	Computer containing destination disk	Computer containing source image file
Partition-to-partition clone	Computer containing source partition	Computer containing destination partition
Back up partition to image file	Computer containing source partition	Computer receiving destination image file
Restore partition from image file	Computer containing destination partition	Computer containing source image file

Select which computer is the master (the computer from which you control the connection), and which is the slave (the other computer participating in the connection). All operator input must occur on the master computer.

You must have two Ghost boot disk sets with which to start both the master and slave computers. You can create the boot disks using the Ghost Boot Wizard.

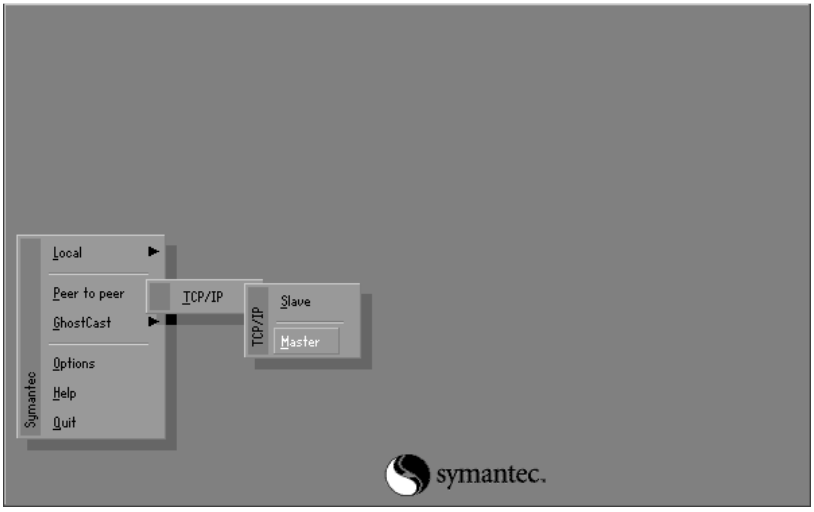
For more information on creating boot disks and boot images, see the *Symantec Ghost Implementation Guide*.

Note: You must create both boot disk sets in the same version of Symantec Ghost. You cannot use one boot disk created in Symantec Ghost 7.5 and one boot disk created in Symantec Ghost 8.2 in the same task.

To establish a peer-to-peer connection with Ghost.exe

1. Insert the first Ghost boot disk into the floppy disk drive of each computer.
2. Restart each computer.

3 Insert the second Ghost boot disk into the floppy disk drive of each computer and start Ghost.exe.



4 On the slave computer, on the main menu, do one of the following:

- In a USB connection, click **Peer to peer** > **USB** > **Slave** to start the computer as the slave computer.
- In an LPT connection, click **Peer to peer** > **LPT** > **Slave** to start the computer as the slave computer.
- In a TCP/IP connection, click **Peer to peer** > **TCP/IP** > **Slave** to start the computer as the slave computer.
  Note the IP address displayed in the Slave Connect dialog box.

5 On the master computer, on the main menu, do one of the following:

- In a USB connection, click **Peer to peer** > **USB** > **Master** to start the computer as the master computer.
- In an LPT connection, click **Peer to peer** > **LPT** > **Master** to start the computer as the master computer.
- In a TCP/IP connection, click **Peer to peer** > **TCP/IP** > **Master** to start the computer as the master computer.
  Type the IP address displayed on the slave computer.

Creating a backup image file

You can create a backup of a hard disk or one or more partitions.

The backup is saved as an image file, which you can store on the following:

- Second hard disk
- Second partition on your hard disk (partition backup only)
- LS120 Superdisk, JAZ, or ZIP disk
- CD-R/RW or DVD-R/RW/+R/+RW
  For more information on saving an image file directly to a CD/DVD, see the *Symantec Ghost Implementation Guide*.
- FireWire hard disk
- USB 1.1/2.0 hard disk
- Tape
- Locally mapped network file server
- Another computer using a peer-to-peer connection

Compression may affect the speed of your operation. When you select a compression level, Ghost.exe estimates the amount of space available for the destination image file. If there is insufficient space, Ghost.exe prompts you to enable spanning of image files.

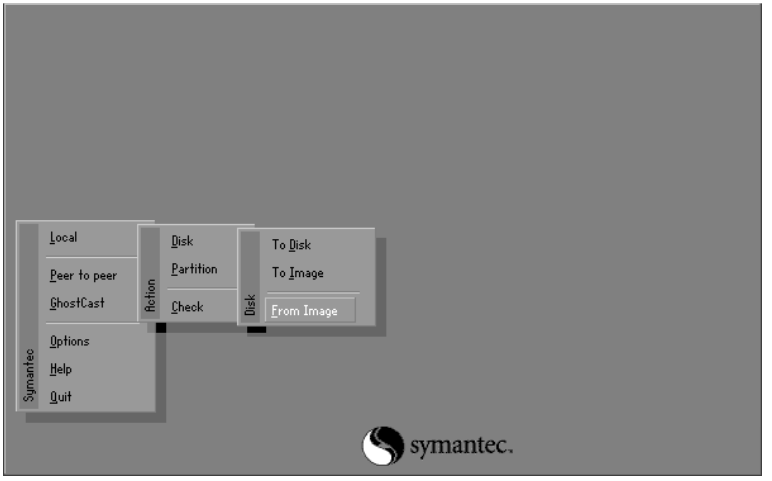
Backing up a hard disk to an image file

When you back up a hard disk, a copy of the entire disk is saved as an image file.

To back up a disk to an image file

1. On the Ghost.exe main menu, do one of the following:
   - Local: Click **Local** > **Disk** > **To Image**.

- Peer-to-peer connection: Click **Disk** > **To Image**.



2. In the Source Drive dialog box, select the source disk.
   The Source Drive dialog box shows details of every disk that Ghost.exe finds on the local computer.
3. In the File Locator dialog box, type the image file destination and name.
4. In the Image file description dialog box, type a description of the image file.
   You can modify this description on the Console or in Ghost Explorer.
5. Click **Save**.
6. If Ghost detects that there is not enough space for the image file you are prompted to select compression:
   - For no compression, click **No**.
   - For low compression, click **Fast**.
   - For high compression, click **High**.

   For more information on image files and compression, see the *Symantec Ghost Implementation Guide*.
7. In the Compress Image? dialog box, select a compression option.
8. If Ghost detects that there is not enough space for the image file you are prompted to enable spanning.

9 Check the details and ensure that the correct options are selected.

10 Do one of the following:

- 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.

11 If spanning is required, do one of the following:

- Insert the next media, then click **OK**.
- Click **Browse**, then select the location of the next span of the image file.

For more information on image files and volume spanning, see the *Symantec Ghost Implementation Guide*.

12 Verify the integrity of the image file.
See "Verifying integrity" on page 34.

Backing up a partition to an image file

You can create an image file from one or more partitions to use as a backup or to clone onto another partition or disk.

To back up a partition to an image file

1 On the main menu, do one of the following:

- Local: Click **Local** > **Partition** > **To Image**.
- Peer-to-peer connection: Click **Partition** > **To Image**.

2 In the Source Drive dialog box, select the source drive.
The Source Drive dialog box contains the details of every disk that Ghost.exe finds on the local computer.

3 In the Source Partition dialog box, select the source partitions to include in the destination image file.
The Source Partition dialog box contains the details of all the partitions on the selected source disk. You can select multiple partitions.

4 Click **OK**.

5 In the File Locator dialog box, select the image file destination and name.

6 In the Image file description box, type a description of the image file.

7 Click **Save**.

8 If Ghost detects that there is not enough space for the image file you are prompted to select compression:

- For no compression, click **No**.
- For low compression, click **Fast**.
- For high compression, click **High**.

For more information on image files and compression, see the *Symantec Ghost Implementation Guide*.

9 In the Compress Image? dialog box, select a compression option.

10 If Ghost detects that there is not enough space for the image file you are prompted to enable spanning.

11 In the Proceed with partition image creation? dialog box, do one of the following:

- 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 If spanning is required, do one of the following:

- Insert the next media, then click **OK**.
- Click **Browse**, then select the location of the next span of the image file.

For more information on image files and volume spanning, see the *Symantec Ghost Implementation Guide*.

13 Verify the integrity of the image file when it has been created.
See "Verifying integrity" on page 34.

Restoring from an image file

You can restore a hard disk or a partition.

The restore is made from a previously created image file that is stored on one of the following:

- Second hard disk
- Second partition on your hard disk
- JAZ or ZIP disk
- CD-R/RW
- DVD
- FireWire hard disk
- USB 1.1/2.0 hard disk
- Tape
- Mapped network drive
- Drive on another computer (peer-to-peer)
- Drive or partition being restored

Restoring a hard disk from an image file

When you restore a hard disk, it is overwritten by the contents of the image file.

To restore a disk from an image file

1. On the main menu, do one of the following:
   - Local: Click **Local** > **Disk** > **From Image**.
   - Peer-to-peer connection: Click **Disk** > **From Image**.
2. In the File Locator dialog box, do one of the following:
   - Type the path and file name of the image file.
   - Click **Browse** to locate the image file.
     Specify the drive or device and select the full path name. The image file may reside on a local drive or on a locally mapped network file server. When using a peer-to-peer connection, the image file is located on the slave computer.
3. Press **Enter**.
4. In the Destination Drive dialog box, select the destination disk.
   Choose carefully as this is the disk that will be overwritten.

The Destination Drive dialog box shows the details of every drive that Ghost.exe finds on the local computer.

5 In the Destination Drive Details dialog box, confirm or change the destination disk partition layout.

The Destination Drive Details dialog box shows a suggested partition layout for the destination disk. By default, Ghost.exe tries to maintain the same size ratio between new disk partitions.

You can change the size of any target FAT, NTFS, or Linux Ext2/3 partition by entering the new size in megabytes.

You cannot enter a value that exceeds the available space, is beyond the file system's limitations, or is not large enough to contain the data held in the source image.

Warning: The Destination Drive Details dialog box shows a suggested partition layout for the destination drive once the cloning process is completed. This partition layout may mirror the source drive layout. Therefore, the destination drive details appear similar to the source drive.

---

6 Click **OK**.

7 Do one of the following:

- Click **Yes** to proceed with the disk cloning.
  Ghost.exe creates the destination disk using the source image file disk details. If you need to abort the process, press **Ctrl+C**, but be aware that this leaves the destination disk in an unknown state.
- Click **No** to return to the menu.

Warning: Only click Yes if you are sure that you want to proceed. The destination disk is completely overwritten with no chance of recovering any data.

---

8 If prompted to insert an image span, when prompted, do one of the following:

- Insert the next media, then click **OK** to continue.
- Click **Browse** to restore from a different location, then type the location and file name of the image file span.

9 Restart the computer when the disk image restore is complete.

10 Run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination disk.

Restoring a partition from an image file

When you restore a partition, it is overwritten by the data from an image file.

To restore a partition from an image file

1. On the main menu, do one of the following:
   - Local: Click **Local** > **Partition** > **From Image**.
   - Peer-to-peer connection: Click **Partition** > **From Image**.
2. In the File Locator dialog box, do one of the following:
   - Type the path and file name of the image file.
   - Click **Browse** to locate the image file.
     Specify the drive or device and select the full path name. The image file may reside on a local drive or on a locally mapped network file server. When using a peer-to-peer connection, the image file is located on the slave computer.
3. Press **Enter**.
4. In the Source Partition dialog box, select the source partition from the image file.
   The Source Partition dialog box contains the details of all of the partitions in the image file.
5. In the Destination Drive dialog box, select the destination disk.
   The Destination Drive dialog box contains the details of every disk that Ghost.exe finds on the local computer.
6. In the Destination Partition dialog box, select the destination partition.
   Select an existing partition carefully as this is the partition that will be overwritten.
   The Destination Partition dialog box contains the details of all of the partitions on the selected destination disk. You can create a new partition if space is available. If you create a new partition, it can be resized during the cloning operation.

7 In the Proceed with partition restore? dialog box, do one of the following:

- Click **Yes** to proceed with the partition cloning.
  Ghost.exe overwrites the destination partition using the partition details contained in the image file. If you need to abort the process, press **Ctrl+C**, but be aware that this leaves the destination partition in an unknown state.
- Click **No** to return to the menu.

Warning: Only click Yes if you are sure that you want to proceed. The destination partition is completely overwritten with no chance of recovering any data.

---

8 If prompted to insert an image span, when prompted, do one of the following:

- Insert the next media, then click **OK** to continue.
- Click **Browse** to restore from a different location, then type the location and file name of the image file span.

9 Restart the destination computer when the partition copy is complete.

10 Run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination partition.

Cloning disks and partitions

By default, Ghost.exe tries to maintain the same size ratio between new disk partitions. However, you should note the following:

- You can change the size of any destination FAT, NTFS, or Linux Ext2/3 partition by entering the new size in megabytes.
- You cannot enter a value that exceeds the available space, is beyond the file system's limitations, or that is not large enough to contain the data held in the source partition.

Cloning disk to disk

When you clone disk to disk, Ghost.exe copies the contents of one hard disk onto another.

To clone disk to disk

1. On the Ghost.exe main menu, do one of the following:
   - Local: Click **Local** > **Disk** > **To Disk**.
   - Peer-to-peer connection: Click **Disk** > **To Disk**.
2. In the Source Drive dialog box, select the source disk.
   The Source Drive dialog box shows the details of every disk that Ghost.exe finds on the local computer.
3. In the Destination Drive dialog box, select the destination disk.
   Choose carefully as this is the disk that will be overwritten.
   If a peer-to-peer connection method is used, the destination disk can be any of the slave computer's disks. However, if this is a local disk-to-disk copy, then the source disk is unavailable for selection.
4. Confirm the destination disk layout.

   Warning: The Destination Drive Details dialog box shows a suggested partition layout for the destination drive once the cloning process is completed. This partition layout may mirror the source drive layout. Therefore, the destination drive details appear similar to the source drive.
5. Click **OK**.
6. When the "Proceed with disk clone?" prompt appears, do one of the following:
   - 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.
   - Click **No** to return to the menu.

   Warning: Only click Yes if you are sure that you want to proceed. The destination disk is overwritten with no chance of recovering any data.

7 Restart the computer.

Warning: You should remove one of the hard disks before you restart your computer. If you leave two hard disks in the computer, damage can occur to both of the bootable operating systems.

8 Run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination disk.

Cloning partition to partition

When you clone partition to partition, Ghost.exe copies the contents of one partition onto another.

To clone from partition to partition

1 On the main menu, do one of the following:
- Local: Click **Local** > **Partition** > **To Partition**.
- Peer-to-peer connection: Click **Partition** > **To Partition**.

2 In the Source Drive dialog box, select the source disk.
The Source Drive dialog box shows details of every disk that Ghost.exe finds on the local computer.

3 In the Source Partition dialog box, select the source partition.
The Source Partition dialog box shows the details of all of the partitions on the selected source disk.

4 In the Destination Drive dialog box, select the destination disk.
The Destination Drive dialog box shows the details of every disk that Ghost.exe finds on the destination computer. For peer-to-peer connections, the slave computer is the destination.

5 In the Destination Partition dialog box, select the destination partition.
Select an existing partition carefully as this is the partition that is overwritten.
The Destination Partition dialog box shows the details of all of the partitions on the selected destination disk. If this is a local partition-to-partition copy, then the source partition is unavailable for selection. However, you can create a new partition if space is available. If you create a new partition, it can be resized during the cloning operation.

6 Click **OK**.

7 When the final Proceed with Partition Copy? prompt appears, do one of the following:

- 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 disk in an unknown state.
- Click **No** to return to the menu.

Warning: Only click Yes if you are sure that you want to proceed. The destination partition is completely overwritten with no chance of recovering any data. This is the last chance to back out.

8 Restart the destination computer when the partition copy is complete.

9 Run Symantec Disk Doctor, Chkdsk, ScanDisk, or a similar utility to verify the integrity of the destination partition.

Verifying integrity

After a backup, restore, or clone operation, check the integrity of the partition, hard disk, or computer.

Verify an image file or disk

To verify the integrity of an image file

- On the computer on which the image file is saved, on the main menu, do one of the following:
  - Local: Click **Local** > **Check** > **Image File**.
  - Peer-to-peer connection: Click **Check** > **Image File**.

To verify the integrity of a disk

1 On the main menu, do one of the following:

- Local: Click **Local** > **Check** > **Disk**.
- Peer-to-peer connection: Click **Check** > **Disk**.

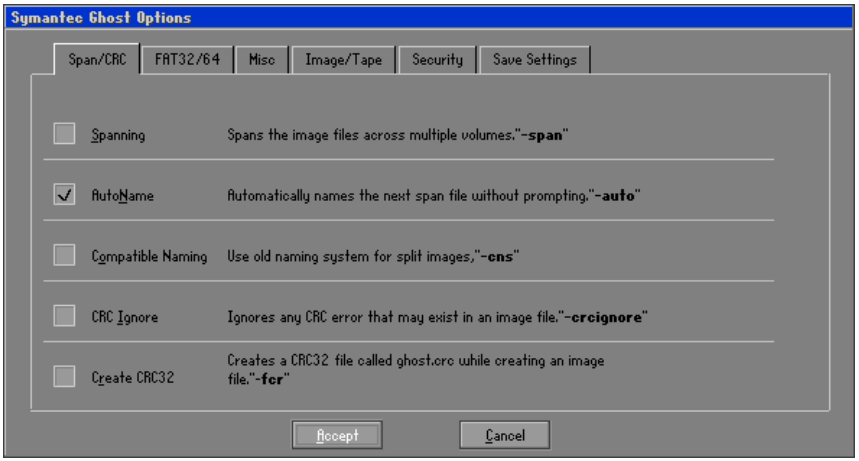
2 Select the source disk to verify.

3 Click **OK**.

4 Click **Yes** to start the disk check.

Adding switches to your Ghost.exe operation

You can include a number of options (or switches) that can also be entered using the command line. These switches are set in the Ghost.exe user interface.



To add switches to your Ghost.exe operation

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

2 Select the options to include in your current cloning task.

Tab	Command-line options
Span/CRC	-span, -auto, -cns, -crcignore, -fcr
FAT 32/64	-f32,-f64, -fatlimit
Misc	-sure, -fro, -rb, -fx
Image/Tape	-ia, -ib, -id -tapebuffered, -tapeeject, -tapesafe, -tapeunbuffered
HDD access	-ffx, -fnx, -ffi, -fni, -ffs, -fns
Security	-pwd, -locktype=type

See "Command-line switches" on page 147.

3 On the Save Settings tab, click **Save Settings** to confirm the list of active switches listed.

4 Click **Accept** to include the settings in the current task.

Running Ghost32.exe in Windows

Ghost32.exe is a Win32 version of Ghost.exe and is designed to run on Microsoft Windows 9x/NT/2000/XP/PE. Using Ghost32.exe you can perform most Ghost operations on hard drives that are accessible from these operating systems, and communicate with the GhostCast Server.

If you run Ghost32.exe within Windows, note the following:

- The partition on which Windows is installed cannot be overwritten.
- On Windows 9x/Me if you overwrite a disk or partition, you may have to restart the computer. On Windows NT/XP/2000 you should not have to restart the computer.
- Ghost32.exe does not automatically restart the system.
- Hard disk sizes may appear smaller than their actual sizes. Ghost32.exe can only access the shown destination size. The remaining space is not used.
- Ghost32.exe does not support mount point volumes on Windows NT/2000/XP computers.

Compatibility with Ghost.exe

Ghost32.exe shares the following functions with Ghost.exe:

- Both Ghost.exe and Ghost32.exe can be a master or slave in a TCP/IP peer-to-peer operation.
- Image files created with Ghost.exe and Ghost32.exe are interchangeable.

Ghost32.exe differs from Ghost.exe in the following ways:

- Can be run on Microsoft Windows 9x/Me/NT/2000/XP.
- LPT peer-to-peer is not supported.
- USB peer-to-peer is not supported.
- Cannot use with a disk or partition that has files open during the operation. For example, the system partition.
- When writing to CD/DVD, Ghost32.exe is not copied onto the CD/DVD.

Using Ghost32.exe to write an image file to CD/DVD

Ghost32.exe is installed with the Symantec Ghost Console and the Symantec Ghost Standard Tools; however, if you want to use Ghost32.exe to write to a CD/DVD, then you must ensure access to the following files:

Table 1-2 Required files

File	Description
Ghostcdr.dll	Ghostcdr.dll is installed with Ghost32.exe. Ensure that Ghostcdr.dll is in the path.
NT drivers	If you are running an NT-based operating system (Windows NT/2000/XP), then you must install the required drivers from a command prompt. Use the executable, Afsinst.exe, to install the drivers. Afsinst.exe is on the Symantec Ghost CD in the following directory: \Extras\OAKCDR\WinNT_2k_XP\

To install drivers for Ghost32.exe to write to a CD/DVD on Windows NT/2000/XP

1. On the Windows taskbar, click **Start** > **Run**.
2. At the command prompt, type
   E:\Extras\OAKCDR\WinNT_2k_XP\Afsinst.exe /install /noflag
   where E: is the drive letter for the CD drive.
3. Restart the computer.

Starting Ghost32.exe

You can start Ghost32.exe from Windows Explorer.

To start Ghost32.exe

1. On the Windows taskbar, click **Start** > **Programs** > **Accessories** > **Windows Explorer**.
2. Open the directory in which you installed Symantec Ghost.
   The default directory is Program Files\Symantec\Ghost.
3. Double-click **Ghost32.exe**.

Ghost32.exe operations are executed using the same procedures as Ghost.exe.

See "About Ghost.exe" on page 19.

Chapter 2

Configuration Client (stand-alone)

This chapter includes the following topics:

Introducing the Configuration Client (stand-alone)

Use the Configuration Client feature to apply configuration settings to a computer directly. This lets you run a post clone configuration without the Console.

There are some differences between the Configuration Client and the post clone configuration from the Console. The differences are as follows:

- Configuration Client allows the addition of Microsoft Windows NT/XP/2000 computers to a domain. However, you must create the computer account on the domain before using the Configuration Client. For the computer account to work, you must first add security permissions for Windows 2000 and Windows XP native mode Active Directory domain controllers.
- Configuration Client supports an extra option to disable itself after running. This works on stand-alone client installations only, and disables the Configuration Client from running on that computer after it is run the first time. To use the Configuration Client again on that computer, you must uninstall and reinstall the Configuration Client.

To use the stand-alone configuration

1. Install the Symantec Ghost Configuration Client or Console client on the target computer.
   For more information on installing the Configuration Client, see the *Symantec Ghost Implementation Guide*.
2. Write a program to generate the configuration data file.
   See "Generating the configuration data file" on page 40.
3. Run the program to generate the configuration data file, gvpcfg.bin.
4. Apply the configuration data file to the target computer.
   See "Running the Configuration Client using Ghost.exe" on page 41.

Generating the configuration data file

To generate the configuration data file, you must write a program that calls MachConf.dll, the .dll file supplied by Symantec Ghost. MachConf.h lists the settings and values required for creating a configuration data file.

The following example files, on which to base your program, are included:

- Genghostfile.cpp
- Genghostfile.vcproj
- Genghostfile.sln
- StdAfx.cpp
- Stdafx.h
- MachConf.h

All of the example program files, .dll files, and Help files are on the Symantec Ghost CD in the following directory:

\Extras\Source\Genghostfile

The configuration data file gvpcfg.bin is generated.

Running the Configuration Client using Ghost.exe

If you are using Ghost.exe to restore a computer, you can use OmniFS.exe to copy the configuration file after the restore.

To run the Configuration Client using Ghost.exe

1. Ensure that the data configuration file and OmniFS.exe are available on the target computer.
   For example, on a floppy disk.
2. Restore the computer using Ghost.exe.
3. After the restore, but before restarting your computer, use OmniFS.exe to copy the data configuration file into the root directory of the system drive.

Operating system	Root directory
Microsoft Windows 9x computers	c:\
Microsoft Windows NT/2000/ XP computers	%systemdrive%\ **Note:** If a computer has Microsoft Windows installed on a partition other than the active/boot partition copy the data configuration file to the active/boot partition.

   For example, omnifs copy a:\gvpcfg.bin 0.1:\gvpcfg.bin
   See “Copying files and directories” on page 137.

When the computer is restarted, the configuration data file is processed and the configuration data is applied to the computer.

Running the Configuration Client without using Ghost.exe

You can also run the Configuration Client without using Ghost.exe.

To run the Configuration Client without using Ghost.exe

1 Copy the data configuration file into the root directory of the system drive as follows, overwriting the existing data file.

Operating system	Root directory
Microsoft Windows 9x computers	c:\
Microsoft Windows NT/2000/XP computers	%systemdrive%\ **Note:** If a computer has Microsoft Windows installed on a partition other than the active/boot partition copy the data configuration file to the active/boot partition.

2 Restart the computer.
The configuration data file is processed and the configuration data is applied to the computer.

Error logging during a stand-alone configuration

Any errors generated during the stand-alone configuration are logged as follows:

- Microsoft Windows NT/XP/2000: Event log
- Microsoft Windows 9x/Me: Error file, c:\lastpostconfigurationstatus.txt

Section 2

GhostCasting image files

Chapter 3

Using GhostCasting to create and restore images

This chapter includes the following topics:

About GhostCasting

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

The GhostCast Server supports three forms of data transfer for transferring files:

- Unicasting
- Direct Broadcasting
- Multicasting

GhostCasting makes workstation migration and rollouts more efficient and may eliminate replicated network traffic. You can use it through the Windows interface, command-line switches, batch files, or a combination of all three methods.

Two applications are used in GhostCasting: one on the network server and another on every client workstation to be restored or backed up.

- The GhostCast Server restores image files to multiple clients or creates an image file from a single connected client.
- On a client workstation, Ghost.exe receives and writes the image file to the local disk.

GhostCasting supports:

- Ethernet networks
- Token ring networks
- Image file creation
- Multicast-enabled routers
- Automatic IP address selection using BOOTP or DHCP
- Session start scheduling
- Partition-only GhostCasting
- Multiple, simultaneous sessions, or one session per server

Preparing for GhostCasting

Before GhostCasting, you must set up the required software and hardware.

To prepare for GhostCasting

1. Set up the network hardware.
   - Install the network adapter.
   - Connect cabling.
   - Set up the network adapter using the manufacturer's installation program.
   - Run the network adapter test program to check the network adapter and cabling.
2. Determine the IP and networking settings.
   - BOOTP/DHCP vs. manual configuration
   - Network adapter drivers
   - Other overall requirements

   See "GhostCasting and IP addresses" on page 65.

Creating the model computer

Create a model computer to serve as a template for client computers. This is the first step in creating a Symantec Ghost image. Set up a computer with Windows and all of its drivers installed and configured as you want all of your computers configured.

If you are creating a model computer for Windows NT computers, see the Online Knowledge Base article: “How to clone a Windows NT or Windows 2000 workstation” at:

http://service1.symantec.com/support/ghost.nsf/docid/1999012209340925

You may need to create a model computer for each unique hardware setup. For example, if you have some computers with SCSI disks and some with IDE disks, you need to have separate images for them. However, on Windows 2000/XP computers, Microsoft Sysprep can help you create a generic template image for different hardware setups.

Note: Ensure that Windows NT/2000/XP computers are not domain members before taking an image.

Creating a GhostCast Server

The GhostCast Server creates or distributes a copy of an image file to Symantec Ghost clients in a session composed of one server, a single image file, and one or more similar clients. The session name acts as a key. The session name identifies the session, and is used by clients to indicate the session that they are to join.

To create a GhostCast Server

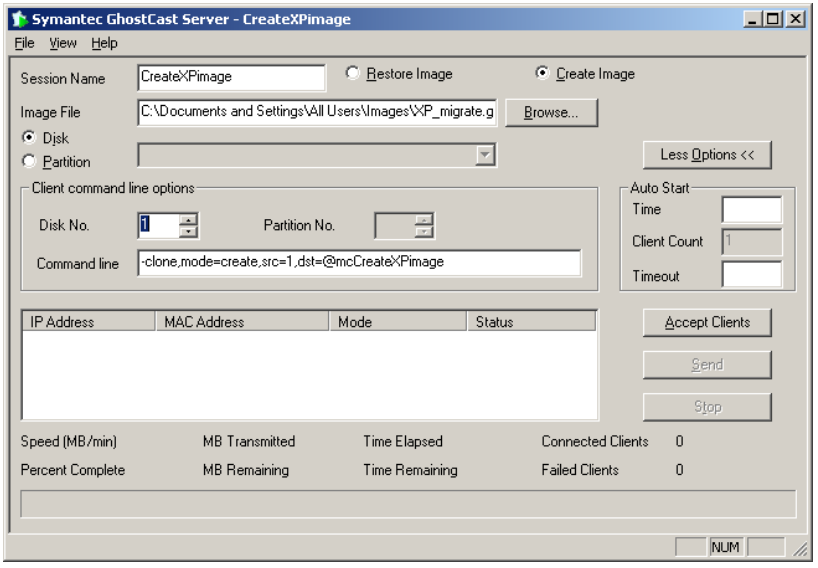
1. Install GhostCast Server (Ghostsrv.exe).
   For more information on installing GhostCast Server, see the *Symantec Ghost Implementation Guide*.
2. Create a boot disk that contains Ghost.exe for the client computers.
   For more information on creating a boot disk with network support, see the *Symantec Ghost Implementation Guide*.

Starting a GhostCast session

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

To start a GhostCast session

1 On the GhostCast Server computer, on the Windows taskbar, click **Start** > **Programs** > **Symantec Ghost** > **GhostCast Server**.



2 In the GhostCast Server window, in the Session Name box, type a session name.

A GhostCast session name can be any alphanumeric sequence of characters and must be unique on your network. You can use spaces on the GUI but not with command-line switches. Session names are not case-sensitive.

Creating an image file

To create an image file, you must first start a GhostCast session from the GhostCast Server. Once you create a session on the server, join the GhostCast session from the source computer.

To create an image file using the GhostCast Server

1 In the GhostCast Server window, click **Create Image**.

2 Do one of the following:

- In the Image File box, type the name and full path of the image file that you are creating.
- Click **Browse** to find the location.

You can overwrite existing files.

3 Do one of the following:

- 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 boxes are filled in.

5 Start Ghost.exe on the destination client computers and begin a GhostCast session.
See "To connect a source computer to a GhostCast session" on page 49.

Once the GhostCast session is started on the server, you can start the client computer from a boot disk and have it join the session.

To connect a source computer to a GhostCast session

1 Create a GhostCast session on the GhostCast Server.
See "To create an image file using the GhostCast Server" on page 48.

2 Using the Ghost network boot disk, start Ghost.exe on the client computer.

3 On the Ghost.exe menu, click **GhostCasting**, then select one of the following:

Multicast	Connect to the session using Multicasting.
Direct Broadcast	Connect to the session using direct broadcasting.
Unicasting	Connect to the session using Unicasting.

4 In the GhostCast Session Name to Join dialog box, type the session name.

5 Click **OK**.

6 Select the disk from which to take an image.

7 Click **OK**.

8 Select the partition from which to take an image, if required.

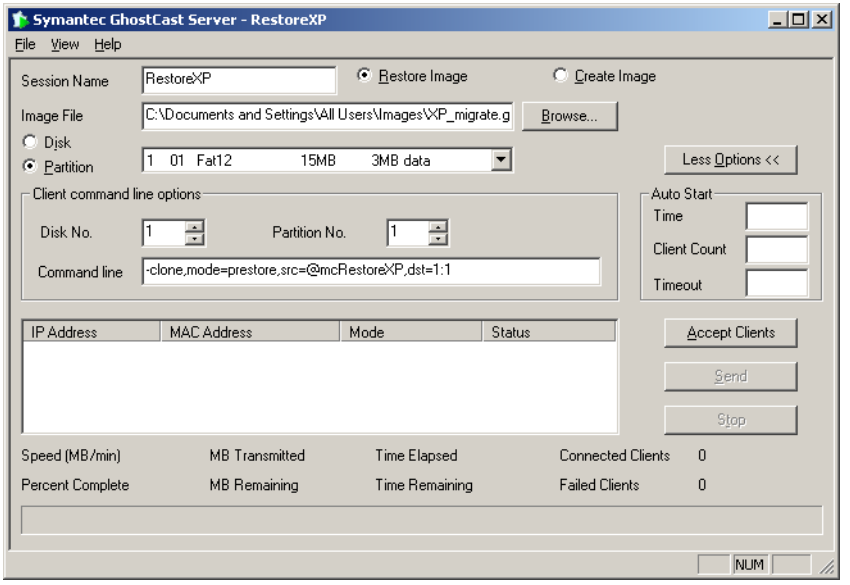
9 Click **OK**.

10 Select the level of compression that you require.

11 Click **Yes** to begin.
See "Running Ghost.exe on a client computer" on page 59.

Restoring an image file onto client computers

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



Restore an image file onto client computers

Select the image to restore onto the client computers.

To restore an image onto client computers using the GhostCast Server

1. Click **Restore Image** to send an image file to all connecting clients.
2. Do one of the following:
   - In the Image File box, type the name and full path of the image file containing the image.
   - Click **Browse** to find the location.
3. On the File menu, click **Image Description** to view or modify a description of the image file.
   The disk or partition settings must be selected. If the file selected is not a valid image file, an error message appears.

4 Do one of the following:
   - Click **Disk** to restore an image of an entire disk.
   - Click **Partition** to restore 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 boxes are filled out.

6 Join the client computers to the GhostCast session.
   See "To join a GhostCast session to restore an image file to client computers" on page 51.

7 Click **Send** to start the image restore and the GhostCast session when all of the required clients have joined the session.

The progress indicator shows the status of the GhostCast session as it proceeds, along with other image file and transfer details. The statistics shown are based on the image file size and reflect the sizes after compression. The speed shows the actual amount of data being sent over the network in megabytes-per-minute from the image file. The client status changes to In Progress.

If you close the GhostCast Server or turn off the computer once a GhostCast session has started, the GhostCast session stops and a warning message appears.

You must start Ghost.exe on the client computer and join the clients to the GhostCast session.

To join a GhostCast session to restore an image file to client computers

1 On the client computers, use the Ghost Boot Disk to start Ghost.exe.

2 On the Ghost.exe menu, click **GhostCasting**, then select one of the following:

Multicast	Connect to the session using Multicasting
Direct Broadcast	Connect to the session using Direct Broadcasting
Unicasting	Connect to the session using Unicasting

3 In the GhostCast Session Name to Join dialog box, type the session name.

4 Click **OK**.

5 Select the disk to restore.

6 Click **OK**.

7 Select the partition to restore, if required.

8 Click **OK**.

9 Click **Yes** to indicate that the computer is ready for the image restore to begin.
See "Running Ghost.exe on a client computer" on page 59.

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

Controlling the GhostCast session from the server

In the GhostCast session, you can specify the client disk or partition to restore from the server. You can also define command-line options to execute as part of the cloning task.

Control the GhostCast session from the server

Use command-line options to execute specific options on the client computer.

To create an image file using the GhostCast Server and command-line options

1 On the GhostCast Server, start a GhostCast session to create an image file.
See "To create an image file using the GhostCast Server" on page 48.

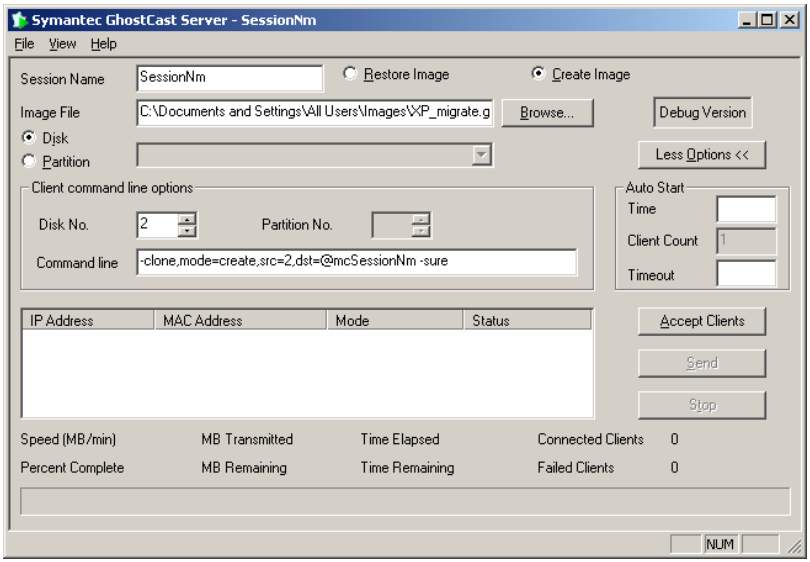
2 Click **More Options**.

3 In the Disk No. box, type the disk number.

4 In the Partition No. box, type the partition number if you are creating an image of a partition.
The client clone command appears in the Command line box.

5 Add other switches to the command line to execute specific command-line options on the client computer, if required.
For example, if the initial command is:
-clone,mode=pcreate,src=2,dst=@mcSessionNm
Add the following switches to avoid prompts and restart the client computer after the image has been extracted:
-clone,mode=pcreate,src=2,dst=@mcSessionNm -sure -rb

Only use the -sure switch when you are certain that you are writing from the intended disk or partition.



6 Click **Accept Clients** to accept the client computer into the session.

7 Start the client computers in DOS.

8 Run Ghost.exe using the -ja switch to log on to the GhostCast session from the command line:
ghost.exe -ja=SessionNm

9 Confirm your choices on the client computers if the -sure switch was not used.
See "Running Ghost.exe on a client computer" on page 59.

To restore an image onto client computers using the GhostCast Server

1 Create a GhostCast session to restore an image from the GhostCast Server.

2 Click **More Options**.

3 In the Disk No. box, type the disk number.

4 In the Partition No. box, type the partition number, if required.

5 In the Command line box, type the client clone command.

Add other switches to the command line to execute specific commands on the client computer.

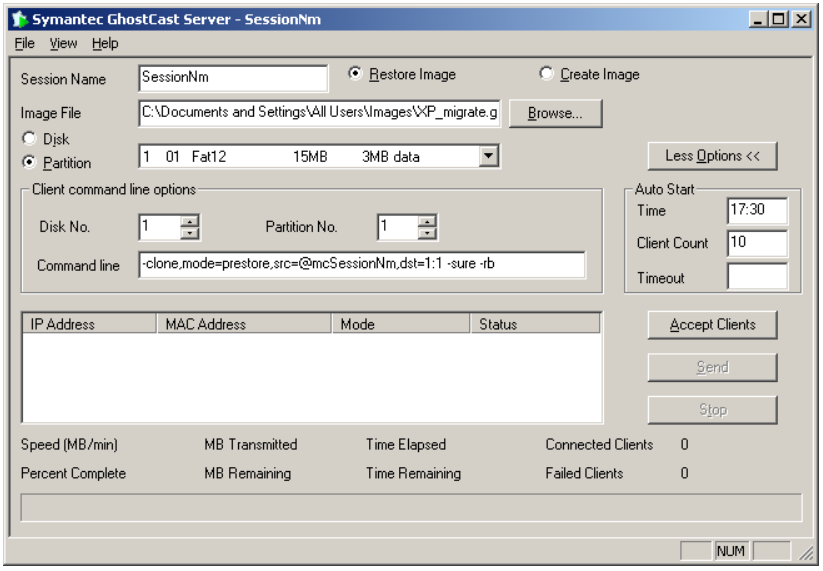
For example, if the initial command is:

-clone,mode=prestore,src=@mcSessionNm,dst=1:1

Add the following switches to avoid prompts and restart the client computer after the image has restored:

-clone,mode=prestore,src=@mcSessionNm,dst=1.1 -sure -rb

Only use the -sure switch when you are sure that you are writing to the intended disk or partition.



6 Click **Accept Clients** to accept the client computer into the session.

7 Start the client computers in DOS.

8 Run Ghost.exe using the -ja switch to log on to the GhostCast session from the command line:

ghost.exe -ja=SessionNm

9 Confirm your choices on the client computers if the -sure switch was not used.

See “Running Ghost.exe on a client computer” on page 59.

Setting Auto Start parameters

When your GhostCast session includes restoring an image file to client computers, you can set the server to start the session automatically. The start time can be based on a single parameter or a combination of parameters.

If you specify more than one Auto Start parameter, the session starts when one of the conditions is fulfilled.

To set Auto Start parameters

1. In the GhostCast Server window, click **More Options**.
2. Do one or more of the following:
   - To use the time parameter, type a specified time using a 24-hour clock and within the next 24-hour time period.
     For example, 5:30 AM would be 05:30, and 5:30 PM would be 17:30.
   - To use the number of clients parameter, type the number of clients that are connected to the session.
     For example, if the threshold is set to 10, then the server waits and accepts clients until the tenth client. Once the tenth and final client is accepted, the server stops accepting clients and starts sending out to the connected client computers.
   - To use the timeout parameter, type a number of minutes after the last client joined.
     For example, if the timeout is set to 15, the server waits indefinitely until the first client is accepted. After the first client joins, the 15 minute countdown starts. If no more clients join, the session starts 15 minutes later. If another client joins before the 15 minutes timeout, the timeout counter resets to 15 minutes and starts counting down again.

Setting the data transfer mode

You can set the data transfer mode to optimize the use of your network hardware setup. Used in conjunction with network bandwidth limits, you can optimize the way data files are transferred over your network.

Table 3-1 lists the transfer options.

Table 3-1 Transfer options

Mode	Description	Use if
Unicast	Each packet is addressed to one computer. One stream of data is sent for each client.	You are transferring a data packet to one or two computers only.
Directed broadcast	Data sent to all computers on a specified subnet. If clients are on more than one subnet, one stream is sent to each subnet.	Your network hardware does not support Multicasting.
Multicast	Data sent to all computers on the network that have requested the data. Only one stream of data is sent.	Unicast or subnet targeted broadcasting are not appropriate.

Multicasting is usually the most efficient option for the following reasons:

- Only one stream of data is sent out for all clients.
- Multicasting sends packets only to client computers that have requested data from the GhostCast Server.

This requires the support of appropriately configured routers and switches. You can alter settings globally or for a GhostCast session.

Symantec Ghost attempts to use Multicasting by default. If you have set the data transfer mode to Unicast or Directed broadcast, then Symantec Ghost uses that method. If Directed broadcast or Multicasting fails, then Symantec Ghost attempts to use Unicast.

For more information on optimizing data transfer over a network and setting Symantec Ghost Console options, see the *Symantec Ghost Implementation Guide*.

To set the data transfer mode

1. In the Symantec GhostCast Server window, on the File menu, click **Options**.
2. Click **Force Mode**.
3. Select one of the following:
   - Multicast
   - Directed Broadcast
   - Unicast
4. Click **OK**.

Controlling the amount of network bandwidth used

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

You can enter a value for restoring an image, creating an image, or both. The values are saved and loaded the next time that you run the GhostCast Server. However, if you run a GhostCast session from the command line, the limits that are set on the command line are used for that session only.

See "GhostCast Server command-line options" on page 62.

Limiting network bandwidth is useful in some circumstances. Consider the following:

- By limiting network bandwidth, you can increase performance on the network for users who are not the intended recipients of image files.
- If your network hardware does not support multicasting, then limiting bandwidth is helpful in many situations.

Table 3-2 provides a guide to network hardware setups and when you may or may not want to limit network bandwidth.

Table 3-2 Limiting network bandwidth

Limit network bandwidth for	Hub only	Layer 2 switch	Layer 3 switch or multicasting compatible router and layer 2 switch
Unicast	Yes	No	No
Subnet targeted broadcast	Yes	Yes	Yes
Multicast	Yes	Yes	No

In situations where you would not limit network bandwidth, the hardware directs the traffic to intended recipients only, and all other users should be unaffected.

To set a limit for network bandwidth

1. In the Symantec GhostCast Server window, on the File menu, click **Options**.
2. In the Options dialog box, check **Limit data throughput for**.
   If this option is not enabled, then no limit is set.

3 In the Restoring box, type the maximum MB per minute to set a limit for restoring an image.

4 In the Creating box, type the maximum MB per minute to set a limit for creating an image.
The ideal maximum usage to expect is:

100 BaseT	300 MB per minute
10 BaseT	60 MB per minute

Viewing and changing GhostCast Server session options

In the Options dialog box you can specify session parameters.

You can specify a range of multicast addresses. Addresses in the following range are valid: 224.0.2.0-239.255.255.255. To specify an exact address set the end address to the same as the start address. By setting a wide range of addresses you can limit the chance of conflict if you run two or more GhostCast operations simultaneously. This option should be used by advanced users only.

To view or record GhostCast Server options

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

2 If you want to use a specified multicast address range, click **Use Specified Multicast Address Range**, then type the multicast From and To addresses.

3 Click **Multicast Scope TTL** to set the time to live.
This limits how far the data passes through a network. Time to live is decremented by every router through which the data packet passes.

4 Select one of the following:

Restart On Completion	Restart the GhostCast Server, accepting clients and using the same Auto Start parameters.
Close GhostCast Server On Completion	Close Symantec GhostCast Server once the session is complete.

5 Click **Log clients** to create a log that lists GhostCasting session details, including when a session took place, the computers involved, and whether the session was successful.
The log is saved to the path specified.

6 In the Log Level box, select a log level to set a level of diagnostic GhostCast logging.
See "Generating a GhostCast log file" on page 255.

7 In the Log File box, type a destination log file location.

Running Ghost.exe on a client computer

When using GhostCasting, the client executable, Ghost.exe, restores a GhostCast copy of an image file onto the client computer or creates an image file onto the GhostCast Server.

Ghost.exe runs under DOS and uses a packet driver interface to the network card. The TCP/IP settings are stored in a configuration file Wattcp.cfg that is located in the same directory as Ghost.exe.

As with all Symantec Ghost applications, DHCP, BOOTP, and manually set IP addresses are supported.

See "Transfer methods and hardware setup" on page 209.

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

See "Command-line switches" on page 147.

For a GhostCasting session, the selection of the partition or drive to write to, or read from, on the client is specified either on the client, or in the command-line option on the server. Use the -ja switch on the client to run the operation from the server.

See "Creating a backup image file" on page 24.

For any GhostCasting session, the session name on the entry screen of the client should match the GhostCast Server session name.

Chapter 4

GhostCasting from the command line

This chapter includes the following topics:

Running GhostCast Server from the command line

You can run the Symantec GhostCast Server from the command line by including switches with ghostsrv.

You can run GhostCast Server from the command line. Use a batch file or third-party scheduler application to start the server.

The syntax for running GhostCast Server is as follows:

ghostsrv filename session [options]

Where:

filename	Specifies the path and file name of a disk image file.
session	Specifies the session name.

See "GhostCast Server command-line options" on page 62.

Starting the GhostCast session

Once you have created a GhostCast session and the client computers have appeared on-screen, you can start the transmission.

To start the session transmission

- When all clients have connected, click **Start**.

GhostCast Server command-line options

Table 4-1 lists the GhostCast Server command-line switches.

Table 4-1 GhostCast Server switches

Switch	Description
-Ncount	Starts the GhostCast transmission after count clients have joined the session.
-Ttime	Starts sending to a session automatically after a specified time (24-hour hh:mm format), with a maximum of 24 hours.
-Ominutes	Starts transmission minutes after the last client connection.
-Llevel	Creates a log file specifying log level E, S, W, I, or A.
-Ffilename	Specifies log file name for the -L option and is by default, Ghostlog.txt.
-C	Closes ghostsrv application after GhostCast session completion.
-D	Uses create from client mode, restore to client is the default.
-R	Restarts the GhostCast session on completion, waits for client connections again after GhostCasting is complete.
-P	Specifies partition mode operation. If restoring to clients, the partition number must be given, if creating an image from client, no partition number is required.
-Mxxx.xxx.xxx.xxx	Sets the multicast address to xxx.xxx.xxx.xxx, addresses between 224.0.2.0–239.255.255.255 are valid.
-Mxxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx	Specifies a range of multicast addresses, the address is chosen from within this range. Addresses between 224.0.2.0–239.255.255.255 are valid.
-DISKnumber	Specifies the client disk number to which to restore or create the image file.

Table 4-1 GhostCast Server switches

Switch	Description
-PARTnumber	Specifies the client partition number to which to restore or create the image file.
-Gswitch	Specifies switches to include in the command line and those used by the Ghost application.
-HLxxx	Sets the maximum amount of bandwidth consumed while restoring an image, where xxx is the number of megabytes per minute.
-HDxxx	Sets the maximum amount of bandwidth consumed while creating an image, where xxx is the number of megabytes per minute.
-TTLxxx	Sets the multicasting time to live.

Command-line option examples using GhostCast Server

Following are examples for using GhostCast Server.

Table 4-2 GhostCast Server command-line examples

Summary	Syntax	Description
Creating an image file of a complete disk from a client computer and saving to image file c:\test123.gho using the session name labmodel	ghostsrv c:\test123.gho labmodel -d	Starts a GhostCast session called labmodel and creates or overwrites the image file c:\test123.gho. The first connecting client's IP address appears on-screen, and the session starts automatically. The client computer indicates the source drive to use for the image file creation.
Creating an image file of a partition from a client computer to an image file	ghostsrv c:\test123.gho TestSession -d -p	Starts a GhostCast session called TestSession and creates or overwrites the image file c:\test123.gho. The first connecting client's IP address appears on-screen, and the session starts automatically. The client computer indicates the source drive and partitions to include in the image created.
Restoring a disk image file onto client computers	ghostsrv.exe c:\test123.gho TestSession	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. Start the session transmission. See "Starting the GhostCast session" on page 62.

Table 4-2 GhostCast Server command-line examples

Summary	Syntax	Description
Restoring a specific partition from an image file onto client computers	ghostsrv c:\test123.gho TestSession -p2	Starts a GhostCast session called TestSession, and uses the second partition in the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen.
GhostCasting a specific partition from an image file to a specific partition on a destination drive	ghostsrv c:\test123.gho TestSession -p1 -DISK1 -PART2	Starts a GhostCast session called TestSession, uses the first partition in the image file c:\test123.gho, and places it in the second partition of the clients' first disk. The connecting clients' IP addresses appear on-screen. Start the GhostCast transmission. See "Starting the GhostCast session" on page 62.
Specifying the number of clients to Auto Start	ghostsrv c:\test123.gho TestSession -n10	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. Once ten clients have connected, the session transmission starts automatically.
Specifying a time for Auto Start	ghostsrv c:\test123.gho TestSession -t13:30	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. At half past one in the afternoon (1:30 PM), the session transmission starts automatically.
Specifying time-based and client-count Auto Start and automatic closing	ghostsrv c:\test123.gho TestSession -t13:30 -n10 -c	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. At either half past one in the afternoon (1:30 PM), or after 10 clients join the session, transmission starts automatically. Ghostsrv does not wait for both conditions to be met. When the GhostCast session is completed, ghostsrv closes down as requested.
Isolating problems	ghostsrv c:\test123.gho TestSession -la -ferrlog.txt -n10	Starts a GhostCast session called TestSession and uses the image file c:\test123.gho. The connecting clients' IP addresses appear on-screen. Once 10 clients connect, the session transmission starts automatically and a log file, Errlog.txt, is created for debugging. Creating a log file reduces the performance of the GhostCast transmission.

Chapter 5

GhostCasting and IP addresses

This chapter includes the following topics:

About IP addresses for GhostCasting

An IP network using locally specified addresses requires each manually setup computer to have:

- A unique IP address
- The correct subnet mask
- The default gateway (optional)

Specify the TCP/IP configuration parameters using one of the following methods:

- Locally on a computer in a configuration file
- Automatically using a BOOTP or DHCP server

Locally specified IP addresses

The GhostCast Server receives its locally specified IP addresses, subnet masks, and default gateways from the TCP/IP parameters in the Network option of the Windows Control Panel.

Examples of Wattcp.cfg client configuration files

The following example displays the IP details on a computer and the details in the Wattcp.cfg file.

IP details:

- IP address: 192.168.100.3
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.100.1

Wattcp.cfg:

- IP = 192.168.100.3
- Netmask = 255.255.255.0
- Gateway = 192.168.100.1

If the server and client are within the same subnet, a default gateway is not required. If they are on a separate subnet then a default gateway must be supplied.

Using BOOTP/DHCP to assign IP addresses

If a BOOTP or DHCP server is installed on the network, you may take advantage of DHCP or BOOTP for IP address assignment. A DHCP server is included in Windows NT Server release 4.0 and Windows 2000. Other DHCP and BOOTP applications are available for various operating systems and can be used with GhostCasting.

If you are GhostCasting to many clients, not having to edit a unique Wattcp.cfg file on every client may be advantageous. Balanced against this is the additional complexity of the DHCP setup.

BOOTP/DHCP automatically defined IP address

Specifying a local configuration for every computer on an IP network can be inconvenient or impractical. GhostCasting supports BOOTP and DHCP servers.

You must run the BOOTP or DHCP server to specify a computer's IP address. The BOOTP/DHCP server listens on the network for computers requesting an IP address, and replies with the address that the BOOTP/DHCP server is configured to provide. The BOOTP/DHCP server must be configured to provide the IP address, subnet mask, and (optionally) the default gateway.

Section 3

Creating executables to roll out applications

Chapter 6

Getting started with AutoInstall

This chapter includes the following topics:

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.

Hardware and software restrictions

AutoInstall is designed to install packages to computers with the same hardware and same operating system as the model computer.

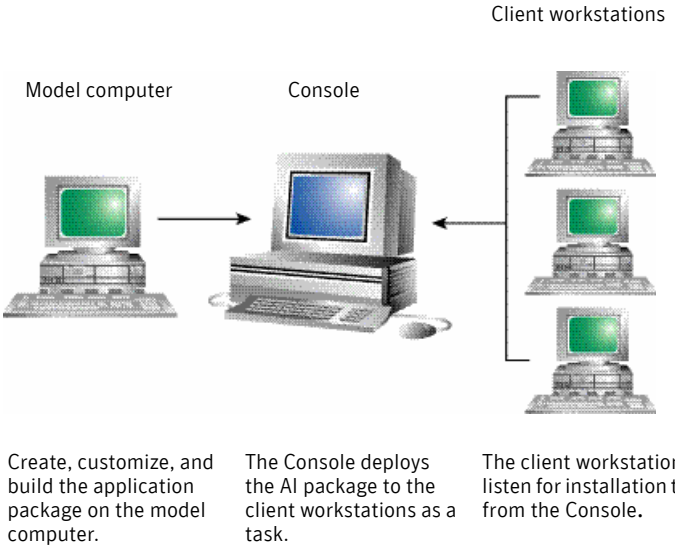
Using AutoInstall

Ensure that AI Builder is installed on the Console server (AI Builder is included in the Console installation) then perform the following procedures:

- Install AI Builder and AI Snapshot on the model computer.
- Scan to capture existing system information.
- Install the software that you would like to deploy.
- Scan a second time to capture system information again to determine changes.
  AI Builder automatically builds and saves the file created by AI Snapshot as an executable AI package. You can use AI Builder to customize the installation script, prior to building, or after building the executable, if necessary.

- Use the Symantec Ghost Console to deploy the AI package to target workstations.

See "Creating AI packages" on page 77.



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 the same operating system and service packs to those that will receive the finished AI package. Ideally, this computer should have only the operating system installed and have network support to connect to the Console.

If Microsoft Installer is not installed on the computer then you are asked if you want to install it. If you want to include the installation of Microsoft Installer in the AI package then do not install it now.

To install AI Snapshot and AI Builder on the model computer

1. Insert the Symantec Ghost CD into the CD-ROM drive.
2. In the Symantec Ghost installation window, click **Install Tools**.
3. Click **Install AI Snapshot**.
4. Click **Next**.

5 Do one of the following:
   - Click **Yes** to install Microsoft Installer 2.0 on the computer.
   - Click **No** to prevent Microsoft Installer being installed on the computer.

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

7 Do one of the following:
   - Confirm the installation location.
   - To select a different location for the installed files, click **Change**.

8 Click **Next**.

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

10 Click **Install**.

Setting up target computers

The AutoInstall client program is installed as part of the Symantec Ghost client software.

For more information on installing the Console client, see the *Symantec Ghost Implementation Guide*.

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

Installing Microsoft products using AutoInstall

There are some issues you may need to consider when using AutoInstall to install Microsoft software.

Installing Microsoft service packs

Symantec does not recommend using AutoInstall to install Microsoft service packs.To install service packs use the Transfer Files and Execute Commands tasks from the Console.

For more information, see the *Symantec Ghost Implementation Guide*.

Letting the model computer restart

If you use AI Snapshot to create an installation script to include in an AI package executable, you must capture system information and build the executable AI package before restarting the computer.

If you are installing non-Microsoft software, then you can allow restarts and configure the application before performing the comparison scans and building the AI package.

Adding uninstall commands

You can add an AutoInstall uninstall command to an AI package if you are deploying non-Microsoft software. This feature does not work with Microsoft products because you must build the AI package before any restarts.

Using AutoInstall to install Office XP

Due to the new Product Activation feature in Microsoft Office XP, you must stop Office XP from locking to the model computer before cloning. By using Microsoft Office Installer commands, you can prevent the hardware detection and activation process from occurring until Office XP is deployed to the client computers and launched for the first time.

Note: You must have a Volume License Key from Microsoft to perform this installation.

To install Office XP using AutoInstall

1. Download the Microsoft patch for enterprise deployments specified in Microsoft Knowledge Base article number Q304226 at:
   http://support.microsoft.com/support/kb/articles/Q304/2/26.ASP
2. Install AI Snapshot.
3. Start AI Snapshot and perform the first system scan.
4. Run Office XP setup using the following command line:
   driveletter:\Setup.exe enterprise_image="1" nousername="1" pidkey="[Enter your Volume License Key here]"/qb+
   Type the Volume License Key without any hyphens.
5. Apply the Microsoft patch for enterprise deployments specified in the Microsoft Knowledge Base article number Q304226.
6. Perform a system compare and build the package.
   Do not let the computer restart after installing Microsoft Office XP and the patch.

How to replicate Office XP

Office XP can be built into a single package on Windows Me/2000/XP. However, a multi-package deployment is required when distributing Office XP to Windows 98 and NT4.

Before using one of these solutions you must have the following:

- The Microsoft patch for enterprise deployments specified in the Microsoft Knowledge Base article number Q304226
  You can find the article at:
  http://support.microsoft.com/support/kb/articles/Q304/2/26.ASP
- A Volume License Key from Microsoft

Replicate Office XP

Because scans and builds must occur before restarts you must create two packages for deployment of Office XP on Windows 98 and Windows NT 4. These packages must be deployed separately and in order. The first package contains Microsoft Installer Update and Internet Explorer. The second package contains Office XP. Because the first package contains Internet Explorer a system administrator must log on manually to each client to complete the installation before deploying the second package.

To replicate Office XP on Windows 98 and NT4

1. Perform the first scan.
2. Start \Office XP\Setup.exe to install new version of MSI. Cancel the Office XP installation.
3. Run System Files Update from:
   \Office XP_path\FILES\OSP\[LCIDnumber]\OSP.MSI, where LCIDnumber represents the language ID number of your Office XP Suite. For example, 1033 for English.
4. Perform a compare scan and build a system update package before the restart. Do not let the machine restart before performing the scan and building the package.
5. Restart the computer.
6. Perform the first scan again.
7. Launch Office XP installation via the following command line:
   "Office XP_path\Setup.exe" ENTERPRISE_IMAGE="1" NOUSERNAME="1" PIDKEY="{Product_ID_KEY}"
   See Table 6-1, “Command line parameters,” on page 75.

8 After the MS Office XP installation finishes, apply the Microsoft patch.

9 Perform a compare scan and build an Office XP package before allowing the system to restart.

10 Move both created packages and deploy them to their respective operating systems in order and as separate tasks.

Note: The first package contains Internet Explorer and therefore a system administrator will have to log on manually to each client to complete the installation before deploying the second package.

To replicate Office XP on Windows 2000/Me/XP

1 Perform the first scan.

2 Launch Office XP installation via the following command line:
"Office XP_path\Setup.exe" ENTERPRISE_IMAGE="1" NOUSERNAME="1" PIDKEY="{Product_ID_KEY}"
See Table 6-1, “Command line parameters,” on page 75.

3 After the MS Office XP installation finishes, apply the Microsoft patch.

4 Perform a compare scan and build an Office XP package before allowing the computer to restart.

5 Build an Office XP package.

Table 6-1 details the parameters used in the Office XP installation from the command line.

Table 6-1 Command line parameters

Parameter	Description
Setup.exe	The setup file for MSI. If MSI is already installed, Office XP MSI script file (PROPLUS.MSI) can be called instead.
ENTERPRISE_IMAGE [boolean] - 1	Prevents Setup.exe from creating a digital license identification based on the hardware components of the computer used to create the original hard disk image. This setting lets Setup generate a unique digital license identification on each user computer when any Office application is started on the new computer.
NOUSERNAME [boolean] - 1:	If this parameter is set to 1, then Office prompts for the user name the first time the user runs any Office application. By default the property is not set (property is clear).

Table 6-1 Command line parameters

Parameter	Description
PIDKEY [string] - ["xxxxxxxxxxxxxxxxxxxxxxxxx"]:	Allows an administrator to submit a Product ID number on the command line. Do not include dashes when entering Product ID number.

Chapter 7

Creating AI packages

This chapter includes the following topics:

Creating an installation script for a software installation

Creating the installation script 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 installation script file that contains the differences.

The default name for the installation script is Install.aic.

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 only have the operating system installed.

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 drive C, 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.

To take a snapshot of the model system

1. Disable any programs that are running in the background.
2. If the installation process includes restarting the computer, disable any programs that execute during the restarting process.
3. On the Windows taskbar, click **Start** > **Programs > Symantec Ghost > AI Snapshot**.
4. Click **Options**.
5. Change the Search Path or Temporary Work Directory, if desired.
6. Click **OK**.
7. Click **Next**.
   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 (the first scan), 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 package is built.

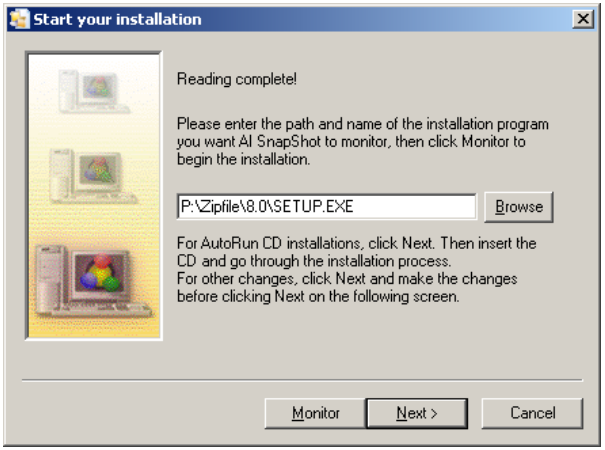
Install the software to be packaged

You can install the software from the network, or from a CD. If you are installing the software from an autorun CD, the initial installation steps are automatically performed.

To monitor the software installation from the network

1. In 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**, then navigate to the file.



2 Click **Monitor**.

3 During the installation, select the options in the application being installed 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 any restart by clicking **No** or pressing **Ctrl-Esc** to continue creating the AI package.
- For all other installations, restart the computer if the installation requires it.

5 Type a name for the installation package when the software installation is complete. The default name is INSTALL.

To monitor the software installation from an autorun CD

1 In the Start Your Installation screen, click **Next**.

2 Insert the autorun CD into the CD-ROM drive.

3 Follow the installation instructions for the software package.

4 Type a name for the installation package when the software installation is complete. The default name is INSTALL.

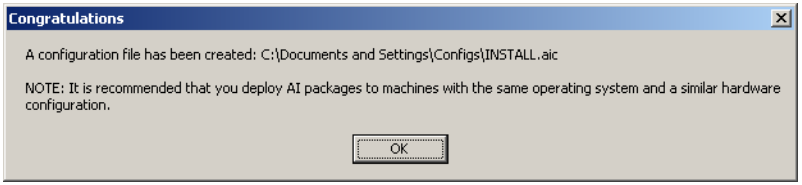
Capturing system information again to determine changes

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

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.

To take another snapshot of the model computer

1. In the Is Software Installation Complete window, click **Compare** for AI Snapshot to check the new configuration against the original configuration.
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 or add an uninstall command.
     See "Customizing and building AI packages" on page 81.
     Once the installation script has been modified, the package should be built before any further changes are made to the model computer. This prevents the changes from being included in the package.
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 is created, you can use AI Builder to modify and rebuild the package.

Note: AI Builder does not build the package if it will exceed 2 GB.

The installation script is an ASCII text file that is 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. 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 on the client.

Note: If the customized installation requires user interaction 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.

See "To include an uninstall command in a build package" on page 86.

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 line number in the .aic 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 is

generated, you can use the Run option on the Build menu to test the installations that you create.

An example of variables and commands in AutoInstall

Using the commands and variables in an AutoInstall script lets you ask for and receive user input, run commands, and customize AutoInstall. The following example script gives the user a choice of options, and then installs a file.

A sample script follows.

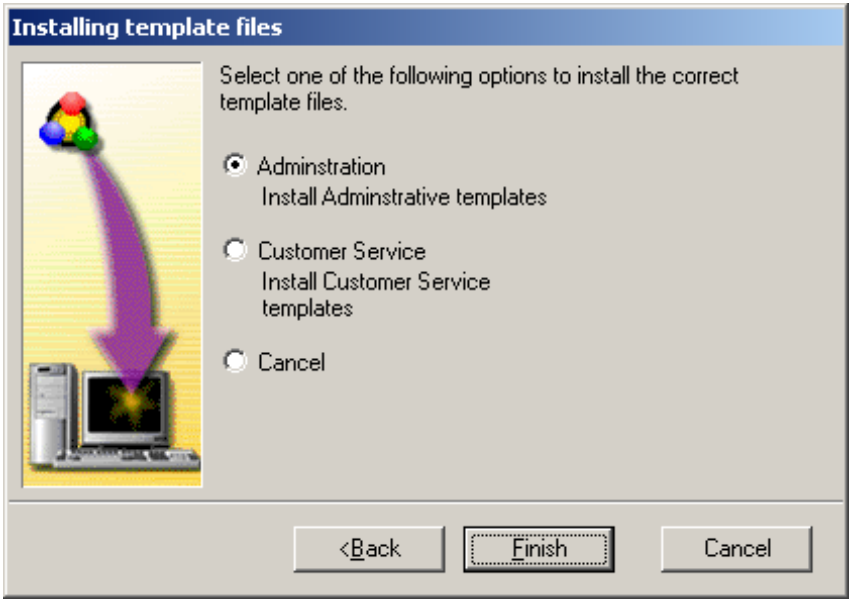
```
UNINSTALL: yes, packagename="Distribute Files Package"

BEGINFIRSTSCREEN title="Installing template files"

This program lets you install template files to your hard drive.

ENDFIRSTSCREEN

BEGINGROUP EXCLUSIVE, caption="Installing template files"

Select one of the following options to install the correct template
files.

01 [x] Administration

Install Administrative templates

02 [ ] Customer Service

Install Customer Service templates

03 [ ] Cancel

ENDGROUP

POPMESSAGE 0, fontsize=23

Installing administration templates

EndPop

POPMESSAGE 01

Installing customer service templates

EndPop

IF GROUP = 01

FILE: "Admin.000", overwrite=ask, popid=00, From="C:\Documents and
Settings\Administrator\Admin.dot"

SHORTCUT: "$ALLUSERSDIR$", "Administration"

ENDIF

IF GROUP = 02

FILE: "CUST_S~1.000", overwrite=ask, popid=01, From="C:\Documents
and Settings\Administrator\Cust_service.dot"

SHORTCUT: "$ALLUSERSDIR$", "Customer Service"

ENDIF

IF GROUP = 01
```

```
BEGINLASTSCREEN title="Files Install", caption="Files Install"
The file has been successfully installed onto your computer.
ENDLASTSCREEN
ENDIF
IF GROUP = 02
BEGINLASTSCREEN title="Files Install", caption="Files Install"
The file has been successfully installed on your computer.
ENDLASTSCREEN
ENDIF
```

This example provides three choices for the user:

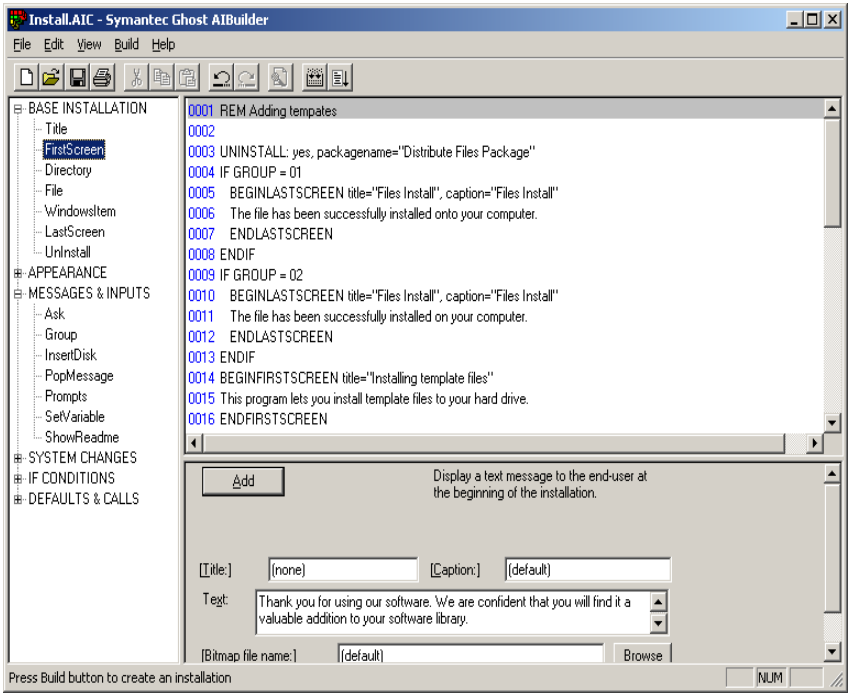
- To install templates for administration personnel
- To install templates for customer service personnel
- To cancel without installing any files

An AI package is created using AI Builder commands and variables. The package is distributed to users and is executed on client computers. The user can then run the AI package and install files as required.



Customizing installation scripts

Installation scripts can be modified as they are created. They can also be modified after the AI package is built by opening the package in AI Builder.



The customizing options appear in the left pane, and details of the selected option appear in the bottom right pane. The installation script is in the top right pane.

Table 7-1 outlines the command types that are available in AI Builder.

Table 7-1 AI Builder command types

Command type	Description
Base Installation	Defines how the installation begins. For example, select WindowsItem to add, remove, or replace items within a program group.
Appearance	Defines how the installation appears to the user. For example, select IntroScreen to display a graphic when the installation begins.
Messages & Input	Adds messages that require user input. For example, select Prompts to change the messages that display during the installation.
System Changes	Makes changes to Windows during the installation. For example, select Registry to insert or delete items in the Windows registry.
If Conditions	Lets you include If statements for unattended installations. For example, select IfMemory() to check a memory value during the installation.
Defaults & Calls	Set up defaults and include calls to external programs. For example, select RunAtExit to run an external program at the end of the installation.

See "AI Builder variables, commands and conditions" on page 173.

To customize an installation script

1 Do one of the following:

- In AI Snapshot, click **Modify** if you have just created an installation script.
- In AI Builder, select the AI package that you want to modify.

2 In the AI Builder window, in the left pane, 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.

3 Select a command.

4 In the AI Builder window, in the right pane, type 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 complete.

7 Build the AI package.
See "Building AI packages" on page 86.

Adding an uninstall command to the installation script

The uninstall program is placed in the default directory and a hidden file, Uninstall.aic, is created that captures the changes made during the installation. Successive installations modify the Uninstall.aic 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, select BASE INSTALLATION, then click **UnInstall** to include an uninstall package.

2 Check **Remove Groups During Uninstall** to remove any program groups that were created during the installation.
Use this option cautiously as some users might select an existing group for the installation, or add files to the group after installation.

3 Type the name for the uninstall in the space provided.
This name appears on-screen when the uninstall runs.

4 Click **Add** to record the options that you have chosen.

Building AI packages

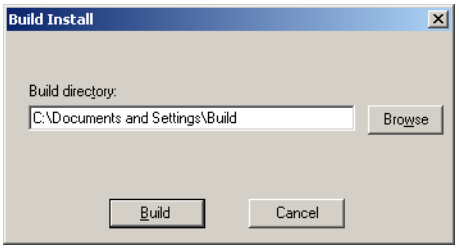
When you have made all of the changes to your installation script that you require, you can build the AI package.

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 is created if the model computer is the same as it was when the installation script was created.

Modify installation scripts and AI packages

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.aic).
The default location is:
C:\Documents and Settings*Current user*\Application Data\Symantec\Ghost\Working\Configs\

4 Double-click the file to open it.
You can then customize the file as required.

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:\Documents and Settings*Current user*\Application Data\Symantec\Ghost\Working\
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 on setting Deploy AI Package properties, see the *Symantec Ghost Implementation Guide*.

When the distribution server tells the target workstation that an AI package is available for installation, the Symantec Ghost client runs the executable.

Section 4

Updating Security Identifiers (SIDs) and computer names

Chapter 8

Updating Security Identifiers (SIDs) and computer names

This chapter includes the following topics:

Making SID changes with Sysprep and Ghost Walker on NT-based clients

Client computers must be uniquely identified to operate on a network. This is achieved using the Security Identifier (SID) and the computer name. When you restore an image onto a number of client computers, you must assign unique identifiers as part of the task. There are a number of tools available to do this. Symantec Ghost supports two of them: the Microsoft application Sysprep, and the Symantec utility Ghost Walker.

Symantec Ghost Walker capabilities

Ghost Walker has the following capabilities:

- Runs in native DOS, allowing the SID to be changed without an additional restart following a clone operation.
- Alters the computer SID to a unique and randomly generated value.
- Alters the SIDs of all local workstation users present on the operating system installation.
- Alters all local workstation user SIDs in Access Control Lists (ACLs) for file and registry objects so that local users retain user profiles and access rights.
- Alters computer names for Windows 95, 98, Me, NT, XP, and 2000 operating systems. This does not change the computer name within the Symantec Ghost Console.

Symantec Ghost Walker limitations

Ghost Walker has the following limitations:

- Computer name change functionality is limited. A new name must contain the same number of characters as the original.
- It is not officially endorsed by Microsoft.

Microsoft Sysprep capabilities

Microsoft Sysprep has the following capabilities:

- Invokes the Windows 2000 Setup Wizard (normally only seen during installation) so that users can enter new user, license, and identification details.
- Can be configured to trigger a driver database rebuild, letting Windows 2000/XP use plug and play to detect all device drivers required for the new hardware environment and to discard any unused drivers. Use of this option is not supported by Symantec Ghost.
- Allows alternate mass storage controller drivers to be installed during the initial post clone boot. The newly cloned operating system can then start in the new hardware environment to the point when plug-and-play detection can be safely invoked.

- Supports almost all of the unattended installation parameters set, including computer name, domain, network settings, and more. This provides a comprehensive set of tools for reconfiguring the newly cloned computer and also allows a fully automated process to be conducted.
- Optionally alters the identity of the operating system installation by changing the SID.

Microsoft Sysprep limitations

Microsoft Sysprep has the following limitations:

- Does not change the SID of a local workstation user and therefore does not have to alter SIDs located in file or registry Access Control Lists (ACLs).
- Requires an additional restart.
- 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.

SID changing limitations

SID changing is an approximate technology, as you can only change SIDs in known locations.

Problems arise because of the following factors:

- A growing number of third-party and Microsoft applications are taking their own private or derived copies of the computer name and SID and storing them in proprietary formats in registry and file locations making them inaccessible to SID changes.
- Microsoft technologies such as Windows 2000/XP NTFS File Encryption, Windows NT, and Windows 2000/XP Protected Storage make use of SIDs as unique tokens. They use local workstation user SIDs as part of the encryption key that controls access to encrypted information. If the SID is changed it renders encrypted data unreadable.

Warning: For these reasons, you are strongly advised to test computer environments and the applications on them before mass rollouts or upgrades.

Losing access to external data objects

Changing the SID of a workstation or a clone of a workstation that has been in use for some time may be more problematic than changing the SID of a newly installed workstation or a clone of a newly installed workstation. When a workstation user, as opposed to a domain user, creates data objects on computers that are participating in a workgroup or a peer-to-peer environment, security information is created for those data objects that are based on the user's SID (which is based on the workstation SID).

When Ghost Walker updates the SID, it not only changes the computer SID, but also all of the workstation user and group SIDs. This is done because user and group SIDs are assumed to be based on the workstation's computer SID (which is now updated). This may mean that the security information on external computers no longer matches the new SIDs of the workstation users, which may result in a loss of access to those data objects.

Identifying user names and passwords across workstations

If there are two workstations in a domain that have two users with the same user name and password, the domain gives each of them access to the other’s resources even if their SIDs are different. This is a fairly common situation following cloning.

Updating the SID on a workstation does not stop this situation from occurring. You must change the password of one of the users.

Using Ghost Walker

Ghost Walker lets you alter identification details of Windows 95, Windows 98, Windows Me, Windows NT, and Windows 2000/XP computers following a clone operation. Each Windows 95, 98, or Me computer can be assigned a unique name. Each Windows NT or 2000/XP computer can be assigned a unique computer name and a computer 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 GUI 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

The Ghost Walker window lists all bootable Windows 95, 98, Me, NT, XP, and 2000 systems on the computer. Ghost Walker determines that there is an installed operating system if a full set of registry hive files and the operating system kernel executable are located in their normal locations.

Ghost Walker lists the following operating system details:

- Logical ID (system ID generated by Ghost Walker)
- Drive number
- Partition number
- Volume label (partition name)
- Partition file system type
- Computer name
- Operating system type, version, or build

To alter identification details for a client computer using Ghost Walker

1. Remove any Windows NT/2000/XP workstations that are members of a server domain.
   You must add the workstation to the Domain using the new SID and computer name once you have completed the update.
2. Run DOS.
3. In the command line, type **Ghstwalk.exe**.
4. Press **Enter**.
   Ghost Walker lists all interpretable volumes on the computer.
   - If there is one operating system on the computer, details of this operating system appear in the top pane and all volumes appear in the bottom pane.
   - If there is more than one operating system on the computer, details of all existing operating systems appear in the top pane.
5. If there is more than one operating system on the computer, in the Select a System ID box, type an ID to select an operating system and select **V - Change Additional Vols** to add or remove non-bootable volumes to be updated.

Warning: You must include any additional non-bootable volumes that may have security information or shortcuts containing the computer name of the bootable operating system embedded in them. Failure to do so results in mismatched data and a loss of security access.

---

6 To change the computer name, type **N**, then press **Enter**.
The new name must be the same length as the previous name. The box 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 Windows NT and 2000 computers, a new SID.
The computer name and SID updates occur in the following locations:
- The registry of the selected operating system
- The file system on which the operating system resides
- Any additional volumes selected for the update

8 If you removed a Windows 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|/?]
```

Table 8-1 describes the command-line options.

Table 8-1 Command-line options

Switch	Description
/CN=	Specifies a new computer name.
<new_computer_ name>	The new name must be the same length as the original name and cannot contain any of the following characters: /\[]”:;|<>+=,?* To include spaces in the computer name, enclose the computer name in quotes. For example, /CN="EW PC 123"

Table 8-1 Command-line options

Switch	Description
/CN= "<random_computer_name_format>"	Replaces the original computer name with a randomly generated name using the <random_computer_name_format> template. The <random_computer_name_format> template specifies which sections of the new name are randomly generated and the type of random value to place in that location. Only one instance of the following keywords is permitted in a template: <RANDOM_NUMERIC> - Generate random numbers <RANDOM_ALPHA>- Generate random letters <RANDOM_HEX> - Generate random hex digits (0-9, A-F) **Examples:** /CN="PC<RANDOM_NUMERIC>" replaces the computer name with a name that starts with PC, followed by a series of random digits between 0 and 9. /CN="ID<RANDOM_ALPHA>X" replaces the computer name with a name that starts with ID, followed by a series of random letters, ending with the character X. /CN="<RANDOM_ALPHA>" replaces the computer name with a name that is randomly generated using letters. The random output fills out the format string to produce a new computer name of the same length as the original name. Ensure that the format string allows enough room to embed at least one random character without exceeding the length of the original name.
/BV=<drv:part>	Specifies the drive number and partition number of the bootable operating system installation to update. If there is more than one operating system, then this switch must be included in the command.
/AV=<drv:part>	Specifies the drive number and partition number of an additional volume containing a file system to update. ■ More than one volume may be specified by repeating the argument for each additional volume. ■ This switch cannot be combined with /AV=ALL.
/AV=ALL	Specifies that all other volumes are to be included as additional volumes. /AV=ALL cannot be combined with the /AV=<drv>:<part> switch.
/SURE	Specifies that the update should start without user confirmation.

Table 8-1 Command-line options

Switch	Description
/BATCH	Specifies that the update should start without user confirmation and operation during error situations requires no user input.
/DIAG	Specifies that the utility can only generate diagnostic dumps and log files (not update the computer name or SID).
/IGNORE _DOMAIN	Specifies that Ghost Walker should not check Windows NT or 2000 installations for domain membership.
/REBOOT	Restarts the computer after a successful update.
/REPORT [=<filespec>]	Generates a report containing details of the update to \UPDATE.RPT. An alternate report file can be specified.
/LOGGING	Specifies that diagnostic logging is generated to the Gwalklog.txt file. Recommended for Technical Support use only.
/SAFE_ LOGGING	Ensures that all diagnostic logging gets flushed to disk by closing and reopening the Gwalklog.txt file after every log statement. This results in very slow execution. Recommended for Technical Support use only.
/#E=<license file>	Specifies a Ghost license file to activate Ghost Walker.
/H|/HELP|/?	Shows command-line syntax Help.
/SID= <replacement SID>	Specifies a replacement SID to be used instead of a randomly generated one. The replacement SID must be in the format S-1-5-21-xxx-xxx-xxx and have the same number of characters as the original SID.
/IGNORE_ ENCRYPTFILES	Disables the warning generated by Ghost Walker when it encounters Windows 2000/XP NTFS encrypted files during its initial disk scan. Changing the SID of a Windows 2000 installation results in indecipherable NTFS encrypted files.
/MNUPD= <registry path>	Specifies a registry location that you want Ghost Walker to search for instances of the computer name to update them. This registry key and its subkeys are searched for matched instances of the computer name (of the same length). If any are found, they are updated to the new computer name. Multiple registry locations may be specified with multiple instances of this switch.

Table 8-1 Command-line options

Switch	Description
@<argumentfile>	Specifies a file containing command-line switches that Ghost Walker should open and read in addition to those specified in the command line. The argument file should only contain one argument on each line. Do not include “” in the file.
/FNI	Disables the direct IDE drive access method.
/FNS	Disables the direct SCSI drive access method.
/FNX	Disables the Extended Int0x13 drive access method.

Following is an example of command line use:

```
GHSTWALK /BV=1:2 /AV=1:1 /AV=2:1 /CN=”WS4-<RANDOM_HEX>-443”/SURE /
REBOOT
```

The above command line does the following:

- Updates the Windows 95, 98, Me, NT, XP, or 2000 installation located on the second partition of the first disk.
- Updates file systems on additional volumes on the first partition of the first and second disks.
- Changes the computer name to one starting with WS4- and ending with -443, placing random hexadecimal values in the remaining spaces until the new name is the same length as the old one. For example, WS4-53ADF76-443.
- Does not prompt the user for final confirmation.
- Reboots after the computer name is changed.

Chapter 9

Sysprep

This chapter includes the following topics:

Introducing Sysprep

Sysprep is a Microsoft utility that helps prepare Microsoft Windows 2000/XP computers for cloning, and customizes the configuration settings when a computer is cloned. It is available on the Microsoft Web site, or it may be on your Microsoft Windows installation CD.

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

If the source or target computers are running Microsoft Windows 2000 or Microsoft Windows XP Professional, then Sysprep uses a file called Sysprep.inf that you can edit to provide computer-specific information before and after completing a cloning task. Sysprep uses Sysprep.inf in three ways:

- As a source of information that is usually provided to the user through prompts.
- To alter configuration settings that are not provided for in the Sysprep user interface.
- To specify defaults that the Mini-Setup Wizard uses to configure the destination computers after receiving the image.

If the source or target computers are running Microsoft Windows XP Home, then Sysprep uses the Windows Welcome to request computer-specific information from user input.

Some data from Sysprep.inf is used to prepare the source computer for duplication and customization before creating the image. Some of the settings specified in Sysprep.inf are applied by Sysprep after you restore the image back onto the destination computers. Sysprep.inf is not included with the Sysprep download from Microsoft. You must create Sysprep.inf according to Microsoft guidelines or with the tools provided by Microsoft.

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

It is recommended that you read the documents listed in Table 9-1, even if you are familiar with Sysprep.

Table 9-1 Sysprep documentation

Get information on	From
How to deploy Microsoft Windows 2000 using Sysprep	The Microsoft Windows 2000 Professional CD: ■ Support\Tools\Depoly.cab\Deptool.chm ■ Support\Tools\Deploy.cab\Unattend.doc
How to deploy Microsoft Windows XP using Sysprep	The Microsoft Windows XP Professional CD: ■ Support\Tools\Deploy.cab\Deploy.chm ■ Support\Tools\Deploy.cab\Ref.chm

Note: Do not use Sysprep and a configuration task to set the same configuration settings in case of conflict between the settings. For example, do not instruct Sysprep to add a computer to a domain and set this in a configuration task.

Setting up Sysprep

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

Symantec Ghost supports Sysprep version 1.1 for Windows 2000 and Sysprep version 2.0 for Windows XP. The version that is included with Windows 2000 is Sysprep version 1.0 which has reduced functionality.

Adding a Sysprep configuration

Once you have copied the Sysprep files on to your computer, you can set up and configure a version from the Console. The configuration can be added from the Tools menu, or as you are creating an image create task.

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

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

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

Support\Tools\Deploy.cab

To add a Sysprep configuration

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

   If you do not install the Sysprep files, your Sysprep tasks fail to execute.
3. Type a name for the version of Sysprep that you are installing.
4. Click **Create**.
5. In the Browse For Folder window, browse for the Sysprep folder location, then select the **Sysprep** folder.
6. Click **OK**.
7. Sysprep.exe and Setupcl.exe must be present in the Sysprep folder for Sysprep to install the files.
   All files in the Sysprep folder and subfolders (except for the empty ones) are installed in the Console local data area. Before you create a Sysprep image,

all folders and files from that location are copied to the Console client computer.

Overwriting a Sysprep configuration

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

To overwrite a Sysprep configuration

1. On the Windows taskbar, click **Start** > **Programs** > **Symantec Ghost > Ghost Console**.
2. On the Tools menu, click **Sysprep Configurations**.
3. In the drop-down list, select a Sysprep configuration.
4. Click **Create**.
5. Click **OK** to overwrite the existing Sysprep configuration.
6. In the Browse For Folder window, browse for the new Sysprep folder location, then select the **Sysprep** folder.
7. Click **OK**.
8. Click **OK**.

Deleting a Sysprep configuration

If you delete a Sysprep configuration, all Sysprep files for that version are removed from the Console local data area.

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

To delete a Sysprep configuration

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

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

Sysprep and the Console client interact in two ways:

- Image create task
- Image restore task

Image create task

During a create image file task, Sysprep does the following:

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

Image restore task

During a restore task, Sysprep does the following:

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

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

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

- Sysprep uses either the Mini-Setup Wizard along with information specified in Sysprep.inf, or the Windows Welcome, to gather configuration parameters and then complete its post-cloning configuration.

  Note: If mandatory configuration settings are not defined in Sysprep.inf, the user is prompted for them in the Mini-Setup Wizard.
  See "Configuring Sysprep.inf" on page 107.

- If Sysprep has been enabled to change the SID, it changes it once the Console client computer has been configured.
  See "Making SID changes with Sysprep and Ghost Walker on NT-based clients" on page 91.
- 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.

Cloning with Sysprep

Include Sysprep in an image restore task by including an image file that was created in an image create task using Sysprep.

To create an image with Sysprep

1. On the Windows taskbar, click **Start** > **Programs** > **Symantec Ghost** > **Ghost Console**.
2. On the File menu, click **New** > **Image Create Task**.
3. Complete the Network and the General image create details.
   For more information on setting image create task properties, see the *Symantec Ghost Implementation Guide*.
4. On the Sysprep tab, click **Run Sysprep on this machine before creating the image**.
5. Select a Sysprep configuration.
   You can also add a Sysprep configuration now.
   See "Adding a Sysprep configuration" on page 103.
6. Click **Tell Sysprep to perform a SID change when restoring this image to a destination machine** for Sysprep to change the SID on the destination computer.
   If this option is selected, then do not use Ghost Walker to perform a SID change when restoring an image onto client computers.

See "Making SID changes with Sysprep and Ghost Walker on NT-based clients" on page 91.

7 Leave Run the MiniSetup wizard to process the sysprep.inf file selected for Sysprep to run the Mini-Setup Wizard when cloning Microsoft Windows XP Professional.
If this option is not selected, then the Windows Welcome appears instead of the Mini-Setup Wizard the next time the computer is started.

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

9 Click **Edit Sysprep** to make changes to the Sysprep.inf file for this task.
You can configure the file to let Sysprep set up the client computers without user interaction.
See "Editing, restoring, or reloading Sysprep.inf" on page 108.

Using Sysprep switches

If you are using other Sysprep switches, consult Sysprep documentation and ensure that they do not conflict with the Ghost operation. The following Sysprep switches are generated automatically by Symantec Ghost or are set in the Console:

```
-mini
-nosidgen
-quiet
-reboot
-reseal
```

Configuring Sysprep.inf

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

See "Overwriting a Sysprep configuration" on page 104.

You can configure Sysprep in many ways. To have Sysprep.inf apply the computer name, you must request that Sysprep randomly generates the computer name. If you do not, Sysprep supplies a default name to the MiniSetup

Wizard and the user is prompted to confirm it. To request a randomly generated computer name, use the following parameter:

[UserData]
ComputerName=*

See "Making SID changes with Sysprep and Ghost Walker on NT-based clients" on page 91.

Editing, restoring, or reloading Sysprep.inf

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

See "Configuring Sysprep.inf" on page 107.

To edit, restore, or reload Sysprep.inf

1. In the Properties for New Task window, on the Sysprep tab, click **Edit Sysprep**.
2. Edit the Sysprep.inf file.
   The file can be configured to let Sysprep set up the client computers without user interaction.
   See "Configuring Sysprep.inf" on page 107.
3. Select one of the following:

Option	Description
OK	Saves your changes.
Restore	Returns to the Sysprep.inf file that was used when the task was first created.
Reload	Replaces Sysprep.inf with the configuration template Sysprep.inf.

Section 5

Symantec Ghost utilities

Chapter 10

Managing partitions using GDisk

This chapter includes the following topics:

Introducing GDisk

GDisk is a utility that lets you create partitions, reinitialize master boot records, delete data, and wipe your disks in many different ways.

Two versions of GDisk are included with Symantec Ghost:

Version	Description
GDisk.exe	Runs in DOS
GDisk32.exe	Runs from the command line in a Windows operating system. Not all GDisk command-line switches can be run with GDisk32.

GDisk is a complete replacement for the Fdisk and Format utilities and offers the following features:

- On-the-fly formatting
- Extensive partition reporting
- High-security disk wiping
- The ability to hide a partition or make a hidden partition visible

Unlike Fdisk, which uses interactive menus and prompts, GDisk is command-line driven. This offers quicker configuration of a disk's partitions and the ability to define GDisk operations in a batch file.

Run GDisk

GDisk.exe must be run in DOS mode. GDisk32.exe can be run from within Windows.

To run GDisk.exe

1. Start your computer in DOS mode.
2. At the DOS prompt, type **progra~1\symantec \ghost\GDisk** followed by the required disk and switches.

To run GDisk32.exe

1. On the Windows taskbar, open a DOS window.
2. At the DOS prompt, type **progra~1\symantec \ghost\GDisk32** followed by the required disk and switches.

Overview of the main command-line switches

GDisk has ten 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:

Table 10-1 GDisk main commands

Mode	Switch	Explanation
Create	/cre	Creates primary DOS partitions and extended DOS partitions (DOS only).
Delete	/del	Deletes partitions of any type, including non-DOS partitions (DOS only).
Status (default)	/status	Lists information on the specified fixed disk and its partitions.
Activate	■ /act ■ /-act	Activates and deactivates a partition (specifying it as the bootable partition).
Hide	■ /hide ■ /-hide	Hides or unhides an existing partition.
Reinitialize MBR	/mbr	Reinitializes the Master Boot Record (DOS only).
Batch	/batch	Uses batch-mode command execution.
Disk wipe	/diskwipe	Wipes the contents of the whole disk (DOS only).
Boot.ini	/bootini	Makes a modification to the Windows NT/2000/XP boot menu (DOS only).
View	/view	Lets you view the overwrite pattern on a diskwipe.

Online Help for command-line switches

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

Version	Help switch
GDisk.exe	C:\progra~1\symantec\ghost\gdisk /?
GDisk32.exe	C:\progra~1\symantec\ghost\gdisk32 /?

Note: An additional switch not shown is the /VERSION switch. This switch shows the version information for the GDisk and GDisk32 executable.

More detailed Help is available by qualifying the Help command with the switch for one of the nine main modes of operation.

For example, to view the detailed Help file for Hide, type one of the following command lines:

Version	Command line
GDisk.exe	C:\progra~1\symantec\ghost\gdisk /hide /?
GDisk32.exe	C:\progra~1\symantec\ghost\gdisk32 /hide /?

Switches common to all GDisk commands

You can use switches for any of the ten main GDisk operations.

Table 10-2 Switches common to all GDisk commands

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.

Table 10-2 Switches common to all GDisk commands

Switch	Explanation
/sure	Suppresses prompting to confirm the operation and has the same functionality as /y.
/r	Causes GDisk to restart the computer if the operation is successful.
/forceusb	Forces USB support to start, even when the USB controller is being run by something else. -forceusb attempts to take over the USB Host Controller and then attempts to return it to the previous state once the Ghost operation is complete. This works for controllers as follows: ■ EHCI controllers with BIOS support are taken over and then returned to the BIOS. ■ UHCI controllers with BIOS support are taken over and then returned to the BIOS. For example, the keyboard is returned after the Ghost operation is finished. ■ OHCI controllers with BIOS support are taken over but not returned to the BIOS. Note the following: ■ Use this switch with caution. ■ Avoid using the forceusb switch to take over a USB controller from a driver, for example, Iomega USB drivers. You may encounter problems if you do this.
/nousb	Disables USB support.
-force1394	Forces FireWire support to start, even when the FireWire controller is being run by something else. -force1394 attempts to take over the FireWire Host Controller. To enable native BIOS support you must restart the computer. Note the following: ■ Use this switch with caution. ■ Avoid using the force1394 switch to take over a FireWire controller from a driver, for example, Iomega FireWire drivers. You may encounter problems if you do this.
-no1394	Disables FireWire support.

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 an NTFS partition or a dynamic disk partition.

The create switch functions with GDisk.exe only.

Note: When GDisk creates a FAT32 partition, it aligns the first data sector to a 4 KB boundary from the start of the partition.

The syntax for the create command is as follows:

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

For example, to create a FAT32 formatted partition that uses the entire disk, type the following command:

gdisk 1 /cre /pri /for /q

Table 10-3 Create switches

Switch	Explanation
disk	Represents the physical fixed disk, from 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.
/end	Creates the partition at the end of the free space. If this switch is not used, then the partition is created at the beginning of the free space. If the command line specifies that all of the available space is to be used to create the partition, then the /end switch is ignored.

Table 10-3 Create switches

Switch	Explanation
/for	Formats the new partition once it has been created. Unless the /ntfat16 or /-32 switches are used, the partition type is determined by the following: ■ If the partition is less than 16MB: FAT12 ■ If the partition is between 16MB and 512MB: FAT16 ■ If the partition is greater than 512MB: FAT32
/q	Performs a quick format if used in combination with the /for switch. If you do not use this switch, then GDisk performs a surface scan of the partition and marks any bad sectors.
/v[:label]	Gives the new formatted partition the specified label when used in combination with the /for switch.
/-32	Indicates that the partition is not formatted as FAT32. Limits primary and logical partitions to 2048 MB. Partitions over 16 MB are formatted as FAT16. This switch is useful if the operating system does not support FAT32, such as Windows NT 4.
/ntfat16	Lets you create a FAT16 primary or logical partition, up to 4097 MB. The cluster size is 64 KB. Partitions over 16 MB are formatted as FAT16. Windows 9x and DOS systems may be unable to access partitions that are created with this switch and 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.

This switch functions with GDisk.exe only.

Note: The switch must be used when you delete Linux partitions if LILO resides in the MBR.

The syntax for this command is as follows:

gdisk disk /mbr [/wipe]

Table 10-4 /mbr switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 8.
/mbr	Reinitializes the boot code in the Master Boot Record.
/wipe	Deletes the partition on the disk.

Showing information about disks

The status switch shows information about the fixed disks and partitions on a disk, including the model of the disk. You must specify the disk number to get information about the partitions on a disk.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

Version	Command syntax
GDisk.exe	gdisk [disk] [/status] [/raw] [/lba] [/ser]
GDisk32.exe	gdisk32 [disk] [/status] [/raw] [/lba] [/ser]

Table 10-5 /status switches

Switch	Explanation
disk	Represents the physical fixed disk, from 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 previously prepared text file.

If the name of a text file is supplied along with the batch mode switch, GDisk opens the file and executes the commands within it until all commands have been executed or one of the commands encounters an error.

For example:

C:\> gdisk /batch:cmds.txt

If the batch mode switch is supplied without a file name, GDisk prompts you for the commands to execute.

Note: To use GDisk32.exe in the example commands, replace gdisk with gdisk32.

Command-line arguments that apply to all of the batch commands can be specified on the original command line along with the batch mode switch. The lines found in the batch file (or typed at the prompt) are appended to the already partially formed command line.

Following is a sample batch command file called Two-new.txt. Blank lines and lines starting with the number (hash) symbol are considered comments. These lines are ignored. In the following example, the commands do not specify the fixed disk on which to operate:

 # delete all partitions
/del /all
 # create formatted FAT16 primary DOS partition and then create an extended
 # partition
/cre /pri /-32 /for /q
/cre /ext
 # create formatted FAT16 logical DOS partition
/cre /log /-32 /for /q

The following command deletes all partitions and creates two new ones on the second fixed disk with confirmation prompting turned off:

gdisk 2 /y /batch:two-new.txt

The following four commands to be executed are a combination of the original command plus the commands from the batch file:

gdisk 2 /y /del /all
gdisk 2 /y /cre /pri /-32 /for /q
gdisk 2 /y /cre /ext
gdisk 2 /y /cre /log /-32 /for /q

Batch files may be nested recursively. For example, a second file called Std_init.txt contains the following lines:

1 /batch:two-new.txt
2 /batch:two-new.txt

As a result, the following command performs the actions of two-new.txt on both fixed disks:

gdisk /batch:std-init.txt

Understanding FAT16 partitions in Windows NT

FAT16 partitions can be up to 4 GB using 64 K clusters in Windows NT. GDisk can create a FAT16 partition using 64 K clusters when the /ntfat16 switch is added to the create partition command line. This switch disables the creation of FAT32 partitions and allows the creation of FAT16 partitions up to 4 GB.

Note: DOS and Windows 9x do not support FAT16 partitions using 64 K clusters and are limited to 2 GB FAT16 partitions.

Deleting and wiping your disk

GDisk lets you delete data and partitions on your disk or wipe your entire disk. You cannot delete a dynamic disk partition with the /del switch.

The switch /del /all deletes all partitions that are on the disk. Any other space that has not been used for creating a partition is not deleted. Deleting an extended partition also deletes any logical partition within it.

The /diskwipe switch wipes the entire disk, partitions, partition table, MBR, and all used and unused space.

For more information on the conformance of GDisk to the U.S. Department of Defense requirements, see the DoD_wipe.pdf on the Symantec Ghost CD.

These switches function with GDisk.exe only.

The syntax for the delete switch is as follows:

GDisk.exe: gdisk disk /del {/pri[:nth]|/ext[:nth]|/log:nth|/p:partn-no|/all} [/qwipe|/dodwipe|/customwipe:n][/[-]hpa]

Table 10-6 /del switches

Switch	Explanation
disk	Represents the physical fixed disk, from 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.
/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 1 pass of deleting the data on the disk.
/dodwipe	Overwrites the partition's data area before deleting the partition. Makes 6 passes of deleting the data on the disk.
/customwipe:n	Overwrites the partition's data area n times before deleting the partition. n can be set from 1 to 100. /customwipe:6 is equivalent to a sanitize /dodwipe operation.

The syntax for the diskwipe switch is as follows:

GDisk.exe: gdisk disk /diskwipe [dodwipe| /customwipe:n][/[-]hpa]

Table 10-7 /diskwipe switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 8.
/diskwipe	Wipes the contents of the entire disk. Using this switch on its own wipes all partitions.
/dodwipe	Overwrites the disk including all partitions. Makes 6 passes of deleting the data on the disk.

Table 10-7 /diskwipe switches

Switch	Explanation
/customwipe:n	Overwrites the disk's data area n times and deletes partitions. n can be set from 1 to 100. /customwipe:6 is equivalent to a sanitize /dodwipe operation.
/hpa	Wipes any HPA/PARTIES area found on the disk.
/-hpa	Ignores any HPA/PARTIES area found on the disk.

Following are examples of the delete and wipe switches:

- gdisk 1 /del /all /qwipe completes one pass to delete all partitions and data on disk 1.
- gdisk 1 /del /p:2 /qwipe wipes partition 2 on disk 1 with one pass.
- gdisk 1 /diskwipe /customwipe:15 wipes the entire disk with 15 passes.

Wiping Host Protected Areas (HPA)/PARTIES

During execution of a DoD disk wipe, GDisk attempts to detect an HPA/PARTIES area on the disk.

The sequence of the wipe is as follows:

- If GDisk detects such an area then it shall notify the user that it was found and ask the user whether this area should be unlocked so that it can be erased.
- If the user requests that the area be unlocked then GDisk will attempt to unlock the area, otherwise GDisk continues, ignoring the HPA area.
- If the area is not password protected and is successfully unlocked then GDisk notifies the user and erases the entire disk including the HPA/PARTIES area.
- If the area is password protected and cannot be unlocked then it notifies the user that the unlock failed and asks if the users wants to continue. The user is also informed that the HPA/PARTIES area could possibly be unlocked using the BIOS.
- If the user wants to continue then GDisk continues to erase the disk, ignoring the HPA/PARTIES area.

There are two optional command line switches:

- /-hpa: GDisk does not look for an HPA on the disk.
  For example:
  gdisk 1 /diskwipe /dodwipe /-hpa performs a DoD disk wipe without checking for an HPA on the disk. If an HPA area is present it is not wiped.
- /hpa: GDisk detects and attempts to unlock the HPA on the disk. If the area cannot be unlocked then GDisk exits.
  For example:
  gdisk 1 /diskwipe /dodwipe /hpa performs a DoD disk wipe attempting to unlock any HPA on the disk.

Confirming a disk wipe

The view:n command-line switch lets you view the overwrite pattern on the disk to confirm the overwrite has occurred. This lets you display one or more sectors, starting at sector n, of a physical disk on screen (by default, 1 sector shall be displayed). Sector numbers start at 0.

There are two optional arguments as follows:

- num:m: m sectors are displayed starting at the sector indicated in the view command.
  If num:m is not specified then GDisk defaults to displaying only one sector as indicated by view:n.
- page: GDisk waits for you to press a key after each page of sector content is displayed. You can press q to exit.
  If page is not specified then GDisk defaults to outputting the contents of the sectors specified continuously until finished.

Each sector is displayed as a table with 16 columns containing the sector offset, then hex bytes, and lastly 16 ASCII characters representing each byte. The table has n rows where n depends on the sector size. This is usually 32 rows (sector size of 512 bytes).

For example:

gdisk 1 /view:0 /num:3 displays sectors 0, 1, and 2 on screen

The output displays as follows:

```
Physical Disk 1, Sector 0:
-----------------------------------------------------------
00000000  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000010  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000020  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000030  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000040  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000050  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000060  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
00000070  16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16  ................
```

Activating or deactivating a partition

A computer starts in an active partition. Using the /act or /-act switches, you can choose the partition to which the computer starts.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

Version	Command syntax
GDisk.exe	gdisk disk /[-]act /p:partn-no
GDisk32.exe	gdisk32 disk /[-]act /p:partn-no

Table 10-8 /act switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 8.
/act	Activates a partition.
/-act	Deactivates a partition.
/p:partn-no	Indicates the partition to activate or deactivate. Only primary partitions can be activated. Use the number reported by GDisk in standard display mode (not using /lba or /raw) for partn-no.

Hiding or unhiding a partition

You can hide a partition so that a user cannot see it.

Depending on the version of GDisk that you require, the syntax for this command is one of the following:

Version	Command syntax
GDisk.exe	gdisk disk /[-]hide /p:partn-no
GDisk32.exe	gdisk32 disk /[-]hide /p:partn-no

Table 10-9 /hide switches

Switch	Explanation
disk	Represents the physical fixed disk, from 1 to 8.
/hide	Hides a partition.

Table 10-9 /hide switches

Switch	Explanation
/-hide	Unhides a partition.
/p:partn-no	Indicates the partition to hide or unhide. Use the number reported by GDisk in standard display mode (not using /lba or /raw) for partn-no.

Modifying the Windows NT/2000/XP boot menu

The /bootini switch lets you make a modification to a Windows NT/2000/XP boot menu. The following modifications are supported:

- Displaying a list of current boot entries
- Adding an entry to boot.ini
- Removing an entry from boot.ini
- Setting the default boot option and timeout

This switch functions with GDisk32.exe only.

When GDisk32 changes the state of boot.ini, a copy of the current boot.ini is created. Table 10-10 lists the boot.ini copy names.

Table 10-10 Original and copy names

Original boot.ini filename	Boot.ini copy name
Named boot.ini	boot_GDISK32_copy.ini
Not named boot.ini and with a period. For example: my.ini	my_GDISK32_copy.ini
Not named boot.ini and without a period. For example: myBootFile	_GDISK32_copy is appended to the end of the file name: myBootFile_GDISK32_copy

Specifying the boot.ini path and file name

The /inifile switch is common to all operations performed with the /bootini switch.

/inifile lets you specify the full path and file name of the current Windows NT/2000/XP boot.ini file. This lets you locate boot.ini if it is not on drive C.

The default value for this switch is C:\boot.ini.

Displaying the list of current boot entries

Use the /bootini switch to display the existing boot menu for the current Windows NT/2000/XP operating system.

The syntax for this command is as follows:

gdisk32 /bootini [/inifile:filename]

Adding an entry to boot.ini

There are two types of functions that you can add to a boot.ini file:

- Starting another installation of Windows NT/2000/XP that resides on a different partition.
- Starting a non-Windows NT/2000/XP operating system that resides on a different partition.

GDisk does not add an entry to boot.ini in the following cases:

- An entry with the description already exists in Boot.ini (case insensitive).
- The referenced partition is of type Extended.
- The referenced partition is hidden.

The following table describes the function of each switch for both types of entries.

Table 10-11 Boot.ini switches

Switch	Explanation
/bootini	Modifies boot.ini.
/add	Creates a new entry in boot.ini.
/d:diskno	Represents the physical fixed disk, from 1 to 8.
/p:partno	Indicates the partition from which to boot.
/desc:description	Specifies the description to appear in the NT boot loader menu.

Table 10-11 Boot.ini switches

Switch	Explanation
/inifile:filename	Specifies the full path and file name for boot.ini. The default value is C:\boot.ini.
/bsectfile:filename	Specifies the boot sector file to create. For example, C:\bsect.dat.
/winnt	Adds an entry to start a Windows NT/2000/XP operating system.
/sysfolder:folder	Specifies the system folder on the Windows NT/2000/XP operating system from which to start. The default value is Winnt.
/r	Restarts after the execution of the command.

Adding an entry to start Windows NT/2000/XP

The syntax for this command is as follows:

gdisk32 /bootini /add /d:disknumber/p:partno /desc:description /winnt [/sysfolder:folder] [/inifile:filename] [/r]

This entry uses the Advanced RISC Computing (ARC) style path to describe the relative disk location for the entry. The entry has the following format:

<ARC style path>\<system folder>="description"

For example:

multi(0)disk(0)rdisk(0)partition(1)\winnt="Boot NT System"

For more information, see the Microsoft Knowledge Base article Q102873 - "BOOT.INI and ARC Path Naming Conventions and Usage."

Note the following:

- GDisk uses only Multi(X) syntax when describing ARC style paths, as opposed to SCSI(X).
- GDisk always uses multi(0)disk(0) as the beginning of the ARC style path.
- /winnt instructs GDisk32 to create an ARC style entry and must be used if the target operating system is Windows NT/2000/XP. If this switch is not used, then GDisk32 creates an entry as if the target operating system is not Windows NT/2000/XP.
- /sysfolder lets you specify the Windows system folder on the target operating system. The system folder is usually Winnt. If the system folder is not Winnt, then provide the path to this folder, but do not include the root directory.
  For example, use /sysfolder:"2k\WinNt", not /sysfolder:"f:\2k\WinNt".

Adding an entry to start a non-Windows NT/2000/XP operating system

The syntax for this command is as follows:

gdisk32 /bootini /add /d:diskno/p:partno /desc:description [/inifile:filename] [/bsectfile:filename] [/r]

This entry to boot.ini references a boot sector file used to continue the boot up process.

The entry has the following format:

<full path to boot sector file>\<boot sector file>="description"

For example:

C:\bootos2s.dat="Boot OS/2 System"

When adding this entry, GDisk does the following:

- Reads the first sector of the targeted partition (boot sector).
- Writes out the contents of that sector to a boot sector file.
- Adds a reference to that boot sector file to boot.ini.

The /bsectfile switch is optional. It is used if you want the created bootsect.dat file to be saved somewhere other than the default location.

You must specify the full path and file name for the boot sector file that is created when you use the /bsectfile switch.

GDisk32 does the following by default:

- Builds the file name from the entry descriptions, omitting any invalid characters under DOS rules for 8.3 file name format.
- Creates the boot sector file in the root directory of the C drive and gives it a .dat file extension.
  For example:
  gdisk32 /add /d:1 /p:2 /desc:“* Boot OS/2 ***”**
  This produces a boot sector file C:\bootos2.dat.

Removing an entry from boot.ini

The syntax to remove an entry from boot.ini is as follows:

gdisk32 /bootini /remove /entry:number [/inifile:filename] [/r]

Table 10-12 /remove switches

Switch	Explanation
/remove	Removes the entry from boot.ini.
/entry:number	Removes the ID of the entry from boot.ini.

If the entry to be removed is the default boot option, then GDisk removes the entry and sets the first entry in the remaining list as the default boot entry.

GDisk does not remove the entry if it is the only entry in boot.ini.

Setting the default boot option and timeout

Use the /default switch to set the default boot option and timeout.

The syntax for this command is as follows:

gdisk32 /bootini /default [/entry:number] [/timeout:sec] [/inifile:filename] [/r]

Table 10-13 Default boot option and timeout switches

Switch	Explanation
/default	Sets the default boot option and timeout.
/entry:number	Sets the ID of the entry as the default boot option.
/timeout:sec	Sets the number of seconds before the default boot option is selected.

Support for large hard disks

GDisk 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 you create partitions for use in Windows 95/98:

- On a system with PC BIOS that does not support interrupt 13h extended disk services, 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 that starts or ends past the limit.

Remember the following information when you create partitions for use in Windows NT:

- According to the Microsoft Knowledge Base, Windows NT NTFS bootable partitions cannot exceed 7.8 GB (8,455,716,864 bytes). This information is detailed in the Microsoft Knowledge Base Article "Windows NT Boot Process and Hard Disk Constraints," Article ID: Q114841.
  Non-bootable NTFS partitions do not have this size limitation.
- Windows NT cannot start from partitions that start or end beyond the 1024-cylinder boundary. If this condition exists, Windows 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 Microsoft Knowledge Base Article "IBM DTTA-351010 10.1 GB Drive Capacity Is Inaccurate," Article ID: Q183654.

Chapter 11

Manipulating files and directories using OmniFS

This chapter includes the following topics:

About OmniFS

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

OmniFS32 performs the same functions, but runs them in a Windows environment.

What OmniFS does

OmniFS performs selected file input/output operations on a file system that is not accessible from a utility's operating environment. In particular, OmniFS accesses NTFS volumes from DOS or Windows 9x, and FAT32 volumes from Windows NT.

OmniFS supports scripting and batch mode execution.

OmniFS operating environments

Table 11-1 lists the two versions of OmniFS.

Table 11-1 OmniFS versions

Executable	Operating system
OmniFS	PC-DOS, MS-DOS
OmniFS32	Windows 9x/NT/2000/XP/Me/WinPE

Long file names are supported on NTFS file systems, but currently support for long file names on FAT depends on the operating system and access method. If you use the OmniFS library to access a file system, then long file names are supported. You can use the access method switches to directly access a file system.

Using OmniFS

You can execute OmniFS from the command line only. The executables are called OmniFS.exe and OmniFS32.exe. Running OmniFS without any arguments provides a list of the interfaces and lists the access method switches.

The following interfaces are supported for both OmniFS.exe and OmniFS32.exe:

omnifs [/accessmethods] <operation to perform> <operation arguments, if any>	Performs the file operation and exits. It uses the exit code to signal whether or not the operation was successful, making it suitable for batch mode execution.
omnifs [/accessmethods] /script=<script file name>	Performs all of the operations that are nominated in the script file and exits. It uses the exit code to signal whether or not the operation was successful. If any operation nominated in the script file is unsuccessful, the execution stops at that point and the utility exits, signalling the failure.
omnifs help	Lists the available commands.

Access method switches

You can use any of the following access method switches before any operation. Not all access methods are relevant to the Win32 version, OmniFS32.exe.

/dl=n	Specifies the number of hard drives present.
/ffi	Prefers use of Direct IDE Access (DOS only).
/ffs	Prefers use of Direct ASPI/SCSI Access.
/ffx	Prefers use of Extended Int13h (DOS and 9x only).
/fna	Disables asynchronous i/o.
/fni	Disables Direct IDE Access support (DOS only).
/fns	Disables Direct ASPI/SCSI Access support.
/fnu	Disables IDE UDMA support (DOS only).
/fnx	Disables Extended Int13h support (DOS and 9x only).

/forceusb — Forces USB support to start, even when the USB controller is being run by something else. -forceusb attempts to take over the USB Host Controller and then attempts to return it to the previous state once the Ghost operation is complete. This works for controllers as follows:

- EHCI controllers with BIOS support are taken over and then returned to the BIOS.
- UHCI controllers with BIOS support are taken over and then returned to the BIOS.
  For example, the keyboard is returned after the Ghost operation is finished.
- OHCI controllers with BIOS support are taken over but not returned to the BIOS.

Note the following:

- Use this switch with caution.
- Avoid using the forceusb switch to take over a USB controller from a driver, for example, the Ghost peer-to-peer USB driver. You may encounter problems if you do this.

/nousb — Disables USB support.

/x — Uses Ghost Disk Library-based access in preference to native (operating system) access when performing operations.

This switch accesses a file system directly, even if it is mounted by the operating system.

Accessing files and folders with names that contain spaces

When using any of the OmniFS operations on files or folders that contain spaces in the file name or folder name, you must use one of these methods.

To display the directory for the folder My Documents in volume 1, use one of the following:

```
OmniFS dir "1:\My Documents"
OmniFS dir 1:"\My Documents"
```

The following example would not work:

```
OmniFS dir 1:\"My Documents"
```

Listing drive identifiers

An NTFS file system cannot be mounted by DOS and therefore does not have a drive letter assigned by DOS. Use the info or diskinfo command to list the drive identifiers that are assigned by OmniFS on a computer.

In all cases, the characters :\ distinguish the volume identifier from the path name.

Using the info command

The output of the command c:\>omnifs info might look like the following:

1:		**[a:\]**	**Volume Removable Drive**
2:	**(28.47GB)**	**[c:\]**	**Active Volume FAT32 l:[ASURA] *cloneable***
3:		**[d:\]**	**Volume CD Drive**
4:		**[p:\]**	**Volume l:[AppsFTP] Network Drive**
5:		**[s:\]**	**Volume l:[Data] Network Drive**
6:		**[t:\]**	**Volume l:[Users] Network Drive**
7:		**[z:\]**	**Volume Network Drive**
8:	**(15.66MB)**		**Diag Volume Unknown *cloneable***
9:	**(2.07GB)**		**Active Volume NTFS l:[Source] *cloneable***
10:	**(956.81MB)**		**Diag Volume Unknown *cloneable***

The output provides you with the information that is needed to compile the script files or to set up the batch files. The identifier for the volume (partition) that is not recognized by the current operating environment should match the volume number in this list.

For example, to copy a file from drive C to the 2.07 GB NTFS volume in the example above, specify the following operation:

```
omnifs copy c:\test\data.txt 9:\test\data.txt
```

or

```
omnifs copy c:\test\data.txt 9:\test\
```

Using the diskinfo command

You can also identify volumes with the diskinfo command.

For example, the output of c:\>omnifs diskinfo might look like the following:

Disk:	**1**	**(95.42GB)**	**M:[Maxtor 4 G100H5 GAK8] S:[G5001MGF]**
	1.1	**(87.89GB)**	**[C:\] Active Volume NTFS l:[Rasfline] Primary**
		(7.53GB)	**Unused Space Primary**
Disk:	**2**	**(3.01GB)**	**M:[QUANTUM FIREBALL EX3 A0A.] S:[673826342323]**
	2.1	**(55.09MB)**	**Active Volume EXT2 Primary**
	2.2	**(2.95GB)**	**[E:\] Volume FAT32 Primary**
		(3.94MB)	**Unused Space Primary**

The output provides additional information that is required to address partitions by the physical arrangement on the drives. Volume labels can also be used. To copy a file from the NTFS partition to the FAT32 partition in the example above, you can use the following syntax:

```
omnifs copy Rasfline:\test\data.txt 2.2:\test\data.txt
```

OmniFS operations

These are the supported OmniFS operations:

- Attrib
- Copy
- Rename
- Delete
- Deltree
- Dir
- Info
- Diskinfo
- Help
- Version
- Mkdir

Commands are not case sensitive.

Setting the attribute for a file

The syntax for the attrib command is as follows:

attrib [+r][-r][+s][-s][+h][-h] <source>

The source argument must be specified as an absolute path. This command sets or clears the file attributes to read only, system or hidden.

Copying files and directories

The syntax for the copy command is as follows:

copy <source> <destination>

Both the source and destination arguments must be specified as absolute paths.

For example:

- Copy a file from a volume that is accessible to the current operating system, to a folder test on a volume that is inaccessible to it:

  ```
  copy a:\temp\test.txt 2:\user\data.txt
  ```

- Copy a file from a volume that is inaccessible to the current operating system, to a volume that is accessible to it:

  ```
  copy 2:\user\data.txt a:\temp\test.txt
  ```

In both examples the absolute path to the files must be valid.

If the source argument points to a directory, the copy operation copies all of the files and subdirectories from the source location to the destination location. In this case, the destination argument must point to a valid directory. The last portion of the destination path is created if required.

If the first argument points to a file and the second argument points to a directory, the file is created with the same name as the source file in the destination directory.

Renaming files and directories

The syntax for the rename command is as follows:

rename <source> <destination>

Both the source and destination arguments must be specified. The source argument must be specified as an absolute path and the destination argument must contain the new name only, and not the new location.

For example:

```
rename 2:\user\data.txt "my data.txt"
```

This renames 2:\user\data.txt to 2:\user\ my data.txt.

The following operation is illegal because the destination argument contains a location:

```
rename 2:\user\data.txt 2:\temp\"my data.txt"
```

Deleting a file

The syntax for the delete command is as follows:

delete <source>

The source argument must be specified as an absolute path, and the path must be valid. No wildcard characters are accepted.

For example:

```
delete 2:\user\data.txt
```

A directory can be deleted only if it is empty.

Deleting a directory

The syntax for the deltree command is as follows:

deltree <source>

This command is similar to delete, but the source is a directory. The contents of the directory, including all subdirectories, are deleted before the directory is deleted.

Listing a directory

The syntax for the directory listing command is as follows:

dir <source>

The source argument must be specified as an absolute path, and the path must be valid.

For example:

```
dir 2:\user
```

The output is similar to that of the 4Dos dir command.

Listing all volumes on a computer

The syntax for the info command is as follows:

info

The info operation has no parameters, and outputs the list of all the volumes that OmniFS is able to detect on the computer, regardless of whether they are recognizable by the current operating system or not.

Listing partitions and file systems on a computer

The syntax for the diskinfo command is as follows:

diskinfo

Diskinfo has no parameters, and outputs a list of the partitions on the system and the file systems (if any) recognized in those partitions.

Listing the commands

The syntax for the help command is as follows:

help

The help command lists the OmniFS commands.

Displaying the OmniFS version and copyright

The syntax for the version command is as follows:

version

This command displays the OmniFS version number and copyright.

Creating a directory

The syntax for the mkdir command is as follows:

mkdir <destination>

This command creates a directory. The destination argument must include an absolute path, and all components of the path except for the last directory must exist.

For example:

```
mkdir 2:\user\test
```

The directory 2:\user must already exist.

Using OmniFS to recover files

If a Clone task has failed on a client computer and the computer cannot start in Windows, you can use OmniFS to do a directory listing of preserved files in the File Preservation Metadata File, and to copy the files to other locations.

There are two formats you can use for designating drives:

- Format c_drive when the origin partition was a FAT partition accessible from DOS.
  For example,
  omnifs dir pf:\e_drive\data
- Format disk_1\partition_2 when the origin partition was NTFS or hidden FAT.
  For example,
  omnifs dir pf:\disk_1\partition_2\data

Table 11-2 lists the commands you can use for recovering files. No other OmniFS commands are supported for use with the File Preservation Metadata File.

Table 11-2 OmniFS recovery commands

Command line	Description
omnifs dir pf:\c_drive\path	Displays a directory listing from the File Preservation Metadata File of the preserved files if the File Preservation Metadata File is in the current directory. If a path is not included, a full listing is displayed. The drive must be included in the command, in the format c_drive or e_drive. For example, omnifs dir “pf:\c_drive\My Documents” Displays all preserved files from c:\My Documents.
omnifs dir pf:\c:\recovery:\c_drive\path	Displays a directory listing from the File Preservation Metadata File of the preserved files if the File Preservation Metadata File is not in the current directory. If a path is not included, a full listing is displayed. The drive must be included in the command, in the format c_drive or e_drive. For example, omnifs dir pf:\c:\recovery:\c_drive\Data Displays all preserved files from c:\Data from the File Preservation Metadata File which is located in c:\recovery.

Table 11-2 OmniFS recovery commands

Command line	Description
omnifs copy pf:\source destination	Copies all files listed in the File Preservation Metadata File to the specified location. For example, omnifs copy pf:\1.2:\ 1:1\temp Copies all files listed in the File Preservation Metadata File, which is in the root directory of the second partition of the first disk, to the temp directory on the first partition on the first disk. This example uses the notation that lets you avoid having to use a drive letter.
omnifs delete pf:\source destination	Deletes specified file. For example, omnifs delete pf:\1.2:\ghost: disk_0\partition_1\recovery\extra.txt Deletes the extra.txt file in the directory recovery listed in the File Preservation Metadata File that is in the Ghost directory on the second partition on the first disk.
omnifs deltree pf:\source destination	Deletes specified directory. For example, omnifs deltree pf:\1.2:\ghost: \recovery Deletes the directory recovery and all files within the directory.

Using a script file

The script file format that is recognized by the utility uses the following rules:

- Each line in the script file begins with the operation and is followed by all of the required arguments for the nominated operation.
- When specifying operation arguments with long file names, use quotation marks (as you would on the command line).
- Empty lines in the script file will be ignored.

An example of the script file is as follows:

```
copy a:\temp\user.dat 2:\user\profile.dat
copy a:\userdir 2:\user\data
delete 2:\user\data\copy.bat
rename 2:\user\data\catalog.cpy catalog.dat
```

The user can execute the set of commands provided in the script file using the following command:

```
omnifs /script=scriptfs.txt
```

Each command in the script file is echoed to the screen immediately before execution.

OmniFS scenarios

OmniFS can be used from the command line, with a batch file and with a script file.

Using OmniFS from the command line

In this scenario OmniFS is executed from the command line.

The user executes a single operation. For example:

```
omnifs copy a:\temp\user.dat 2:\user\profile.dat
```

Or the user executes a set of commands provided in the script file. For example:

```
omnifs /script=scriptfs.txt
```

Following are the contents of Scriptfs.txt:

```
copy a:\temp\user.dat 2:\user\profile.dat
copy a:\userdir 2:\user\data
delete 2:\user\data\copy.bat
rename 2:\user\data\catalog.cpy catalog.dat
```

Using OmniFS with a script file

This scenario uses a batch file and a script file to copy, delete, and rename files on a volume that is not recognized by the operating system on the computer.

Following are the contents of a batch file, Goomnifs.bat:

```
omnifs /script=scriptfs.txt
```

Following are the contents of Scriptfs.txt:

```
copy a:\temp\user.dat 2:\user\profile.dat
copy a:\userdir 2:\user\data
delete 2:\user\data\copy.bat
rename 2:\user\data\catalog.cpy catalog.dat
```

This scenario would be more efficient than using a batch file.

Using OmniFS with a batch file

This scenario uses a batch file to copy, delete, and rename files on a volume that is not recognized by the operating system on the computer.

Following are the contents of a batch file, Goomnifs.bat:

```
omnifs copy a:\temp\user.dat 2:\user\profile.dat
omnifs copy a:\userdir 2:\user\data
omnifs delete 2:\user\data\copy.bat
omnifs rename 2:\user\data\catalog.cpy catalog.dat
```

OmniFS error handling

If an error occurs during the OmniFS operation, an error file, OmniFSer.txt, is created in the current directory.

Correcting the date and time

When you copy files from a FAT partition to an NTFS partition under DOS, there is a time zone issue that must be addressed.

The date and time data in the FAT file system are local to the computer that the files are on. NTFS, however, uses UTC (Universal Time Coordinated) dates and times, also known as Greenwich Mean Time. Therefore, to set the date and time data correctly, OmniFS needs to know the time zone that the computer is in. This can be done either in the autoexec.bat file or from the command line, using the DOS environment variable, tz. For example:

```
set tz=aaa[+|-]h[h][bbb]
```

Where:

- aaa is the abbreviation for your standard time.
- [+|-]h[h][:mm] is a one to two digit signed number indicating the difference as number of hours West of Greenwich.
- bbb (which can be omitted) is the abbreviation for your daylight (summer) time zone.

For example:

Auckland, Wellington

```
set TZ=NST-12
```

US and Canada Central Time

```
set TZ=EST+6
```

Central America

```
set TZ=CST+5
```

There is no significance in the abbreviation string other than it must be three alphanumeric characters.

Following are examples with part hour time differences:

India (Delhi)

```
set TZ=IST-5:30
```

Nepal (Katmandu)

```
set TZ=NST-5:45
```

These settings are in contrast to Windows times zones, which are the number of hours East of Greenwich, in which Auckland would be GMT+12.

Section 6

Appendixes

Appendix A

Command-line switches

This chapter includes the following topics:

Using Symantec Ghost with switches

Symantec Ghost can be run in the following ways:

- Interactively with no command-line switches
- Interactively with selected switches
- Automated in batch files (batch mode)

The Symantec Ghost command-line switches are used to alter Symantec Ghost behavior and automate procedures.

A hyphen (-) or a slash (/) must precede all switches except @filename. Switches are not case sensitive.

If you are adding switches from the Advanced Options dialog box, some of the switches, for example the -clone switch, are not applicable to your task. Because you are already performing a backup, restore, or clone operation, the -clone switch is redundant.

To list Symantec Ghost command-line switches

- In the Ghost directory, type one of the following:
  - **ghost.exe -h**
  - **ghost.exe -?**

Command-line switches

@filename	@filename specifies a file that contains additional command-line switches that Symantec Ghost should read. Filename indicates the path and file name of the command-line switch file. The command-line switch file can include any Symantec Ghost command-line switch. The Symantec Ghost command-line switch file must be a text file with each switch on a separate line. This lets you exceed the DOS command-line limit of 150 characters. For example: **ghost.exe @ghswitch.txt** For this command-line switch, the Ghswitch.txt file reads: -clone,mode=pcreate,src=1:2,dst=g:\part2.gho -fcr -sure
-afile=filename	Replaces the default abort error log file name, Ghosterr.txt, with 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 restored. This switch is the default behavior for Symantec Ghost.
-batch	Batch mode switch. Prevents abort messages from waiting for user acknowledgment, and removes user interaction prompts. The return value of Ghost.exe must be checked to identify whether the operation was successful. Symantec Ghost returns 0 on success and 1 or higher on failure or error. See "Batch file example" on page 168.
-bfc	Handles bad FAT clusters when writing to disk. If this switch is set, and the target partition is FAT, Symantec Ghost checks for and works around bad sectors and all free sectors are verified. This option may slow Symantec Ghost operation substantially.
-blind	Prevents any GUI display. The blind switch must be used with switches that do not require any user input, for example, the clone switch. Using this switch lets you execute Ghost operations on a computer with no video adapter.

-bootcd

When writing an image directly to a CD/DVD writer, makes the CD/DVD bootable. You need a bootable floppy disk in drive A. If you use the -sure switch with -bootcd, and a floppy disk is not in drive A, then a non-bootable CD/DVD is created.

-buffersize=x

Ghost creates an image file using a buffer of size x where x = number of KB. The default size of the buffer is automatically calculated by Symantec Ghost. The buffersize switch lets you override this size. You can set the buffer size value from 1 to 32.

-chkimg,filename

Checks the integrity of the image file indicated by filename.

-clone

Ghost.exe operation switch. This switch allows automation of Ghost.exe operations and has a series of arguments that define the operation parameters.

See "Using the clone switch" on page 161.

-cns

Reverts the naming of spanned files to the system used by versions of Symantec Ghost prior to Symantec Ghost 6.5. If this switch is not used, then the naming of spanned files conforms to Microsoft application guidelines. You do not need to use this switch when reading an existing file. Use this switch when the first five characters in a file name must be unique.

For example:

With -cns	Without -cns
Filename.gho	Filename.gho
Filename.001	Filen001.ghs
Filename.002	Filen002.ghs

-CRC32

The -CRC32 switch lists the files on a disk or partition or creates an image file with CRC values and then verifies the list against the original or a copy. The purpose is to allow both quick listing of the contents of an image file and verification that a disk created by Symantec Ghost contains the same files as the original.

See "Using the -CRC32 switch" on page 169.

-crcignore

Ignores CRC errors. CRC errors indicate data corruption. This switch overrides CRC error detection and may allow a corrupted image file to be used. Using this switch leaves the corrupted files in an unknown state. You can use this switch to help you extract files from a corrupted image file.

-cvtarea

Creates a file, Cvtarea.tmp, that is the location of the MFT when the FAT32 partition is converted to NTFS. This switch operates in a similar manner to the cvtarea program that Microsoft provides in Deploy.cab on the Windows XP installation CD.

For more information, see the Microsoft Web site:

http://www.microsoft.com/hwdev/tech/storage/ntfs-preinstall.asp

The file is created in the root directory of the partition during a partition or disk restore and is created as a contiguous space on the disk. The largest size allowed is 4 GB. If the file is larger than this, it is truncated to 4 GB.

The syntax for this switch is as follows:

-cvtarea,filename=xxx,size=yyy{%disk,%free,KB,MB,GB}, firstcluster=zzz{%disk,%free,KB,MB,GB}

The default settings are as follows:

filename	cvtarea.tmp
size	12%disk
firstcluster	1|3 GB|33%disk Defaults to: ■ 1/3 of the partition size if the partition size is less than 2 GB ■ 1 GB if the partition size is less than 6 GB ■ 3 GB if the partition size is equal to or greater than 6 GB

-dd

Dumps disk metrics information to the dump log file, Ghststat.txt. The file location can be altered using the -dfile=filename switch.

-dfile=filename

Changes the path and file name of the dump log file created using the -dd switch.

-dl=number

Specifies the number of hard disks present. Valid numbers are between 1 and 8. This may help when the BIOS does not report the number of drives correctly.

-dlist=drives

Specifies a list of drives to search for span files. If a span file cannot be found, then the drive letters in dlist are substituted one by one to look for the file on other drives.

For example, the command ghost -dlist=CDEFG instructs Symantec Ghost to look for files on C, D, E, F, and G drives. The path remains the same.

-f32

Lets Symantec Ghost convert all FAT16 volumes to FAT32 volumes when the destination partition to convert is larger than 256 MB in size. Ensure that the installed operating systems can access the volumes that will be converted to support FAT32.

-f64

Lets Symantec Ghost resize FAT16 partitions to be larger than 2047 MB using 64 KB clusters. This is only supported by Windows 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 KB clusters are not wanted.
-fcr	Creates a CRC32 file, Ghost.crc, while creating an image file. See "Using the -CRC32 switch" on page 169.
-fdsp	Preserves the signature bytes on the destination disk when performing a disk-to-disk or image-to-disk cloning operation.
-fdsz	Clears the signature bytes on the destination disk. This is the default for disk-to-disk and image-to-disk operations.
-femax	When an extended partition is created in a disk-to-disk or image-to-disk operation, the femax switch ensures that the extended partition takes up all free space.
-ffatid	Forces the FAT partition id. This switch changes the partition id to the recommended partition id for the FAT partition within the destination image file or the destination partition table. This switch only takes effect if the source is a disk or partition, not an image file. For example, if you are cloning a partition of type 0xA0 (some unknown partition id), and Symantec Ghost sees it as a valid FATx (FAT12/FAT16/FAT32) partition, then the partition id is changed from 0xA0 to FATx. This was default Symantec Ghost behavior before Symantec Ghost 7.5. This switch allows for backward compatibility.
-ffi	Prefers the use of direct IDE access for IDE hard disk operations.
-ffs	Prefers the use of direct ASPI/SCSI disk access for SCSI hard disk operations.
-ffx	Prefers the use of Extended Interrupt 13h disk access for hard disk operations.
-finger	Shows the fingerprint details written on a hard disk created by Symantec Ghost. The fingerprint details include the process used to create the disk or partition and the time, date, and disk on which the operation was performed.
-fis	Uses all available disk space when creating partitions. By default, Symantec Ghost often leaves a small amount of free space at the end of the disk. Because partitions must be aligned to cylinder boundaries, Symantec Ghost may leave up to 8 MB free even when -fis is specified.
-fni	Disables direct IDE access support for IDE hard disk operations.
-fns	Disables direct ASPI/SCSI access support for SCSI hard disk operations.
-fnx	Disables extended INT13 support for hard disk operations.

-force1394

Forces FireWire support to start, even when the FireWire controller is being run by something else. -force1394 attempts to take over the FireWire Host Controller. To enable native BIOS support you must restart the computer.

Note the following:

- Use this switch with caution.
- Avoid using the force1394 switch to take over a FireWire controller from a driver, for example, Iomega FireWire drivers. You may encounter problems if you do this.

-forceusb

Forces USB support to start, even when the USB controller is being run by something else. -forceusb attempts to take over the USB Host Controller and then attempts to return it to the previous state once the Ghost operation is complete. This works for controllers as follows:

- EHCI controllers with BIOS support are taken over and then returned to the BIOS.
- UHCI controllers with BIOS support are taken over and then returned to the BIOS. For example, the keyboard is returned after the Ghost operation is finished.
- OHCI controllers with BIOS support are taken over but not returned to the BIOS.

Note the following:

- Use this switch with caution.
- Avoid using the forceusb switch to take over a USB controller from a driver, for example, the Ghost peer-to-peer USB driver. You may encounter problems if you do this.

-fro

Forces Symantec Ghost to continue cloning even if the source contains bad clusters.

-fx

Causes Symantec Ghost to exit to DOS after an operation is complete. By default, Symantec Ghost prompts the user to restart or exit when the operation has finished. If Symantec Ghost is run as part of a batch file, it is sometimes useful to exit back to the DOS prompt after completion so that further batch commands are processed.

See “-rb” on page 157.

-ghostoncd

Includes Ghost.exe on a CD/DVD when writing an image to a CD/DVD.

-h or -? or -help

Shows the Symantec Ghost command-line switch Help page.

-ia

The image all switch forces Symantec Ghost to perform a sector-by-sector copy of all partitions. By default, when copying a partition from a disk to an image file or to another disk, Symantec Ghost examines the source partition and decides whether to copy just the files and directory structure, or to do a sector-by-sector copy. If it understands the internal format of the partition, it defaults to copying the files and directory structure. Generally this is the best option. However, if a disk has been set up with special hidden security files that are in specific positions on the partition, the only way to reproduce them accurately on the target partition is through a sector-by-sector copy. If you use this switch to create an image of a dynamic disk, then the image must be restored to a disk with identical geometry.

-ial

Forces a sector-by-sector copy of Linux partitions. Other partitions are copied normally.

-ib

The image boot switch copies the entire boot track, including the boot sector, when creating a disk image file or copying disk-to-disk. Use this switch when installed applications, such as boot-time utilities, use the boot track to store information. By default, Symantec Ghost copies only the boot sector, and does not copy the remainder of the boot track. You cannot perform partition-to-partition or partition-to-image functions with the -ib switch.

-id

The image disk switch is similar to -ia (image all), but also copies the boot track, as in -ib (image boot), extended partition tables, and unpartitioned space on the disk. When looking at an image with -id, you see the unpartitioned space and extended partitions in the list of partitions. The -id switch is primarily used by law enforcement agencies that require forensic images.

When Symantec Ghost restores from an -id image, it relocates partitions to cylinder boundaries and adjusts partition tables accordingly. Head, sector, and cylinder information in partition tables is adjusted to match the geometry of the destination disk. Partitions are not resizeable. You will need an identical or larger disk than the original.

Symantec Ghost does not wipe the destination disk when restoring from an -id image. Geometry differences between disks may leave tracks on the destination disk with their previous contents.

Use the -ia (image all) switch instead of the -id switch when copying partition-to-partition or partition-to-image. An individual partition can be restored from an image created with -id.

-imgdesc

Adds a single-line image file description to the image file with the following restrictions:

- Cannot include any new lines
- Cannot be used with -imgdescfile
- Must be used with the clone switch
- Clone switch mode must be create, dump, pcreate, or pdump

-imgdescfile=filename

Specifies a text file that contains an image file description to be added to the image file with the following restrictions:

- Cannot be used with -imgdesc
- Must be used with the clone switch
- Clone switch mode must be create, dump, prcreate, or pdump

-ir

The image raw switch copies the entire disk, ignoring the partition table. This is useful when a disk does not contain a partition table in the standard PC format, or you do not want partitions to be realigned to track boundaries on the destination disk. Some operating systems may not be able to access unaligned partitions. Partitions cannot be resized during restore and you need an identical or larger disk.

-ja=sessionnm

Connects to the GhostCast Server using the specified session name. Set the disk and possibly partition to be cloned on the GhostCast Server.

-jaddr=<id_address>

Use the IP address for the GhostCast Server.

-jl:x=filename

Creates a log file to assist in diagnosing GhostCasting and TCP/IP peer-to-peer problems. The amount of information logged is set by the log level x. The log level x can be E (errors), S (statistics), W (warnings), I (information), or A (all) in increasing order of logging detail. The file name indicates the path and file name of the log to be created. In general, the error and statistic levels do not affect session performance. All other levels may reduce performance and should be used for diagnostic purposes only.

-jm=[u|d|m]

Use unicasting, direct broadcast, or multicasting.

-js=n

Sets to n the number of router hops Symantec Ghost is allowed to cross in an attempt to find the GhostCast Server. (Default is 16.)

-lockinfo

Shows the type code and information stored in the BIOS or the Pentium III Processor ID.

For example:

Type	Based On	Value
M	Manufacturer	Compaq
P	Product name	Deskpro EN Series SFF
V	Version	Award Software
S	Serial number	H925CKH60020
U	UUID	2DA9379B4707D31185E8C800A4F232BC
C	M&P combined	Compaq Deskpro EN Series SFF
I	PIII ID	0000067200028E72A6994A20

-locktype= Type

Lets you lock an image file for use with a specific set of computers defined by the type chosen and the source computer.

For example, ghost -locktype=P creates an image that can be used only on systems that have the same product name type as the source computer.

On computers with multiple processors the processorID bios lock option does not work as intended when running Ghost32.exe. In this situation do not create or restore images with the -locktype parameter set to I. Other -locktype values work as intended.

-lpm

The LPT master mode switch causes Symantec Ghost to automatically go into LPT master mode, and is the equivalent of selecting LPT Master from the main menu.

See “Peer-to-peer connections” on page 210.

-lps

The LPT slave mode switch causes Symantec Ghost to automatically go into LPT slave mode, and is the equivalent of selecting LPT Slave from the main menu.

See “Peer-to-peer connections” on page 210.

-noauto	Disables the automatic naming of spanned image files during creation. The user is prompted for confirmation of the next destination location for the remainder of the image file that is being restored.
-noautoskip	Includes the hibernation and skip files in the image file. These files are excluded by default. For more information on hibernation and skip files, see the *Symantec Ghost Implementation Guide*.
-nofile	Disables the Image File Selection dialog box. Useful when opening directories with large numbers of files and slow links.
-noide	Disables access to IDE devices. This is equivalent to -fni for IDE disks, but noide also affects ATAPI CD writers, tape drives and other IDE devices.
-noindex	Prevents Symantec Ghost from creating an index when creating an image file. This slightly reduces the size of the image file and saves memory but Ghost Explorer is much slower in reading the image file. This switch is useful if you are saving an image file from a large disk with very little memory.
-nolilo	Does not attempt to patch the LILO or GRUB boot loader after a clone. If you use the -nolilo switch, you can restart your computer from a floppy disk or CD after a clone and then run /sbin/lilo or the GRUB install script as the root user to reinstall the boot loader.
-noscsi	Disables access to SCSI devices using ASPI. This is equivalent to -fns for SCSI disks, but noscsi also affects SCSI CD writers, tape drives, and other SCSI devices.
-no1394	Disables FireWire support.
-nousb	Disables USB support.
-ntc-	Disables NTFS contiguous run allocation.
-ntchkdsk	Sets the CHKDSK bit set on a copied NTFS volume. This causes Windows NT to check the integrity of the volume when it is started.
-ntd	Enables NTFS internal diagnostic checking.
-ntic	Ignores the NTFS volume CHKDSK bit. Symantec Ghost checks the CHKDSK bit on an NTFS volume before performing operations. When Symantec Ghost indicates that the CHDSK bit is set, you should run CHKDSK on the volume to ensure that the disk is in a sound state before cloning.

-ntiid

This switch forces Symantec Ghost to ignore the partition table system ids and instead to check the partition contents when detecting NTFS file systems. This switch is useful when the system id is not set to 0x07 for partitions containing NTFS file systems. The partitions would otherwise be inefficiently imaged sector-by-sector. This switch can be used when it is necessary to image a Windows NT4 FTDisk mirrored partition.

Take care when using this switch. Do not use the -ntiid switch with volume sets and stripe sets.

To clone mirrored partitions (also known as Windows NT software RAID partitions)

1. With Windows NT disk administrator, break the mirror set.
2. Using the -ntiid switch, clone one of the mirror partitions.
3. Resize as desired. Partitions can only be resized by Symantec Ghost during a disk operation. When performing a partition operation, the target partition size must already be established.
4. After cloning, recreate the mirror set using the Windows NT disk administrator. The disk administrator creates the partitions in the mirror set.

-ntil

Ignores NTFS log file check (inconsistent volume).

-or

The override switch allows the override of internal space and integrity checks and lets you put a very big image into a small partition. The operation fails if it is unable to write to the limited partition size. This switch lets you override spanning, which fails if there is limited space. Avoid using this switch.

-pfile

Saves the File Preservation Metadata File that holds the location of preserved files to a specified location. By default, it is saved to the current directory.

For example,

ghost - pfile=c:\pathname

Where pathname is the directory for the File Preservation Metadata File.

-pmbr

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

-prefghst

If Symantec Ghost has a choice, it attempts to use internal Ghost file system access as opposed to using the operating system for file system access.

This switch is intended for use under instruction from Symantec Technical Support when troubleshooting.

-prefos

If Symantec Ghost has a choice, it attempts to use the operating system for file system access as opposed to using the internal Ghost file system access.

This switch is intended for use under instruction from Symantec Technical Support when troubleshooting.

-preserve	Preserves files specified by the preservedest switch. The task fails if the specified files do not exist. To preserve files or directories other than the image file the syntax is as follows: **-preserve=filepath[=newpath] [,filepath[=newpath]...]** Each filepath can refer to an individual file or a directory. All files and subdirectories of a specified directory are preserved. If a file does not exist then the restore fails. After a Clone step in a task, all preserved files are added back to the partition specified by the -preservedest=n switch, renaming them to newpath where specified. You must use -preserve with -preservedest.
-preservedest=n	Where n is the number of the partition relative to the destination disk, not relative to the partitions being restored. Specifies the partition to which files specified with the preserve switch are restored.
-preservedimage deleteafterclone	Deletes a preserved image file once the restore has completed successfully. This switch overrides the default, which is to retain the preserved image file.
-preserveifexists	Preserves files specified by the preservedest switch if they exist. The task does not fail if the specified files do not exist. To preserve files or directories other than the image file the syntax is as follows: **-preserveifexists=filepath[=newpath] [,filepath[=newpath]...]** Each filepath can refer to an individual file or a directory. All files and subdirectories of a specified directory are preserved. If a file does not exist then the restore fails. After a Clone step in a task, all preserved files are added back to the destination specified by the -preservedest=n switch, renaming them to newpath where specified. You must use the -preserveifexists switch with -preservedest.
-pwd and -pwd=x	Specifies that password protection be used when creating an image file. x indicates the password for the image file. If no password is given in the switch, Symantec Ghost prompts for one. You can enter a maximum of 10 alphanumeric characters.
-quiet	The quiet mode switch disables status updates and user intervention.
-rb	Restarts after finishing a restore or copy. After completing a restore or copy operation, the target computer must be restarted so that the operating system can restore the new disk/partition information. Normally, Symantec Ghost prompts the user to restart or exit. -rb tells Symantec Ghost to restart automatically after it completes the restore or copy. This is useful when automating Symantec Ghost in a batch command file. See "-fx" on page 152.
-recover	Sets the default to recover preserved files if a previous restore has failed and the File Preservation Metadata File still exists. If this switch is not used the default is set to abort.

-script

Allows you to specify a series of commands (one per line) that Symantec Ghost will execute in sequential order.

For example:

ghost -script=script.txt

Following is an example of script.txt:

-clone,mode=create,src=2,dst=1:1\drv2.gho
-chkimg,1:1\drv2.gho
-clone,mode=create,src=2,dst=c:\part2.gho
-chkimg,c:\part2.gho

In this example 1:1 is equivalent to c:\.

-skip=x

The skip file switch causes Symantec Ghost to exclude the indicated files during a create or restore operation. A skip entry can specify a single file, a directory, or multiple files using the * wildcard. File names must be given in short file name format and all path names are absolute. Only FAT system files can be skipped. It is not possible to skip files on NTFS or other file systems. The skip switch may only be included in the command line once. To specify multiple skip entries, they must be included in a text file indicated using -skip=@skipfile. The format of the skip text file, skipfile, matches the format used with the CRC32 vexcept option.

For example:

- **-skip=\windows\user.dll**
  Skips the file User.dll in the Windows directory.
- **-skip=*\readme.txt**
  Skips any file called Readme.txt in any directory.
- **-skip=\ghost*.dll**
  Skips any file ending with .dll in the Ghost directory.
- **-skip=\progra~1**
  Skips the program files directory (note the short file name).
- **-skip=@skipfile.txt**
  Skips files as outlined in Skipfile.txt. For example:
  ****.tmt**
  [partition:1]
  \windows
  ****.exe**
  [Partition:2]
  ****me.txt**
  This Skipfile.txt file would skip all *.tmt files on any partition, the Windows directory, all *.exe files on the first partition, and any file that ends with me.txt on the second partition.

-span

Enables spanning of image files across volumes.

Do not use this switch if you are running Ghost.exe to write an image file directly to a CD-R/RW. Ghost.exe automatically spans CD-R/RW disks if required.

-split=x	Splits image file into x MB spans. Use this switch to create a forced-size volume set. For example, if you want to force smaller image files from a 1024 MB drive, you could specify 200 MB segments. For example: **ghost.exe -split=200** This divides the image into 200 MB segments.
-sure	Use the -sure switch in conjunction with -clone to avoid being prompted with the final question “Proceed with disk clone - destination drive will be overwritten?” This command is useful in batch mode.
-sze	Sets the size for the destination partitions for either a disk restore or disk copy operation. When numbering partitions in the -sze switch, do not include the hidden Ghost partition. This switch is intended to be used in the Additional command line in the Console. All functionality of -sze switches are supported. See “Setting a destination size for the clone switch” on page 165.
-szee	Forces Symantec Ghost to keep the sizes of all destination partitions the same as in the source partition (no resizing). This switch can be used with or without the -clone switch. See “Setting a destination size for the clone switch” on page 165.
-szef	Forces Symantec Ghost to keep the sizes of all destination partitions, except for the first one, the same as in the source partition. The first partition uses the remaining disk space. This switch can be used with or without the -clone switch. See “Setting a destination size for the clone switch” on page 165.
-szel	Forces Symantec Ghost to keep the sizes of all destination partitions, except for the last one, the same as in the source partition. The last partition uses the remaining disk space. This switch can be used with or without the -clone switch. See “Setting a destination size for the clone switch” on page 165.
-tapebuffered	Default tape mode. Sets the ASPI driver to report a read/write as successful as soon as the data has been transferred to memory. Useful when using older or unreliable tape devices or sequential media.
-tapeeject	Forces Symantec Ghost to eject the tape following a tape operation. If the tape drive does not support remote ejection you must eject and insert the tape manually before further use. Earlier versions ejected the tape by default. By default, Symantec Ghost does not eject the tape. It rewinds the tape before exiting to DOS.
-tapebsize=x	Specifies the tape block size in units of 512 bytes, where x is a number between 1 and 128.
-tapespeed=x	Allows control of tape speed, where x is 0 to F. 0 is the default. 1 to F increases tape speed. Only use this when the tape does not work correctly at the speed used by Symantec Ghost.

-tapeunbuffered	Sets the ASPI driver to report a read/write as successful only when the data has been transferred to the tape drive. This can occur before the data is physically written to the medium.
-tcpm[:slave IP address]	The TCP/IP master mode switch causes Symantec Ghost to go into TCP/IP master mode automatically, and is the equivalent of selecting TCP/IP Master from the main menu. The IP address of the slave computer may be specified. See "Peer-to-peer connections" on page 210.
-tcps	The TCP/IP slave mode switch causes Symantec Ghost to go into TCP/IP slave mode automatically, and is the equivalent of selecting TCP/IP Slave from the main menu. See "Peer-to-peer connections" on page 210.
-unpreserveimage	After a failed restore, do not preserve the image file that was used on the failed restore.
-usbm	The USB master mode switch causes Symantec Ghost to go into USB master mode automatically, and is the equivalent of selecting USB Master from the main menu. See "Peer-to-peer connections" on page 210.
-usbs	The -usbs switch causes Symantec Ghost to go into USB slave mode automatically, and is the equivalent of selecting USB Slave from the main menu. See "Peer-to-peer connections" on page 210.
-vdw	If the -vdw switch is set, Symantec Ghost uses the disk's verify command to check every sector on the disk before it is written. This option may slow Symantec Ghost operation substantially.
-ver	Shows the version number of Symantec Ghost.
-z	Runs compression when saving a disk or partition to an image file. The greater the compression, the slower the transmission, as follows: ■ -z or -z1: Low compression (fast transmission) ■ -z2: High compression (medium transmission) ■ -z3 through -z9: Higher compression (slower transmission) For more information on image files and compression, see the *Symantec Ghost Implementation Guide*.

Accessing files

You can use one of two formats to access files:

- Drive letter: For example,
  c:\My Images\image.gho
- Disk and partition: This lets you specify an otherwise inaccessible file, for example, a file located on a file system not recognized by DOS, such as NTFS, or a file on a hidden partition. It provides an alternative to using drive letters.
  For example,
  src=1:2\image.gho
  In this example, Image.gho resides on an NTFS file system on the second partition of the first disk.
  This format cannot be used with the -afile=filename switch.

Using the clone switch

Some cloning switches for use in Ghost can be specified on the GhostCast Server.

The syntax for the clone switch is:

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

Defining the type of clone command

MODE defines the type of clone command.

The syntax is as follows:

MODE={copy | restore | create | pcopy | prestore | pcreate}

Table A-1 Mode commands

Switch	Action
copy	Disk-to-disk copy
restore **Note:** The load switch is replaced by the restore switch. The load switch is still fully functional and is interchangeable with restore.	File-to-disk restore

Table A-1 Mode commands

Switch	Action
create **Note:** The dump switch is replaced by the create switch. The dump switch is still fully functional and is interchangeable with create.	Disk-to-file backup
pcopy	Partition-to-partition copy
prestore **Note:** The pload switch is replaced by the prestore switch. The pload switch is still fully functional and is interchangeable with prestore.	File-to-partition restore
pcreate **Note:** The pdump switch is replaced by the pcreate switch. The pdump switch is still fully functional and is interchangeable with pcreate.	Partition-to-file backup (allows multipartition Ghost backup selection)

Cloning combination options

Table A-2 illustrates the possible cloning operations that you can perform.

Table A-2 Cloning operations

Mode	Source	Destination
copy	■ disk	■ disk
restore	■ file ■ GhostCast Server tape ■ CD-ROM ■ USB 1.1 and 2.0 Mass Storage Device ■ DVD ■ FireWire hard disk	■ disk
create	■ disk	■ file ■ GhostCast Server tape ■ CD writer ■ USB 1.1 and 2.0 Mass Storage Device ■ DVD ■ FireWire hard disk

Table A-2 Cloning operations

Mode	Source	Destination
pcopy	■ disk:partition	■ disk:partition
prestore	■ file:partition ■ GhostCast Server (no partition specified) tape:partition ■ CD:image:partition ■ USB 1.1 and 2.0 Mass Storage Device ■ FireWire hard disk	■ disk:partition
pcreate	■ disk:partition ■ partition:partition You can specify more than one partition.	■ file ■ GhostCast Server tape ■ CD writer ■ USB 1.1 and 2.0 Mass Storage Device ■ DVD ■ FireWire hard disk

Setting a source for the clone switch

The syntax for this switch is as follows:

SRC={disk | file | multicast | tape}

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

Table A-3 Source options for cloning

Switch	Source	Explanation
disk	drive number	Source disk drive number. Numbers start at 1. For example: SRC=1 A partition on a drive can also be specified. Numbers start at 1. For example: SRC=1:2
file	filename	The source image file name. For example: SRC= g:\source.gho A partition in an image file can also be specified. For example: SRC=g:\source.gho:2 Files can also be read from a CD-ROM drive.

Table A-3 Source options for cloning

Switch	Source	Explanation
tape	@MTx	The tape drive number. Numbers start at 0. For example: SRC=@MT0 A partition on a tape can also be specified. For example: SRC=@MT0:3
CD ROM	@CDx	The CD or DVD drive number. If you have a CD reader and a CD writer, in the Ghost.exe user interface you would see @CD1 and @CD2. The number is optional if you are specifying an operation from the command line. You can specify partitions for the image stored on a CD for a restore operation. For example: SRC=@CD1:2
Preservation file	@PF	An image file that was preserved during a restore that failed. For example: ghost -recover -clone,mode=[p] load, src=@pf,...

Setting a destination for the clone switch

The syntax for this switch is as follows:

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

DST defines the destination location for the operation.

Table A-4 Destination options for cloning

Switch	Destination	Explanation
disk	drive	The destination disk drive number, such as DST=2. A partition on a drive can also be specified. For example: DST=2:1 To create a new partition, type a destination partition one greater than the existing number of partitions, if there is enough free space.
file	filename	The destination image file name. For example: DST= g:\destination.gho
tape	@MTx	The tape drive number. Numbers start at 0. For example: DST=@MT0

Table A-4 Destination options for cloning

Switch	Destination	Explanation
cd/ dvdwriter	@CDx	The CD or DVD writer drive number. Numbers start at 1. For example: DST=@CD1 If you have a CD reader and a CD writer, in the Ghost.exe user interface you would see @CD1 and @ CD2. The number is optional if specifying an operation from the command line.

Setting a destination size for the clone switch

The SZE switch sets the size of the destination partitions for either a disk restore or disk copy operation. This is optional. Multiple partition size switches are supported.

The number of size switches depends on the number of partition sizes that you want to specify. There may be none.

You can use the sze switch in the Advanced command-line options in the Console.

SZE{E | F | L | n={xxxxM | mmP| F | V}}

Table A-5 Destination size options for cloning

Switch	Explanation
n=xxxxM	Indicates that the nth destination partition is to have a size of xxxxMB (for example, SZE2=800M indicates partition two is to have 800 MB).
n=mmP	Indicates that the nth destination partition is to have a size of mm percent of the target disk. Due to partition size rounding and alignment issues, 100% physical use of disk space may not be possible.
n=F	Indicates that the nth destination partition is to remain the same size on the destination as it was on the source. This is referred to as a fixed size.
n=V	Indicates that the partition may be made bigger or smaller depending on how much disk space is available. This is the default.
E	Indicates that the sizes of all partitions remain fixed.
F	Indicates that the sizes of all partitions except the first remain fixed. The first partition uses the remaining space.
L	Indicates that the sizes of all partitions except the last remain fixed. The last partition uses the remaining space.

Examples of clone switch usage

Table A-6 describes clone switches and their functions.

Table A-6 Clone switch usage examples

Switch	Function
ghost.exe -clone,mode=copy,src=1,dst=2	Copies local disk one to local disk two.
ghost.exe -lpm -clone,mode=create,src=2,dst=c:\drive2.gho	Connects a master computer using LPT to another computer running Ghost.exe in slave mode, and saves a disk image of local disk two to the remote file c:\drive2.gho. The slave computer can be started with ghost.exe -lps.
ghost.exe -clone,mode=pcopy,src=1:2,dst=2:1 -sure	Copies the second partition of local disk one to the first partition of local disk two, without the final warning prompt.
ghost.exe -clone,mode=restore,src=e:\savedsk.gho,dst=1 -sure	Restores the disk image file Savedsk.gho that is held on the server drive that is mapped locally to drive E onto local disk one. Performed without the final warning prompt. This example is typical of a command line included in a batch file to automate workstation installations from a network file server.
ghost.exe -clone,mode=pcreate,src=1:2,dst=g:\part2.gho	Saves the second partition of disk one to an image file on mapped network drive G.
ghost -clone,mode=prestore,src=g:\part2.gho:2,dst=1:2	Restores partition two from a two-partition image file on mapped drive G onto the second partition of the local disk.
ghost.exe -clone,mode=restore,src=g:\2prtdisk.gho,dst=2sze1=60P,sze2=40P	Restores disk two from an image file and resizes the destination partitions into a 60:40 allocation.

Table A-6 Clone switch usage examples

Switch	Function
ghost.exe -clone,mode=copy,src=1,dst=2,sze2=F	Clones a two-partition disk and keeps the second partition on the destination disk the same size as on the source disk, and lets the first partition use the remaining space, leaving no unallocated space.
ghost.exe -clone,mode=create,src=1,dst=2:3\image.gho	Saves disk one to the image file image.gho located on the third partition of the second disk. This works only if the third partition of the second disk is NTFS file system.
ghost.exe -clone,mode=prestore,src=2:3\image.gho:5,dst=4:2	Restores the fifth partition of the image file image.gho, which is located on the third partition of the second disk, to the second partition on the fourth disk. This switch only works if the third partition on the second disk is NTFS.
ghost.exe-clone,mode=restore,src=g:\3prtdisk.gho,dst=1,sze1=450M,sze2=1599M,sze3=2047M	Restores disk one from an image file and resizes the first partition to 450 MB, the second to 1599 MB, and the third to 2047 MB.
ghost.exe -clone,mode=restore,src=g:\2prtdisk.gho,dst=1,szeL	Restores a disk from an image file and resizes the last partition to fill the remaining space.
ghost.exe -clone,src=@MCsessionname,dst=1 -sure	Restores disk one from an image file being sent from the GhostCast Server with the session name “sessionname” without the final warning prompt.
ghost.exe -clone,src=1,dst=@MCsessionname -sure	Creates an image file of disk one to an image file being created by the GhostCast Server with the session name “sessionname” without the final warning prompt.
ghost.exe -clone,mode=create,src=2:2,dst=@MT0	Creates an image file of the second partition on disk 2 onto the first tape drive.

Table A-6 Clone switch usage examples

Switch	Function
ghost.exe -clone,mode=pcreate,src=2:1:4:6,dst=d:\part146.gho	Creates an image file with only the selected partitions. This example selects partitions 1, 4, and 6 from disk 2.

Batch file example

This example restores disk one from an image file sent by the GhostCast Server using session name SN and resizes the first partition to 450 MB, the second to 1599 MB, and the third to 2047 MB. This is done in a batch file with no user intervention. The batch file commands change depending on the success or failure of the Symantec Ghost operation.

Batch file contents:

```
@ECHO OFF
ghost.exe
-clone,src=@mcSN,dst=1,sze1=450M,sze2=1599,sze3=2047M -batch
IF ERRORLEVEL 1 GOTO PROBLEM
ECHO Symantec Ghost exited with value 0 indicating success.
REM ** Add any commands required to run if Symantec Ghost
REM succeeds here**
GOTO FINISH
:PROBLEM
ECHO Symantec Ghost returned with an Error value 1 or higher
ECHO Symantec Ghost operation was not completed successfully
REM **Add any commands required to run if Symantec Ghost
REM fails here **
:FINISH
ECHO Batch File Finished
```

Using the -CRC32 switch

CRC checking works file-by-file with FAT partitions. NTFS partitions are CRC-checked within an image file by each MFT table. It is not possible at present to obtain a list of files failing a CRC check with an NTFS file system. When a CRC file is created for an NTFS partition, only a single CRC value is generated. You can also create a CRC file from an image file and verify it against a disk.

The full syntax for this switch is as follows:

-CRC32,action={create|verify|pcreate|pverify|dcreate|dverify}, src={{disk}|{partition}|{file}},crcfile={file}|{partition},vlist={file},vexcept={file}

The parameters in Table A-7 can be used with the -CRC32 switch.

Table A-7 Parameters for the -CRC32 switches

Parameter	Explanation
create	Create an ASCII CRC32 file from a disk
verify	Verify a disk from a CRC32 file
pcreate	Create an ASCII CRC32 file from a partition
pverify	Verify a partition from an ASCII CRC32 file
dcreate	Create an ASCII CRC32 file from an image file
dverify	Verify an image file from an ASCII CRC32 file
crcfile	ASCII CRC32 file (default=Ghost.crc)
vlist	Verification list file (default=Ghost.ls)
vexcept	Verification exception file (no default)

Examples of -CRC32 usage

This table provides some examples of how you can use the -CRC32 switch.

Table A-8 -CRC32 usage examples

Switch	Function
ghost.exe -fcr	Creates a CRC32 file (called Ghost.crc) while making an image file.
ghost.exe -fcr=d:\test.crc	Creates a CRC32 file (called Test.crc) while making an image file.

Table A-8 -CRC32 usage examples

Switch	Function
ghost.exe -crc32, action=create,src=1,crcfile=ghost.crc	Creates a list of files and CRC32 values for a disk.
ghost.exe -crc32,action=dverify,src= x:dumpfile.gho,crcfile=ghost.crc	Verifies the list against an image file.
ghost.exe -crc32,action=pverify,src= 1:2,crcfile=filename.crc:2	Verifies a partition 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	Creates an ASCII CRC32 file from the primary hard drive. Note that the default disk is the primary drive. The default ASCII CRC32 file is Ghost.crc.
ghost.exe -crc32,action=create,src= 2,crcfile=myfile.txt	Creates an ASCII CRC32 file, Myfile.txt. This example uses disk 2 as the source drive and the output file.
ghost.exe -crc32,action=verify	Verifies the contents of the primary disk against a default ASCII CRC32 file, Ghost.crc (in the current directory). The default disk is the primary drive. The default verification list file is Ghost.ls.
ghost.exe -crc32,action=verify,src= 1,crcfile=myfile.txt,vlist=myfile.out	Verifies the contents of the primary disk, 1, against the CRC32 file, Myfile.txt. Same as previous example, but specifies the disk, CRC file, and list file. This example uses disk 1 as the source drive, Myfile.txt as the ASCII CRC32 file, and Myfile.out as the verification list file.
ghost.exe -crc32,action=verify,src= 1,crcfile=myfile.txt,vlist=myfile.out,vexcept=my file.exc	Verifies the contents of the primary disk against a CRC32 file. Same as above with the inclusion of the EXCEPTION argument that excludes compared files based upon its entries.

Files not checked with CRC

The switch vexcept=filename specifies files that are not checked with CRC. This is normally used to exclude files that are always changed on start up. A sample exception file follows:

[ghost exclusion list]
\PERSONAL\PHONE
[partition:1]
\WINDOWS\COOKIES*.*
\WINDOWS\HISTORY*
\WINDOWS\RECENT*
\WINDOWS\USER.DAT
\WINDOWS\TEMPOR~1\CACHE1*
\WINDOWS\TEMPOR~1\CACHE2*
\WINDOWS\TEMPOR~1\CACHE3*
\WINDOWS\TEMPOR~1\CACHE4*
[partition:2]
****.1**
[end of list]

The exclusion list is case-sensitive; all files should be specified in uppercase. The (*) wildcard symbol follows UNIX rules, and is more powerful than the MS-DOS (*) wildcard. In particular, it matches the (.) character as well as any other character, but other characters can follow the *. Therefore a wildcard of *br* matches any files containing the letters br, such as, Brxyz.txt, Abr.txt, and Abc.dbr.

The specification of \WINDOWS\COOKIES*.* in the previous example means match all files in the \WINDOWS\COOKIES subdirectory that have extensions. To match all files with or without extensions, use WINDOWS\COOKIES*.

Use short file names in exclusion files. Files specified before the first [Partition:x] heading are used to match files in any partition.

A directory of * matches any subdirectory, regardless of nesting. The previous exclusion file matches any file with an extension of .1 in any subdirectory on the second partition. Apart from this, use wildcards for files, not for directories.

Numbering the Virtual Partition

Ghost.exe does not see the Virtual Partition when it runs from the command line. The numbering of the partitions is consistent with the numbering that appears when you run the Ghost.exe user interface.

If you use GDisk to view the disk, the Virtual Partition is displayed with the volume label VPSGHBOOT. Therefore, the partition numbering that you can see in GDisk is not the same as the partition numbering in Ghost.exe.

Appendix B

AI Builder variables, commands and conditions

This chapter includes the following topics:

AutoInstall AI Builder menus

Many of the menu commands in AutoInstall AI Builder are self-explanatory. Table B-1 details the commands that are proprietary to AI Builder.

Table B-1 AI Builder proprietary commands

Command	Description
Build > Build	Compress new files only, and build an installation.
Build > Run	Execute the most recently built installation.
Edit > Rem	Turn the highlighted commands into remarks or REM lines. AI Builder ignores all remark lines when it processes the Configuration file. REM lets you add remarks to the .aic file or prevent a command from executing without erasing the command from the file.
Edit > UnRem	Remove the remark commands.

Commands

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.

The commands are grouped in the left pane of AI Builder under the following headings:

- Base Installation
- Appearance
- Messages & Inputs
- System changes
- Defaults and Calls
- If Conditions

Some of the commands support using variables.

See "Using variables in commands and assigning values" on page 202.

Base Installation

The base installation commands include the following:

- Title
- FirstScreen
- Directory
- File
- WindowsItem
- LastScreen
- UnInstall

Title

Customize the title that appears in the top left pane of the screen when the user receives an installation. You can specify the title and subtitle wording, as well as the font appearance.

FirstScreen

Customize a message that appears at the beginning of the installation, providing additional installation information to the user. Enter the title and caption wording. Use carriage returns for line breaks. AI Builder sizes the width of the message box automatically.

You can also select a bitmap to appear on the left side of the message box. The bitmap should be 125 pixels wide and 275 pixels high. It can have up to 256 colors.

FirstScreen can be used many times.

Directory

Specify the installation path options. Your options include:

- Installing the program in the default directory, as well as an alternate directory. To create a subdirectory in the default directory, use the File command. To create a subdirectory relative to the default directory, use the $DEFAULTDIR$ variable.
- Prompting the user to type an installation path, suggest a path, or prevent the user from changing the installation drive or directory.
- Specifying the minimum disk space required for the installation. AI Builder prompts the user if the system has less than the minimum disk space.
- Displaying additional messages or bitmaps to the user.

File

Specify the files to include in the application image. Identify the directories into which the files are copied.

Each file or directory of files in the installation set needs a File command associated with it. You can create an individual File command for each file, or use wildcards to combine File commands. The order of the File commands determines the order in which files are copied.

Your File options include:

- Including individual files or directories of files.
- Specifying where the installation files are located on the distribution source media. If no value is specified, files are installed from where the installation program was executed. The source function is commonly used to install from a CD-ROM or network drive, or to backup files on the user's system.
- Specifying where to install files. This is not the same as the default directory. The most common use for the Destination box is to create a

subdirectory in the default directory. To install files in the Windows directory or other special directory, enter a variable in the Destination box, such as $WINDIR$, $WINSYSDIR$, $WINTEMPDIR$, $PROGFILESDIR$, $DIRn$, $SOURCEDIR$, $LOCATEDIR$, or $ASKn$. Click System Variable to display a list of variable names.

You can also specify a directory path in the Destination box. For example, c:\ installs the files to the root directory on the C drive. Use \ to install the files on the root of the default directory. Use .. to install files to the directory above the default directory. Only use a path you are sure already exists on the user's system.

- Specifying whether to overwrite a file if it already exists on the user's system. Click Yes to overwrite existing files. Click No to leave existing files intact. You can also choose to ask the user whether to overwrite existing files using the Ask parameter. When you select New, an overwrite occurs only if the existing file is older (based on time/date stamp) than the file in the installation set. If the file is a .vbs, .dll., exe, or .ocx file, the age is based on the internal version number instead of the time/date stamp.
- Selecting the file's DOS attribute after installation: read only, archive, hidden, or system. If you do not select an attribute, the default is to Normal, which allows read/write access.
- Installing a file only if the user selects certain parameters, such as the Group ID.
- Displaying a pop-up message as files are copied. This message remains on the screen until the next file with a Pop ID is specified or until the end of file copying.
- Displaying a bitmap on the left, middle side of the background screen. You can also specify a wave sound.
- The following advanced settings are also available:

Setting	Description
No shrink	Removes the file compression. This is common when the installation files are on a CD-ROM and you want the files to be accessible to the user without using the installation program.
No bind	Prevents combining the specified file with the .exe file, leaving them as independent files that are accessible outside the installation program. If unchecked, the installation program combines all files into a single file and binds it to the installation executable.
No uninstall	Leaves the specified file on the user's system when the user runs the uninstall program.

Setting	Description
Fonts	Installs the file to the font directory and registers it in Windows. This automatically sets up the new font.
Shared	Adds a ShareDLL specification to the file. On installation it registers this file as a shared DLL in the registry key, HKLM\Software\Microsoft\Windows\CurrentVersion\Shared DLLs. Uninstalling this package unregisters this file.
Self-register	Registers the file in the Windows registry during the installation. The file must be an autoregistering file, such as a .dll, .ocx, or .vbx file. If the file does not autoregister, use the Registry command to manually specify the registration parameters.
Temp	Specifies that the file is copied to the Windows temp directory for use during installation. It is removed after installation.

WindowsItem

Select the Windows program group and associated icon.

Your options include:

- Creating a Windows program group.
- Adding, removing or replacing items within a program group. If you add an item that already exists, the Add command keeps the original item, as well as the new item. If you replace an item, only the new one exists. The remove command isn't generally used for installations. You can create a separate configuration file that removes a program group or program group icon. You must specify both the program group and item to remove an item.
- Adding additional command-line entries and the associated working directory that executes when the user runs the program icon.
- Specifying an icon for the program group item, either by file name or index number. If the icon is embedded in a program file, and there are multiple icons in the file, the index number specifies the icon that appears. For example, 1 means the first icon embedded in the program file.

LastScreen

Add a personalized message that appears at the end of the installation. It lets you provide additional installation information to the user.

Your options include:

- Defining a title and caption.
- Specifying text to appear to the user. Use returns for line breaks. AI Builder automatically sizes the width of the message box.
- Specifying a bitmap to appear on the left side of the message box. The bitmap should be 125 pixels wide by 275 pixels high. It can have up to 256 colors.

UnInstall

Specify whether an uninstall program is created for the user. The uninstall program is placed in the default directory and creates a hidden file, Unstall.aic, that captures the changes made during the installation. Successive installations modify the Unstall.aic file so that the uninstall program returns the system to its state before the first installation. You can delete any program groups that were created during the installation. Use the Remove Groups During Uninstall option carefully as some users might select an existing group for the installation or add files to the group after installation.

Appearance

The appearance commands include the following:

- Animation
- IntroScreen
- IntroSound
- ScreenColor
- ScreenGraphic

Animation

Display still or animated pictures during the file copy or search process. The files appear sequentially so that they produce an animated effect.

The bitmaps should be 55 pixels wide by 55 pixels high. They can have up to 256 colors.

IntroScreen

Display a graphic as the installation begins.

Your options include:

- Choosing the bitmap that appears and whether it covers the full screen.
- Specifying how long the bitmap appears on-screen. The user can avoid the bitmap by touching a key.

IntroSound

Specify a sound file to play as installation begins.

ScreenColor

Select the background color for the installation screen. You can select a color for the entire screen, or choose a top and bottom color for a gradient effect.

ScreenGraphic

Display a graphic during installation. You can set the bitmap that appears and its location on the screen.

The ScreenGraphic command is generally used to display company logos. AI Builder automatically makes the bitmap background transparent. If you do not want to use a transparent bitmap, change the upper-left pixel to a different color.

Messages & Inputs

The messages and inputs commands include the following:

- Ask
- Group
- PopMessage
- Prompts
- SetVariable
- ShowReadme

Ask

Prompt the user for input and store it in the $ASKn$ variable. The user can type information or answer a Yes/No question.

Your options include:

- Assigning a numeric value to the $Askn$ variable, where n equals the number you select.
  For example, if you select 3, the variable is $Ask3$. Once you collect input from the user, you can use the $ASKn$ variable with the WinItem, IniFile, AddText, Config, Autoexec, RunAtExit, File, and other commands.
- Using Caption to specify the title that appears on the top border of the dialog box.
- Entering the message the user sees in the Prompt box. Use the Text box to type a more detailed description of the question.
- Using the User Entry and Yes and No buttons to specify whether the user enters information or answers a Yes/No question.
- Entering a suggested value. This information appears in the entry box on the dialog box.
- Using the Yes prompt and No prompt to specify the words that appear on the Yes and No buttons. Yes and No are the defaults, but you can use Agree and Disagree or a combination you choose.
- Entering a text file name to display a message during installation. The Text File Name box is useful for displaying a copyright file or license agreement.
- Selecting a bitmap to appear on the left side of the message box. The bitmap should be 125 pixels wide by 275 pixels high. It can have up to 256 colors.

Group

Provide the user with installation options, such as which files are copied during installation. This command defines the file groups and creates a dialog box detailing the user's choices. It is generally used to provide different installation options, such as adding the program documentation to the complete installation, instead of including only the program files for a light installation.

Your options include:

- Caption: The dialog box title.
- Prompt: The message that instructs the user to select one or more items in the dialog box.
- Selecting whether the options use check boxes or radio buttons. Check boxes let the user select one or more items. They are displayed in a scrollable list. Radio buttons let the user select only one item. You can create up to 24 check boxes and radio buttons, but only the first 8 buttons appear in the dialog

box. If you have a lot of options, you can divide them into subgroups of the original group.

- Selecting a bitmap to display on the left side of the message box. The bitmap should be 125 pixels wide and 275 pixels high. It can have up to 256 colors.
- Entering the name of the selectable item in the Item name box and assigning it an identification number. This number is used by the File command to determine which files are installed. It can also be used in an If statement. You can also set the item to be selected by default. The user can select it or deselect it during installation.
- Text: A more detailed description of the item.
- Item name, Selected, and Text: Repeated so that you can enter multiple items at once.

PopMessage

Display text to the user when the installation is copying files.

Your options include:

- Pop ID: Controls when the message appears during file copying. The Pop ID is set in the File command.
- Selecting a font name and size for the message.
- Typing the text that appears within the pop-up message box.

Prompts

Change the default messages that the user sees during the installation. Click the prompts to apply them to the .aic file.

Option	Description
AutoexecPrompt	Asks the user for permission to change the Autoexec.bat file.
BackPrompt	Defines the word that appears on the Back button. The underline character, when pressed in conjunction with the Alt key, creates a shortcut to the button.
BadDrivePrompt	Appears when the user specifies a drive that is not available. The prompt for drive name is based on the DefaultDir, Dir2, and Dir3 commands.
BrowseButton Prompt	Defines the word that appears on the Browse button.

Option	Description
BrowseCaption Prompt	Defines what appears in the title bar of the Browse dialog box.
BrowseDrivePrompt and BrowseDirPrompt	Defines the drive and directory that appear by default in the Browse dialog box.
CancelPrompt	Defines the word that appears on the Cancel button.
ConfigPrompt	Appears when the Config command is used. It asks the user for permission to change the Config.sys file.
CopyFilePrompt	Defines what appears while the installation copies files to the user's system.
CopyTitlePrompt	Defines the title that appears when files are copied during installation.
FileExistPrompt	Appears when the overwrite=ask parameter is used with the File command.
FileNotFoundPrompt	Appears when a file name specified in the .aic file is not found on the installation disk. This usually occurs when the user inserts the wrong disk in the drive.
FinishPrompt	Defines the word that appears on the Finish button.
IniFilePrompt	Appears when the INIFILE command asks the user for permission to modify an .ini file.
InsertDiskPrompt	Appears when the user is prompted to insert the next disk.
LocatePrompt	Appears when AI Builder is scanning for files on the user's system. It is associated with the Locate command.
NextPrompt	Defines the word that appears on the Next button.
NoAllPrompt	Defaults all answers to No.
NoGroupPrompt	Appears when the BeginGroup command is used and the user has not selected at least one program group.
NoPrompt	Defines the word that appears on the No button.
NoSpacePrompt	Appears when there is not enough disk space on the user's system. It is used in conjunction with the MinDiskSpace command.
OKPrompt	Defines the word that appears on the OK button.
QuitPrompt	Appears when the user clicks Cancel during an installation.

Option	Description
RebootPrompt	Appears when the Reboot command is used. It asks the user for permission to restart the system.
RecoverPrompt	Message that is displayed when an AI package fails to deploy. The message is shown on a message box with Yes/No buttons. Clicking Yes continues package deployment from the point of failure; clicking No starts package deployment from the beginning.
ReplaceFileCaption	Message that is presented to the user to request confirmation of file replacement.
ReplaceLockFile Prompt	Appears when the user's computer needs to be restarted in order to replace files that are open and locked by the system.
UninstallBegin Prompt	Appears when the user runs the uninstall program.
UninstallEndPrompt	Appears when the uninstall program finishes.
UninstallTitlePrompt	Defines the title that appears at the top of the uninstall screen.
WarningCaption	Defines the caption for warning messages.
YesAllPrompt	Defaults all answers to Yes.
YesPrompt	Defines the word that appears on the Yes button.

SetVariable

Create a custom variable name and assign a string value to it. If the value contains all numbers, it is tested as a number instead of a string. The value can be a constant, a system value, or from previous user input. The value is not case sensitive.

This command is commonly used for easier readability, or to give a label to a constant.

ShowReadme

Specify a text file that appears at the conclusion of the installation process.

System changes

The system changes commands include the following:

- AddText
- Autoexec
- Backup
- Config
- Copy
- Delete
- IniFile
- Reboot
- Registry
- Regserver
- Rename
- Shortcut
- NTService
- WinGroup

AddText

Create or edit a text file to include in the installation.

Your options include:

- Creating or modifying a text file.
- Adding text to the specified text file in the indicated position. The position can be a number or string. If you enter a positive number in the Position box, the text is placed the specified number of lines from the top of the text file. Negative entries count up from the bottom of the text file. The text is inserted in the file unless you click Replace.
  If you enter a string, the installation program finds the string in the text file and inserts the specified text below the string or replaces it. You can use a wildcard as the last character.
  For example,
  FILES=*.
  Installation searches for a text line that starts with the string to the left of the asterisk and either adds a line after it or replaces it, depending on the options you select.

Autoexec

Modify the user's Autoexe.bat file. You can use this command multiple times in one application image.

Your options include:

- Adding the default installation path to the user's Autoexec.bat file.
- Adding an additional path to the user's Autoexec.bat file.
- Adding a line to the end of the user's Autoexec.bat file.
- Adding a SHARE command to the file. The /F parameter is the minimum part of the SHARE command. This allocates the specified bytes of memory to hold file sharing information. The /L parameter specifies the minimum number of simultaneous file-region locks. Refer to your operating system documentation for more information.
- Displaying a dialog box to ask the user for permission to make the specified changes.

Backup

Create a backup subdirectory under the default installation directory, $DefaultDir$, and back up any file that will be overwritten during installation. All overwritten files are copied to the backup directory whether or not they were in the same directory originally.

Config

Specify changes to the user's Config.sys file. It is sometimes used to add a device driver that is required by the newly installed software. If AI Builder makes a change to the user's Config.sys file, it creates a backup of the original named Config.bak.

This command can be used multiple times in the .aic file. Your options include:

- Setting the minimum value for the Buffers command in the user's Config.sys file.
- Setting the minimum files value for the Files command in the user's Config.sys file.
- Adding a line to the user's Config.sys file.
- Displaying a dialog box to ask the user for permission to make the specified changes.

Copy

Copy a file from one location to another. This command is often used to make copies of files from one directory on the user's system to another directory.

Your options include:

- The original path and file to be copied.
- The destination, if the destination file already exists. It is overwritten if it is older than the source file.

Delete

Lets you delete a file during the installation. The file can be on the user's system or a part of the installation set.

IniFile

Create or modify an .ini file on the user's system.

Your options include:

- Specifying the .ini file you want to create or modify.
- Entering the section of the file in which the new line will be placed. If the section doesn't already exist, AI Builder creates it.
- Entering the parameter that appears to the left of the equal sign. For example, if the line is HOSTDIR=c:\temp, then HOSTDIR is the Entry parameter.
- Entering the parameter that appears to the right of the equal sign. For example, if the line is HOSTDIR=c:\temp, the c:\temp is the String parameter.
- Adding a line to the .ini file even if a line with the same entry value exists in the section. If Add is unchecked, AI Builder replaces a line with the same entry value with the new line.
- Asking the user for permission to modify the .ini file.

Reboot

Restart the user's system after the installation.

Your options include:

Option	Description
System	Restart the operating system. In Windows 9x/NT, this is equivalent to restarting Windows. In Windows 3.x, it is equivalent to a warm restart. It closes Windows and restarts DOS.
Windows	Restart Windows. In Windows 9x/NT, this is equivalent to stopping all programs and logging off from Windows. In Windows 3.x, it is equivalent to exiting to DOS and restarting Windows.

Registry

Insert, delete, or modify items in the Windows registry. There can be multiple Registry commands in a single .aic file.

Options include entering the name of the registry key that you want to insert, delete, or modify, and then entering the action you want to perform.

Your options include:

Action	Description
Delete	Removes the key from the registry.
New	Adds a key to the registry.
Query	Specifies where in the structure the key and associated values should be stored.

To create a new key or modify the existing key organization, use the new or delete commands.

To add information to the registry, use the New and Query functions. Use the Key command followed by one or more Value statements. Single Key commands and all Value statements begin with the BeginRegistry command and end with EndRegistry.

Regserver

Register a self-registering component, for example, an .ocx or .dll file.

Rename

Rename a file on the user's system or on the installation disks. You specify the existing file name and associated path, and the new file name and path.

Shortcut

Create a shortcut on the user's system.

Your options include:

- Specifying the command-line executable the shortcut invokes, any additional command-line parameters, and the working directory for the command-line arguments.
- Specifying the shortcut name that appears to the user.
- Defining whether the shortcut is visible by all users or just the user currently logged on to the Windows operating system.
- Specifying an icon for the shortcut, either by file name or index number. If the icon is embedded in a program file, and there are multiple icons in the file, the index number specifies the icon that appears. For example, 1 means the first icon embedded in the program file.
- Specifying the size of the window in which the specified executable runs.

NTService

Start or stop a service on a Windows NT system.

Your options include:

- If you stop a service, it stops at the beginning of the installation, before any files are installed.
- If you start a service, it occurs after all of the file commands are executed, so that the service file is in the correct location to be executed.

WinGroup

Let the user choose an existing program group or create a new one. The WinGroup command displays the current Windows program groups so that the user can select from the list or create a new one.

Your options include:

- Entering a default program group name.
- Specifying a message that prompts the user for a Windows group name.

Defaults and Calls

The defaults and calls commands include the following:

- BlankLine
- FontName
- OverWriteFile
- ProgressBar
- Rem
- RunAtStart
- RunAtMiddle
- RunAtExit

BlankLine

Insert a blank line in the .aic file. This has no effect on the execution of the file.

FontName

Enter the font that is used as the default font in dialog boxes. The font is used when no font is specified for the individual dialog boxes.

This command is useful for international users as the default font (MS Sans Serif) does not display some international character sets, such as Japanese and Chinese.

OverWriteFile

Defines what happens when a file in the installation set already exists on the user's system. This command is used when no entry is made in the File command.

Your options include:

Option	Description
No	Leaves existing files intact.
Ask	Asks the user whether to overwrite existing files.
New	Overwrites if the existing file is older (based on time/date stamp) than the file in the installation set. If the file is a .vbs, .dll, exe, or .ocx file, the age is based on the internal version number instead of the time/date stamp.
Yes	Overwrites files.

ProgressBar

Specify the total file size so that the progress bar moves smoothly. If you let AI Builder collect files, compress them, and build the installation, AI Builder already knows this value. You only need this command if you build disks manually.

Rem

Add a remark to the configuration file. The compiler ignores remark lines.

RunAtStart

Run an external program at the beginning of the installation.

Your options include:

- Specifying an .exe, .com, .bat, .pif, or .dll file to execute.
- Entering command-line parameters for the executable files.
- Entering the function that is run from a .dll library, as well as an input variable that is necessary to run the .dll. The $DLLRETURN$ variable uses an integer, unless you add str after the variable. For example, 128, str is an acceptable variable name.
- Specifying whether the .dll returns a value. The default return type is an integer. If your .dll returns a string, check the Function Returns a String option. The string is saved in the $DLLReturnStr$ variable.

RunAtMiddle

Run an external program before file copying.

Your options include:

- Specifying an .exe, .com, .bat, .pif, or .dll file to execute.
- Entering command-line parameters for the executable files.
- Entering the function that is run from a .dll library, as well as an input variable that is necessary to run the .dll. The $DLLRETURN$ variable uses an integer, unless you add str after the variable. For example, 128, str is an acceptable variable name.
- Specifying whether the .dll returns a value. The default return type is an integer. If your .dll returns a string, check the Function Returns a String option. The string is saved in the $DLLReturnStr$ variable.

RunAtExit

Run an external program at the end of the installation.

Your options include:

- Specifying an .exe, .com, .bat, .pif, or .dll file to execute.
- Entering command-line parameters for the executable files.
- Entering the function that is run from a .dll library, as well as an input variable that is necessary to run the .dll. The $DLLRETURN$ variable uses an integer, unless you add str after the variable. For example, 128, str is an acceptable variable name.
- Specifying whether the .dll returns a value. The default return type is an integer. If your .dll returns a string, check the Function Returns a String option. The string is saved in the $DLLReturnStr$ variable.

If Conditions

You can include the following If statements for unattended installations:

- If $ASKn$
- If $SYSn$
- If $variable$
- If CPU()
- If DiskSpace()
- If DOSVer()
- If FileVer()
- If CDROM()
- If Group
- If IsFile()
- If Locate()
- If Memory()
- Else
- EndIf
- ExitMessage
- If Search()
- If SoundCard()

- If Video()
- If WinVer()

If $ASKn$

$ASKn$ values are assigned by collecting user input in response to an Ask command. There are nine variables, $ASK1$ through $ASK9$.

For example:

ASK3: "", prompt="Enter your serial number:"

IF $ASK3$ <> "1B456Q9"

EXITMESSAGE

Invalid serial number - installation terminated

EXIT

ENDIF

The user is prompted to enter a serial number and the response is stored in the variable $ASK3$. The If statement compares the user's value to 1B456Q9. If it isn't the same, the exit message appears and the installation ends.

Refer to the EXITMESSAGE/EXIT command for usage information. The values stored in the $ASKn$ variables are strings and are compared alphabetically. For example, 99 is considered larger than 100 because the first character 9 is larger than the first character 1.

If $SYSn$

Test a condition against the $System$ value.

$SYSTEM$, $SYS2$, and $SYS3$ values are assigned by collecting input that the user enters during the installation program. The user must type a dash (-) in front of the value to assign it to a variable.

Example 1:

If the user enters install -update, the $System$ variable becomes update.

Example 2:

If the user enters setup -d:\network -c:\local -update, the $System$ variable becomes d:\network, $Sys2$ becomes c:\local, and $Sys3$ becomes update.

Example 3:

IF $SYSTEM$ <> open_sesame

EXITMESSAGE

Incorrect password - installation terminated.

EXIT

ENDIF

This example expects the user to enter a password on the command line, such as open_sesame, and checks the entry. If it does not match, installation is aborted.

If $variable$

Test a condition against the $variable$ value. The $variable$ gets its input from the SetVariable command. The value can be tested against a constant or a system variable.

Example 1:

ASK1: "", prompt="What day of the week is today?"

SET day_of_week = "$ASK1$"

IF day_of_week = "Tuesday"

BEGINFIRSTSCREEN

Today is Tuesday. Your installation may proceed.

ENDFIRSTSCREEN

ELSE

EXITMESSAGE

Today is not Tuesday. This installation should be run only on a Tuesday.

EXIT

ENDIF

A text value corresponding to the day of the week had been set earlier in the script with the SETVARIABLE command, as shown. If the day of the week is correct, a short message appears. Otherwise, installation is aborted.

Example 2:

A numeric value can also be checked. If the text value contains all digits, it is assumed to be a number.

Thus

SET A="6"

IF A<"1234"

is true, because the number 6 is less than the number 1234, but

SET A="6a"

IF A<"1234"

is false, because 6 alphabetizes higher than 1.

If CPU()

This command detects the user's system and lets the installation perform differently based on the user's CPU.

Select the comparison (equal to, less than, and so on) and the CPU value from the lists.

If DiskSpace()

The If DiskSpace( ) condition detects the free space on the specified drive, and lets the installation perform differently based on the available space. AI Builder automatically detects available disk space for installing files. Therefore, the If DiskSpace( ) command is usually not needed. You can also specify required space in the DefaultDir/Dirn command.

If DOSVer()

DOSVer() =|>|<|>=|<=|<>value or DOSVER() = range(value1, value2) is a function that returns the version number of the DOS operating system. You may compare against a single value or provide a range to compare against.

Example 1:

IF DOSVer() >= 5

ELSE

EXITMESSAGE

Not compatible with your DOS version - install ended.

EXIT

ENDIF

This example checks for DOS 5.0 or greater on the user's system.

Example 2:

IF DOSVer() = range(3.1,4.9)

ELSE

EXITMESSAGE

Not compatible with your DOS version - install ended.

EXIT

ENDIF

This example checks for at least DOS version 3.1 but less than version 5.0.

If FileVer()

Use the If FileVer( ) condition to check the time stamp or internal version number of a specific file. It is generally used to determine if certain files need to be installed or to determine the version of an application that is currently installed on the user's computer.

If CDROM()

This command detects whether the user's system has a CD-ROM drive.

If Group

GROUP is assigned the value of the file group that the user has selected for installation.

See "Group" on page 180.

For example:

IF GROUP=10, 20

WINITEM: "Zip Finder", "$defaultdir$\zip.exe", "ZIPman"

ENDIF

If the user selects group 10 or 20 (as defined in the Group command), then AI Builder creates a program group and program item. The values are separated by commas and are in an Or relationship. If the user selects a group that matches any of the values provided, then the condition is considered true and AI Builder executes true_commands.

If the user selects the first and third groups (which the administrator assigned to group numbers 10 and 30), then IF GROUP = 10,20 is true because group number 10 is selected.

If IsFile()

If IsFile([path]file name) checks for the existence of a file within a specific directory on the user's system. If the file is found, ISFILE() is assigned the value of true; if the file is not found, then the function is assigned the value of false. The file name parameter is the file to be searched for and the optional path parameter is used to specify a specific drive and directory. You can use variables as the path parameter (for example, $WINDIR$, $SYSTEM$, $SOURCEDIR$, $LOCATEDIR$, and so on).

For example:

IF ISFILE("$WINDIR$\myprog.ini")

RENAME: "$windir$\myprog.ini" "$windir$\myprog.inx"

ENDIF

An existing file, Myprog.ini, is renamed to Myprog.inx, if it exists in the Windows directory on the user's system. You can also use this function to determine if a directory exists by using a \ after the directory name, ISFILE(c:\xyz\), for example.

If Locate()

If Locate(file name, drive/dir) searches the user's system for a specific file. It searches all directories on some or all drives. If the function does not find the specified file, it assigns a value of false. Otherwise, it assigns the value of true and files the $LocateDir$ value with the file path. The file name parameter is the name of the file to be searched for and the optional drive/dir parameter (you can type in any drive letter or directory name) is used to limit the search to a specific drive or directory. The optional local parameter limits the search to all local drives, and the optional network parameter limits the search to all network drives. Note that CD-ROM drives are treated as local or network drives and are searched, which may be a slow process.

For example:

IF LOCATE("zipcode.exe", c)

DEFAULTDIR: "$LOCATEDIR$"

ELSE

DEFAULTDIR: "c:\zipcode"

ENDIF

This example searches the C drive on the user's system for the file Zipcode.exe. If found, the suggested installation directory is set to the directory containing

Zipcode.exe. If it isn't found, the suggested installation directory is set to C:\Zipcode.

If Memory()

If Memory() returns the total memory of the computer.

For example:

IF MEMORY()<2000K

EXITMESSAGE

Not enough memory.

ENDIF

This example checks to see if the computer has 2 MB of RAM and if it does not, it exits.

Else

Create an Else condition within an If statement.

EndIf

The EndIf statement is required to end an If condition.

ExitMessage

Add a message that appears at the end of the installation based on an If condition. Type the title of the message box and the text to appear. Use carriage returns for line breaks. AI Builder automatically sizes the width of the message box. The ExitMessage command is only available within an If statement.

For example:

IF LOCATE("zipcode.exe")

DEFAULTDIR: "$LOCATEDIR$"

ELSE

EXITMESSAGE

A previous version of the software was not found.

You may not install this upgrade.

EXIT

ENDIF

This example checks for a previously installed copy of Zipcode.exe. If it is not found, it displays a message and exits the installation immediately.

Note: If there is only a blank line or single space on the line between EXITMESSAGE and EXIT, the installation terminates silently. A message does not appear and is not required.

If Search()

If Search() searches a text file for the occurrence of a specific text string. It skips the occurrence of the string if it is on a line beginning with skipstring. It searches within the section bracketed by search-after-string and search-before-string. When found, the function returns a true condition for use in the If statement and assigns the variable $SEARCH$ with the numeric value of the line number in which the string was found. It also assigns values to $LEFT$ and $RIGHT$ variables. These two variables contain the text that appears to the left and the right of the string. Most frequently, this function is used with the ADDTEXT command to edit a line in an existing text file.

Example 1:

IF Search("zipcode.exe","c:\Autoexec.bat")

ADDTEXT: "$LEFT$zipcode.exe -USA$RIGHT$", "c:\Autoexec.bat", "$SEARCH$", replace

ENDIF

This example searches the text file C:\Autoexec.bat for the string Zipcode.exe. If it is found, then the parameter -USA is inserted into the line immediately after Zipcode.exe. Any other text in that line, either in front of or following Zipcode.exe, is maintained.

Example 2:

ASK1: "your name", prompt="Please enter your name:"

IF Search("Sir","$sourcedir$\readme.txt")

ADDTEXT: "$LEFT$$ASK1$$RIGHT$", "$defaultdir$\readme.txt", "$SEARCH$", replace

ENDIF

This example prompts the user for a name and assigns the value to $ASK1$. The SEARCH function searches the Readme.txt file that is on the source drive for Sir. The line number in which Sir appears in this text file is assigned to the variable $SEARCH$. The ADDTEXT command locates that line and replaces it with the user's name (as stored in $ASK1$). It restores whatever came before Sir by using $LEFT$, and whatever was to the right of Sir by using $RIGHT$.

Example 3:

IF SEARCH("Drive=","$windir$\pcloan.ini", ";", begin="[Network]", end="[end]")

ADDTEXT: "$LEFT$Drive1=$RIGHT$", "$windir$\pcloan.ini", "$SEARCH$", replace

ENDIF

You can also replace a line in a specific section in an .ini file. This example searches in the section labeled Network for the occurrence of Drive= and substitutes the value Drive1. Note that this example skips any line starting with a semicolon (;).

If SoundCard()

If SoundCard() checks for a sound card on one of the serial ports on the user's system. If a sound card is detected, a value of true is returned.

For example:

IF SOUNDCARD()

FILE: "sound.000", FROM="c:\sound\sound.drv"

ELSE

FILE: "nosound.000", FROM="c:\sound\nosound.drv"

ENDIF

The file Sound.drv is installed if a sound card is detected. Otherwise, it installs the file Nosound.drv.

If Video()

If Video returns three values describing the video display capability of the user's computer: number of colors supported, horizontal resolution, and vertical resolution. Any of the numbers can be omitted.

Example 1:

IF VIDEO() > 3,640,480

FILE: "color.000", FROM="c:\video\color.drv"

ELSE

FILE: "bw.000", FROM="c:\video\bw.drv"

ENDIF

If the user's video capability is greater than 640 horizontal resolution by 480 vertical resolution, and 3 colors, then Color.drv is installed. Otherwise, Bw.drv is installed.

Example 2:

IF VIDEO() > 3

FILE: "color.000", FROM="c:\video\color.drv"

ELSE

FILE: "bw.000", FROM="c:\video\bw.drv"

ENDIF

In this example, only the number of colors is checked.

Example 3:

IF VIDEO() > 640,480

FILE: "color.000", FROM="c:\video\color.drv"

ELSE

FILE: "bw.000", FROM="c:\video\bw.drv"

ENDIF

The example checks the resolution.

If WinVer()

If WinVer() =|>|<|>=|<=|<>value or WinVer() = range(value1, value2) returns the version number of the Windows operating system. This is a Windows only function. You can compare against a single value or provide a range to compare against.

The value of a Window's version is the same as the value defined by Microsoft: 3.1 for Windows 3.1; 3.11 for Windows for Workgroups; 3.5 for Windows NT 3.5; 3.51 for Windows NT 3.51; 3.95 for Windows 95; and 4.0 for Windows NT 4.0.

Example 1:

IF WINVER() >= 3.1

ELSE

EXITMESSAGE

Not compatible with your Windows version - install ended.

EXIT

ENDIF

This example checks whether the user has Windows 3.1 or later installed.

Example 2:

IF WINVER() = range(3.5,3.9)

ELSE

EXITMESSAGE

Not compatible with your Windows version - install ended.

EXIT

ENDIF

This example checks whether the user has at least Windows version 3.5 but less than Windows version 4.0. In other words, it checks to see that the user is running Windows NT 3.5x.

Using variables in commands and assigning values

Many AI Builder commands support using variables. Variables are assigned values based on the user's unique system or input. For example, the $WINSYSDIR$ variable can be used as part of the directory path in several commands. This variable is assigned the value of the Windows system directory. When used with the File command, it lets you install files into the user's Windows system directory, despite the fact that each user may have this directory in a different location.

All of the variable commands are used in conjunction with other commands. Refer to the individual commands for examples and specific applications.

The available variables are as follows:

- $ALLUSERSDIR$
- $ASKn$
- $COMPUTERNAME$
- $CURUSERDIR$
- $DEFAULTDIR$
- $DEFAULTDRIVE$
- $DIRn$
- $DLLRETURN$ and $DLLRETURNSTR$
- $LOCATEDIR$
- $LOCATEDRIVE$
- $MACHINENAME$
- $MODEMCOM$
- $PROGFILESDIR$
- $SEARCH$, $LEFT$, and $RIGHT$
- $SOURCEDIR$
- $SOURCEDRIVE$
- $SYSTEM$, $SYS2$, and $SYS3$
- $Variable$
- $WINDIR$, $WINDRIVE$, $WINSYSDIR$, and $WINTEMPDIR$
- $WINHELPDIR$
- $WINGROUP$

$ALLUSERSDIR$

$ALLUSERSDIR$ is assigned the Common Programs (WinNT) or Programs (Win9x) subdirectory of the All Users directory. The All Users directory is given by the following registry key:

Registry key	Description
WinNT	Common Programs entry in HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer \Shell Folders
Win9x	Programs entry in HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer \Shell Folders

$ASKn$

$ASK1$ through $ASK9$ are assigned values if the ASK1 through ASK9 commands are used, respectively. Each is assigned a value after the user has been prompted for information (see the ASK1 through ASK9 commands).

Common uses include:

- A request for personalization information (such as user name and company) to personalize the installed software.
- A request for a serial number to verify that installation is authorized.

$COMPUTERNAME$

$COMPUTERNAME$ is the NetBIOS name of the computer. This command is identical to $MACHINENAME$.

$CURUSERDIR$

$CURUSERDIR$ is assigned the value of $SystemDir$\Profiles\Username for the currently logged on user. This variable is supported in the Windows NT environment only. It is most commonly used to assign desktop shortcuts, Send To or Start Menu settings, and other entries in the user profile for the currently logged on user only, instead of to the Default User or All Users. This value includes both the disk drive and the directory path. When an install occurs, the value is read from the destination computer's system.

$DEFAULTDIR$

$DEFAULTDIR$ is assigned the value of the primary directory in which the installation occurs. This value includes both the disk drive and the directory path. Typically, the administrator assigns a suggested value using the DEFAULTDIR command and gives the user the option of changing it. The variable is assigned its value after the user has had a chance to change the value so that it accurately reflects where to install the files.

Common uses include:

- Adding the installation directory to the user's PATH.
- Adding a device driver to the Config.sys file.
- Providing the installation directory path to an external executable.

$DEFAULTDRIVE$

$DEFAULTDRIVE$ is assigned the value of the default installation drive, for example, C. This variable is similar to $DEFAULTDIR$. However, it contains the drive value (one letter) only and not the directory value. It is assigned the value after the user enters information in response to the DEFAULTDIR prompt.

$DIRn$

$DIR2$ through $DIR9$ are assigned values if the DIR2 through DIR9 commands are used, respectively. Each is assigned a value after the user is prompted for a path (see the DIR2 through DIR9 commands).

Common uses include:

- Adding the installation directory to the user's PATH.
- Adding a device driver to the Config.sys file.
- Providing the installation directory path to an external executable.

$DLLRETURN$ and $DLLRETURNSTR$

$DLLRETURN$ and $DLLRETURNSTR$ are assigned values when a .dll is executed using the RUNATSTART, RUNATMIDDLE, and RUNATEXIT commands and the executed .dll function generates a return value. Many .dlls do not generate return values. If the return value from the .dll is a string instead of a number, the returned string is stored in the variable $DLLRETURNSTR$. To specify that the .dll returns a string, check the RunAtStart, RunAtMiddle, RunAtExit commands.

$LOCATEDIR$

$LOCATEDIR$ is assigned a value with the LOCATE function. LOCATE searches the user's system for a particular file, and $LOCATEDIR$ is assigned the value of the directory path in which the file was located. This value includes both the disk drive and the directory path. Refer to the LOCATE command for more information.

Common uses include:

- Setting the installation directory to the directory in which a previous version of the software is found. For example, you are upgrading and you want to install in the directory in which the user installed the last version of the software.
- Installing a file in another application's directory. For example, you supply a script file for a database program and you want this script to reside in the database program's directory rather than the directory in which your software is being installed.

$LOCATEDRIVE$

$LOCATEDRIVE$ is assigned a value with the LOCATE function. LOCATE searches the user's system for a particular file, and $LOCATEDRIVE$ is assigned the value of the drive in which the file was located. This variable is similar to $LOCATEDIR$. However, it contains the drive value (one letter) only and not the directory value. Refer to the LOCATE command for more information.

$MACHINENAME$

$MACHINENAME$ is assigned a value corresponding to the computer name stored in the user's system. This variable is useful for a silent installation customization.

$MODEMCOM$

$MODEMCOM$ is assigned a value corresponding to the COM port in which the modem was found. Values are 1, 2, 3, and so on. This variable is assigned its value when the FINDMODEM() function is used.

$PROGFILESDIR$

$PROGFILESDIR$ assigns the value of the Program Files directory for a particular computer. This value includes both the disk drive and the directory path. When an install occurs, the value is read from the destination computer's system.

$SEARCH$, $LEFT$, and $RIGHT$

$SEARCH$, $LEFT$, and $RIGHT$ are assigned values using the SEARCH function. The SEARCH function is used within an If statement to search the user's text file for a text string. If the text string is found, the variable $SEARCH$ is assigned the numeric value of the line number in which the string was first found in the user's text file. $LEFT$ is assigned the string value of whatever is on the line in the user's text file to the left of the searched for string. $RIGHT$ is assigned the string value of whatever is on the line in the user's text file to the right of the searched for string. For example, the tenth line in the user's text file is:

c:\dos\share /l:500

Search for share and the three variables are defined as follows:

$SEARCH$ = 10

$LEFT$ = c:\dos

$RIGHT$ = /l:500

These variables (along with the If function and ADDTEXT function) can be used to edit specific lines in text files. Common uses of these variables are:

- Adding parameters to commands currently in Autoexec.bat or Config.sys files without removing existing parameters.
- Editing a line in a database or network control text file.

$SOURCEDIR$

$SOURCEDIR$ is assigned the value of the drive and the directory on which the installation occurs. Usually this is the root directory of the floppy disk drive, which has your installation disk in it. This value includes both the disk drive and the directory path.

Common uses include:

- Passing the location of the original installation disk to an external program invoked with the RunAtExit command.
- Using the variable to remove a file from the installation disk (using the DELETE command) to prevent a second installation.

$SOURCEDRIVE$

$SOURCEDRIVE$ is assigned the value of the drive on which the installation occurs and is usually the floppy disk drive that has your installation disk in it. This variable is similar to $SOURCEDIR$. However, it contains the drive value (one letter) only and not the directory value.

For example, you can use a variable to define a device driver for a CD-ROM drive in an .ini file using the INIFILE command or Config.sys file using the CONFIG command.

$SYSTEM$, $SYS2$, and $SYS3$

$SYSTEM$, $SYS2$, and $SYS3$ are text variables that are assigned the value that the user types on the command line when running the installation program.

For example, if the user types install -update -c:\data -15236, $SYSTEM$ is assigned the value update, $SYS2$ is assigned the value c:\data, and $SYS3$ is assigned the value 15236. If the user types setup -d:\network, $SYSTEM$ is assigned the value d:\network. The dash (-) must precede the text that the user types on the command line. If the dash is omitted, the parameter is interpreted as the .aic file name.

Common uses include:

- Allowing variables to be passed from one installation to a second installation.
- Providing a user-supplied variable for testing with an If statement.

$Variable$

$Variable$ is a custom-named text variable that is equal to a constant or one of the other variables listed. The name between the dollar signs may be up to 20 characters long. Spaces are not allowed, but you can use the underscore (_) and dash (-) as separators. The text value is not case sensitive. If the value of $variable$ contains all digits, the value is evaluated as a number and not text. For example, Tuesday, TUESDAY, and tuesday are all equivalent text values. The variable 6 would be evaluated as less than 1234, but 6a would be evaluated as greater than 1234zzz.

Common uses include:

- Allowing variables meaningful names.
- Providing a user-named variable for testing with an If statement.

$WINDIR$, $WINDRIVE$, $WINSYSDIR$, and $WINTEMPDIR$

$WINDIR$, $WINDRIVE$, $WINSYSDIR$, and $WINTEMPDIR$ are assigned the directory path of the Windows directory, the drive letter on which Windows is located, the Windows system directory, and the Windows temporary directory, respectively.

Common uses with the FILE command include:

- Installing fonts or drivers into the Windows system directory.
- Copying or updating .ini files in the Windows directory.

$WINHELPDIR$

$WINHELPDIR$ is supported in the Windows 95/NT environment only. This variable is assigned the directory path of the Windows Help directory.

For example, copying application Help files with the FILE command into the Windows 95/NT Help directory.

$WINGROUP$

$WINGROUP$ is assigned a value only if the WINGROUP command is used. It is assigned a value after the user has been prompted for the name of a Windows program group into which to install the software.

See "WinGroup" on page 188.

It takes on the value of whatever the user has entered.

For example, installing icons into the specified program group (with the WINITEM command).

Appendix C

Transfer methods and hardware setup

This chapter includes the following topics:

Transfer and hardware requirements

Before using Symantec Ghost, consider the transfer and hardware requirements for the transfer method that you want to use. Ensure that all hard drives are installed correctly and that the BIOS of the system is configured and shows the valid parameters of the drives.

Peer-to-peer connections

Peer-to-peer connections enable Symantec Ghost to run on two computers, copying drives and partitions and using image files between them.

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/minute, Symantec Ghost provides support for the Parallel Technologies universal DirectParallel cable. For peer-to-peer USB port connections, use a USB 1.1 cable that supports a host-to-host connection and a data transfer of approximately 20-30 MB/minute. Symantec Ghost does not support the following:

- Removal/addition of drives while Symantec Ghost is running.
- USB 2.0 peer-to-peer.
- Starting from a USB floppy disk drive.

Due to problems with USB controllers, you should disable BIOS USB keyboard and mouse support when using Symantec Ghost with a USB device. In most cases this is identified as Legacy support in the BIOS.

Symantec Ghost supports one USB 1.1 controller; therefore, you may have to try different ports to execute a Ghost USB peer-to-peer operation.

ECP is the best option for LPT connections. Symantec Ghost must be running under DOS on both computers.

See "USB and DirectParallel cables" on page 215.

TCP/IP connections

Connect the computers with an Ethernet or token ring network interface card and an established network connection, which includes one of the following:

- Crossover cable
- Coaxial or twisted pair cable
- Ethernet or token ring (network interface card)
- Ethernet or MSAU hub

SCSI tape 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 following example:

```
device=C:\scsitape\aspi4dos.sys
```

The driver can be included on a Ghost boot disk with the Standard Ghost Boot Disk option.

Refer to the documentation included with your SCSI tape device for more information.

GhostCasting

For GhostCasting transfers, the following hardware and software are required:

- Ethernet or token ring NIC
- Established network connection
- Optional multicast-enabled router
- Optional BOOTP/DHCP software

Set up the NIC using the manufacturer's installation program and run the NIC test program to check the NIC and cabling.

Removable media

The removable media drive, media, and media drivers for use in DOS are required.

CD-ROM and DVD usage

A CD/DVD writer and blank CD-R/RW or DVD media as suitable by the writer's manufacturers are required.

For more information on image files and CD/DVD writers, see the *Symantec Ghost Implementation Guide*.

Mapped network volume

An installed network interface card and established network connection are required to use a mapped network volume for cloning.

Network file server access within Windows is unavailable when Symantec Ghost runs in DOS. To access a network file server, a DOS network client boot disk must be created. A network client boot disk contains the appropriate network drivers and network client software to allow connection to a network. You can create a boot disk for connecting to a Microsoft network volume or an IBM LAN server.

For more information on creating boot images and disks with the Ghost Boot Wizard, see the *Symantec Ghost Implementation Guide*.

Internal drives

To work with internal drives, ensure that each of the drives is properly configured. This means that if fixed IDE drives are in use, then the jumpers on the drives are set up correctly and the BIOS of the computer is configured for the disk arrangement. Both the source and the destination drives must be free from file corruption and physical hard drive defects.

USB devices

When using a USB device Symantec Ghost supports:

- USB hubs
- Devices that must comply to the Mass Storage Specification, Bulk only

Symantec Ghost does not support the removal or addition of drives while Symantec Ghost is running.

Symantec Ghost does not support using a peer-to-peer USB cable with peer-to-peer drivers from a boot disk and another USB mass storage device on the same controller. Ghost internal USB support only starts when nothing else is controlling the controllers. You can use the switches -forceusb and -nousb to force USB support or disable USB support, but these switches should be used with caution.

See “Command-line switches” on page 147.

FireWire devices

Symantec Ghost does not support the removal or addition of drives while Symantec Ghost is running.

To be supported by Symantec Ghost, the FireWire drive must comply to the following standards:

- Controllers must comply to the 1394 Open Host Controller Interface (OHCI) 1.0 Specification.
- Devices must comply to the Serial Bus Protocol 2 (SBP-2).
- Devices must support SCSI Primary Commands 2.0 (SPC-2).

Third-party device

Install the DOS driver as outlined in the device documentation.

Appendix D

USB and DirectParallel cables

This chapter includes the following topics:

Parallel Technologies cables

Parallel Technologies USB and DirectParallel Universal Fast Cable provide high-speed data transfer and can significantly increase Symantec Ghost performance.

USB and DirectParallel connection cables are available directly from Parallel Technologies as follows:

- http://www.lpt.com
- Telephone:
  - 800.789.4784 (U.S.)
  - 425.869.1119 (International)
- Fax: 253.813.8730
- Email: sales@lpt.com

For peer-to-peer connections, Symantec Ghost supports USB 1.1 cables and USB 1.1 controllers. Some USB 2.0 controllers may work, but Symantec Ghost does not support this configuration.

The USB and DirectParallel connection cables can also be used for high-speed computer-to-computer file transfer and networking in Windows 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
- USB Net Linq Network Bridge cable, model 2K398
- USB Net Linq Network Bridge cable, model 00115G

Appendix E

Wattcp.cfg network configuration file

This chapter includes the following topics:

About the Wattcp.cfg configuration file

The Wattcp.cfg configuration file contains the TCP/IP networking configuration details for Symantec Ghost. The Wattcp.cfg file is not required for the GhostCast Server, Ghostsrv.exe.

Wattcp.cfg is created automatically in the virtual partition and when you create a boot package using the Ghost Boot Wizard.

The Wattcp.cfg file specifies the IP address and the subnet mask of the computer and lets you set other optional network parameters. The file should be located in the current directory where Ghost.exe is started.

Comments in the file start with a semicolon (;). Options are set using the format option = value. For example:

```
receive_mode=5;set receive mode
```

Wattcp.cfg keywords

The keywords in the Wattcp.cfg configuration file are listed in Table E-1.

Table E-1 Wattcp.cfg keywords

Keyword	Description
IP	Specifies the IP address of the local computer. Each computer must have a unique IP address. Symantec Ghost supports the use of DHCP and BOOTP servers and defaults to using them when the IP address is left blank or is invalid. DHCP and BOOTP provide automatic assignment of IP addresses to computers. This lets identical boot disks be used on computers with similar network cards. For example: IP=192.168.100.10
Netmask	Specifies the network IP subnet mask. For example: NETMASK=255.255.255.0
Gateway (optional)	Specifies the IP address of the gateway. This option is required when routers are present on the network and when participating computers are located on different subnets. For example: GATEWAY=192.168.100.1
Bootpto (optional)	Overrides the timeout value in seconds for BOOTP/DHCP. For example: BOOTPTO=60
Receive_Mode (Ethernet only)	Overrides the automatically configured packet driver mode used by Symantec Ghost. The modes, in order of preference, are 4, 5, and 6. The default mode is 4. Some packet drivers misrepresent their abilities in receiving multicast information from the network and allow the use of packet receive modes that they do not support. The packet driver should be set to mode 4 so that it only accepts the multicast packets required. If the packet driver does not support this mode, mode 5 can be used to collect all multicast packets. The final option, mode 6, configures the packet driver to see all packets being sent on the network. For example: RECEIVE_MODE=6

Appendix F

Cloning with Linux

This chapter includes the following topics:

Supported configurations

Symantec Ghost can copy or clone many different Linux distributions. However, Symantec Ghost is sensitive to any possible changes in Ext2/3 file systems and LILO and GRUB specifications. If changes are made to these specifications, Symantec Ghost may no longer support the Linux distribution.

See "Boot configuration" on page 220.

Symantec Ghost is not sensitive to kernel versions. Use the -ial and -nolilo command-line switches to resolve problems with any incompatibilities.

See "Command-line switches" on page 148.

Symantec Ghost copies or clones any x86-based Linux system with full support for Ext2/3 file systems (type 0x83) containing 1 KB, 2 KB, or 4 KB block sizes. Other file systems, such as ReiserFS, are cloned on a sector-by-sector basis and cannot be resized during cloning.

Linux systems that use LILO or GRUB as their boot loader in the MBR or in the active Ext2/3 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 copies file systems inside these extended partitions, but restores them as DOS extended partitions. This is not known to cause problems with Linux systems after cloning.

Symantec Ghost does not support Linux if there is no valid boot record in the disk MBR and more than one partition on a disk is installed with LILO or GRUB. If the Linux disk is set up to start from a partition MBR there can be only 1 partition with a LILO or GRUB boot record in its MBR.

Symantec Ghost has been tested with the following versions:

- Red Hat up to version 9.0
- Mandrake up to version 9.1
- SuSE up to version 8.2

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 /etc/lilo.conf file to determine the boot configuration. If this file does not match the boot configuration, Symantec Ghost may be unable to patch LILO during cloning.

Symantec Ghost assumes that GRUB has been installed in the standard /boot/grub directory or /grub in a /boot partition and uses the standard filename /boot/grub/stage 2. Non-standard GRUB installations are not supported.

If a boot loader for Linux other than LILO or GRUB is used, or the preceding conditions are not met, Symantec Ghost clones the system but the new disk probably will not boot. The system should be started from the Linux distribution rescue disk or a floppy boot disk, and the boot loader should be reinstalled by running /sbin/lilo, the GRUB install script, or an equivalent.

Warning: Always have a boot disk available in case of problems starting a Linux system after cloning.

Symantec Ghost utility support

Ghost Explorer substantially supports Ext2/3 file systems within image files, including the restoration, deletion, and addition of files within these file systems. Problems arise when files that have names that are illegal on Windows are manipulated. Ghost Explorer cannot manipulate device files or symbolic links. Sparse files are expanded on restoration, and hard links are broken.

GDisk does not create any Linux file systems or recognize any partitions within a Linux extended partition.

Appendix G

Customizing Symantec Ghost functionality

This chapter includes the following topics:

Introducing customization

Symantec Ghost functionality can be customized. In some situations, the holder of a license may want to provide versions of Symantec Ghost that have some features disabled.

Limiting functionality from the environment file

To limit Symantec Ghost functionality, edit the Symantec Ghost environment file. The environment file includes:

- The licensed user's details
- The maximum number of licensed concurrent users
- Additional product licensing information
- Functionality switches

Table G-1 lists the available switches.

Table G-1 Environment file switches

Switch	Description
LOAD	Loads disk or partition from image file actions
DUMP	Dumps disk or partition to image file actions
WRITE	Stops Symantec Ghost from writing to destination partition or disk
DISK	Performs disk-to-disk and partition-to-partition actions
PEER	Connect via LPT, USB, or TCP/IP peer-to-peer
FPRNT	Creates a fingerprint that is a hidden mark on a cloned drive or partition that includes the following: ■ Process used to create the drive or partition ■ Time the operation was performed ■ Date the operation was performed ■ Disk number
IMGTMO	Sets the maximum age of an image file in days
TIMEOUT	Disables Symantec Ghost until a valid license is reapplied

To limit 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 with switchname=n in the bound executable.
3. Ensure that the Ghost.env file is in the same directory as Ghost.exe.
4. Run Symantec Ghost using the following command:
   C:\ghost> ghost.exe
5. If you have an environment file with a name other than Ghost.env, at the command line, run Symantec Ghost with the following switch and your environment file name:
   C:\ghost> ghost.exe -#e=filename.env

Examples of customized functionality

The next two sections describe examples of how system administrators can customize functionality for end users of Symantec Ghost.

Image file restoration only

A company may have 100 laptops in use by its sales staff, with the IT system administrator controlling the organization and maintenance of these laptops. Each laptop in use could include a copy of Symantec Ghost and a model image file burned on a CD-ROM for fast system restoration by the user. The system administrator can configure the Symantec Ghost edition that is burned onto the CD-ROM to enable only image file restoration, thus removing the possibility of end users attempting to use other Symantec Ghost functions.

Enabling image file restoration only

The administrator's version of Symantec Ghost has all of the options available after binding the original environment file. The CD-ROM version of Symantec Ghost is activated with:

Switches: load=y,dump=n,disk=n,peer=n
KeyNum: 12345
License: BM-512
MaxUsers: 10
Name: ABC Inc
Address1: 200 John Wayne Blvd.
Address2: Irvine, CA 91024

Backup tool only

Symantec Ghost can be used as a backup tool. In the example above, it may be advisable to disable the load option so that image file creation procedures can be carried out without the possibility of users accidentally overwriting their local drives. Restoration would require the availability of another executable, or the use of Ghost Explorer.

You can use Symantec Ghost as a backup tool with the following switches:

load=n,dump=y,disk=n,peer=n

OEM version of Symantec Ghost

Symantec Ghost can be further customized for OEM customers. Contact Symantec Sales for more information about this version.

Appendix H

Adding DOS drivers to the Ghost Boot Wizard

This chapter includes the following topics:

About adding DOS drivers

The process described here details how to add DOS drivers to the Ghost Boot Wizard. You can create a boot disk that supports network interface cards (NICs) that are not currently available in Symantec Ghost.

For more information, see the Ghost Boot Wizard chapter in the *Symantec Ghost Implementation Guide*.

The following is an overview of the process for adding DOS drivers to the Ghost Boot Wizard:

- Download the driver from the manufacturer's Web site.
- Make a driver template.
- Get the PCI information.

Downloading the driver from the manufacturer's Web site

Download the latest drivers from the NIC manufacturer.

To download drivers from the manufacturer's Web site

1. Go to the manufacturer's Web site.
   Use a search engine if the name is not obvious. Once you have found the Web site there is usually a section titled Support or Driver downloads.
2. Download the driver archive.
   Often there is more than one archive for a card. If you have a choice, then download the archive for DOS, and the archive for Windows. The SCO, Linux and NetWare drivers are not required.
3. Unpack the archive into a directory.
   The archives are usually self-extracting.
4. Read Readme.txt from the archive to see which drivers are included.
   All cards should come with NDIS drivers, and some cards also have packet drivers.

Making a driver template

The second step in the process is to create a driver template.

Make a driver template

When you make a driver template in the Ghost Boot Wizard, the setup boxes may be automatically completed. If this does not happen you must manually complete the boxes.

To start creating a driver template

1. On the Windows taskbar, click **Start** > **Programs** > **Symantec Ghost** > **Ghost Boot Wizard**.
2. In the Ghost Boot Wizard window, click **Network Boot Disk**.
3. Click **Next**.
4. Select one of the following:
   - Add: Add a new template.
   - Modify: Change an existing template.
5. Click **NDIS2 Driver**.

6 Click **OK**.

7 On the NDIS Driver tab, click **Setup**.

8 Select the folder that holds the NDIS2 driver that you previously downloaded.
The NDIS2 driver is usually in a subdirectory called ndis\dos. If this directory does not exist, the NDIS driver will be in a directory with a similar name.

9 Click **OK**.
All boxes in the dialog box are automatically completed. If this is not successful, then you must complete the details.

10 Click **OK**.

To complete details on the NDIS driver tab

1 On the NDIS driver tab, click **Browse**.

2 Find the NDIS2 driver file.

3 Open Windows Explorer.

4 In the NDIS2 driver file directory, use Notepad to open Protocol.ini.
The Protocol.ini file looks similar to this:

```
;Module description for Adaptec 69XX Ethernet PCI Adapter Family
; DriverName       = EMPCI$
;
; Optional Parameters :
;
;   NetAddress       = "000000000000"
;   MaxTransmits     = 1 - 8
;   MaxReceives      = 1 - 8
```

5 Copy the text that follows Drivername =.
In the above example, you would copy the text EMPCI$. Ensure that you maintain the case.

6 Click **OK**.
If the template is new then rename it.
The standard convention for naming a template is <Manufacturer><Name of card>. Readme.txt usually lists the cards with which the driver can be used, so name the template to reflect this.
For example, Adaptec 69XX Ethernet PCI Adapter Family.

Getting the PCI information

The Ghost Boot Wizard and the Symantec Ghost Console require PCI information. It can be accessed only by manually opening the hidden Ghost Boot Wizard template.

To get the PCI information

1. Press **Control** on the keyboard and select the copyright message on the first page of the Ghost Boot Wizard.
   The folder in which the templates are stored appears.
2. Open Windows Explorer, and open the folder containing the templates.
   Ensure that you can view hidden files.
3. Double-click **Mcassist.cfg**.
   The contents of Mcassist.cfg looks similar to this:

```
# This file is used by the Ghost Boot Wizard.
# You should not attempt to edit this file yourself
DRIVER-TYPE = NDIS
DRIVER-NAME = El90x.dos
NDIS-NAME = EL90X$
RECEIVE-MODE = 0
PCI-TAG = 10B7 9000 : 3C900-TPO Fast Ethernet$
PCI-TAG = 10B7 9001 : 3C900-Combo Fast Etherlink$
```

4. In Notepad open the Windows 95 driver configuration file downloaded from the manufacturer's Web site. This is called <name of driver>.inf and is usually in its own directory.
   Find the lines that look similar to the following:

```
[HP]
%en1207d.DeviceDesc%=en1207d.ndi,PCI\VEN_1113&
DEV_1211&SUBSYS_1207103C
%en1207d.DeviceDesc%=en1207d.ndi,PCI\VEN_1113&DEV_1211&
SUBSYS_9207103C
```

5. Copy the PCI vendor ID and the PCI Device ID.
   These are stored as 4-digit hexadecimal numbers. In the example above, the correct numbers follow VEN_ and &DEV_, namely 1113 and 1211.

6 Add a new line to Mcassist.cfg that reads as follows:

```
PCI-TAG = <vendor ID> <device ID> : <name of card>$
```

In this example, both lines in the Windows configuration file are the same. Only one line is added to Mcassist.cfg.

For example,

```
PCI-TAG = 1113 1211 : HP EN1207D-TX PCI Fast Ethernet Adapter$
```

7 Save **Mcassist.cfg**.

8 Restart the Ghost Boot Wizard.

Appendix I

Installing Symantec Ghost from the command line

This chapter includes the following topics:

Choosing an interface type for installation

Microsoft Windows Installer lets you choose the interface that you 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.

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 from 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. Table I-1 lists the syntax for this installation.

Table I-1 Basic installation syntax

Installation package	Syntax
Symantec Ghost Console	msiexec /i “<path to msi package>\Symantec Ghost.msi” /qb
Standard Tools AutoInstall	msiexec /i “<path to msi package>\Symantec Ghost.msi” /qb GHOSTINSTALLTYPE=“xxxxxxx” where xxxxxxx is one of the following: ■ Server Tools = Standard Tools only ■ AutoInstall = AutoInstall
Console client	msiexec /i “<path to msi package>\Client.msi” /qb
Configuration client (standalone)	msiexec /i “<path to msi package>\Client.msi” /qb GHOSTINSTALLTYPE=“Configuration”

- The Silent interface mode does not show any dialog boxes or error messages. If you alter any default settings, you must pass this information through as parameters from the command line. To install a component of Symantec Ghost, use the syntax in Table I-1, but with the switch /q, not /qb. For example, to install Symantec Ghost Console, the syntax is:
msiexec /i "c:\temp\Symantec Ghost.msi" /q

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. You cannot install a client package using this mode. The syntax for this installation is:
msiexec /j “<path to msi package>\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 lets users with access to the network location install Symantec Ghost from this location. This installation requires administrative privileges. The syntax for this installation is as follows:
  msiexec /a "<path to msi package>\"installation package".msi"
- The Repair installation lets you repair the current installation. It is accessed once Symantec Ghost is installed on your computer. You can activate this by using Add/Remove Programs in the Control Panel. You can also run this mode from the command line. The syntax for this installation is as follows:
  msiexec /f "<path to msi package>\ "installation package".msi"
  The switch /fa reinstalls all files, /fu rewrites all required user registry entries, and /fs overwrites any existing shortcuts.
  The /f switch reinstalls all required files, registry entries, and shortcuts, but it ignores any property values entered in the command line.
- The Modify installation mode lets you change the user's current configuration. To do this, use Add/Remove Programs in the Control Panel. On Windows 2000/XP, click Change. You cannot use this mode for a client package.

Installing from the command line

You can specify parameters when installing Symantec Ghost from the command line by setting installer properties. The syntax for these properties is as follows:

msiexec /i "c:\temp\Symantec Ghost.msi" /q PROPERTY = VALUE

The property name must be in uppercase, and the value is case-sensitive.

In Windows 2000/XP, Msiexec.exe is in the path by default, so it can be called from any directory. On Windows NT computers with Microsoft Installer 2.0 installed, Msiexec.exe is in the path by default. On Windows 9x computers, 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 not running Windows XP and you do not have Windows Installer version 2 installed, then the installation must be performed through a setup file. Setup.exe and ClientSetup.exe are located in the same directory as the installation package.

If you are installing in Administrative mode, you do not 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.

An error file, Ghmsierr.txt, is generated in the Windows System folder if the installation fails.

When installing the Symantec Ghost Console, you must set company name and email address in the command line, or the installation fails. When installing Standard Tools or AutoInstall these properties are optional.

Table I-2 shows the package properties that can be set from the command line when installing one of these components.

Table I-2 Symantec Ghost package properties

Property	Default value	Description
INSTALLDIR	Program files\Symantec\Ghost	Destination directory.
USERNAME	Registered user	User name.
COMPANYNAME	Registered company	Company name.
EMAILADDRESS	No default	Email address.
GHOSTINSTALLTYPE	Server	Installs one of the following: ■ Symantec Ghost Console ■ Standard Tools ■ AutoInstall
LICENSECERTIFICATE		License certificate number. 10 digits.
GHOSTNGSERVERUSERNAME	GHOST_<Registered machine name>	Configuration Server user name.
GHOSTNGSERVERPASSWORD	GHOST_<Registered machine name>	Configuration Server password.

Table I-3 shows the package properties that can be set from the command line when you install a client.

Table I-3 Client package properties

Property	Default value	Description
GHOSTCONSOLESERVERNAME	No default	Symantec Ghost Console
INSTALLDIR	Program files\Symantec\Ghost	Destination directory
GHOSTINSTALLTYPE	Client	Installs one of the following: ■ Console client ■ Configuration client (Standalone)

Table I-4 contains the switches that can be used with Setup.exe and ClientSetup.exe.

Table I-4 Setup.exe switches

Switch	Description
/a	Runs installation in Administrative installation mode.
/s	Runs installation in Silent installation mode.
/x	Uninstalls the application.
/v	Passes the parameters to the installation. All of the parameters must be enclosed in quotation marks and the opening quotation mark must immediately follow the /v switch. Any other quotation marks must be preceded by a backslash.

The following command line installs Symantec Ghost in a specified folder, registering Symantec Ghost with the user name in silent mode:

setup.exe /v"USERNAME=\"Me\" INSTALLDIR=\"c:\temp\" /qn"

Uninstalling from the command line

You can uninstall Symantec Ghost from the command line using Microsoft Installer.

To uninstall Symantec Ghost from the command line

- At the command prompt, type the following command:
  Msiexec /x "<path to msi package> \msipackagename.msi" [/q or /qb]
  The switches /q and /qb are optional.
  See "Installing from the command line" on page 235.

Appendix J

Troubleshooting

This chapter includes the following topics:

Ghost.exe error messages

A Symantec Ghost error message consists of an error number and a description.

A Ghosterr.txt file is generated when an abort error occurs.

See "Diagnostics" on page 253.

More information about Ghost.exe error messages is available on the Symantec Ghost Technical Support Web site:

www.symantec.com/techsupp

See "Technical support" on page 3.

Table J-1 details some error messages that you may encounter.

Table J-1 Error messages

Error code	Description
8006, 8008	The trial period of the evaluation has expired. Visit the Symantec Web site at http://www.symantec.com for details on how to purchase Symantec Ghost.
10030	Symantec Ghost was unable to communicate with the GhostCast Server. Check that the GhostCast session name is correct, and the GhostCast Server is ready to accept clients.
10098	The partition number must be included in the command-line switches. See "Command-line switches" on page 148.
10010	Incorrect path/file syntax. Ensure that the path and file name are correct. Also make sure that you have the proper user rights to read or create the image file.
19906	Symantec Ghost was unable to establish a connection with the GhostCast Server. See "About the Wattcp.cfg configuration file" on page 217.
19910, 20070	No packet driver was found. See Table J-4, "Symantec GhostCast errors," on page 244.
19913	Cannot find the BOOTP/DHCP server. Ensure that the computer is connected to the network and that a BOOTP or DHCP server is set up for this subnet.
19916	Duplicate IP address detected. An IP address has been allocated that is already in use.
19900	The GhostCast session is set up incorrectly. Ensure that the TCP/IP settings are correct.
CDR101: Not ready reading drive X, Abort, Retry, Fail	A system error message. This error is not caused by Symantec Ghost. It is caused by malfunctioning hardware or software configurations. The image file on the CD is not readable. To verify this, go into DOS and copy the image file off of the CD-ROM using copy verification, copy /v.

Ghost32.exe error

If you start Ghost32.exe when writing to a CD using Nero, the write operation fails.

Symantec Ghost Console errors

If a task to restore a backup fails and your backups are stored in a mapped network location, ensure that the network connection is still available.

Table J-2 details some error messages that you may encounter.

Table J-2 Console error messages

Error code	Description
c0000005	This is a general error message that has more than one cause. You can try one of the following options to help to resolve the problem: ■ Read the Online Knowledge Base article, “Error: "...c0000005..." when using Ghost”: http://service1.symantec.com/support/ghost.nsf/docid/2001071015394825 ■ When the error occurs a description of the error is copied to the clipboard. Paste this error and send it to Symantec Technical Support for help with this problem.
19235	This is a general error message that has more than one cause. Read the Online Knowledge Base article, “Error: "19235 or 19225 - Decompression error" when restoring images to client computers”: http://service1.symantec.com/support/ghost.nsf/docid/1998123009383425

Using dual NIC computers

Symantec Ghost does not support dual or multiple NIC client computers. Using Symantec Ghost with dual NIC computers may cause problems.

The post configuration settings will apply to only one adapter. DOS only works with one adapter. There may be a problem in selecting which adapter to load drivers for.

You can configure Protocol.ini on the Ghost Network Boot Disk to specify which NIC to use.

For more information, see the Online Knowledge Base article “How to use a different NIC on a client computer that has multiple NICs”:

http://service1.symantec.com/support/ghost.nsf/docid/2000031306515725

If you have a client computer with dual or multiple NICs and a static IP address you may get the error message:

Unable to obtain IP address via DHCP

A workaround for this is to edit Wattcp.cfg with the correct IP address. To prevent Wattcp.cfg being overwritten when a task is run, you must save it in the directory in which Ghost is installed, by default:

c:\Program Files\Symantec\Ghost

Using Ghost with NTFS files

There are some errors that may occur when using Ghost with NTFS files.

Table J-3 Errors when using Ghost with NTFS files

Error message	Description
Error 25002 - Unhandled condition encountered: Attr translation will result in corruption of MFT table	This error occurs when Ghost has finished mapping the location of disk clusters used to store data for an NTFS file and determines that it cannot allocate enough space to store those cluster mappings. This situation can occur with very fragmented or compressed NTFS files. Possible workarounds include the following: ■ Defragmenting the source drive before cloning or creating an image. ■ Using the -ntc- switch, which lets Ghost attempt to allocate disk clusters at or near their original location on the source volume. This minimizes the amount of disruption to the cluster mappings and the subsequent space required to store the mappings.
Error 25058 - "Unable to locate enough contiguous free space to load run. Increase the destination partition size or run Ghost with -NTC- switch."	This error occurs when Ghost can not find a large enough free space to store a section of an NTFS file. There may be enough total free space in smaller allocations scattered about the volume to store the contents of the file but, due to the fact that Ghost does not attempt to break up contiguous sections of files as they are cloned, it produces this error. Cloning of volumes with minimal free space and containing large files comprised of a small number of contiguous sections will be particularly vulnerable to this error. Possible workarounds include the following: ■ Defragmenting the source drive before cloning or creating an image. ■ Using the -ntc- switch, which lets Ghost attempt to allocate disk clusters at or near their original location on the source volume. This minimizes the amount of disruption to the cluster mappings and the subsequent space required to store the mappings.

Table J-3 Errors when using Ghost with NTFS files

Error message	Description
Error 24010 - "Encountered BAD used MFT Record - run CHKDSK"	This error can occur when cloning or creating an image from a source NTFS volume. It may be caused by either corruption or by a bad sector on the drive. Possible workarounds include the following: ■ If the file system is corrupted, running CHKDSK /F on the NTFS volume before attempting to clone it again will pick this up. ■ If the problem is due to a bad sector, run Ghost with the -fro switch to force Ghost to read sectors one-by-one if it detects a bad sector during a read of a range of bad sectors.
Error 25030 - "NTFSGetClusterCount failed"	This error can occur when Ghost is cloning or creating an image of an NTFS volume. It is most likely to have been caused by file system corruption. A possible workaround is to do the following: ■ If this is a file system corruption, run CHKDSK /F on the volume.

Symantec GhostCast errors

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

- You have the latest version of Symantec Ghost and the latest version of the Symantec GhostCast Server.
  The latest versions of Symantec Ghost, the Symantec GhostCast Server, and all Symantec Ghost-related utilities are available at:
  http://www.symantec.com/techsupp/files/ghost/ghost.html
- You have the latest drivers for your network card installed.
  The manufacturer of your network card or computer should have the latest drivers available on its Web site.

Table J-4 lists specific answers to GhostCasting errors. Use the solution most closely related to the problem that you are experiencing.

Table J-4 Symantec GhostCast errors

Problem	Solution
When I launch Symantec Ghost, I am unable to select GhostCasting.	Symantec Ghost uses a packet driver or NDIS2 drivers to perform GhostCasting. If Symantec Ghost does not detect a packet driver in memory, or if the packet driver is inappropriate for your network card, the GhostCasting option is not available. You must have a boot disk that loads the appropriate packet driver or NDIS2 drivers for your network card. Use the Ghost Boot Wizard to create a packet driver boot disk. For more information on creating a boot disk with network support and setting up packet drivers, see the *Symantec Ghost Implementation Guide*.
Symantec Ghost times-out after I type a session name.	This is usually caused by a connectivity problem between the server and the client. To determine the source of the problem: ■ Verify the spelling of the session name on both the client and the GhostCast Server. ■ Check all physical connections, including cabling, hubs, routers, switches, and so on for physical problems. ■ Verify that any routers present between the server and the client are configured properly and have GhostCasting enabled. ■ Check the Wattcp.cfg file for a valid IP address and subnet mask if you are using static IP. ■ Confirm that there is a network communication topology problem by connecting the Console and client to a dumb hub or cross over cable and using static IP to try to complete the task. You can also try pinging the IP address of the client computer from the server computer. **To ping the IP address of the client computer** 1 Start the client computer. 2 On the Symantec Ghost main menu, click **GhostCast** and select one of the following: ■ Unicast ■ Direct Broadcast ■ Multicast Do not enter a session name; stop at the dialog box requesting the session name. This will initialize the IP address. 3 Ping the client from the server. If you are not able to ping the client, there is a communication problem and IP packets are not being passed between these computers.

Table J-4 Symantec GhostCast errors

Problem	Solution
When I begin sending data via GhostCasting, the session fails or times out.	Add a RECEIVE_MODE=X value to the Wattcp.cfg file. Add RECEIVE_MODE=5 first, then try 6. See "About the Wattcp.cfg configuration file" on page 217. If you are GhostCasting across routers or switches, you must enable a GhostCasting protocol on these devices. For more information on GhostCast protocols, refer to your router or switch documentation.

Symantec Ghost and legacy network cards

Windows 95 and 98 are plug-and-play operating systems. They reconfigure most network cards if they find an IRQ conflict. Because GhostCasting runs on a DOS level and DOS is not a plug-and-play operating system, IRQ conflicts may arise.

Most newer network cards come with a software configuration utility that automatically checks for IRQ conflicts and reconfigures the card if a conflict exists. Otherwise, you must manually change the IRQ of the network card. Refer to your network adapter manual for more information on changing the IRQ address of your card.

DOS drivers can also have problems detecting the type and speed of your network. A DOS configuration utility that may have been supplied by the network card manufacturer lets you set these explicitly.

Running command-line or scheduled tasks

Normal task logging can be viewed from the Console task log.

For more information on monitoring Symantec Ghost Console activity, see the *Symantec Ghost Implementation Guide*.

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 on creating a backup regime, see the *Symantec Ghost Implementation Guide*.

Problems running Symantec Ghost

Some errors may occur that do not produce an error code.

Network card not found/Card not installed

This error can occur if a driver cannot find a network card installed on your computer. The error can occur when you start your computer with a Ghost boot disk. Check the following:

- Ensure that you selected the correct network card template when you created the Ghost boot disk.
- Ensure that the plug-and-play operating system setting in the BIOS does set up plug-and-play devices.
  Locate the Plug and Play OS setting in the BIOS configuration screens. Some network cards require that this setting be set to No before they function in DOS. See your computer manual for instructions specific to your computer. If the driver still fails to load, set the plug-and-play operating system setting explicitly to Yes and try again.
  Your BIOS may phrase the name of this setting differently; its function is the same.

Cannot start from drive A

If your computer does not check drive A first on startup, use your computer's Setup program to change its settings. The Setup program may be named differently on your computer, for example, BIOS settings or CMOS settings. You may need to refer to the computer manufacturer's documentation for the key sequence to enter the Setup program.

Be careful when you make changes using your computer's Setup program. If you have never used it before, you may want to refer to your computer manufacturer's documentation.

To change your computer's settings

1. Restart your computer.
2. When a message appears telling you the key or keys to press to run Setup, press the appropriate key or keys.
3. Set the Boot Sequence to boot drive A first and drive C second.

Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program's Help system, refer to the documentation that came with your computer, or contact your computer manufacturer.

4 Save the changes, then exit the Setup program.

Windows blue screen

If you are restoring, backing up, or cloning a computer onto another Windows computer with incompatible hardware, you may get a blue screen. To prevent this problem, do not use incompatible hardware, or on Windows 2000/XP use Sysprep when creating the image file.

Try restoring the computer using the -fdsp or -fdsz switch and ensuring the partition sizes are the same on the destination drive as in the image file.

See "Sysprep" on page 101 and "Command-line switches" on page 147.

Missing hibernation file

If the hibernation file is missing, the following message may appear:

"Cannot hibernate because there is no hibernation file or the hibernation file has an error."

Recreate the hibernation files according to the instructions for your Windows operating system.

Getting out of the virtual partition

If your client computer is stuck in the virtual partition, you can use the executable Ngctdos.exe to restart your computer back into Windows.

To restart your client computer back into Windows

1 At the command line, type **ngctdos -hide**

2 Press **Enter**.

Cancelling a Ghost.exe operation

If you start a Ghost.exe operation, you can abort the process by pressing Ctrl+C. Be aware that this leaves the destination image file in an unknown state.

Installing and uninstalling Symantec Ghost

If you are having problems installing or uninstalling Symantec Ghost, providing a log file of the installation or uninstallation assists Technical Support in analyzing the problem.

Add the following to the end of a command line to create a Logfile.txt file in the root directory of drive C: - **/l*v c:\logfile.txt**

See "Installing from the command line" on page 235.

To add logging to the end of a command line for Windows NT/2000/XP installations, use the following command line:

Msiexec.exe /i <install package location> /l*v c:\logfile.txt

Where <install package location> is the path to the installation package that you want to install.

For example,

d:\Install\SymantecGhost.msi, or d:\Install\Client\Client.msi.

Connecting using USB peer-to-peer

If you cannot connect using USB peer-to-peer, then try altering the drivers that are installed. You could also try different ports.

For more information on installing USB peer-to-peer drivers, see the *Symantec Ghost Implementation Guide*.

Writing to or restoring from a recordable CD or DVD

If you are having problems saving a file directly to or restoring from a CD-R/RW or DVD, there are a number of possible solutions.

Supported CD-R/RW and DVD drives

Symantec Ghost supports a large number of CD-R/RW and DVD drives. Check that your drive is listed here:

http://service1.symantec.com/SUPPORT/ghost.nsf/docid/2003081215321125

Inaccessible CD-ROM drive

When writing to a compatible CD-R/RW drive, the drive may not be accessible to Symantec Ghost. To discover whether this is a problem, check Ghosterr.txt, located in the same directory as the Ghost executable.

See "Diagnostics" on page 253.

IDE CD-ROM drives

To see if an IDE CD-R/RW drive is inaccessible to Symantec Ghost, open Ghosterr.txt or the log file.

The IDE sections are named one or more of the following:

- IDE
- IDE for PIO
- IDE for UDMA

If the word Unavailable appears under these headings, then check the following:

- Ensure that the firmware for your CD-R/RW drive is current.
  Check the Web site for the CD-R/RW drive manufacturer for the most current firmware.
- Update the computer BIOS with the latest version, following the computer manufacturer's instructions.
  The computer BIOS may not be enabled to detect the IDE drive.
- Check the controller to which the IDE drive is attached.
  The IDE drive might be attached to a controller that requires a driver for access. Check the documentation for the controller to determine whether you need to load an IDE driver when starting your computer. Drivers may be needed for controllers that are included on the computer's motherboard.
  Reading and writing from a CD-R/RW drive are different processes. You may be able to access a CD-R/RW drive from DOS to read the drive, but not to write to the drive.

SCSI CD-R/RW drives

To see if a SCSI CD-R/RW drive is inaccessible to Symantec Ghost, open Ghosterr.txt or the log file. The SCSI section is named ASPI.

If the word Unavailable appears under the ASPI heading, then check the ASPI files loaded from Config.sys. The following files must be loaded:

- aspi2dos.sys
- aspi4dos.sys

- aspi8dos.sys
- aspi8u2.sys

These drivers can be found in the following directory:

c:\Documents and Settings\All Users\Application Data\Symantec\Ghost\Template\Common

All SCSI controllers require an ASPI driver. The listed ASPI files are sufficient for most SCSI controllers. The controller might require a driver that is usually supplied with the controller. Copy the driver to the bootable floppy disk and edit Config.sys to load the driver. The controller's documentation should include the correct syntax for loading the driver from DOS. If you do not have the driver, then contact the controller's manufacturer.

If the correct ASPI drivers are loaded, then update the computer BIOS and the controller BIOS with the latest versions, following the manufacturer's instructions.

For example, older versions of the BIOS for the Adaptec 2940 controller card are not compatible with Symantec Ghost.

CD-R/RW disc

The CD disc to which you are writing may have a problem. Try the following:

- Use an unformatted CD-RW disc.
  To write an image to a CD-RW disc that you have already used, use the CD-RW utility to wipe all information off the disc, including the file system.
- Try a second disc.
  If you have tried one disc only, then you have not eliminated the possibility of a damaged disc. Try again, using an unused new disc.
- Try a different brand of disc.
  Some CD-R/RW drives do not work with low quality discs or specific manufacturers of discs. Try a different brand.
- Use a standard 650 MB CD-R/RW disc.
  Symantec Ghost or the CD-R/RW drive may have problems with high speed discs or with discs that record more information.

Loading Ghost.exe from the floppy disk drive

If you are loading Ghost.exe from a floppy disk, a problem can be resolved by loading Ghost.exe from a hard drive instead.

For example, if you are creating an image file of the first partition, copy Ghost.exe to the second partition. Edit Autoexec.bat to start Ghost.exe from the second partition as follows:

d:\ghost.exe

Do not load Ghost.exe from the partition that is being cloned.

Outdated computer BIOS

Your computer might have an old BIOS version. Check the manufacturer's Web site for an update. Follow the manufacturer's instructions for updating the BIOS.

Outdated CD-R/RW drive BIOS

The CD-R/RW drive might have an old BIOS version. An update to the BIOS often fixes problems. Check the manufacturer's Web site for an update. Follow the manufacturer's instructions for updating the BIOS.

Using PC-DOS or MS-DOS

If you put PC-DOS system files on the boot disk, replace them with MS-DOS system files. You can choose MS-DOS while creating the boot disk.

For more information on providing MS-DOS, see the *Symantec Ghost Implementation Guide*.

High compression

Try using a lower or no compression when creating the image file.

Using third-party software to write to the CD-R/RW disc

If you are unable to write directly to a CD-R/RW disc using Symantec Ghost, you can create the Ghost image and then use third-party software to write to the CD-R/RW disc.

To write an image to CD using third-party software

1. Create the Ghost image file and save it to a temporary location.
2. Collect and edit the other required files.
3. Use third-party software to save the image file and other required files to the CD-R/RW disk.
4. Do one of the following:
   - Make the CD bootable, including the drivers to let Ghost read the CD.
   - Create a boot disk using the CD/DVD Startup Disk with Ghost option in the Ghost Boot Wizard. This disk will be required when you want to restore the image from the CD.

If you use software to write an image file directly to the CD, you may experience problems when restoring the image file. Software designed to write directly to a CD, such as Adaptec Direct CD, uses a different file format. Therefore the copied files are not recognized by Ghost.

If you are writing directly to a CD using third-party software, use a program that lays out the format of the disc before it writes it, such as Adaptec E-Z CD Creator.

Symantec Ghost does not provide technical support for third-party software, but details on this method can be found in the knowledge base on the Symantec Support Web site.

Restoring from an image spanned over multiple CD/DVDs

Using GhostCast to restoring from an image spanned over multiple CD/DVDs fails because GhostCast cannot find the second Ghost image on the second CD. A GhostCast session cannot be interrupted to prompt for the second CD. The workaround is to copy each of the image files to the same directory, and use GhostCast to restore the image from that directory.

Appendix K

Diagnostics

This chapter includes the following topics:

Hard drive detection and diagnostic information

Symantec Ghost can generate diagnostic reports that outline the hard drive devices detected, other system-related information, and error conditions when they are detected.

View Log

If you are running tasks from the Console, a task log may be generated. This can help in diagnosing problems.

For more information on viewing the task log, see the *Symantec Ghost Implementation Guide*.

Abort error file (Ghosterr.txt)

An error message consists of an error number, a description, and possibly a suggestion of how to remedy the problem.

The Symantec Ghost abort error file includes these details along with additional drive diagnostics and details required to assist Technical Support in diagnosing the cause of the problem.

The Symantec Ghost abort error file is generated when Symantec Ghost detects an erroneous condition that Symantec Ghost is unable to recover from or work around. The Ghosterr.txt file is generated in the current directory. If this location is read-only, the Ghosterr.txt file output location should be redirected.

The location and file name of the abort file can be altered using the -afile=drive:\path\filename command-line switch.

See "Troubleshooting" on page 239.

Creating a full diagnostic statistics dump summary

A full diagnostic statistics dump summary file contains the detected hard disk geometry details along with other Symantec Ghost statistics. The full Symantec Ghost diagnostic statistics dump can be created using the command-line switch -dd. The default statistics dump file name is Ghststat.txt. You can alter the location and file name by adding the -dfile=drive:\path\filename command-line switch.

For example:

ghost.exe -dd -dfile=c:\diagnose\log.txt

Elementary network testing techniques

There are two methods that you can use to test networking functionality:

- Testing TCP/IP functionality
- Generating a GhostCast log file for Technical Support to use in diagnosing problems

Testing TCP/IP functionality

There are several testing utilities available in the Microsoft TCP/IP application suite. Examples are the output of two Windows TCP/IP utilities, Ping.exe and Ipconfig.exe.

The Ping.exe utility shows TCP/IP networking response and can be used to show connectivity between computers. For a mapped network volume connection, a client can ping the server and vice versa to check that they have basic connectivity at any time. For GhostCast connections, Symantec Ghost only responds to a ping request sent from another computer if it is in GhostCast or TCP/IP peer-to-peer mode and running Ghost in that mode.

Ping utilities that do not indicate multicast packets can traverse between two points on a network. This determines that Unicast will work, but not necessarily Multicast or Direct Broadcast. For example, a ping test may indicate successful TCP/IP operation between two computers on differing subnets, while GhostCast packets may not be able to cross due to a nonmulticast-enabled router that separates the subnets.

Pinging a local host shows basic local TCP/IP functionality.

Pinging another computer

The address used in this example identifies the local host on the network.

On the GhostCast Server, a DOS prompt dialog box is run with the following session:

C:\> Ping 192.168.100.3
Pinging [192.168.100.3] with 32 bytes of data:
Reply from 192.168.100.3: bytes=32 time<10ms TTL=128
Reply from 192.168.100.3: bytes=32 time<20ms TTL=128
Reply from 192.168.100.3: bytes=32 time<20ms TTL=128
Reply from 192.168.100.3: bytes=32 time<20ms TTL=128

The outcome of the first command indicates that the client using the IP address 192.168.100.3 received the ping request and replied. This indicates basic TCP/IP operation between the two computers. This does not indicate that multicast packets can traverse between the two computers.

On Windows NT/2000/XP computers run IPconfig to show the Windows IP configuration and the IP address for the local area connection.

On Windows XP/2000 computers you can view the Local area connection Properties page on My Network Places to view the local area connection.

Generating a GhostCast log file

You can generate a GhostCast log file for Technical Support diagnostic purposes. Logging can slow down the GhostCasting process and should be used to assist in diagnosing problems noted during normal use.

The diagnostic levels in order of increasing detail are shown in Table K-1.

Table K-1 Diagnostic levels

Diagnostic level	Description
Error	Reports any unrecoverable error that occurs during the GhostCast session. Use of this level should not affect session performance.
Statistics	Reports all errors and additional statistic information on completion of the session. Use of this level should not affect session performance.
Warning	Reports all statistic level details and includes any additional warning messages. Use of this level may affect session performance.

Table K-1 Diagnostic levels

Diagnostic level	Description
Information	Reports all warning level details and adds additional diagnostic information. Use of this level may affect session performance.
All	Reports all logging messages. Use of this level reduces GhostCast session performance.

Generating a GhostCast Server log file

You can generate a log file while running the Symantec GhostCast Server.

To generate a GhostCast Server log file

1. On the GhostCast Server, on the File menu, click **Options**.
2. 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 box, type the log file location and name.
   - Click **Browse** to select a location for the file.
4. Use the Symantec GhostCast Server as required.
   The Symantec GhostCast Server can be used for normal operation and the log file can be inspected upon completion.

Generating a GhostCast Client log file

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

To generate a GhostCast Client log file

1. Add the logging switch -jl:loglevel = filename, where loglevel specifies the diagnostic reporting level. (E, S, W, I, or A.)
   For example:
   ghost.exe -jl:a=d:\filename
   See "Command-line switches" on page 147.
2. Select a location for the log file other than the drive being written to by Symantec Ghost. It should have sufficient space to create the file.
   For example, to create a GhostCast log file, D:\Logs\Multi.log, to log all information while using GhostCasting in interactive mode:
   ghost.exe -jl:a=d:\logs\multi.log
3. Run Ghost.exe.
4. Connect to the GhostCast Server.

On completion, the log is written to the selected location.

Index

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z