symantec™

Norton Internet Security™ 2003

User's Guide

Norton Internet Security™ 2003 User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 6.0

PN: 10024898

Copyright Notice

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

Standard Template Library

This product utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators.

Trademarks

Symantec, the Symantec logo, Norton Internet Security, Norton Personal Firewall, LiveUpdate, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Rescue Disk is a trademark of Symantec Corporation.

Microsoft, MS-DOS, MSN, Windows and the Windows logo are registered trademarks of Microsoft Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Pentium is a registered trademark of Intel Corporation.

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

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (“SYMANTEC”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS “YOU” OR “YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE “AGREE” OR “YES” BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE “I DO NOT AGREE” OR “NO” BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. LICENSE:

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

YOU MAY:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

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; and

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

YOU MAY NOT:

A. copy the printed documentation which 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 a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. 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 a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

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

3. SIXTY DAY MONEY BACK GUARANTEE:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty (60) day period following the delivery to you of the Software.

4. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL

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

5. DISCLAIMER OF DAMAGES:

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

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

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

6. 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.

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. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

This product utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright • 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright • 1994. Hewlett-Packard Company.

If you're installing Norton Internet Security for the first time

Start here

Determine which file system your computer uses.

1 On your desktop, double-click My Computer, right-click drive C, then click Properties.

? Which file system are you using?

- FAT (Windows 98/Me/2000/XP)
  See "If you use a FAT file system" on page 6.
- NTFS (Windows 2000/XP only)
  See "If you use an NTFS file system" on page 7.

For detailed instructions and an animated Web tutorial that walks you through each step of the process, go to www.service.symantec.com/installtutorial

If you use a FAT file system

Check for viruses that affect installation.

1 **Insert the Norton Internet Security CD into your CD-ROM drive and restart your computer.**

If you do not have a Norton Internet Security CD or cannot start your computer from a CD, create Emergency Disks on another uninfected computer.

See "Create Emergency Disks" on page 30.

2 **Run a full system scan.**

? **Was a virus found?**

- Yes
  Run a virus scan again using the Delete switch.
- No
  See "Finish installation" on page 8.

! **For detailed instructions and an animated Web tutorial that walks you through each step of the process, go to www.service.symantec.com/installtutorial**

If you use an NTFS file system

Check for viruses that affect installation.

Can you establish a connection to the Internet?

- **Yes**
  Go to http://security.symantec.com and follow the on-screen instructions to scan for threats.
- No
  For Windows XP: Go to service.symantec.com
  For Windows 2000: Go to service.symantec.com
  See "Finish installation" on page 8.

Was a virus found?

- Yes
  Write down the name of the virus and go to http://securityresponse.symantec.com to locate specific removal instructions.
- No
  If you have not already done so, install Norton Internet Security.

  See "Finish installation" on page 8.

For detailed instructions and an animated Web tutorial that walks you through each step of the process, go to www.service.symantec.com/installtutorial

Finish installation

After you've checked for viruses, it's safe to install Norton Internet Security.

1. **Uninstall any other antivirus programs on your computer.**

   On your desktop, use the Add/Remove Programs Control Panel to select the program to uninstall.

2. **Close all open programs on your computer including the items running in the Windows system tray.**

3. **Install Norton Internet Security from the Norton Internet Security CD.**
   See "Install Norton Internet Security" on page 31.

? **Did you see the message "Norton Internet Security has been installed successfully"?**

- Yes
  See "After installation" on page 38.
- No
  Write down the error message on the screen and go to http://service.symantec.com for further assistance.

Contents

If you're installing Norton Internet Security for the first time

Start here 5
If you use a FAT file system 6
If you use an NTFS file system 7
Finish installation 8

Chapter 1 Responding to emergencies

If you suspect that you have a virus 17
Respond to virus threats 18
If you think your computer is under attack 18
Recover from an emergency 19
Prevent future problems 20

Chapter 2 About Norton Internet Security

What's new in Norton Internet Security 2003 21
Norton Internet Security features 22
About Norton Personal Firewall 23
About Norton AntiVirus 24

Chapter 3 Installing Norton Internet Security

System requirements 27
Supported email clients 28
Supported instant messenger clients 29
Before installation 29
Prepare your computer 29
Create Emergency Disks 30

Install Norton Internet Security 31
    If the opening screen does not appear 35
Register your software 36
After installation 38
    Restart your computer 38
    Use the Security Assistant 39
If you have Norton SystemWorks installed 45
If you need to uninstall Norton Internet Security 46

Chapter 4 Norton Internet Security basics

Access Norton Internet Security 49
    Access Norton Internet Security from the system tray 50
    Access Norton AntiVirus from the Windows Explorer toolbar 51
Work with Norton Internet Security 52
    Access Norton Internet Security protection features 52
    Use the Security Monitor 53
    Respond to Norton Internet Security alerts 55
    Use Alert Tracker 56
    Check your computer’s vulnerability to attack 58
    Identify the source of communications 58
    Stop Internet communication with Block Traffic 60
Customize Norton Internet Security 60
    About General options 61
    About LiveUpdate options 61
    About Firewall options 62
    About Web Content options 63
    About Email options 64
Customize Norton AntiVirus 65
    About System options 65
    About Internet options 67
    About Other options 68
Password-protect options 68
    Reset options passwords 70
Temporarily disable Norton Internet Security 71
    Temporarily disable Auto-Protect 72
Create Rescue Disks 73
    About Rescue Disks 73
    Create a Rescue Disk set 73
    Test your Rescue Disks 74
    Update your Rescue Disks 74

For more information 75
    Look up glossary terms 75
    Use online Help 75
    Readme file and Release Notes 76
    Use the User's Guide PDFs 77
    About Norton Internet Security on the Web 78
    Explore online tutorials 79
    Subscribe to the Symantec Security Response newsletter 80

Chapter 5 Keeping current with LiveUpdate
About program updates 81
About protection updates 82
About your subscription 82
When you should update 83
    Request an update alert 83
If you run LiveUpdate on an internal network 83
If you can't use LiveUpdate 84
Obtain updates using LiveUpdate 84
Set LiveUpdate to Interactive or Express mode 85
    Turn off Express mode 85
Run LiveUpdate automatically 86

Chapter 6 Controlling access to protected computers
Control how people use your computer 89
    Connect to a network 89
    Enable file and printer sharing 90
    Organize computers into network zones 91
    Identify computers to Norton Internet Security 93
Control how users access the Internet 96
    If you access the Internet via a cable or DSL router 96
    If multiple computers share a single Internet connection 96
    If your ISP uses a proxy server 96
Control how outside users access your network 98
    If you run a Web server 98
    If you run an FTP server 98
    If you run Symantec pcAnywhere 99
    If you run a Virtual Private Network 99

Chapter 7 Guarding against intrusion attempts

How Norton Internet Security protects against network attacks 102
Norton Personal Firewall monitors communications 102
Intrusion Detection analyzes communications 103
Visual Tracking locates attackers 104
Ensure that Norton Personal Firewall and Intrusion Detection are enabled 104
Customize firewall protection 105
Change the Security Level slider 105
Change individual security settings 106
Reset security settings to defaults 108
Customize firewall rules 108
How firewall rules are processed 108
About the default firewall rules 109
Create new firewall rules 110
Manually add a firewall rule 114
Change an existing firewall rule 118
Reset firewall rules to the default settings 119
Customize Intrusion Detection 120
Exclude specific network activity from being monitored 120
Enable or disable AutoBlock 121
Unblock computers 121
Exclude computers from AutoBlock 122
Restrict a blocked computer 122

Chapter 8 Protecting disks, files, and data from viruses

Ensure that protection settings are enabled 125
Manually scan disks, folders, and files 126
Perform a full system scan 127
Scan individual elements 127
If problems are found during a scan 128
Create and use custom scans 128
Run a custom scan 129
Delete a custom scan 129
Schedule scans 130
Schedule a custom scan 130
Edit scheduled scans 131
Delete a scan schedule 132

Chapter 9 What to do if a virus is found

If a virus is found during a scan 134
Review the repair details 134
Use the Repair Wizard 134
If a virus is found by Auto-Protect 135
If you are using Windows 98/98SE/Me 135
If you are using Windows 2000/XP 136
If a virus is found by Script Blocking 137
If a threat is found by Worm Blocking 137
If Inoculation alerts you about a change in system files 138
If you have files in Quarantine 138
If Norton AntiVirus cannot repair a file 140
If your computer does not start properly 141
If you need to use Rescue Disks (Windows 98/98SE/Me) 141
If you need to use Emergency Disks 142
Look up viruses on the Symantec Web site 143
Look up viruses in Norton AntiVirus 143

Chapter 10 Create accounts for multiple users

About Norton Internet Security accounts 145
Create Norton Internet Security accounts 146
Set the startup account 150
Set or change account passwords 150
Assign Norton Internet Security account types to Windows accounts 151
Log on to Norton Internet Security 153
Customize Norton Internet Security accounts 154

Chapter 11 Protecting your privacy

Identify private information to protect 155
Tips on entering private information 156
Privacy Control and SSL 156
Add private information 156
Modify or remove private information 157
Customize Privacy Control 158
Set the Privacy Level 158
Adjust individual Privacy Control settings 159

Chapter 12 Blocking Internet advertisements

How Ad Blocking works 163

Blocking by dimensions 163

Blocking by location 164

Enable or disable Ad Blocking 165

Enable or disable Popup Window Blocking 166

Enable or disable Flash blocking 166

Use the Ad Trashcan 167

Use text strings to identify ads to block or permit 168

How to identify Ad Blocking strings 169

Add an Ad Blocking string 169

Modify or remove an Ad Blocking string 170

Chapter 13 Blocking unwanted email

How Spam Alert works 171

Privacy Control and SSL 172

Enable or disable Spam Alert 172

Create spam filters 173

Customize Spam Alert 176

Spam Alert tips 177

Chapter 14 Protect children with Parental Control

About Parental Control 179

Enable or disable Parental Control 180

Customize Parental Control 181

Restrict Web site access 181

Restrict programs that access the Internet 185

Restrict newsgroup access 187

Chapter 15 Monitoring Norton Internet Security

View the Status & Settings window 192

View the Statistics window 192

Reset information in the Statistics window 193

Review detailed statistics 194

Reset detailed statistics counters 195

Set the statistics displayed in the Detailed Statistics window 195

Keep the Detailed Statistics window visible at all times 196

View Norton Internet Security Logs 196
View the logs 198
Refresh the logs 199
Disable logging 199
Clear the logs 199
Change the size of the logs 200
Adjust the width of a column 201
Print or save logs and statistics 201

Appendix A Troubleshooting Norton Internet Security
Troubleshoot Norton Internet Security problems 204
What is wrong with this Web site? 204
Why can’t I post information online? 206
Why did an email message I sent never arrive? 206
Why won’t a program connect to the Internet? 206
Why doesn’t Norton Internet Security notify me before letting programs access the Internet? 206
Why can’t I print to a shared printer or connect to a computer on my local network? 207
Why can’t I connect to the Internet via my cable modem? 207
Why can’t LiveUpdate get a list of updates? 208
How can a Web site get my browser information? 208
Troubleshoot Norton AntiVirus problems 209
My Rescue Disk does not work 209
The alert tells me to use my Rescue Disks, but I did not create them 209
I cannot start from drive A 210
Auto-Protect does not load when I start my computer 210
I have scanned and removed a virus, but it keeps infecting my files 211
Norton AntiVirus cannot repair my infected files 212
I get an error when testing basic Rescue Disks 212
I can’t receive email messages 213
I can’t send email messages 214

Appendix B About the Internet
How information is transmitted over the Internet 217
About UDP 218
About ICMP 218
About IGMP 218

How Web information is located on the Internet 219
Requesting a page 219
Understanding URLs 220
How ports identify programs on servers 220
Well-known ports 221
How computers are identified on the Internet 222

Appendix C Understanding Internet risks
Risks from hackers 223
The process of a hacker attack 224
Risks from active content 226
Risks from inappropriate content and activities 227
Blocking site and newsgroup categories 227
Restricting access to programs 227
Risks to your privacy 228
Sending private information 228
Understanding cookies 228
Blocking cookies 229
Tracking Internet use 229
Risks from Trojan horses and viruses 230
The likelihood of being attacked 231

Service and support solutions

Glossary

Index

CD Replacement Form

Responding to emergencies

1

If you have an emergency, these procedures can help you find the solution to your problem. Common problems include virus threats and intrusion attempts.

If you suspect that you have a virus

If you have a *virus* on your computer and need to start the computer from an uninfected disk to remove the virus, you can use the Norton Internet Security CD as an Emergency Disk to start the computer and remove the virus. The DOS-based Norton AntiVirus uses the virus definitions from the Norton Internet Security CD, and is not as up-to-date as virus definitions obtained using LiveUpdate.

See "I cannot start from drive A" on page 210.

You might need to change your computer's BIOS Setup options to start from the CD-ROM drive.

To start from the Norton Internet Security CD and scan for viruses

1. Insert the Norton Internet Security CD into the CD-ROM drive.
2. Restart your computer.
   The Emergency program scans your computer and removes viruses.

Respond to virus threats

See "What to do if a virus is found" on page 133.

If you have already installed Norton Internet Security, and Norton AntiVirus finds a virus on your computer, there are three possible resolutions:

- Repair the file.
  This action removes the virus from the file.

See "If you have files in Quarantine" on page 138.

- Quarantine the file.
  This action makes the file inaccessible by any programs other than Norton AntiVirus. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec.
- Delete the file.
  This action removes the virus from your computer by deleting the file that contains the virus. Use this action only if the file cannot be repaired or quarantined.

If you think your computer is under attack

If your computer is behaving unpredictably, and you have determined that the behavior is not due to a virus or a corrupted file, you may be the victim of an Internet attack.

If you suspect that someone is attacking your computer, immediately disconnect your computer from the Internet. If you have not yet installed Norton Internet Security, install it now.

If you have installed Norton Internet Security, you can use its security tools to block the attack, investigate the attacker, and prevent this type of attack in the future.

To block and investigate an attack

See "Stop Internet communication with Block Traffic" on page 60.

1. Open Norton Internet Security.
2. Click **Block Traffic**.
   This immediately stops all incoming and outgoing communication with other computers.
3. If you are using the Security Monitor, click **Security Center**.
4. In the Security Center, click **Statistics**.
5. Click **Attacker Details**.
   Your browser opens the Visual Tracking Web page.

See "Identify the source of communications" on page 58.

6 Use Visual Tracking to identify the IP address of the computer that the attacker used.
You can use this information to report the attack to the ISP that owns the IP address.

See "Restrict a blocked computer" on page 122.

7 To block all future connections from this IP address, add this computer to your Restricted Zone.

If you suspect that the attacker has already compromised your computer, install Norton Internet Security, then visit http://security.symantec.com for tools to repair damage and eradicate any threats that the attacker may have placed on your computer.

Recover from an emergency

Once you've dealt with the problem, you can install Norton Internet Security and perform the following activities.

Action	**Description**
Install Norton Internet Security.	Norton Internet Security can keep your computer safe from future attacks and virus emergencies. See "Installing Norton Internet Security" on page 27.
Update your protection.	After installing, run LiveUpdate to ensure that you have the most updated protection. See "Keeping current with LiveUpdate" on page 81.
Set a virus protection schedule.	Norton AntiVirus can scan your computer regularly to ensure that it is protected. See "Schedule scans" on page 130.
Configure your firewall.	The default installation of Norton Internet Security should provide sufficient protection for most users, but you can customize protection by adjusting firewall settings. See "Customize firewall protection" on page 105.
Periodically review program logs and statistics.	Norton Internet Security maintains extensive logs of all of the actions that it takes to protect your computer. Check these logs occasionally to identify potential problems. See "Monitoring Norton Internet Security" on page 191.

Prevent future problems

See "Understanding Internet risks" on page 223.

Norton Internet Security can protect your computer against most Internet attacks and virus emergencies.

To prepare your computer for emergencies:

- Stay informed about viruses and security risks by visiting the Symantec Security Response *Web site* (securityresponse.symantec.com).
- Keep your *browser* up-to-date. Software publishers release new versions to fix vulnerabilities in their browsers.
- Use *passwords* intelligently. For important information, use complex passwords that include uppercase and lowercase letters, numbers, and symbols. Don't use the same password in multiple places.
- Don't run software if you don't trust the publisher and the source from which you received the software.
- Don't open *email* attachments unless you are expecting an attachment and you trust the sender.
- Be sensible about providing personal information. Many sites ask for more information than they need.
- Review the privacy policies of the sites to which you are considering sending information.
- Tell children never to reveal details about themselves to people they meet via instant messenger programs.
- Back up files regularly and keep copies of the last few backups on hand.

About Norton Internet Security

2

Norton Internet Security is a security suite that protects computers from Internet attacks and viruses, guards your privacy, speeds Web surfing by eliminating ads, and blocks inappropriate Internet content.

What's new in Norton Internet Security 2003

Norton Internet Security 2003 now includes:

- Security Monitor
  Gives you fast access to the most-used Norton Internet Security tools
- Spam Alert
  Helps identify and block unwanted email
- Visual Tracking
  Identifies the source of attacks and other Internet communication
- Password protection
  Provides increased security for Norton Internet Security and Norton AntiVirus options
- Block Traffic
  Lets you immediately stop other computers' ability to communicate with your computer
- Alert Assistant
  Helps you understand alerts and potential security issues
- Log Viewer
  Improved version helps you see all of the actions Norton Internet Security takes to protect your computer

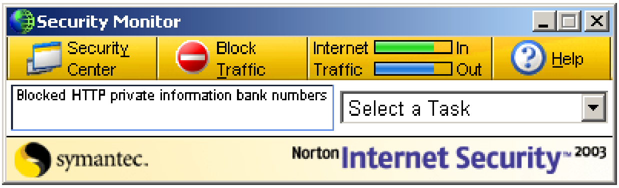
- Privacy Control
  Enhanced version blocks private information in email and instant messages
- Parental Control
  Enhanced version lets parents choose the Web sites, newsgroups, and programs children can use

Norton AntiVirus 2003 contains the following new features:

- Expanded file repair and deletion
  Norton AntiVirus now automatically repairs all repairable files without any interaction with you.
- Instant messenger support and options
  Norton AntiVirus now scans files received by America Online, Yahoo!, and MSN instant messenger programs.
- Worm Blocking
  Norton AntiVirus scans outgoing email attachments for worms and alerts you before sending any *infected files*.

Norton Internet Security features

Norton Internet Security includes Norton Personal Firewall, Norton AntiVirus, and a suite of other security tools that help keep your computer safe. You can get fast access to all Norton Internet Security tools from the new Security Monitor.

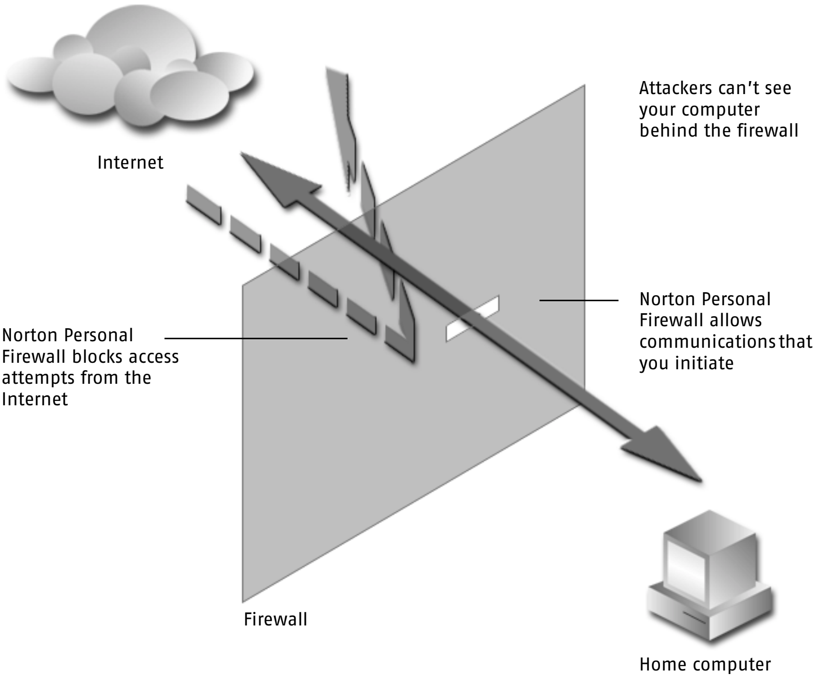


Blocked HTTP private information bank numbers

Internet security can be a complicated topic to understand, so Norton Internet Security now includes the Alert Assistant, which helps you understand security issues, suggests how you can resolve problems, and advises you on avoiding future security problems.

About Norton Personal Firewall

Norton Internet Security includes Norton Personal Firewall, which provides a barrier between your computer and the Internet. A *firewall* prevents unauthorized users from accessing private computers and *networks* connected to the Internet.


Internet
Attackers can't see your computer behind the firewall
Norton Personal Firewall allows communications that you initiate
Norton Personal Firewall blocks access attempts from the Internet
Firewall
Home computer

The Norton Personal Firewall component of Norton Internet Security includes features that prevent unauthorized access to your computer when you are on the Internet, detect possible Internet attacks, protect your personal information, block Internet advertisements to speed your Internet browsing, help eliminate unwanted email messages in your inbox, and protect family members from inappropriate online content.

Norton Internet Security features include:

Intrusion Detection	Intrusion Detection helps keep your computer safe from Internet attacks by scanning each piece of information that enters and exits your computer. If it identifies a potential attack, Intrusion Detection alerts you and automatically blocks the connection that contained the attack. See "Guarding against intrusion attempts" on page 101.
Privacy Control	Privacy Control gives you several levels of control over the kind of information that users can send via the Web, email, and instant messenger programs. You can also control how Privacy Control reacts when Web sites attempt to set and use cookies or learn about your browser. See "Protecting your privacy" on page 155.
Ad Blocking	Ad Blocking speeds up your Web surfing by eliminating banner ads and other slow-loading or intrusive content. Norton Internet Security now also blocks ads made with Macromedia Flash and prevents sites from opening pop-up or pop-under ad windows. See "Blocking Internet advertisements" on page 163.
Spam Alert	Spam (unwanted, sometimes offensive email) is an increasing problem. Spam Alert helps reduce the amount of unwanted email messages that you receive by intelligently filtering incoming messages and clearly marking potential spam. This makes it easy to create filters for your email program that automatically remove spam before you see it. See "Blocking unwanted email" on page 171.
Parental Control	Parental Control helps keep inappropriate Internet content out of the home by letting parents control which Web sites and newsgroups that their children can visit. Parents can also choose the types of Internet applications that children can access, effectively blocking Internet access to chat software or other applications. See "Protect children with Parental Control" on page 179.

About Norton AntiVirus

Norton AntiVirus provides comprehensive virus prevention, detection, and elimination software for your computer. It finds and repairs infected files to keep your data safe and secure. Easy updating of the virus definition service over the Internet keeps Norton AntiVirus prepared for the latest threats.

See "Use the User's Guide PDFs" on page 77.

The *Norton AntiVirus User's Guide* PDF, Nav2003.pdf, includes extensive information about viruses and how they spread.

Norton AntiVirus consists of a memory-resident program, Auto-Protect, and a scanning feature that you can schedule or run manually.

Norton AntiVirus features include:

Virus definition service	Automatically updates your virus definitions. See "Keeping current with LiveUpdate" on page 81.
Bloodhound technology	Detects new and unknown viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data contained in the file. See "What to do if a virus is found" on page 133.
Script Blocking	Detects Visual Basic- and JavaScript-based viruses without the need for specific virus definitions. It monitors the scripts for virus-like behavior and alerts you if it is found. See "What to do if a virus is found" on page 133.
Auto-Protect	Loads into memory when Windows starts, providing constant protection while you work. Checks for viruses every time that you use software programs on your computer, insert floppy disks or other removable media, access the Internet, or use document files that you receive or create. Monitors your computer for any unusual symptoms that may indicate an active virus. See "If a virus is found by Auto-Protect" on page 135.

Installing Norton Internet Security

3

Before installing Norton Internet Security, take a moment to review the system requirements listed in this chapter. Windows 98 and Windows Me users should have several blank 1.44-MB disks available to make Rescue Disks.

System requirements

To use Norton Internet Security, your computer must have one of the following Windows operating systems installed:

- Windows 98, 98SE
- Windows Me
- Windows 2000 Professional
- Windows XP Professional or Windows XP Home Edition

Windows 95 and NT, the server editions of Windows 2000/XP, and the Windows XP 64-bit edition are not supported.

Your computer must also meet the following minimum requirements.

Operating System	Requirements
Windows 98/ 98SE/Me	Intel Pentium processor (or compatible) at 150 MHz or higher 48 MB of RAM (64 MB recommended) 90 MB of available hard disk space (60 MB if you do not install Parental Control) Internet Explorer 5.01 or later (5.5 recommended) CD-ROM or DVD-ROM drive
Windows 2000 Professional	Intel Pentium processor (or compatible) at 150 MHz or higher 64 MB of RAM (96 MB recommended) 90 MB of available hard disk space (60 MB if you do not install Parental Control) Internet Explorer 5.01 or later (5.5 recommended) CD-ROM or DVD-ROM drive
Windows XP Professional or Home Edition	Intel Pentium II processor (or compatible) at 300 MHz or higher 128 MB of RAM 90 MB of available hard disk space (60 MB if you do not install Parental Control) Internet Explorer 5.01 or later (5.5 recommended) CD-ROM or DVD-ROM drive

Supported email clients

Norton Internet Security can scan email messages for private information, spam, and viruses in any POP3-compatible email client, including:

- Microsoft® Outlook® Express 4.0/5.X
- Microsoft Outlook 97/98/2000/XP
- Netscape® Messenger 4.X, Netscape Mail 6.0
- Eudora® Light 3.0, Eudora Pro 4.0, Eudora 5.0

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- POP3s that use SSL (Secure Sockets Layer)
- Web-based email such as Hotmail and Yahoo!
- Lotus Notes mail

Supported instant messenger clients

- AOL Instant Messenger, version 4.3 or later
- MSN Instant Messenger, version 3.6 or later
- Windows Messenger, version 4.0 or later

Before installation

Before you install Norton Internet Security, prepare your computer. If your computer cannot start from a CD, create Emergency Disks.

Prepare your computer

See "If you need to uninstall Norton Internet Security" on page 46.

If you have an older version of Norton Internet Security or Norton AntiVirus, the new version prompts you to remove the older version. If you have a recent version of Norton Internet Security, you can transfer your existing settings to the new version of the program.

You must also uninstall any antivirus programs that are installed on your computer. For more information, see the user documentation that came with the programs.

Quit all other Windows programs before installing Norton Internet Security. Other active programs may interfere with the installation and reduce your protection.

If you're using Windows XP

Windows XP includes a *firewall* that can interfere with Norton Internet Security protection features. You must disable the Windows XP firewall before installing Norton Internet Security.

To disable the Windows XP firewall

1. On the Windows XP taskbar, click **Start** > **Control Panel** > **Network Connections**.
2. If you have created more than one modem or network connection, select the active connection.
3. Click **Network Tasks**.
4. Click **Change settings of this connection**.
5. On the Advanced tab, in the Internet Connection Firewall section, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
6. Click **OK** to close the settings window.
7. Click **OK** to close the Network Tasks window.

Scan for viruses

You should scan your computer for viruses before installing Norton Internet Security. This ensures your computer is protected and that the installation will go smoothly.

See "If you are using the CD as an Emergency Disk" on page 142.

If your computer can start from a CD, you can restart from the Norton Internet Security CD and scan your computer's hard disk for viruses. If your computer cannot start from a CD, you can create Emergency Disks.

The Norton AntiVirus emergency program uses the virus definitions from the Norton Internet Security CD, and is not as up-to-date as virus definitions obtained using LiveUpdate. After installing, you should scan for viruses again.

Create Emergency Disks

See "If you need to use Emergency Disks" on page 142.

Emergency Disks are used to start your computer and scan for viruses in case of a problem. If your computer can start from a CD, you can use the Norton Internet Security CD in place of Emergency Disks and do not need to create them.

If you cannot start your computer from a CD, you can use these instructions to create Emergency Disks on another computer or go to http://www.symantec.com/techsupp/ebd.html and download the Emergency Disk program. Follow the instructions included in the download to create the Emergency Disks.

You will need several formatted 1.44-MB disks.

To create Emergency Disks from the CD

1. Insert the Norton Internet Security CD into the CD-ROM drive.
2. In the Norton Internet Security CD window, click **Browse the CD**.
3. In Windows Explorer, double-click the **Support** folder.
4. Double-click the **Edisk** folder.
5. Double-click **Ned.exe**.
6. In the welcome window, click **OK**.
7. Label the first disk as instructed and insert it into drive A.
8. Click **Yes**.
9. Repeat steps 7 and 8 for the subsequent disks.
10. When the procedure is complete, click **OK**.
11. Remove the final disk from drive A and store the Emergency Disk set in a safe place.

Install Norton Internet Security

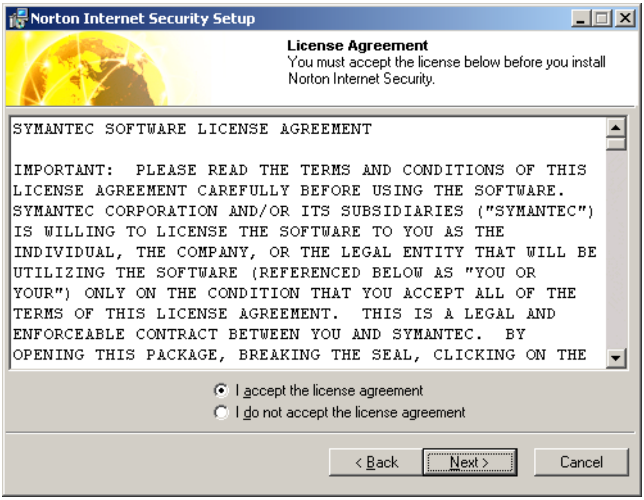
Install Norton Internet Security from the Norton Internet Security CD. Install a copy of Norton Internet Security on each computer that you want to protect.

To install Norton Internet Security

1. Insert the Norton Internet Security CD into the CD-ROM drive.
2. In the Norton Internet Security CD window, click **Install Norton Internet Security**.
   If your computer is not set to automatically run a CD, you must manually open it.
   The first installation window reminds you to close all other Windows programs.

See "If the opening screen does not appear" on page 35.

3 Click **Next**.



License Agreement
You must accept the license below before you install Norton Internet Security.

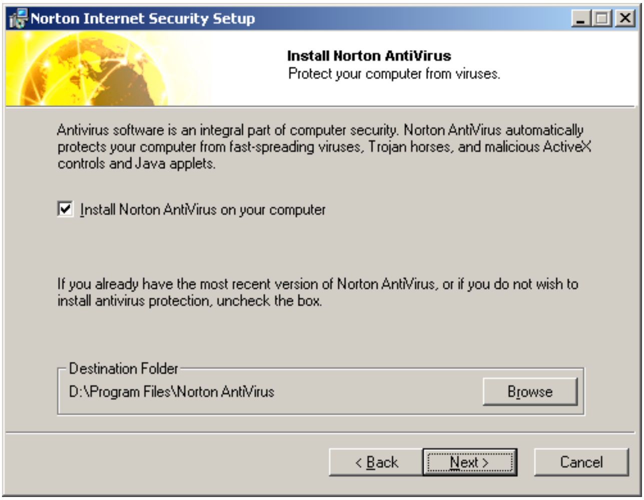
```
SYMANTEC SOFTWARE LICENSE AGREEMENT

IMPORTANT:  PLEASE READ THE TERMS AND CONDITIONS OF THIS
LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC")
IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE
INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE
UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR
YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE
TERMS OF THIS LICENSE AGREEMENT.  THIS IS A LEGAL AND
ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC.  BY
OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE
```

● I accept the license agreement
○ I do not accept the license agreement

4 Read the Licence Agreement, then click **I accept the license agreement**.
If you decline, you cannot continue with the installation.

5 Click **Next**.



Install Norton AntiVirus
Protect your computer from viruses.

Antivirus software is an integral part of computer security. Norton AntiVirus automatically protects your computer from fast-spreading viruses, Trojan horses, and malicious ActiveX controls and Java applets.

☑ Install Norton AntiVirus on your computer

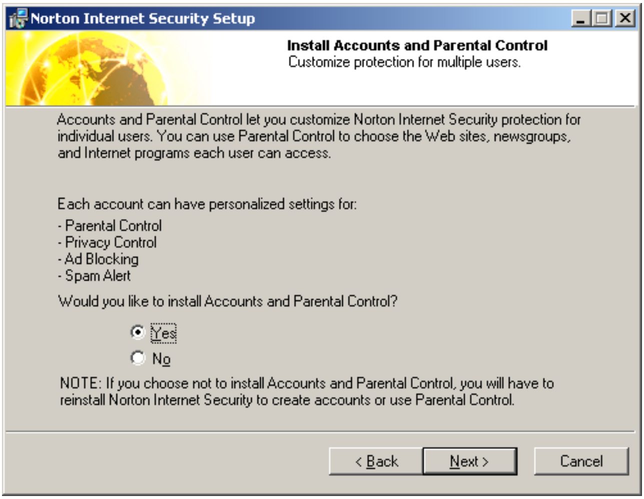
If you already have the most recent version of Norton AntiVirus, or if you do not wish to install antivirus protection, uncheck the box.

Destination Folder
D:\Program Files\Norton AntiVirus

6 To install Norton AntiVirus, check **Install Norton AntiVirus on your computer**, then click **Browse** to specify the location in which you want it installed.

If an updated version of Norton AntiVirus is already on your computer, this window does not appear.

7 Click **Next**.



Install Accounts and Parental Control
Customize protection for multiple users.

Accounts and Parental Control let you customize Norton Internet Security protection for individual users. You can use Parental Control to choose the Web sites, newsgroups, and Internet programs each user can access.

Each account can have personalized settings for:

- Parental Control
- Privacy Control
- Ad Blocking
- Spam Alert

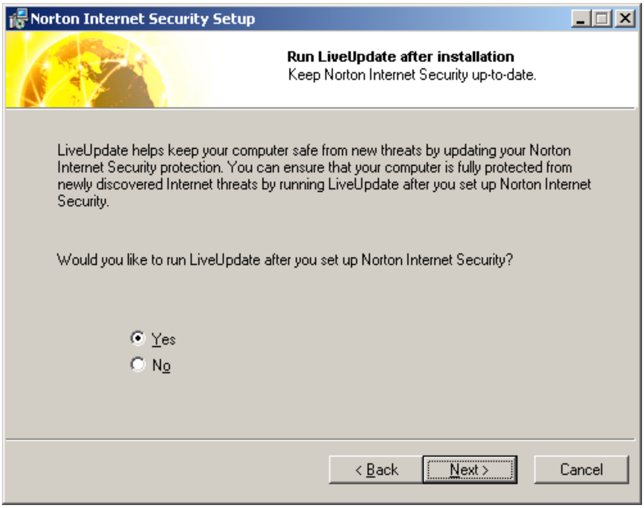
Would you like to install Accounts and Parental Control?

● Yes
○ No

NOTE: If you choose not to install Accounts and Parental Control, you will have to reinstall Norton Internet Security to create accounts or use Parental Control.

8 In the Install Accounts and Parental Control window, select whether you want to install Accounts and Parental Control.
If you do not install these features, you will have to reinstall Norton Internet Security to create accounts or use Parental Control.

9 Click **Next**.



Run LiveUpdate after installation
Keep Norton Internet Security up-to-date.

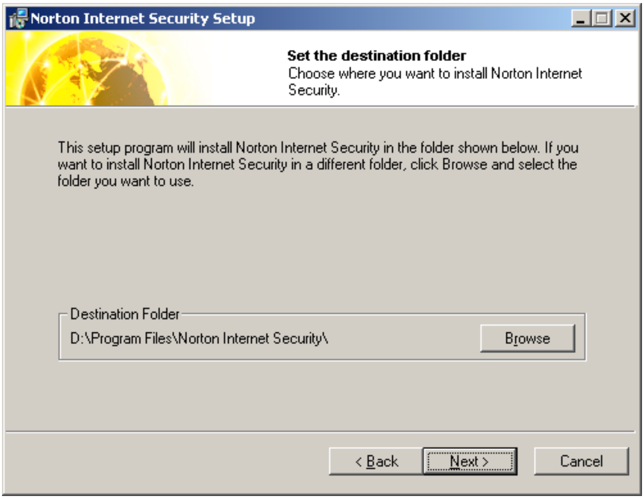
LiveUpdate helps keep your computer safe from new threats by updating your Norton Internet Security protection. You can ensure that your computer is fully protected from newly discovered Internet threats by running LiveUpdate after you set up Norton Internet Security.

Would you like to run LiveUpdate after you set up Norton Internet Security?

● Yes
○ No

10 In the Run LiveUpdate after installation window, select whether you want to run LiveUpdate after the installation is done.

11 Click **Next**.



Set the destination folder

Choose where you want to install Norton Internet Security.

This setup program will install Norton Internet Security in the folder shown below. If you want to install Norton Internet Security in a different folder, click Browse and select the folder you want to use.

Destination Folder

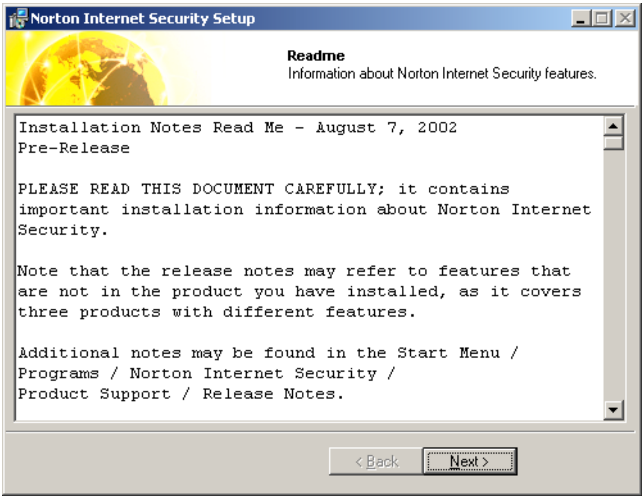
D:\Program Files\Norton Internet Security\

12 Click **Browse** to select a folder into which you want to install Norton Internet Security, if it is other than the default location.

13 Click **Next**.

See "Register your software" on page 36.

14 Click **Next** to begin installing Norton Internet Security.
After Norton Internet Security is installed, the Registration Wizard appears.



Readme
Information about Norton Internet Security features.

```
Installation Notes Read Me - August 7, 2002
Pre-Release

PLEASE READ THIS DOCUMENT CAREFULLY; it contains
important installation information about Norton Internet
Security.

Note that the release notes may refer to features that
are not in the product you have installed, as it covers
three products with different features.

Additional notes may be found in the Start Menu /
Programs / Norton Internet Security /
Product Support / Release Notes.
```

15 Read the readme text, then click **Next**.

16 Click **Finish** to complete the installation.

If the opening screen does not appear

Sometimes a computer's CD-ROM drive does not automatically run a CD.

To start the installation from the Norton Internet Security CD

1 On your desktop, double-click **My Computer**.

2 In the My Computer window, double-click the icon for your CD-ROM drive.

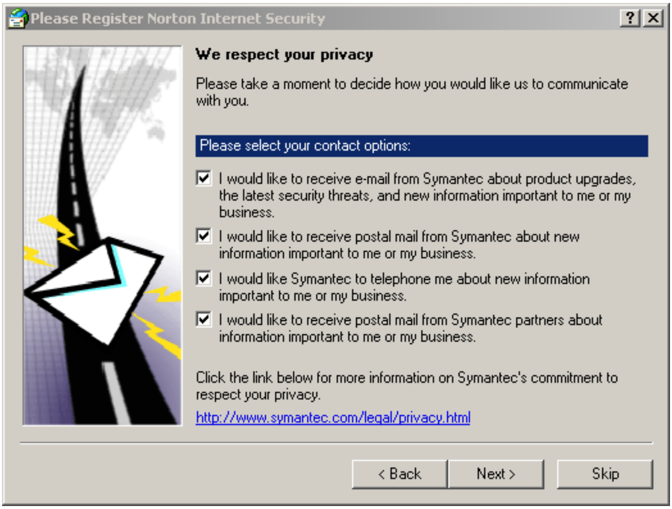
3 In the list of files, double-click **Cdstart.exe**.

Register your software

Use the Registration Wizard to register your software online. If you skip online registration, you can register your software later using the Product Registration option on the Help menu.

To register your software

1 In the first Registration window, select the country from which you are registering and the country in which you live (if different), then click **Next**.



We respect your privacy

Please take a moment to decide how you would like us to communicate with you.

Please select your contact options:

☑ I would like to receive e-mail from Symantec about product upgrades, the latest security threats, and new information important to me or my business.

☑ I would like to receive postal mail from Symantec about new information important to me or my business.

☑ I would like Symantec to telephone me about new information important to me or my business.

☑ I would like to receive postal mail from Symantec partners about information important to me or my business.

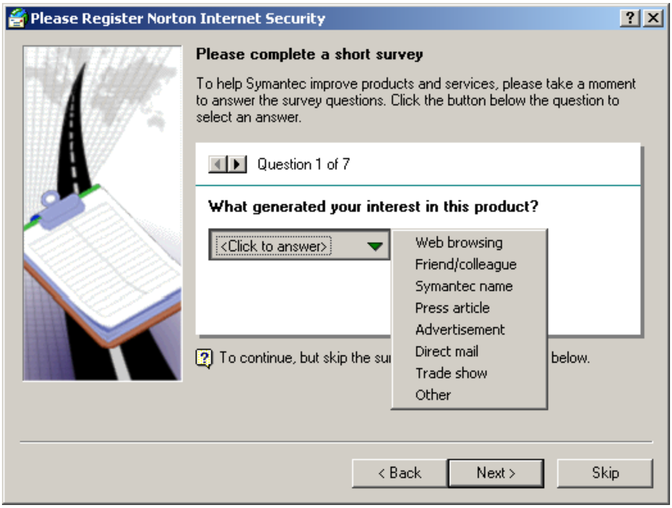
Click the link below for more information on Symantec's commitment to respect your privacy.

http://www.symantec.com/legal/privacy.html

2 If you would like information from Symantec about Norton Internet Security, select the method by which you want to receive that information, then click **Next**.

3 Type your name, then click **Next**.

4 Type your address, then click **Next**.



Please Register Norton Internet Security

Please complete a short survey

To help Symantec improve products and services, please take a moment to answer the survey questions. Click the button below the question to select an answer.

Question 1 of 7

What generated your interest in this product?

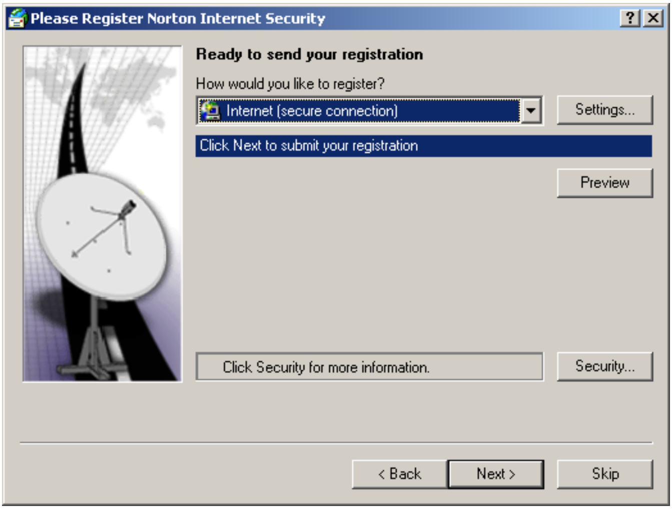
<Click to answer>

- Web browsing
- Friend/colleague
- Symantec name
- Press article
- Advertisement
- Direct mail
- Trade show
- Other

To continue, but skip the su below.

5 Do one of the following:

- Answer the survey questions to help Symantec improve its products and services, then click **Next**.
- Skip the survey by clicking **Next**.



Please Register Norton Internet Security

Ready to send your registration

How would you like to register?

Internet (secure connection)

Click Next to submit your registration

Click Security for more information.

6. Select whether you want to register Norton Internet Security over the Internet or by mail.
   If you want to register by mail, your computer must be connected to a printer that the Registration Wizard can use to print the registration form. If you want to register using the Internet, you must be connected to the Internet.
7. Click **Next**.
8. To get a copy of your registration information for future reference, do one of the following:
   - Write down the serial number.
   - Click **Print**.
9. Click **Next**.
10. Select whether you want to use your existing profile the next time that you register a Symantec product, or type the information as part of registration.
11. Click **Finish**.

After installation

After Norton Internet Security is installed, a prompt appears giving you the option to restart your computer immediately. After restarting, the Security Assistant appears to guide you through the configuration of Norton Internet Security.

Restart your computer

After installation, a prompt appears telling you that you must restart your computer for the updates to take effect.

To restart your computer

❖ In the Installer Information dialog box, click **Yes**.
Configuration of Norton Internet Security is not complete until you restart your computer.

Use the Security Assistant

The Security Assistant helps you quickly configure your Norton Internet Security protection. The Security Assistant is divided into five categories:

- Home Networking
- Program Control
- Privacy Control
- Password Protection
- Parental Control

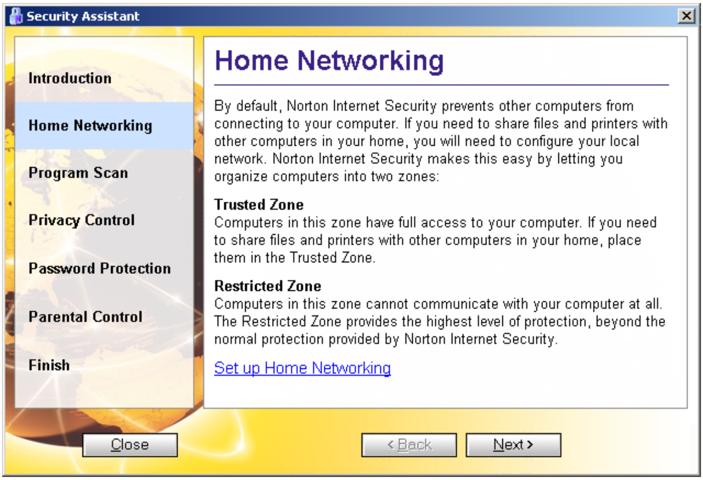
Set up Home Networking

See "Connect to a network" on page 89.

Use Home Networking to identify computers to which you want to grant access to your computer and those to which you want to deny access. The Home Network Wizard can automatically configure your *network* and add computers to your Trusted Zone.

To set up Home Networking

1 In the Security Assistant Roadmap, click **Home Networking**.



Home Networking

By default, Norton Internet Security prevents other computers from connecting to your computer. If you need to share files and printers with other computers in your home, you will need to configure your local network. Norton Internet Security makes this easy by letting you organize computers into two zones:

Trusted Zone
Computers in this zone have full access to your computer. If you need to share files and printers with other computers in your home, place them in the Trusted Zone.

Restricted Zone
Computers in this zone cannot communicate with your computer at all. The Restricted Zone provides the highest level of protection, beyond the normal protection provided by Norton Internet Security.

Set up Home Networking

2 In the Home Networking pane, click **Set up Home Networking**.

3 In the Home Networking Wizard, click **Next**.

4 Follow the on-screen instructions to configure your network.

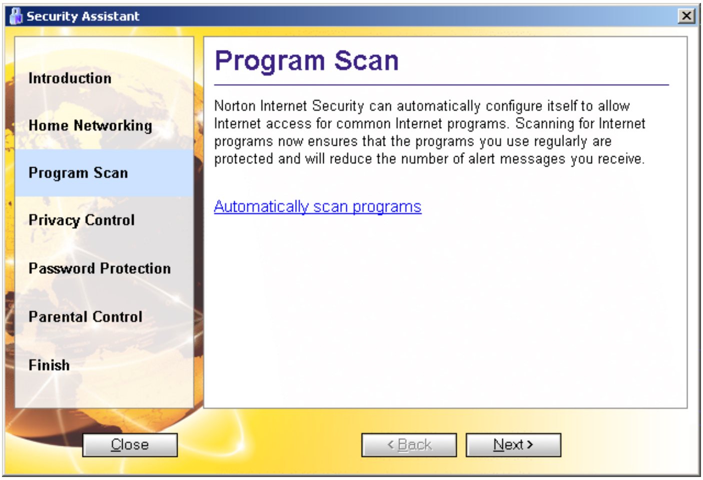
Set up Program Control

See "Scan for Internet-enabled programs" on page 111.

Norton Internet Security can scan your computer for Internet-enabled programs and create access rules for them. When the scan is complete, you can use the results to determine which programs should have access to the Internet and, if desired, adjust their access rules.

To set up Program Control

1 In the Security Assistant Roadmap, click **Program Scan**.

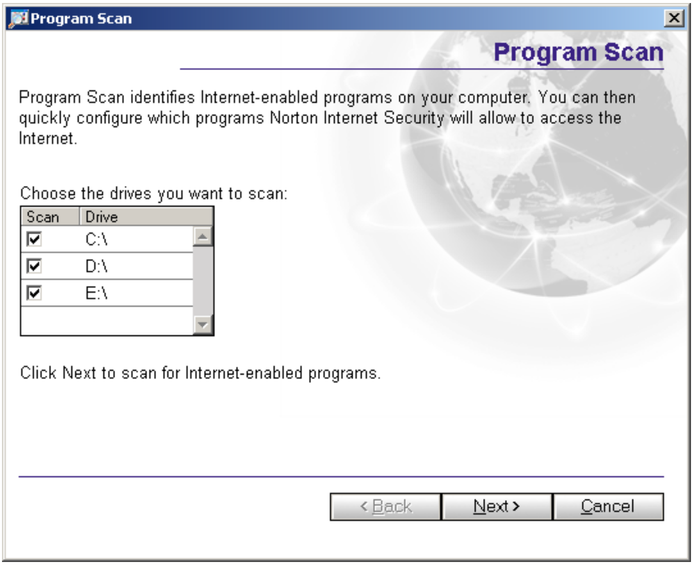


Program Scan

Norton Internet Security can automatically configure itself to allow Internet access for common Internet programs. Scanning for Internet programs now ensures that the programs you use regularly are protected and will reduce the number of alert messages you receive.

Automatically scan programs

2 In the Program Scan pane, click **Automatically scan programs**.



Program Scan

Program Scan

Program Scan identifies Internet-enabled programs on your computer. You can then quickly configure which programs Norton Internet Security will allow to access the Internet.

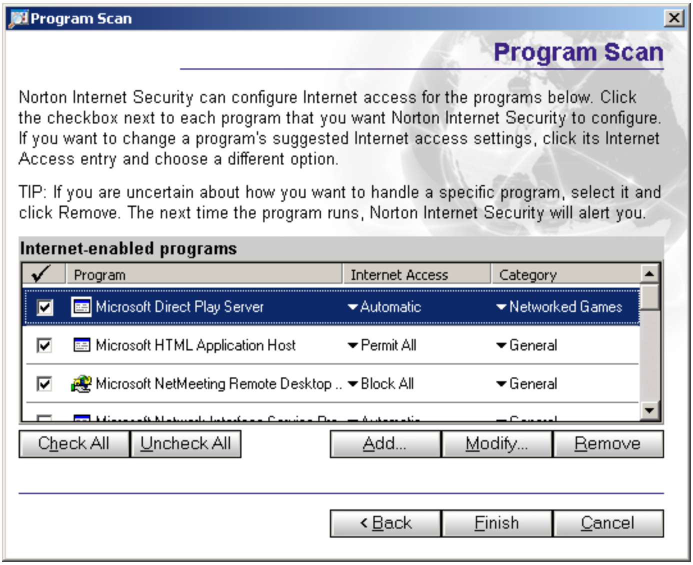
Choose the drives you want to scan:

Scan	Drive
☑	C:\
☑	D:\
☑	E:\

Click Next to scan for Internet-enabled programs.

3 In the Program Scan window, click **Next** to begin the scan.

When the scan is complete, all Internet-enabled programs that were found are listed.



Program Scan

Program Scan

Norton Internet Security can configure Internet access for the programs below. Click the checkbox next to each program that you want Norton Internet Security to configure. If you want to change a program's suggested Internet access settings, click its Internet Access entry and choose a different option.

TIP: If you are uncertain about how you want to handle a specific program, select it and click Remove. The next time the program runs, Norton Internet Security will alert you.

Internet-enabled programs

✓	Program	Internet Access	Category
☑	Microsoft Direct Play Server	▾Automatic	▾Networked Games
☑	Microsoft HTML Application Host	▾Permit All	▾General
☑	Microsoft NetMeeting Remote Desktop ..	▾Block All	▾General
☐	Microsoft Network Interface Service Pro..	▾Automatic	▾General

4 To allow Internet access for a program, check the check box to the left of the program's name.

5 To change the Internet access rule or category of a program, in the Internet Access or Category drop-down lists, select the setting that you want.

6 Click **Finish** when you are done.

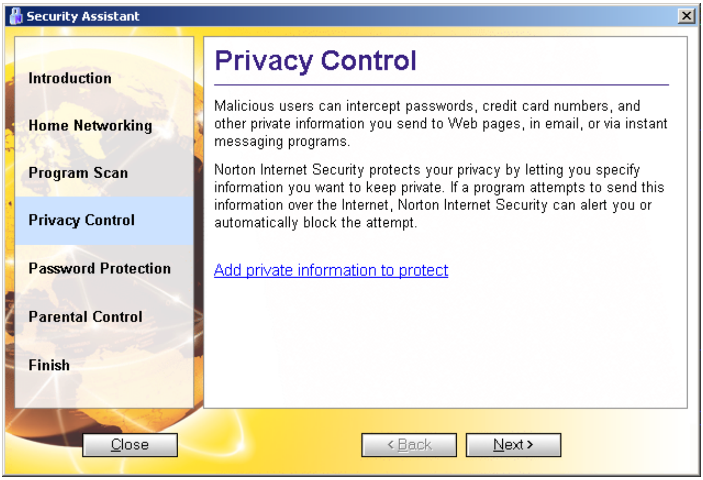
Set up Privacy Control

See "Identify private information to protect" on page 155.

Using Privacy Control, you can identify private information that should have extra protection. Privacy Control can then prevent users from sending this information to *Web sites*, in *email* messages and attached Microsoft Office files, and through supported instant messenger programs.

To set up Privacy Control

1 In the Security Assistant Roadmap, click **Privacy Control**.



Privacy Control

Malicious users can intercept passwords, credit card numbers, and other private information you send to Web pages, in email, or via instant messaging programs.

Norton Internet Security protects your privacy by letting you specify information you want to keep private. If a program attempts to send this information over the Internet, Norton Internet Security can alert you or automatically block the attempt.

Add private information to protect

2 In the Privacy Control pane, click **Add private information to protect**.

3 In the Add Private Information dialog box, under Type of information to protect, select a category.

4 In the Descriptive name text box, type a description to help you remember why you are protecting the data.

See "Tips on entering private information" on page 156.

5 In the Information to protect text box, type the last five or six characters of the information that you want to block from being sent over nonsecure Internet connections.
By entering only partial information, you ensure that untrustworthy people with physical access to your computer cannot steal entire credit card numbers and other information.

6 Click **OK**.

Set up Password Protection

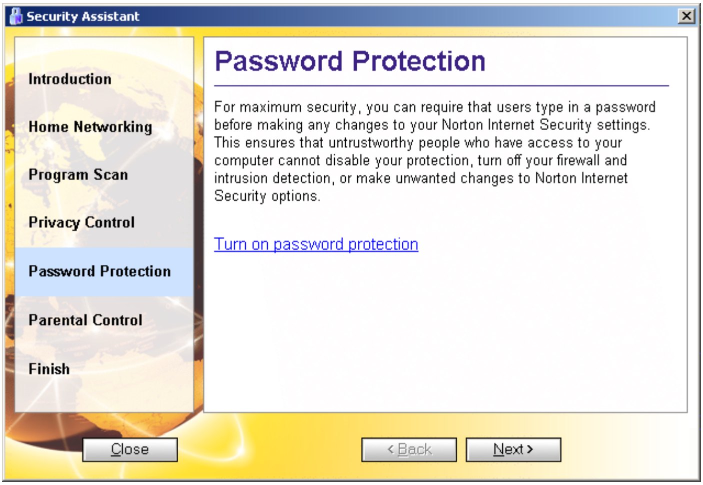
See "Use the Security Monitor" on page 53.

For maximum security, you can require a *password* before allowing anyone to make a change to your Norton Internet Security settings. This ensures that only the people you trust are able to disable your protection, turn off your *firewall* and intrusion detection, or make changes to Norton Internet Security options.

When Password Protection is on, users will have to type in their passwords before making changes to Norton Internet Security settings. If the current user does not have an account password, you must create one.

To protect Norton Internet Security options with a password

1 In the Security Assistant Roadmap, click **Password Protection**.



Password Protection

For maximum security, you can require that users type in a password before making any changes to your Norton Internet Security settings. This ensures that untrustworthy people who have access to your computer cannot disable your protection, turn off your firewall and intrusion detection, or make unwanted changes to Norton Internet Security options.

Turn on password protection

2 In the Password Protection pane, click **Turn on password protection**.

3 In the Password and Confirm Password text boxes, type a password.

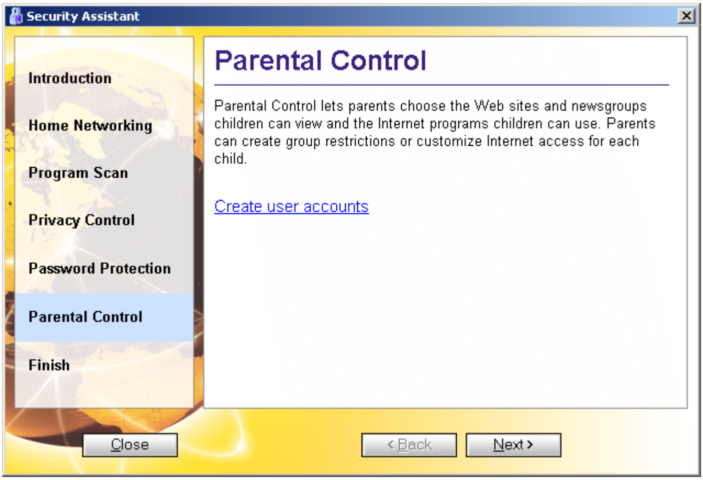
4 Click **OK**.

Set up Parental Control

Parental Control lets you control family members’ access to the Internet. You can block access to *Web sites* and newsgroups that you find inappropriate and you can block access to programs, such as chat, that you don’t want children or other family members to access. Parental Control is disabled by default.

To enable Parental Control

1 In the Security Assistant Roadmap, click **Parental Control**.

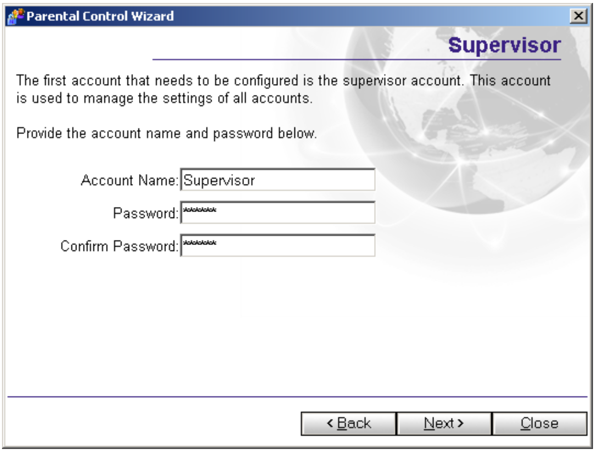


Parental Control

Parental Control lets parents choose the Web sites and newsgroups children can view and the Internet programs children can use. Parents can create group restrictions or customize Internet access for each child.

Create user accounts

2 In the Parental Control pane, click **Create user accounts**.



Supervisor

The first account that needs to be configured is the supervisor account. This account is used to manage the settings of all accounts.

Provide the account name and password below.

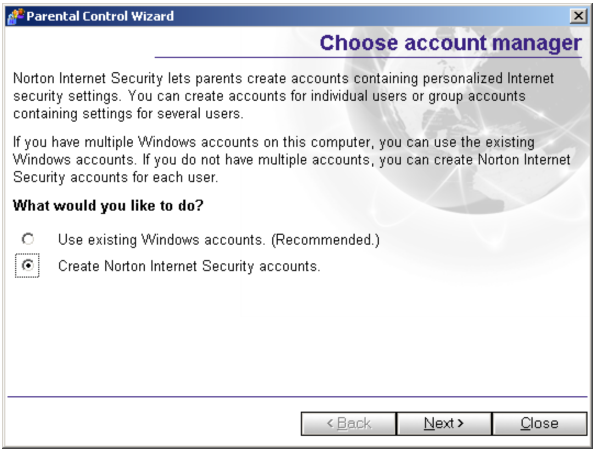
Account Name: Supervisor

Password: ******

Confirm Password: ******

3 In the Supervisor window, choose a name and password for the Supervisor account.
The Supervisor can make changes to any other account. You should choose a password that is difficult to guess.

4 Click **Next**.



Norton Internet Security lets parents create accounts containing personalized Internet security settings. You can create accounts for individual users or group accounts containing settings for several users.

If you have multiple Windows accounts on this computer, you can use the existing Windows accounts. If you do not have multiple accounts, you can create Norton Internet Security accounts for each user.

What would you like to do?

○ Use existing Windows accounts. (Recommended.)
● Create Norton Internet Security accounts.

See "Create accounts for multiple users" on page 145.

5 In the Choose account manager window, do one of the following:

- To use existing Windows accounts, click **Use existing Windows accounts (Recommended)**.
- To create new Norton Internet Security accounts, click **Create Norton Internet Security accounts**.

6 Click **Next**.

7 Follow the on-screen instructions to set up new accounts.

If you have Norton SystemWorks installed

If you have Norton SystemWorks installed on your computer when you install Norton Internet Security, the installer adds a Norton Internet Security tab to the Norton SystemWorks main window and a Norton SystemWorks tab to the Security Center.

To open Norton Internet Security from Norton SystemWorks

1 Open Norton SystemWorks.

2 On the Norton Internet Security tab, click **Launch Norton Internet Security**.

To open Norton SystemWorks from Norton Internet Security

1. Open Norton Internet Security.
2. In the Security Center, on the Norton SystemWorks tab, click **Launch Norton SystemWorks**.

If you need to uninstall Norton Internet Security

If you need to uninstall Norton Internet Security from your computer, use the Uninstall Norton Internet Security option on the Windows Start menu. You can also uninstall only the Norton AntiVirus component of Norton Internet Security.

During uninstall, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton Internet Security

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Uninstall Norton Internet Security**.
   - On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Uninstall Norton Internet Security**.
2. Do one of the following:
   - Click **Remove NAV** to uninstall the Norton AntiVirus component of Norton Internet Security.
   - Click **Remove All** to uninstall the entire product.
3. If you have files in Quarantine, you are asked if you want to delete them. Your options are:

Yes	Deletes the quarantined files from your computer.
No	Leaves the quarantined files on your computer, but makes them inaccessible. To repair or submit the files to Symantec for analysis, reinstall Norton Internet Security.

4. In the Installer Information dialog box, click **Yes** to restart your computer.

If you have no other Symantec products on your computer, you should also uninstall LiveReg and LiveUpdate.

To uninstall LiveReg and LiveUpdate

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **LiveReg**.
4. Do one of the following:
   - In Windows 2000/Me, click **Change/Remove**.
   - In Windows 98, click **Add/Remove**.
   - In Windows XP, click **Remove**.
5. Click **Yes** to confirm that you want to uninstall the product.
6. To uninstall LiveUpdate, repeat steps 1 through 5, selecting LiveUpdate in step 3.

Norton Internet Security basics

After installation, Norton Internet Security automatically protects any computer on which it is installed. You do not have to start the program to be protected.

Access Norton Internet Security

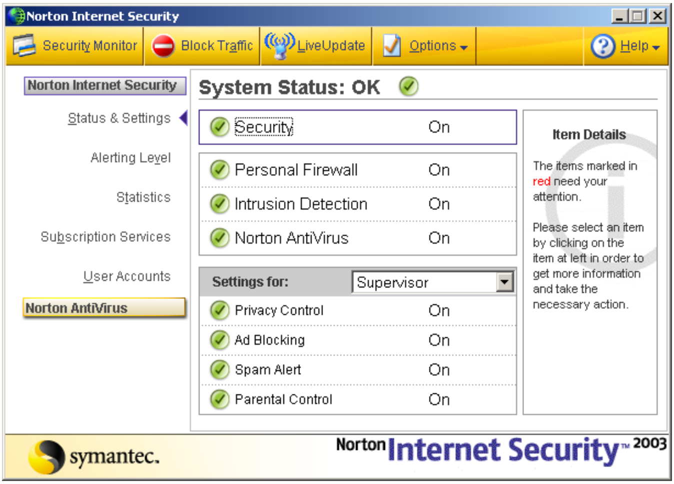
Launch Norton Internet Security to change protection settings or monitor its activities.

To access Norton Internet Security

❖ Do one of the following:

- On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Norton Internet Security**.
- On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Norton Internet Security**.

- On the Windows desktop, double-click **Norton Internet Security**.



System Status: OK

Security	On
Personal Firewall	On
Intrusion Detection	On
Norton AntiVirus	On
Settings for:	Supervisor
Privacy Control	On
Ad Blocking	On
Spam Alert	On
Parental Control	On

Item Details

The items marked in red need your attention.

Please select an item by clicking on the item at left in order to get more information and take the necessary action.

Access Norton Internet Security from the system tray

Norton Internet Security adds an icon to the Windows system tray. On most computers, the system tray is at the far right of the Windows taskbar at the bottom of your screen. Click this icon to open a menu containing frequently used Norton Internet Security tools.

To use the Norton Internet Security system tray menu

1 In the system tray, right-click the Norton Internet Security icon.

2 In the menu that appears, select an item. Items in the menu include:

Norton Internet Security	Opens a Norton Internet Security window.
Hide/View Alert Tracker	Displays or hides the Alert Tracker. See "Use Alert Tracker" on page 56.
Block Traffic	Immediately stops all incoming and outgoing information. See "Stop Internet communication with Block Traffic" on page 60.

Log On/Off	Lets you change the account that is logged on to Norton Internet Security. See "Log on to Norton Internet Security" on page 153.
About Norton Internet Security	Displays detailed information about Norton Internet Security components.
LiveUpdate	Updates your protection. See "Keeping current with LiveUpdate" on page 81.
Help	Displays the Norton Internet Security online Help. See "Use online Help" on page 75.
Disable	Turns off all Norton Internet Security protection features. See "Temporarily disable Norton Internet Security" on page 71.

See "About Global Settings" on page 63.

Use the Norton Internet Security Options to add additional tools to the menu.

Access Norton AntiVirus from the Windows Explorer toolbar

Norton AntiVirus adds a button and menu to Windows Explorer. The button launches a scan of whatever you have selected in the Explorer pane. To access additional Norton AntiVirus tools, click the arrow to the right of the button.

When you first open Windows Explorer after installing Norton Internet Security, you may not see the Norton AntiVirus button and menu.

To display the Norton AntiVirus button and menu

1 In Windows Explorer, on the View menu, click **Toolbars**.

2 Click **Norton AntiVirus**.

You may not be able to access the Norton AntiVirus Windows Explorer menu, depending on your computer's configuration.

Work with Norton Internet Security

Norton Internet Security works in the background, so you may only interact with the program when it alerts you of new network *connections* and possible problems. You can choose to view the new Security Monitor or the standard Security Center window, respond to security problems, and control the number of *alerts* you receive and how the program resolves potential security problems.

Access Norton Internet Security protection features

The default settings for Norton Internet Security provide a safe, automatic, and efficient way of protecting your computer. If you want to change or customize your protection, you can access all Norton Internet Security tools from the Status & Settings window.

Child users cannot make changes to Norton Internet Security settings. All users, regardless of their access levels, can make changes to Norton AntiVirus settings. To protect your settings from unwanted changes, set a password for Norton Internet Security and Norton AntiVirus options. See "Password-protect options" on page 68.

To change settings for individual features

1. Open Norton Internet Security.
2. In the Security Center, do one of the following:
   - Double-click a feature you want to customize.
   - Select a feature, then in the lower-right corner of the window, click **Customize**.
3. Configure the feature.
4. When you are done making changes, click **OK**.

If you have installed accounts, you can create customized settings for Privacy Control, Ad Blocking, Spam Alert, Parental Control, and the Personal Firewall security level. Other settings apply to all accounts.

To change settings for individual accounts

1 Open Norton Internet Security.

2 In the Security Center, do one of the following:

- Double-click a feature you want to customize.
- Select a feature, then in the lower-right corner of the window, click **Customize**.

3 In the features window, in the Settings for drop-down list, select the account you want to configure.

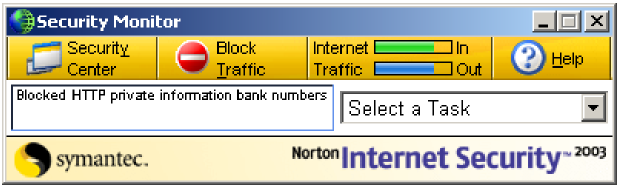
4 Configure the feature.

5 When you are done making changes, click **OK**.

Use the Security Monitor

The Security Monitor collects the most-used Norton Internet Security tools into a compact window. When you're online, place the Security Monitor window in an unused part of your screen. This lets you monitor your *connection*, view information about security events, and personalize your protection without requiring a lot of space on your screen.

When you start Norton Internet Security, it launches the Security Center. You can then switch to the Security Monitor.



Blocked HTTP private information bank numbers

To view the Security Monitor

❖ In the Security Center, in the upper-left corner, click **Security Monitor**.

To view the Security Center

❖ In the Security Monitor, in the upper-left corner, click **Security Center**.

You can display the Security Monitor on top of all other windows. This ensures that it will be visible at all times.

To keep the Security Monitor on top of all other windows

1. Open Norton Internet Security.
2. In the Security Center, click **Options** > **Internet Security**.
3. On the General tab, check **Keep Security Monitor on top of all other programs**.
4. Click **OK**.

Select a task with the Security Monitor

Use the Select a Task menu in the Security Monitor to quickly perform common Norton Internet Security tasks. The Select a Task menu includes:

Task	More information
Scan for viruses	See "Manually scan disks, folders, and files" on page 126.
Test security	See "Check your computer's vulnerability to attack" on page 58.
Edit private information	See "Protecting your privacy" on page 155.
View Log Viewer	See "View Norton Internet Security Logs" on page 196.
Run LiveUpdate	See "Keeping current with LiveUpdate" on page 81.
Run Program Scan	See "Scan for Internet-enabled programs" on page 111.
Create User Accounts	See "Create accounts for multiple users" on page 145.
Setup Home Network	See "Organize computers into network zones" on page 91.

Respond to Norton Internet Security alerts

Norton Internet Security monitors communication activities to and from your computer and lets you know when an activity that may compromise your security is taking place.

When an *alert* appears, read it before you make a decision. Identify what type of alert it is and the threat level. Once you understand the risks, you can make a choice.

Take as much time as you need to make your choice. Your computer is safe from attack while the alert is active.

Norton Internet Security helps you decide on an appropriate action by preselecting the recommended action if one exists. Norton Internet Security cannot suggest recommended actions for all alerts.

Learn more with the Alert Assistant

Each Norton Internet Security alert includes a link to the Alert Assistant. The Alert Assistant includes customized information about each alert, including:

- The type of alert
- The threat level
- The communication that triggered this alert
- What these types of alerts indicate
- How to reduce the number of these alerts you receive

To use the Alert Assistant

1. In any alert window, click the Alert Assistant button.
2. In the Alert Assistant window, review the information about this alert.
3. To respond to the alert, close the Alert Assistant.

Adjust the Alerting Level

The Alerting Level slider lets you control the amount of information that Norton Internet Security *logs* and the number of alerts that it displays.

Supervisors and Adult users can set their own Alerting Levels. Supervisors can also set the Alerting Levels for other users.

Your options are:

Alerting Level	Information Provided	Alert Tracker Messages	Security Alerts	Notifies you when...
Minimal	Critical Internet events	None	Logged, not displayed	Program Control rules are created automatically. Port scans occur. Confidential information is blocked. A remote access Trojan horse program is encountered.
Medium	Important Internet events	Some	Logged, not displayed	Same notification as Minimal, plus: - Programs access the Internet.
High	Important Internet events and complete program activities	Many	Logged and displayed	Same notification as Medium, plus: - Unused ports are blocked. - Cookies and content are blocked.

To adjust the Alerting Level

1 Open Norton Internet Security.

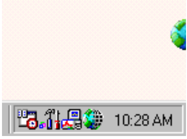
2 In the Security Center, click **Alerting Level**.

3 Move the slider to choose an Alerting Level.

Use Alert Tracker

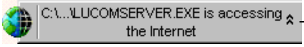
Many of the Internet events that Norton Internet Security monitors are not significant enough to trigger alerts. Alert Tracker provides an easy way to monitor these less-important security events.

Alert Tracker displays the same information that appears in the Security Event field on the Security Monitor. This allows you to monitor your computer's security without having to keep the Security Monitor visible at all times. Alert Tracker also provides a quick way to remove ads from *Web pages*.



Alert Tracker rests on the side of your screen

If you choose to display Alert Tracker, it attaches to either side of the screen on your primary monitor. When a security event occurs, Alert Tracker displays a message for a few seconds and then returns to the side of the screen. If you miss an Alert Tracker message, you can review a list of recent messages.



C:\...\LUCOMSERVER.EXE is accessing the Internet

Alert Tracker opens for a few seconds to display messages

Alert Tracker also contains the Ad Trashcan, which is part of the Norton Internet Security Ad Blocking feature.

See "Use the Ad Trashcan" on page 167.

To view or hide Alert Tracker

1. Open Norton Internet Security.
2. In the Security Center, click **Options** > **Internet Security**.
3. On the General tab, do one of the following:
   - Check **Show the Alert Tracker** to view Alert Tracker.
   - Uncheck **Show the Alert Tracker** to hide Alert Tracker.
4. Click **OK**.

To review recent Alert Tracker messages

1. On the Windows desktop, double-click the Alert Tracker.
2. To the right of the first message, click the arrow if it appears.
3. Double-click an entry to open the Log Viewer.

See "Review detailed statistics" on page 194.

To move Alert Tracker

❖ Drag the half globe to the side of the screen on which you want it to appear.

To hide Alert Tracker from the system tray menu

- In the Windows system tray, right-click the Norton Internet Security icon, then click **Hide Alert Tracker**.

If you hide Alert Tracker, you will not be notified when your computer joins a *network*. Information about the *connection* will still appear in the *logs*.

Check your computer's vulnerability to attack

Use Security Check to test your computer's vulnerability to security intrusions. The Security Check link in Norton Internet Security connects you to the Symantec *Web site*, where you can scan for vulnerabilities and get detailed information about Security Check scans.

You must be connected to the Internet to check your computer's vulnerability.

To check your computer's vulnerability to attack

1. Open Norton Internet Security.
2. Do one of the following:
   - In the Security Center, click **Security**, then click **Check Security**.
   - In the Security Monitor window, on the Select a Task menu, click **Test Security**.
3. On the Security Check Web page, click **Scan for Security Risks**.
4. To learn more about the Security Check tests, click **About Scan for Security Risks**.

When the scan is complete, the results page lists all of the areas that were checked and your level of vulnerability in each one. For any area marked as at risk, you can get more details about the problem and how to fix it.

To get more information about an at-risk area

- On the results page, next to the scan name, click **Show Details**.

Identify the source of communications

Visual Tracking helps you learn more about computers that attempt to connect to your computer. Using Visual Tracking, you can identify the location of the *IP address* used and contact information for the owner of the address. You can use this information to identify the origin of an attack and to learn more about intrusion attempts.

You can trace *connection attempts* from three places in Norton Internet Security:

- Statistics
- Log Viewer
- AutoBlock

To trace a connection attempt from Statistics

1. Open Norton Internet Security.
2. In the Security Center, click **Statistics**.
3. Click **Attacker Details**.
   Your browser opens the Visual Tracking Web page.

To trace a connection attempt from the Log Viewer

1. Open Norton Internet Security.
2. In the Security Center, click **Statistics**.
3. Click **View Logs**.
4. In the left column of the Log Viewer window, under Internet Security, click **Connections**.
5. In the right column of the Log Viewer window, select a connection you want to trace.
6. At the bottom of the Log Viewer window, click the computer's IP address or name.
   Your browser opens the Visual Tracking Web page.

To trace a connection attempt from AutoBlock

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, in the AutoBlock section, select a connection you want to trace.
4. Click **Attacker Details**.
   Your browser opens the Visual Tracking Web page.

When Visual Tracking is finished, it displays a visual representation of where this communication originated and contact information for the owner of the IP address.

Stop Internet communication with Block Traffic

The Security Center and the Security Monitor include a Block Traffic button that lets you immediately halt any communication between your computer and another. This can be a handy way to limit any damage to your computer if it is attacked, if a *Trojan horse* is sending personal information without your permission, or if you inadvertently allow an untrusted person to access files on your computer.

When this option is active, Norton Internet Security stops all communication to and from your computer. To the outside world, it appears that your computer has completely disconnected from the Internet.

If you want to block all traffic into and out of your computer, Block Traffic is more effective than simply using your Internet software to disconnect. Most Internet programs can automatically connect without any input from the user, so a malicious program could reconnect when you are away from the computer.

Block Traffic is meant to be used as a temporary measure while you address a security problem. If you restart your computer, Norton Internet Security automatically allows all incoming and outgoing communication. To continue blocking traffic, click the Block Traffic button in the Security Center or Security Monitor.

To avoid attack while fixing security problems

1. Open Norton Internet Security.
2. In the Security Center or the Security Monitor window, click **Block Traffic**.
3. Use Norton Internet Security tools to address the security problem.
4. When you have fixed the problem, click **Allow Traffic**.

Customize Norton Internet Security

The default Norton Internet Security settings should provide adequate protection for most users. If you need to make changes, Supervisors and Adult users can use the Options menu to access Norton Internet Security and Norton AntiVirus options. The options let you control more advanced settings.

If you are using Windows 2000/XP and you do not have Local Administrator access, you cannot change Norton Internet Security options.

To customize Norton Internet Security

1. Open Norton Internet Security.
2. At the top of the Security Center, click **Options** > **Internet Security**.
3. Select the tab on which you want to change options.

About General options

General options let you control when Norton Internet Security runs, protect program settings with a *password*, and choose visual elements you want to display. Your options are:

Start Norton Internet Security	Select whether you want to run Norton Internet Security manually or automatically whenever Windows starts.
Protect Norton Internet Security Tools	Set a password to protect your security settings from untrustworthy people who have physical access to your computer. See "Password-protect options" on page 68.
Alert Tracker	Toggle the Alert Tracker on and off.
Tray Icon Settings	Display a Norton Internet Security icon on the Windows taskbar that gives you access to program settings. You can also choose to include links to the following Norton Internet Security tools: - Options - Log Viewer - Statistics

About LiveUpdate options

See "Keeping current with LiveUpdate" on page 81.

LiveUpdate options let you enable and disable Automatic LiveUpdate, which automatically checks for Norton Internet Security updates when you are connected to the Internet. For maximum security, you should leave this option checked.

You can choose the Norton Internet Security components you want Automatic LiveUpdate to monitor. You can also choose whether Automatic

LiveUpdate updates the components in the background or alerts you that there are updates available. Your options are:

Norton Internet Security	Improvements to operating system or hardware compatibility and fixes that address performance issues
Personal Firewall	New firewall rules that increase and extend the Personal Firewall's ability to protect your computer
Intrusion Detection	Attack signatures that protect your computer from newly discovered Internet attacks
Parental Control Web site list	Categorized lists of Web sites that have been visited since you installed Norton Internet Security
Spam Alert	Updated spam definitions that identify new types of unwanted email

Norton AntiVirus includes a separate set of LiveUpdate options. See "About Internet options" on page 67.

About Firewall options

Firewall options let you activate advanced protection features and customize the ports your computer uses to view *Web pages*. Most people will not need to make any changes to these settings. Your options are:

Turn on Program Component Monitoring	When a program uses an external software component to connect to the Internet, check firewall rules for each component. This ensures that Trojan horses and other malicious programs cannot attach to safe programs and evade detection.
Turn on Program Launch Monitoring	Program Launch Monitoring helps ensure that Trojan horses and other malicious programs cannot launch and manipulate safe programs without your knowledge. When Program Launch Monitoring is active, you will be alerted whenever an unrecognized program launches another program. You can then choose to allow or block Internet access for the unrecognized program.
HTTP ports	Change the ports that your Web browser uses to download Web pages. The default port for HTTP is port 80, but the HTTP port list contains several other commonly used ports.
Block IGMP	Enable or disable your computer's ability to use IGMP (Internet Group Membership Protocol). IGMP is commonly used to send multimedia files to multicast groups.

Stealth ports	Blocked and inactive ports do not respond to connection attempts. Active ports do not respond to connection attempts with incorrect source or destination information.
Fragmented IP packet handling	Choose whether Norton Internet Security blocks all IP packets that are broken into fragments or only the packets that appear to be part of an attack.

About Web Content options

Web Content options let you control how Norton Internet Security handles interactive online content, ads, and possible privacy intrusions. Web Content options are arranged on three tabs.

About Global Settings

Global Settings let you control the default actions Norton Internet Security takes when Web sites attempt to get information about your *browser* or use animated images, JavaScripts, and other *active content*. Changes to these settings affect all users. Your options are:

Information about your browser	Block or allow Web sites from requesting information about your computer and Web browser.
Information about visited sites	Block or allow Web sites from requesting information about other Web sites you have visited during this session online.
Animated images	Block or allow animated images from running.
Scripts	Block or allow JavaScripts.
Flash ads	Block or allow ads made with Macromedia Flash.

About User Settings

User Settings let you customize *cookie* blocking, pop-up window blocking, and *ActiveX* and *Java* settings for individual sites. Changes to these settings only affect the current user. Your options are:

Cookies	Block or allow Web sites from creating and reading cookie files on your computer.
Java applets	Block or allow Java applets from running.
ActiveX controls	Block or allow ActiveX controls from running.
Pop-up ads	Block or allow pop-up ads.

About Ad Blocking settings

Ad Blocking settings let you specify individual *ad banners* or groups of ad images you want to block or allow on individual sites. See “Use text strings to identify ads to block or permit” on page 168.

About Email options

Email options let you control how Norton Internet Security notifies you when it is scanning email messages for private information and spam. Your options are:

Tray icon	Change the Norton Internet Security icon in the system tray to indicate email messages are being scanned.
Progress indicator	Display the amount of email messages scanned and an estimate of the time remaining in this scan.

Customize Norton AntiVirus

The default settings for Norton AntiVirus provide complete virus protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply.

All the settings for Options are organized into three main categories. The options contained under each category are as follows.

Category	**Options**
System	Auto-Protect ■ Bloodhound ■ Advanced ■ Exclusions Script Blocking Manual Scan ■ Bloodhound ■ Exclusions
Internet	Email ■ Advanced Instant Messenger LiveUpdate
Other	Inoculation (Windows 98/98SE/Me) Miscellaneous

This section does not describe how to change the individual options, but gives a general description of what they do and how you can find them. For specific information about a particular option, check the online Help.

About System options

The System options control scanning and monitoring of your computer. You use System options to determine what gets scanned, what the scan is looking for, and what happens when a virus or virus-like activity is encountered.

With higher levels of protection, there can be a slight trade-off in computer performance. If you notice a difference in your computer's performance after you install Norton Internet Security, you may want to set protection to a lower level or disable those options that you do not need.

Option	Description
Auto-Protect	Determine if Auto-Protect starts when you start your computer, what it looks for while monitoring your computer, and what to do when a virus is found. Bloodhound is the scanning technology that protects against unknown viruses. Use these options to set its level of sensitivity in Auto-Protect. Advanced options determine the activities to be monitored when scanning for virus-like activities and when scanning floppy disks. Exclusions specify the files that should not be scanned by file name extension or by specific file name. Be careful not to exclude the types of files that are more likely to be infected by viruses, such as files with macros or executable files.
Script Blocking	Enable Script Blocking and set what Norton AntiVirus should do if it finds a malicious script. If you are developing or debugging scripts, disable Script Blocking. Otherwise this feature might block the script you are developing.
Manual Scan	Determine what gets scanned and what happens if a virus is found during a scan that you request. Manual Scan options also include Bloodhound and Exclusions subcategories.

About Internet options

Internet options define what happens when your computer is connected to the Internet. You use Internet options to define how Norton Internet Security should scan email and instant messenger attachments, enable Worm Blocking, and determine how LiveUpdates should be applied.

Option	Description
Email	Enable email scanning and Worm Blocking, and define how Norton AntiVirus should behave while scanning email messages. Scanning incoming email protects your computer against viruses sent by others. Scanning outgoing email prevents you from inadvertently transmitting viruses or worms to others. You can choose to scan incoming or outgoing email, or both, and to display an icon or progress indicator while scanning. You can set options to automatically repair, quarantine, or delete infected email with or without interaction with you. Advanced options determine what to do when scanning email.
Instant Messenger	Determine what instant messengers to support, how to configure a new IM, and what happens if a virus is found during an instant messenger session.
LiveUpdate	Enable Automatic LiveUpdate and define how updates should be applied. Automatic LiveUpdate checks for updated virus definitions and program updates automatically when you are connected to the Internet.

About Other options

Other options include Inoculation settings for Windows 98/98SE/Me and Miscellaneous settings. You can enable Inoculation, cause an alert if a system file changes, and set a variety of miscellaneous options.

Option	Description
Inoculation	Enable inoculation and, if a system file changes, choose to update the inoculation snapshot or repair the file by restoring it to its original values. Inoculation options are available only on Windows 98/98SE/Me.
Miscellaneous	Back up file in Quarantine before attempting a repair. (This option is automatically set to On.) Enable Office Plug-in. If you upgrade to Microsoft Office 2000 or later after Norton Internet Security is installed, you must enable this option to automatically scan Microsoft Office files. Alert me if my virus protection is out of date. Scan files at system startup (Windows 98/98SE only). Enable password protection for options.

Password-protect options

You can protect Norton Internet Security and Norton AntiVirus options with *passwords*. This ensures that only the people you trust are able to make changes to your options. If you have installed accounts and have not set a password for a current account, the password you choose will become your account password.

⚠ To protect both Norton Internet Security and Norton AntiVirus options, you must set passwords for both products.

To protect Norton Internet Security options with a password

1. Open Norton Internet Security.
2. At the top of the Norton Internet Security window, click **Options** > **Internet Security**.
3. On the General tab, check **Turn on Password Protection**.
   If the account currently logged on does not have a password, you must select one now.
4. Click **Set Password**.
5. In the Password and Confirm Password text boxes, type a password.
   If you are also setting a password for Norton AntiVirus options, you may want to use the same password for both.
6. Click **OK**.

To protect Norton AntiVirus options with a password

1. Open Norton Internet Security.
2. At the top of the Norton Internet Security window, click **Options** > **Norton AntiVirus**.
3. In the Norton AntiVirus options window, under Other, click **Miscellaneous**.
4. Under How to control access to option settings, check **Enable password protection for options**.
5. In the Password and Confirm Password text boxes, type a password.
   If you are also setting a password for Norton Internet Security options, you may want to use the same password for both.
6. Click **OK**.

Reset options passwords

If you forget your options passwords, you can reset them.

To reset your Norton Internet Security options password

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Uninstall Norton Internet Security**.
   - On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Uninstall Norton Internet Security**.
2. In the Remove Application window, click **Reset Password**.
3. In the password reset dialog box, in the Reset Password Key text box, type the Reset Password Key that appears above the text box.
   The Reset Password Key is case-sensitive.
4. In the New Password and Confirm New Password text boxes, type a new password.
5. Click **OK**.
6. In the Remove Application window, click **Cancel**.
7. In the Norton Internet Security alert, click **Exit**.
8. In the Setup Canceled alert, click **OK**.

To reset your Norton AntiVirus options password

1. Open Norton Internet Security.
2. At the top of the Norton Internet Security window, click **Help** > **About Norton Internet Security**.
3. In the About window, on the Norton AntiVirus tab, click **Reset Password**.
4. In the password reset dialog box, in the Reset Password Key text box, type the Reset Password Key that appears above the text box.
   The Reset Password Key is case-sensitive.
5. In the New Password and Confirm New Password text boxes, type a new password.
6. Click **OK**.
7. In the About window, click **OK**.

Temporarily disable Norton Internet Security

There may be times when you want to temporarily disable Norton Internet Security or one of its features. For example, you might want to view online ads or see if Norton Internet Security is preventing a *Web page* from appearing correctly.

See "About Norton Internet Security accounts" on page 145.

Only Adult or Supervisor users can temporarily disable Norton Internet Security. Child and Teenager users cannot disable any portion of Norton Internet Security.

Disabling Norton Internet Security also disables all of the individual features.

To temporarily disable Norton Internet Security

1. Open Norton Internet Security.
2. In the Security Center, click **Security**.
3. On the right side of the screen, click **Turn Off**.

Norton Internet Security is automatically turned back on the next time you start your computer.

You can also disable individual security features. For example, you might want to see if the Personal Firewall is preventing a program from operating correctly.

To disable a protection feature

1. Open Norton Internet Security.
2. In the Security Center, select the feature that you want to disable.
3. On the right side of the screen, click **Turn Off**.

Temporarily disable Auto-Protect

See "Customize Norton AntiVirus" on page 65.

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. When a virus or *virus-like activity* is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect.

If you have set a *password* for Options, Norton Internet Security asks you for the password before you can view or adjust the settings.

To temporarily disable Auto-Protect

1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under System, click **Auto-Protect**.
4. In the Auto-Protect pane, uncheck **Enable Auto-Protect**.

Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

To enable Auto-Protect

1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under System, click **Auto-Protect**.
4. In the Auto-Protect pane, check **Enable Auto-Protect**.

If the Norton AntiVirus *icon* appears in the Windows tray, you can use it to enable and disable Auto-Protect.

To enable or disable Auto-Protect using the tray icon

1. In the Windows system tray, right-click the Norton AntiVirus icon.
2. Do one of the following:
   - If Auto-Protect is disabled, click **Enable Auto-Protect**.
   - If Auto-Protect is enabled, click **Disable Auto-Protect**.

Create Rescue Disks

Depending upon which *operating system* you are using, you may want to keep a set of Rescue Disks available and keep them up-to-date.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue items and a virus scanner across multiple floppy disks or on a *network* drive. Rescue Disks can be made for the Windows 98/Me operating systems.

A Rescue Disk set consists of one bootable floppy disk, one Norton AntiVirus Program floppy disk, and several Virus Definition floppy disks. If you have Norton Utilities installed, you will also have two Norton Utilities floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.

Rescue Disks contain information specific to the computer on which they were made. If you are using Rescue Disks for recovery, you must use the disks made for your computer. If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer.

Disks can and should be updated whenever you update your virus protection, install new software, or make changes to your hardware.

Create a Rescue Disk set

Rescue Disks can be created at any time. You can start the Rescue Disk Wizard from the Security Center.

See "Temporarily disable Auto-Protect" on page 72.

You should temporarily disable Auto-Protect while you are creating the Rescue Disk set. If you do not restart your computer after creating Rescue Disks, remember to enable Auto-Protect again.

You will need several formatted 1.44-MB disks.

To create Rescue Disks

1. Start Norton Internet Security.
2. In the Security Center, click **Rescue**.
3. Select drive A to create the Rescue Disk set.
4. Click **Create**.

5 Label the disks as specified in the Basic Rescue Disk List window, then click **OK**.

6 Insert the disks as requested.

Test your Rescue Disks

At the end of the Create Rescue Disks process, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.

To test your Rescue Disks

1 Close all open Windows programs.

See "My Rescue Disk does not work" on page 209.

2 Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.
If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly. If the Rescue Disk screen does not appear, you have several options for correcting the problem.

3 Press **Escape** to exit to DOS.

4 Remove the disk from drive A, then slide open the plastic tab on the back of the disk to write-protect it.

5 Restart your computer.

Update your Rescue Disks

You can update your Rescue Disks as often as you like. The Rescue Disk Wizard helps you to update your basic Rescue Disks without having to recreate them.

If you are updating a floppy disk set, make sure your disks are not write-protected before you begin.

To update your Rescue Disks

1. Start Norton Internet Security.
2. In the Security Center, click **Rescue**.
3. Under Select Destination Drive, select drive A.
4. Click **Update**.
5. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A. If the disk is write-protected, slide the plastic tab closed to make it writeable.
6. Click **OK**.
7. Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted.

See "Test your Rescue Disks" on page 74.

For more information

Norton Internet Security provides glossary terms, online Help, this User's Guide in PDF format, tutorials on the *Web*, and links to the Knowledge Base on the Symantec *Web site*.

Look up glossary terms

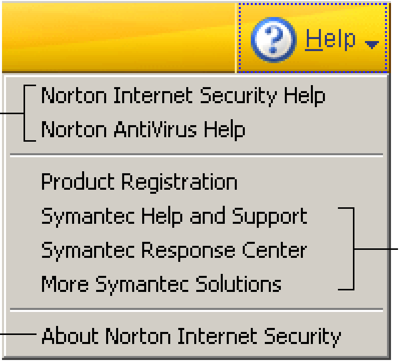
Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. In both locations, clicking a glossary term takes you to its definition.

Use online Help

Help is always available throughout Norton Internet Security. Help buttons or links to more information provide information specific to the task you are completing. The Help menu provides a comprehensive guide to all product features and tasks you can complete.

To access Help

1 At the top of the Security Center, click **Help**.



Online Help table of contents and index

Version, system, and Norton AntiVirus password reset information

Link to Symantec Web sites for more information

2 On the main Help menu, click **Norton Internet Security Help**.

3 In the left pane of the Help window, select one of the following tabs:
- Contents: Displays the Help by topic.
- Index: Lists Help topics in alphabetical order by key word.
- Search: Opens a search field where you can enter a word or phrase.

Window and dialog box Help

Window and dialog box Help provides information about the Norton Internet Security program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

❖ Do one of the following:
- Click the **Tell Me More** link if one is available.
- In the dialog box, click **Help**.

Readme file and Release Notes

The Readme file contains information about installation and compatibility issues. The Release Notes contain technical tips and information about product changes that occurred after this guide went to press. They are installed on your hard disk in the same location as the Norton Internet Security product files.

To read the Readme file

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Product Support** > **Readme.txt**.
   - On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Product Support** > **Readme.txt**.

   The file opens in Notepad.
2. Close the word processing program when you are done reading the file.

The Release Notes can be accessed from the Start menu.

To read the Release Notes

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Internet Security** > **Product Support** > **Norton Internet Security Release Notes**.
   - On the Windows XP taskbar, click **Start** > **More Programs** > **Norton Internet Security** > **Product Support** > **Norton Internet Security Release Notes**.

   The file opens in Notepad.
2. Close the word processing program when you are done reading the file.

Use the User's Guide PDFs

This User's Guide and the *Norton AntiVirus User's Guide* are provided on the Norton Internet Security CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDFs.

To install Adobe Acrobat Reader

1. Insert the Norton Internet Security CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click the **Acrobat** folder.
5. Double-click **ar500enu.exe**.
6. Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDFs from the CD.

To read the User's Guide PDFs from the CD

1. Insert the Norton Internet Security CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click the PDF that you want to view. Your options are:

NIS2003.pdf	This User's Guide
NAV2003.pdf	*Norton AntiVirus User's Guide*

You can also copy the User's Guides to your hard disk and read them from there. The PDFs need approximately 5.5 MB of disk space.

To read the User's Guides from your hard disk

1. Open the location into which you copied the PDF.
2. Double-click the PDF that you want to view. Your options are:

NIS2003.pdf	This User's Guide
NAV2003.pdf	*Norton AntiVirus User's Guide*

About Norton Internet Security on the Web

The Symantec Web site provides extensive information about Norton Internet Security. There are several ways to access the Symantec Web site.

To access the Symantec Web site from the Norton Internet Security main window

1. Click **Help**.
2. Select one of the following:
   - Technical Support Web site: Takes you to the Technical Support page of the Symantec Web site, from which you can search for solutions to specific problems, update your virus protection, and read the latest information about antivirus technology.
   - Visit the Symantec Web site: Takes you to the home page of the Symantec Web site, from which you can get product information on every Symantec product.

The Reports page of Norton AntiVirus contains a link to the Symantec online virus encyclopedia, as does the Windows Explorer toolbar.

To access the Symantec Web site from the Reports page

1. In the Security Center, click **Norton AntiVirus**.
2. Click **Reports**.
3. On the Reports page, next to the Online Virus Encyclopedia heading, click **View Report**.

To access the Symantec Web site from Windows Explorer

1. Open Windows Explorer.
2. On the toolbar, on the Norton Internet Security menu, click **View Virus Encyclopedia**.
   This option connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.

You can always access the Symantec Web site through your Internet browser.

To access the Symantec Web site in your browser

❖ Type the Symantec Web site address, www.symantec.com.

Explore online tutorials

Symantec provides online tutorials that you can use to review many common tasks that Norton Internet Security performs.

To explore the online tutorials

1. Point your browser to www.symantec.com/techsupp/tutorials.html
2. On the tutorials Web page, select the product and version for which you want a tutorial.
3. Click **continue**.
4. In the list of available tutorials for your product, select the one that you want to review.

Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special virus definition releases.

To subscribe to the Symantec Security Response newsletter

1. Point your browser to securityresponse.symantec.com
2. On the security response Web page, scroll down to the reference area of the page, then click **Newsletter**.
3. On the security response newsletter Web page, choose the language in which you want to receive the newsletter.
4. On the subscribe Web page, type the information requested, then click **Subscribe**.

Keeping current with LiveUpdate

5

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

Your normal Internet access fees apply when you use LiveUpdate.

If you are using Norton Internet Security on Windows 2000/XP, you must have Administrator access rights to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files available from Symantec, by subscription, that keep your Symantec products up-to-date with the latest anti-threat technology. The protection updates you receive depend on which product you are using.

Norton AntiVirus, Norton SystemWorks	Users of Norton AntiVirus and Norton SystemWorks receive virus definition service updates, which provide access to the latest virus signatures and other technology from Symantec.
Norton Internet Security	In addition to the virus definition service, users of Norton Internet Security also receive protection updates to the Web filtering service, the intrusion detection service, and Spam Alert. The Web filtering service updates provide the latest lists of Web site addresses and Web site categories that are used to identify inappropriate Web content. The intrusion detection service updates provide the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access attempts to your computer. Spam Alert updates provide the latest spam definitions and updated lists of spam email characteristics. These lists are used to identify unsolicited email.
Norton Personal Firewall	Users of Norton Personal Firewall receive intrusion detection service updates for the latest predefined firewall rules and updated lists of applications that access the Internet.

About your subscription

See "Subscription policy" on page 234.

Your Symantec product includes a complimentary, limited-time subscription to protection updates for the subscription services that are used by your product. When the subscription is due to expire, you are prompted to renew your subscription.

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates and will not be protected against newly discovered threats.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Request an update alert

To ensure your protection updates are current, you can request to receive an email alert whenever there is a high-level virus outbreak or other Internet security threat. The email alert describes the threat, provides detection and removal instructions, and includes advice on keeping your computer safe. You should always run LiveUpdate after you receive one of these alerts.

To request an update alert

1. From your Web browser, navigate to http://securityresponse.symantec.com/avcenter
2. On the Security Response Web page, scroll to the bottom of the page, then click **Symantec security response Free subscription**.
3. On the security alert subscription Web page, fill in the subscription form.
4. Click **Send me FREE Security Alerts**.

If you run LiveUpdate on an internal network

If you run LiveUpdate on a computer that is connected to a network that is behind a company firewall, your network administrator might set up an internal LiveUpdate server on the network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new updates from the Symantec Web site.

Your subscription must be current to obtain new protection updates from the Symantec Web site.

To obtain updates from the Symantec Web site

1. Point your Web browser to securityresponse.symantec.com
2. Follow the links to obtain the type of update that you need.

Obtain updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.

If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.
   You might receive a warning that says that your subscription has expired. Follow the on-screen instructions to complete the subscription renewal.
3. In the LiveUpdate window, click **Next** to locate updates.
4. If updates are available, click **Next** to download and install them.
5. When the installation is complete, click **Finish**.

Some program updates may require that you restart your computer after you install them.

Set LiveUpdate to Interactive or Express mode

LiveUpdate runs in either Interactive or Express mode. In Interactive mode (the default), LiveUpdate downloads a list of updates available for your Symantec products that are supported by LiveUpdate technology. You can then choose which product updates you want to install. In Express mode, LiveUpdate automatically installs all available updates for your Symantec products.

To set LiveUpdate to Interactive or Express mode

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.
3. On the LiveUpdate welcome screen, click **Configure**.
4. On the General tab of the LiveUpdate Configuration dialog box, select **Interactive Mode** or **Express Mode**.
5. If you selected Express Mode, select how you want to start checking for updates:
   - To have the option of cancelling the update, select **I want to press the start button to run LiveUpdate**.
   - To have any updates installed automatically whenever you start LiveUpdate, select **I want LiveUpdate to start automatically**.
6. Click **OK**.

Turn off Express mode

Once you have set LiveUpdate to run in Express mode, you can no longer access the LiveUpdate Configuration dialog box directly from LiveUpdate. You must use the Symantec LiveUpdate control panel.

To turn off Express mode

1. On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
2. In the Control Panel window, double-click **Symantec LiveUpdate**.
3. On the General tab of the LiveUpdate Configuration dialog box, select **Interactive Mode**.
4. Click **OK**.

Run LiveUpdate automatically

You can have LiveUpdate check for protection updates automatically, on a set schedule, by enabling Automatic LiveUpdate. You must continue to run LiveUpdate manually to receive product updates.

Automatic LiveUpdate checks for an Internet connection every five minutes until a connection is found, and then every four hours. If you have an ISDN router that is set to automatically connect to your Internet service provider (ISP), many connections will be made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate in the Norton Internet Security options.

To enable Automatic LiveUpdate

1 Start Norton Internet Security.

2 At the top of the Security Center, click **Options** > **Internet Security**.

If you set a password for Options, Norton Internet Security asks you for the password before you can continue.

3 In the Norton Internet Security Options dialog box, on the LiveUpdate tab, check **Enable Automatic LiveUpdate**.

4 If you want to be notified when updates are available, check **Notify me when Norton Internet Security updates are available**.

5 Select the updates for which you want Automatic LiveUpdate to check.

6 For each type of update you want Automatic LiveUpdate to check for, set how you want those updates to be applied by selecting one of the following:

Automatically update my protection	LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate displays an alert when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
Notify me	LiveUpdate checks for protection updates and asks if you want to install them.

7 Click **OK**.

To delete the schedule for Automatic LiveUpdate, disable Automatic LiveUpdate.

To disable Automatic LiveUpdate

1 Start Norton Internet Security.

2 At the top of the Security Center, click **Options** > **Internet Security**.

If you set a password for Options, Norton Internet Security asks you for the password before you can continue.

3 In the Norton Internet Security Options dialog box, click the **LiveUpdate** tab.

4 In the LiveUpdate pane, uncheck **Enable Automatic LiveUpdate**.

5 Click **OK**.

Controlling access to protected computers

6

You can configure Norton Internet Security to meet your needs in many different situations. You can use the program to control your computer's access to both local computers and computers over the Internet. You can also control how outside users access your computer.

Control how people use your computer

Norton Internet Security monitors all *connections*, including those made among computers in your home. After installation, you may need to adjust some settings to share files, printers, and other resources with other computers.

Connect to a network

Every time that you use Windows file sharing to exchange files with someone, print to a shared printer, or connect to the Internet using a *modem* or broadband connection, your computer joins a *network* of other computers. When you are part of a network, your computer is vulnerable to attacks. Norton Internet Security automatically monitors all new network connections to ensure that your computer is safe.

Normally, your computer connects to a network because of an action that you take. Unexpected connections can be a sign that a malicious program is attempting to send information over the Internet. Some wireless access cards automatically scan for and connect to any network in range. If you travel with a laptop that is equipped with a wireless access card, you may discover that your computer joins wireless networks in airports and other public places.

See "Monitoring Norton Internet Security" on page 191.

Whenever you join a network, Norton Internet Security automatically begins monitoring the connection. You do not need to make any changes in order to be protected. Norton Internet Security notifies you of the new connection and records it in the Connections *log*.

Enable file and printer sharing

Microsoft networking provides file and printer sharing. By default, Norton Internet Security prevents any computers from accessing these *services* on a protected computer.

To share files and give access to printers on your local *network*, you can enable file and printer sharing. If you enable these features on your local network, they are still protected from malicious users on the Internet.

Before enabling file and printer sharing on your local network, ensure that each shared resource is protected by a secure *password*. To learn more about securing shared resources, consult the Help file on your Start menu.

To enable file and printer sharing

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Advanced tab, click **General Rules**.
4. In the General Rules window, select the entry for Windows file sharing or printer sharing.
5. Click **Modify**.
6. In the Modify Rule dialog box, on the Action tab, click **Permit Internet access**.
7. Click **OK**.
8. In the General Rules dialog box, click **OK**.
9. In the Advanced Firewall window, click **OK**.

Organize computers into network zones

Norton Internet Security lets you organize computers on your home network and the Internet into Trusted and Restricted Zones.

Computers that you place in the Trusted Zone are not regulated by Norton Internet Security. They have as much access to your computer as they would have if Norton Internet Security was not installed. Only use the Trusted Zone for computers on your home network with which you need to share files and printers. If a computer in your Trusted Zone is attacked, and an attacker takes control of it, it poses a risk to your computer and all other computers in your Trusted Zone.

Computers that you place in the Restricted Zone are prevented from accessing your computer at all. If a computer is in the Restricted Zone, all communication from it is automatically blocked.

If you have more than one computer in your home, you will likely want to add all of these computers to your Trusted Zone. Only add external computers to your Trusted Zone if you know that their users can be trusted and they have firewall software installed.

The Home Network Wizard is the fastest way to organize computers into zones. You can also manually add individual computers to zones.

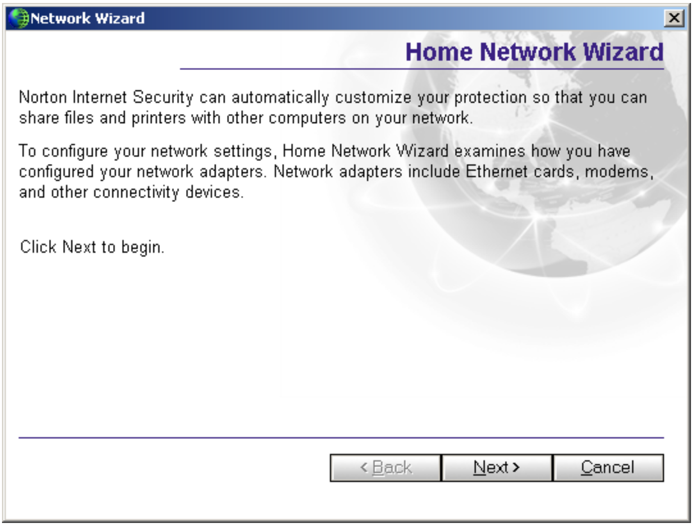
To open the Home Network Wizard from the Security Center

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Home Networking tab, click **Wizard**.

To open the Home Network Wizard from the Security Monitor

1 Open Norton Internet Security.

2 In the Security Monitor, on the Select a Task menu, select **Setup Home Networking**.



Norton Internet Security can automatically customize your protection so that you can share files and printers with other computers on your network.

To configure your network settings, Home Network Wizard examines how you have configured your network adapters. Network adapters include Ethernet cards, modems, and other connectivity devices.

Click Next to begin.

To organize computers into zones with the Home Network Wizard

1 In the Home Network Wizard, click **Next**.

2 In the resulting list, check the network adapters that you want Norton Internet Security to configure automatically and add to your Trusted Zone.

3 Click **Next**.

4 Click **Finish** to close the wizard.

To manually add computers to zones

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Home Networking tab, select the zone to which you want to add a computer.

4 Click **Add**.

See "Identify computers to Norton Internet Security" on page 93.

5 In the Specify Computers window, identify the computer.

6 When you have finished adding computers, click **OK**.

To remove computers from zones

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.

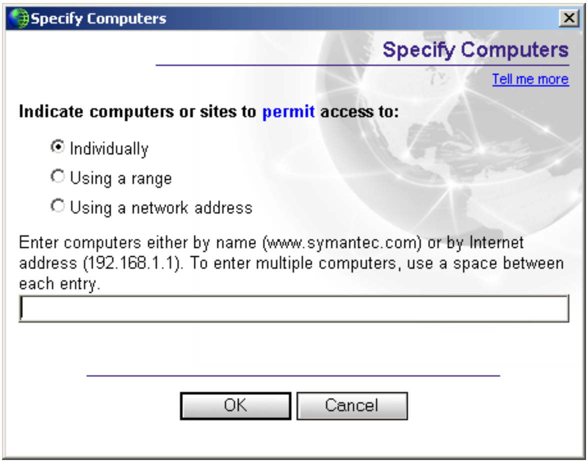
3 Select the computer that you want to remove.

4 Click **Remove**.

5 When you have finished removing computers, click **OK**.

Identify computers to Norton Internet Security

You must identify computers to Norton Internet Security to manually configure network zones, firewall rules, and other protection features. In these cases, the Specify Computers dialog box appears.



Indicate computers or sites to permit access to:

● Individually
○ Using a range
○ Using a network address

Enter computers either by name (www.symantec.com) or by Internet address (192.168.1.1). To enter multiple computers, use a space between each entry.

See "About the Internet" on page 215.

The Specify Computers dialog box lets you specify computers in three ways. In each, you can use *IP addresses* to identify computers.

Find a computer's IP address

There are two procedures for finding a computer's IP address. On Windows 98/Me computers, you can use Winipcfg to find the IP address of a computer. On Windows 2000/XP computers, you can use Ipconfig to find the IP address of a computer.

To find an IP address with Winipcfg

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run dialog box, type **winipcfg**
3. Click **OK**.
4. Select the appropriate network adapter.
5. Record the IP address.

To find an IP address with Ipconfig

1. On the Windows taskbar, click **Start** > **Run**.
2. In the Run dialog box, type **cmd**
3. Click **OK**.
4. At the command prompt, type **ipconfig**
5. Click **OK**.
6. Record the IP address.

Specify an individual computer

The computer name that you type can be an IP address, a *URL* such as service.symantec.com, or a Microsoft Network computer name, such as Mojave. You can find the names of computers on your local network in Network Neighborhood or Network Places on your Windows desktop.

If you don't have TCP/IP bound to Client for Microsoft Networks in Windows Network Properties, you must use IP addresses instead of names for the computers on your local network.

To specify an individual computer

1. In the Specify Computers dialog box, click **Individually**.
2. Type the name or IP address of a single computer.
3. Click **OK**.

Specify a range of computers

You can enter a range of computers by specifying the starting (lowest numerically) IP address and the ending (highest numerically) IP address. All of the computers within that range of IP addresses are included.

In almost every case, the first three of the four numbers of the IP addresses entered should be the same.

To specify a range of computers

1. In the Specify Computers dialog box, click **Using a range**.
2. In the Starting Internet Address text box, type the starting (lowest numerically) IP address.
3. In the Ending Internet Address text box, type the ending (highest numerically) IP address.
4. Click **OK**.

Specify computers using a network address

See "How computers are identified on the Internet" on page 222.

You can identify all of the computers on a single *subnet* by specifying an IP address and a subnet mask. The IP address that you specify can be any address in the subnet that you are identifying.

To specify computers using a network address

1. In the Specify Computers dialog box, click **Using a network address**.
2. In the Network Address text box, type the IP address of a computer on the subnet.
3. In the Subnet Mask text box, type the subnet mask.
   The appropriate subnet mask is almost always 255.255.255.0.
4. Click **OK**.

If you use DHCP

If your *ISP* uses a *DHCP* server to provide IP addresses to users' computers, you must be careful when entering IP addresses.

Instead of identifying a computer with a single IP address, which might change at any time, enter a network address using a base IP address and a subnet mask. Enter values that cover the range of addresses that might be assigned to the computer.

Control how users access the Internet

Norton Internet Security supports most Internet *connection* methods without needing additional configuration.

If you access the Internet via a cable or DSL router

Norton Internet Security works behind a cable or DSL *router* and adds to the protection provided by the router. In some cases, you might want to reduce the protection provided by the router so that you can use programs like NetMeeting or Microsoft Messenger. Norton Internet Security also provides features that might not be available with cable and DSL routers, such as privacy protection.

If multiple computers share a single Internet connection

Norton Internet Security works with most Internet connection sharing programs. To protect your network from many outside attacks, install Norton Internet Security on the gateway computer. For maximum protection against *Trojan horses* or other problem programs that initiate *outbound connections*, install Norton Internet Security on all computers that share the connection.

If your ISP uses a proxy server

Norton Internet Security works with most *proxy* servers. However, you might have to change some settings to maintain full protection.

To determine whether Norton Internet Security works with your proxy server

1. Open Norton Internet Security.
2. In the Security Center, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. Under Web, look at the Bytes Processed counter.
5. Use your browser to connect to a Web site.
   The Bytes Processed counter in the Detailed Statistics window should increase as you access Web pages. This indicates that Norton Internet Security is correctly configured to work with your proxy server.
6. To close the Detailed Statistics window, on the File menu, click **Exit**.

If the Bytes Processed counter stays at 0, then Norton Internet Security is probably not monitoring the port used by your proxy server. You will have to determine which ports your proxy server is using for HTTP communications, then configure Norton Internet Security to monitor those ports.

To determine which port to monitor for HTTP communication

1. Open Norton Internet Security.
2. Use your browser to connect to a Web site.
3. In the Security Center, click **Statistics**.
4. In the Statistics window, click **View Logs**.
5. On the Connections tab, in the Remote column, look at the information.
   There should be a port number following the IP address of the site that you viewed with your browser. This number is the port number that is used to access your proxy server for your Web connection.
6. Record the port number.

To specify which ports to monitor for HTTP communication

1. Open Norton Internet Security.
2. At the top of the Security Center window, click **Options** > **Internet Security**.
3. On the Firewall tab, under HTTP Port List, do one of the following:
   - To add a port to the HTTP Port List, click **Add**, then type the number of the port that you want to monitor for HTTP communication.
   - To remove a port from the HTTP Port List, select the port number in the HTTP Port List, then click **Remove**.
4. Click **OK**.

Control how outside users access your network

Norton Internet Security can protect computers while still allowing outside users to access servers on your *network*. To run *servers* on protected computers, you may have to create firewall rules that let outside users connect to certain ports. For maximum security, only create these rules on the computers running your servers.

If you run a Web server

To let a Web server run behind Norton Internet Security, you must create a firewall rule that allows inbound TCP *connections* on port 80. The easiest way to create these rules is via a Norton Internet Security *alert*.

To create rules for a Web server using a Norton Internet Security alert

1. On the Web server, view your Web site by typing the IP address in the address bar of your browser.
   Norton Internet Security displays an alert.
2. In the alert, in the drop-down menu, click **Automatically configure Internet access**.
3. Click **OK**.

If you run an FTP server

To let an FTP server run behind Norton Internet Security, you must create the following rules:

- Allow inbound TCP connections on port 21.
- Allow outbound TCP connections on port 22.
- Allow inbound TCP connections on ports 1024 to 5000.

The easiest way to create these rules is via a Norton Internet Security alert.

To create rules for an FTP server using a Norton Internet Security alert

1. In the address bar of your browser, type **FTP://** followed by the IP address of your FTP server.
   Norton Internet Security displays an alert.
2. In the alert, in the drop-down menu, click **Automatically configure Internet access**.
3. Click **OK**.

If you run Symantec pcAnywhere

See “Change an existing firewall rule” on page 118.

You should have no problems using Symantec pcAnywhere as either a client or host with Norton Internet Security. For maximum protection, if you run a Symantec pcAnywhere host, edit the rule to limit its use to only the computers with which you use it. This, and Symantec pcAnywhere *passwords*, provide maximum security.

If you run a Virtual Private Network

Norton Internet Security works with the following Virtual Private Networks (VPNs):

- Nortel
- VPNRemote
- PGP
- SecureRemote

With most VPNs, when the VPN client is active, you cannot see the Internet or other computers on your local network. You can only see what is available through the VPN server to which you are connected.

7 Guarding against intrusion attempts

Internet attacks take advantage of the way that computers transfer information. Norton Internet Security can protect your computer by monitoring the information that comes into and out of your computer and blocking any attack attempts.

Information travels across the Internet in the form of *packets*. Along with the data, each packet includes a header that contains information about the sending computer, the intended recipient, how the data in the packet should be processed, and the port that should receive the packet.

Ports are channels that divide the stream of information coming from the Internet into separate paths that are handled by individual programs. When Internet programs run on a computer, they listen to one or more ports and accept information sent to these ports.

Network attacks are designed to take advantage of weaknesses in specific Internet programs. Attackers use tools that send packets containing malicious programming code to a particular port. If a program that is vulnerable to this attack is listening to that port, the code can let the attacker gain access to, disable, or even take control of the computer. The programming code that is used to generate the attacks may be contained inside of a single packet or span several packets.

How Norton Internet Security protects against network attacks

Norton Internet Security includes three tools that protect your computer from intrusion attempts, malicious Web content, and *Trojan horses*:

- Norton Personal Firewall
  Monitors all Internet communication and creates a shield that blocks or limits attempts to view information on your computer
- Intrusion Detection
  Analyzes all incoming and outgoing information for data patterns typical of an attack
- Visual Tracking
  Identifies the computer responsible for the attack

Norton Personal Firewall monitors communications

When Norton Personal Firewall is active, it monitors communications among your computer and other computers on the Internet. It also protects your computer from such common security problems as:

Improper connection attempts	Warns you of any connection attempts from other computers and attempts by programs on your computer to connect to other computers
Trojan horses	Notifies you when your computer encounters destructive programs that are disguised as something useful
Security and privacy incursions by malicious Web content	Monitors all Java applets and ActiveX controls and lets you choose whether to run or block the program
Port scans	Cloaks inactive ports on your computer and detects port scans
Intrusions	Detects and blocks malicious traffic and attempts by outside users to attack your computer

See "Customize firewall protection" on page 105.

You can control the level of protection that Norton Personal Firewall provides by using the Security Level slider. You can also control how Norton Personal Firewall reacts to improper connection attempts, Trojan horses, and malicious Web content.

Intrusion Detection analyzes communications

Intrusion Detection scans each *packet* that enters and exits your computer for attack signatures, arrangements of information that identify an attacker's attempt to exploit a known operating system or program vulnerability.

Norton Internet Security protects your computer against most common Internet attacks, including the following.

Bonk	An attack on the Microsoft TCP/IP stack that can crash the attacked computer
RDS_Shell	A method of exploiting the Remote Data Services component of the Microsoft Data Access Components that lets a remote attacker run commands with system privileges
WinNuke	An exploit that can use NetBIOS to crash older Windows computers

Because attacks may span packets, Intrusion Detection examines packets in two different ways. It scans each packet individually looking for patterns that are typical of an attack. It also monitors the packets as a stream of information, which lets it identify attacks spread across multiple packets.

If the information matches a known attack, Intrusion Detection automatically discards the packet and severs the *connection* with the computer that sent the data. This protects your computer from being affected in any way.

You can modify how Intrusion Detection responds to attacks by excluding attack signatures from being monitored and by enabling or disabling AutoBlock, which automatically blocks all communication with an attacking computer. By excluding certain network behavior from blocking, you can continue to be productive, even while your computer is under attack.

Along with protecting your computer against attacks, Norton Internet Security also monitors all of the information that your computer sends to other computers. This ensures that your computer cannot be used to attack other users or be exploited by *zombies*. If Norton Internet Security detects that your computer is sending information that is typical of an attack, it immediately blocks the connection and warns you about the possible problem.

To reduce the number of warnings that you receive, Norton Internet Security only monitors attacks that are targeted at ports that your computer uses. If an attacker attempts to connect to your computer via an inactive port or a port that has been blocked by the firewall, Norton Internet Security will not notify you because there is no risk of an intrusion.

Norton Internet Security does not scan for intrusions by computers in your Trusted Zone. However, Intrusion Detection does monitor the information that you send to Trusted computers for signs of zombies and other remote control attacks.

See "Keeping current with LiveUpdate" on page 81.

Intrusion Detection relies on an extensive list of attack signatures to detect and block suspicious network activity. Run LiveUpdate regularly to ensure that your list of attack signatures is up to date.

Visual Tracking locates attackers

See "Identify the source of communications" on page 58.

Norton Internet Security now includes Visual Tracking, which lets you get information about the IP address used for a particular connection. This can help you identify the source of an attack.

Ensure that Norton Personal Firewall and Intrusion Detection are enabled

Norton Personal Firewall and Intrusion Detection are automatically enabled when you install Norton Internet Security. It is unlikely that you need to change any settings. However, you can ensure that the firewall and Intrusion Detection are working by following these steps.

To ensure that Norton Personal Firewall is enabled

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.
3. Check **Turn on Personal Firewall** to activate Norton Personal Firewall.

To ensure that Intrusion Detection is enabled

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. Check **Turn on Intrusion Detection** to activate Intrusion Detection.

Customize firewall protection

The default Norton Personal Firewall settings should provide adequate protection for most users. If the default protection is not appropriate, you can customize Norton Personal Firewall protection by using the Security Level slider to select preset security levels, or by changing individual security settings.

Change the Security Level slider

The Security Level slider lets you select Minimal, Medium, or High security settings. When you change the slider position, the protection level changes. Changing the Security Level slider does not affect the protection provided by Intrusion Detection.

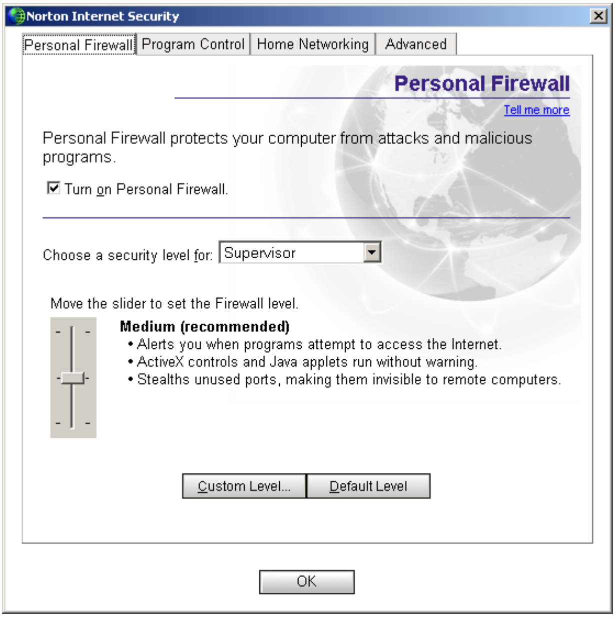
You can set individual Security settings for each Norton Internet Security user.

See "About Norton Internet Security accounts" on page 145.

To change the Security Level slider

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.



Personal Firewall protects your computer from attacks and malicious programs.

☑ Turn on Personal Firewall.

Choose a security level for: Supervisor

Move the slider to set the Firewall level.

Medium (recommended)
- Alerts you when programs attempt to access the Internet.
- ActiveX controls and Java applets run without warning.
- Stealths unused ports, making them invisible to remote computers.

3 In the Personal Firewall window, in the Choose a security level for drop-down list, select the account that you want to change.

4 Move the slider to the Security Level that you want. Your options are:

High	The firewall blocks everything until you allow it. If you have run a Program Scan, you should not be interrupted frequently with Program Control alerts. See "Enable Automatic Program Control" on page 110. You are alerted each time that an ActiveX control or Java applet is encountered. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Medium (recommended)	The firewall blocks everything until you allow it. If you have run a Program Scan, you should not be interrupted frequently with Program Control alerts. ActiveX controls and Java applets run without warning. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Minimal	Firewall blocks connection attempts by Trojan horse programs. ActiveX controls and Java applets run without warning.

Change individual security settings

If the Security Level options do not meet your needs, you can change the settings for Norton Personal Firewall, *Java*, and *ActiveX* protection levels. Changing an individual setting overrides the Security Level, but it does not change the other security settings in that level.

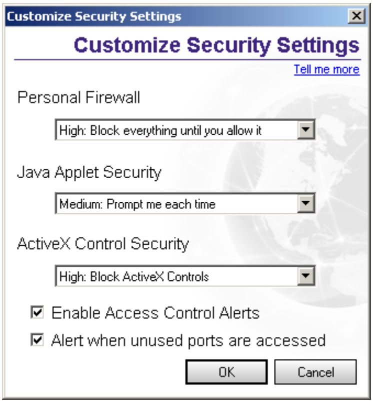
To change individual security settings

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, in the Choose a security level for drop-down list, select the account that you want to change.

4 Click **Custom Level**.



Customize Security Settings

Personal Firewall

High: Block everything until you allow it

Java Applet Security

Medium: Prompt me each time

ActiveX Control Security

High: Block ActiveX Controls

☑ Enable Access Control Alerts

☑ Alert when unused ports are accessed

5 Do one or more of the following:

- On the Personal Firewall menu, select a level. Your options are:

High	Blocks all communication that you do not specifically allow. You must create firewall rules for every program that requests Internet access.
Medium	Blocks many ports that are used by harmful programs. However, it can also block useful programs when they use the same ports.
None	Disables Norton Personal Firewall and allows all Internet communications.

- On the Java Applet Security or ActiveX Control Security menu, select a level. Your options are:

High	Blocks your browser from running any Java applets or ActiveX controls over the Internet. This is the safest, but most inconvenient, option. Some Web sites might not operate properly using this setting.
Medium	Prompts you when Java applets and ActiveX controls are encountered. This lets you temporarily or permanently allow or block each Java applet or ActiveX control that you encounter. It can be bothersome to respond every time that you encounter a Java applet or ActiveX control, but it lets you decide which ones to run.
None	Lets Java applets and ActiveX controls run whenever you encounter them.

- To be notified whenever unknown programs access the Internet, check **Enable Access Control Alerts**.
- To be notified whenever a remote computer attempts to connect to a port no program is using, check **Alert when unused ports are accessed**.

6 Click **OK**.

Reset security settings to defaults

Setting a custom security level disables the Security Level slider. The slider indicates the security level on which your custom level is based, but you cannot use the slider to make changes to your settings. To use the slider to choose a preset security level, you must reset the security level.

To reset security settings to defaults

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, in the Choose a security level for drop-down list, select the account that you want to change.

4 Click **Default Level**.

This resets your security level to medium. Use the Security Level slider to choose one of the other preset security levels.

See "Change the Security Level slider" on page 105.

Customize firewall rules

Firewall rules control how Norton Personal Firewall protects your computer from malicious incoming traffic, programs, and *Trojan horses*. The firewall automatically checks all data coming in or out of your computer against these rules.

How firewall rules are processed

When a computer attempts to connect to your computer, or when your computer attempts to connect to a computer on the Internet, Norton Personal Firewall compares the type of *connection* with its list of firewall rules.

Firewall rules are processed in a set order based on their types. System rules are processed first, followed by program rules, and then Trojan horse rules.

Once a rule that blocks or permits communications is matched, all remaining rules are ignored. In other words, additional rules that match this type of communication are ignored if they appear below the first rule that matches.

For example, you may have a rule that blocks the use of Symantec pcAnywhere on your computer. If you add a rule that permits the use of Symantec pcAnywhere with a specific computer and move the new rule higher in the list, the new rule lets you use Symantec pcAnywhere with that specific computer, but the older rule prevents its use with any other computer.

If no matching rule is found, the communication is blocked. Depending on the Reporting level, an alert may appear.

About the default firewall rules

A number of firewall rules are predefined and enabled when you install Norton Internet Security. These rules provide basic network functionality as well as protect you from known Internet risks. The default firewall rules appear in the general settings and in Trojan horse settings. Examples of default firewall rules include:

Default Inbound DNS Default Outbound DNS	Permits the use of the Domain Name System (DNS).
Default Inbound Bootp Default Outbound Bootp	Permits the use of the BOOTP service. (BOOTP is short for Bootstrap Protocol, which enables a computer to discover its own IP address.)
Default Inbound NetBIOS Name Default Inbound NetBIOS Default Outbound NetBIOS	Controls the use of the NetBIOS name service and the NetBIOS datagram service that are used in file sharing on the Microsoft Network.
Default Inbound Loopback Default Outbound Loopback	Permits inbound and outbound loopback connections to the localhost address of 127.0.0.1. It is usually safe to permit loopback or local connections because the connection originator is typically a trusted program on your own computer. Even with this firewall rule enabled, remote computers are never allowed access to the localhost address by the underlying network.

Default Inbound ICMP Default Outbound ICMP	Permits all types of outbound and safe types of inbound ICMP messaging. ICMP messages provide status and control information.
Default Block Back Orifice 2000 Trojan Default Block NetBus Trojan	Protects you from known remote-access Trojan horse programs.

Create new firewall rules

Norton Internet Security includes Program Control, which helps you create firewall rules as you use the Internet.

See "About Norton Internet Security accounts" on page 145.

Supervisor and Adult users can create and modify firewall rules. Child and Teenager users cannot make any changes to firewall rules.

There are four ways to create firewall rules with Program Control:

Enable Automatic Program Control	Automatically configures access for well-known programs the first time that users run them. This is the easiest way to set up firewall rules.
Use Program Scan	Finds and configures access for all Internet-enabled programs on a computer at once.
Manually add programs	Closely manage the list of programs that can access the Internet.
Respond to alerts	Norton Internet Security warns users when a program attempts to access the Internet for the first time. Users can then allow or block Internet access for the program.

Enable Automatic Program Control

When Automatic Program Control is active, Norton Internet Security can automatically configure Internet access settings for programs the first time that they run. Automatic Program Control only configures Internet access for the versions of programs that Symantec has identified as safe.

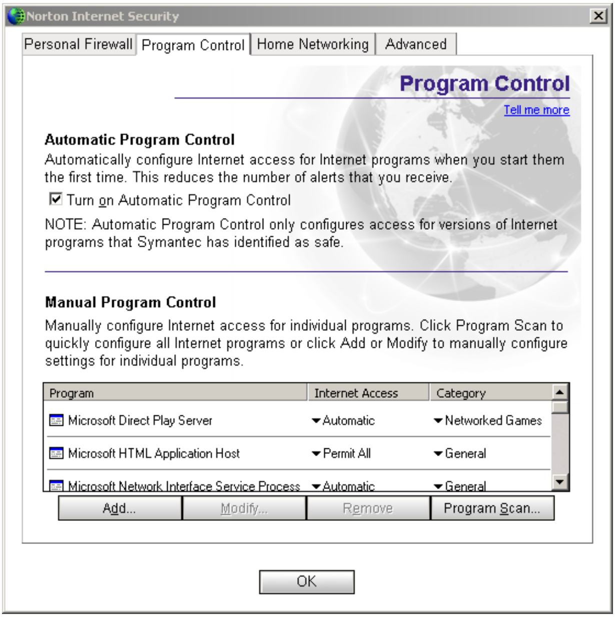
If an unknown program or an unknown version of a known program attempts to access the Internet, Norton Internet Security warns the user. The user can then choose to allow or block Internet access for the program.

See "Keeping current with LiveUpdate" on page 81.

Symantec regularly updates the list of recognized programs. You should run LiveUpdate regularly to ensure that your list is up-to-date.

To enable Automatic Program Control

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.



Automatic Program Control

Automatically configure Internet access for Internet programs when you start them the first time. This reduces the number of alerts that you receive.

☑ Turn on Automatic Program Control

NOTE: Automatic Program Control only configures access for versions of Internet programs that Symantec has identified as safe.

Manual Program Control

Manually configure Internet access for individual programs. Click Program Scan to quickly configure all Internet programs or click Add or Modify to manually configure settings for individual programs.

Program	Internet Access	Category
Microsoft Direct Play Server	Automatic	Networked Games
Microsoft HTML Application Host	Permit All	General
Microsoft Network Interface Service Process	Automatic	General

3. In the Personal Firewall window, on the Program Control tab, check **Turn on Automatic Program Control**.
4. Click **OK**.

Scan for Internet-enabled programs

Scanning for Internet-enabled programs is the quickest way to configure the Personal Firewall. Norton Internet Security scans the computer for programs that it recognizes and suggests appropriate settings for each program.

You can scan for Internet-enabled programs from the Security Center or the Security Monitor.

To scan for Internet-enabled programs from the Security Center

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Program Control tab, click **Program Scan**.
4. Select the disk or disks on your computer that you want to scan.
5. Click **OK**.
6. In the Program Scan window, do one of the following:
   - Check programs that you want to add to the Program Control list.
   - To add all Internet-enabled programs at once, click **Check All**.
7. Click **Finish**.
8. Click **OK**.

To scan for Internet-enabled programs from the Security Monitor

1. Open Norton Internet Security.
2. In the Security Monitor, on the Select a Task menu, click **Program Scan**.
3. Select the disk or disks on your computer that you want to scan.
4. Click **OK**.
5. In the Program Scan window, do one of the following:
   - Check programs that you want to add to the Program Control list.
   - To add all Internet-enabled programs at once, click **Check All**.
6. Click **Finish**.

Manually add a program to Program Control

See "Customize firewall protection" on page 105.

Users can add programs to Program Control to strictly control the programs' ability to access the Internet. This overrides any settings made by Automatic Program Control.

To add a program to Program Control

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Program Control tab, click **Add**.
4. Select the program's executable file.
   Executable file names typically end in .exe.

5 Click **Open**.

6 In the Internet Access Control alert, select the access level you want this program to have. Your options are:

Automatically configure Internet access (Recommended)	Use the default Norton Internet Security settings for this program.
Permit	Allow all access attempts by this program.
Block	Deny all access attempts by this program.
Manually configure Internet Access	Create rules controlling how this program accesses the Internet.

7 If you want to see any risks that this program could pose to your computer, click **Details**.

8 Click **OK**.

Change Program Control settings

After using Norton Internet Security for a while, you may find that you need to change access settings for certain programs. Any changes override settings made by Automatic Program Control.

To change Program Control settings

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Program Control tab, in the list of programs, click the program that you want to change.

4 Click **Modify**.

5 In the Internet Access Control alert, select the access level you want this program to have. Your options are:

Automatically configure Internet access	Use the default Norton Internet Security settings for this program.
Permit this program access to the Internet	Allow all access attempts by this program.

Block this program from accessing the Internet	Deny all access attempts by this program.
Customize Internet access for this program	Create rules controlling how this program accesses the Internet.

6 Click **OK**.

Manually add a firewall rule

While Norton Internet Security automatically creates most of the firewall rules that you need, you may want to add specific rules. Only experienced Internet users should create their own firewall rules.

There are three sets of firewall rules you can customize:

- General Rules
- Trojan Horse Rules
- Program Rules

To add a General Rule

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Advanced tab, click **General Rules**.

4 Follow the on-screen instructions.
See “Write a firewall rule” on page 115.

To add a Trojan Horse Rule

1 Open Norton Internet Security.

2 In the Security Center, double-click **Personal Firewall**.

3 In the Personal Firewall window, on the Advanced tab, click **Trojan Horse Rules**.

4 Follow the on-screen instructions.
See “Write a firewall rule” on page 115.

To add a Program Rule

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Program Control tab, in the list of programs, click **Add**.
4. In the Select a program window, select a program's executable file. Executable file names typically end in .exe.
5. In the Internet Access Control alert, on the What do you want to do menu, select **Create a firewall rule**.
6. Follow the on-screen instructions.
   See "Write a firewall rule" on page 115.

Write a firewall rule

Norton Internet Security leads you through the process of writing your own firewall rules.

To write a firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, click **Add**.
2. In the Add Rule window, select the action that you want for this rule. Your options are:

Permit Internet Access	Allows communication of this type to take place.
Block Internet Access	Prevents communication of this type from taking place.
Monitor Internet Access	Updates the Firewall tab in the Event Log or shows a message each time that communication of this type takes place. This lets you monitor how often this firewall rule is used. ⚠ To monitor a permitted connection, you must create both a monitor and a permit rule. The monitor rule must precede the permit rule.

3. Click **Next**.

4 Select the type of connection the rule should monitor. Your options are:

Connections to other computers	The rule applies to outbound connections from your computer to another computer.
Connections from other computers	The rule applies to inbound connections from another computer to your computer.
Connections to and from other computers	The rule applies to both inbound and outbound connections.

5 Click **Next**.

6 Select the computers the rule should monitor. Your options are:

Any computer	The rule applies to all computers.
Only computers specified below	The rule applies only to the computers, sites, and domains listed.
Adapters	The rule applies to a specific network adapter in your computer. This allows you to customize firewall rules for each of your computer's IP addresses. For example, if your computer is connected to a home network and to the Internet, you might want to set up a rule that permits file sharing on the home network, while another rule blocks file sharing over the Internet.

7 Click **Next**.

8 Select the protocols the rule should monitor. Your options are:

TCP	The rule applies to TCP (Transmission Control Protocol) communications.
UDP	The rule applies to UDP (User Datagram Protocol) communications.
TCP and UDP	The rule applies to both TCP and UDP communications.
ICMP	The rule applies to ICMP (Internet Control Message Protocol) communications. This option is only available when adding or modifying a General Rule.

9 Select the ports the rule should monitor. Your options are:

All types of communications (all ports)	The rule applies to communications using any port.
Only the types of communications or ports listed below	The rule applies to the ports listed. You can add ports to, or remove ports from, the list.

10 Click **Next**.

11 Choose if and how you want Norton Internet Security to track this rule. Your options are:

Do not track this rule	No record of the actions of this rule is made.
Create an Event Log entry	An entry is created in the firewall Event Log when a network communication event matches this rule.
Notify me with an Alert Tracker message	An Alert Tracker message appears when a network communication event matches this rule.
Display Security Alert	A Security Alert dialog box appears when a network communication event matches this rule.

12 Click **Next**.

13 In the **What do you want to call this rule?** text box, type a name for this rule.

14 In the **In which category does this rule belong?** text box, select a category.

15 Click **Next**.

16 Review the new rule settings, then click **Finish**.

17 When you have finished adding rules, click **OK**.

Change an existing firewall rule

You can change firewall rules if they are not functioning the way that you want.

To change an existing firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, click **Add**.
2. Select the rule that you want to change.
3. Click **Modify**.
4. Follow the on-screen instructions to change any aspect of the rule.
5. When you have finished changing rules, click **OK**.

See "Write a firewall rule" on page 115.

Change the order of firewall rules

See "How firewall rules are processed" on page 108.

Norton Internet Security processes each list of firewall rules from the top down. You can determine how Norton Internet Security processes firewall rules by changing their order.

To change the order of a firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, select the rule that you want to move.
2. Do one of the following:
   - To have Norton Internet Security process this rule before the rule above it, click **Move Up**.
   - To have Norton Internet Security process this rule after the rule below it, click **Move Down**.
3. When you are done moving rules, click **OK**.

Temporarily disable a firewall rule

You can temporarily disable a firewall rule if you need to allow specific access to a computer or program.

To temporarily disable a firewall rule

❖ In the General Rules, Trojan Horse Rules, or Program Rules window, uncheck the box next to the rule you want to disable.

Remember to re-enable the rule when you are done working with the program or computer that required the change.

Remove a firewall rule

Remove firewall rules when they are no longer necessary.

To remove a firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, click **Add**.
2. Select the rule that you want to remove.
3. Click **Remove**.
4. When you are done removing rules, click **OK**.

Reset firewall rules to the default settings

Resetting the firewall rules returns all users' firewall protection to the default settings and deletes any changes you have made to firewall rules.

You should only use this procedure in an emergency. Before resetting your firewall rules, try removing recently changed firewall rules.

To reset the firewall rules to the default settings

1. Close all Norton Internet Security windows.
2. In Windows Explorer, double-click **My Computer**.
3. Double-click the hard disk on which you installed Norton Internet Security.
   In most cases, this will be drive C.
4. Open **Program Files** > **Common Files** > **Symantec Shared**.
5. Drag **firewall.rul** to the Recycle Bin.

The firewall will return to its default settings the next time you run Norton Internet Security.

Customize Intrusion Detection

The default Intrusion Detection settings should provide adequate protection for most users. You can customize Intrusion Detection by excluding specific network activity from monitoring, enabling or disabling AutoBlock, and restricting blocked computers.

Exclude specific network activity from being monitored

In some cases, benign network activity may appear similar to a Norton Internet Security attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by safe behavior, you can create an exclusion for the attack signature that matches the benign activity.

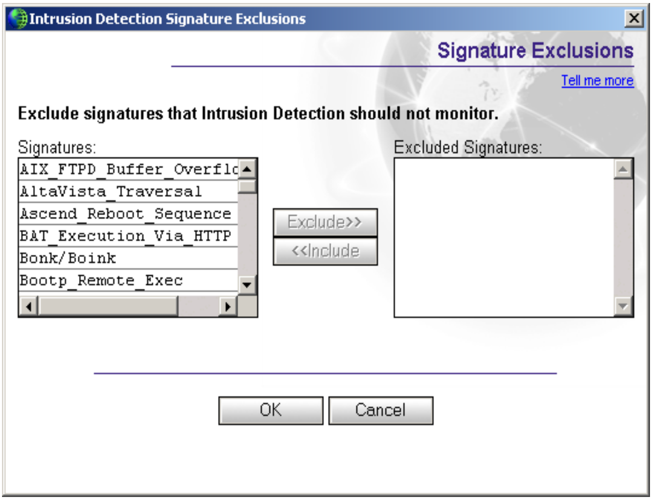
Each exclusion that you create leaves your computer vulnerable to attacks. Be very selective when excluding attacks. Only exclude behavior that is always benign.

To exclude attack signatures from being monitored

1 Open Norton Internet Security.

2 In the Security Center, double-click **Intrusion Detection**.

3 In the Intrusion Detection window, click **Signatures**.



Exclude signatures that Intrusion Detection should not monitor.

Signatures:

AIX_FTPD_Buffer_Overflc
AltaVista_Traversal
Ascend_Reboot_Sequence
BAT_Execution_Via_HTTP
Bonk/Boink
Bootp_Remote_Exec

4 In the Signatures list, select the attack signature that you want to exclude.

5. Click **Exclude**.
6. When you are done excluding signatures, click **OK**.

If you have excluded attack signatures that you want to monitor again, you can include them in the list of active signatures.

To include attack signatures

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, click **Signatures**.
4. In the Excluded Signatures list, select the attack signature that you want to monitor.
5. Click **Include**.
6. When you are done including signatures, click **OK**.

Enable or disable AutoBlock

When Norton Internet Security detects an attack, it automatically blocks the *connection* to ensure that your computer is safe. The program can also activate AutoBlock, which automatically blocks all incoming communication from the attacking computer for a set period of time, even if the incoming communication does not match an attack signature.

AutoBlock stops all inbound communications with the attacking computer for 30 minutes.

To enable or disable AutoBlock

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, check or uncheck **Turn on AutoBlock**.

Unblock computers

In some cases, Norton Internet Security may recognize normal activity as an attack. If you can’t communicate with computers that you should be able to communicate with, they may be on the list of computers currently blocked by AutoBlock.

If a computer that you need to access appears on the list of computers currently blocked by AutoBlock, unblock it. If you have changed your protection settings and want to reset your AutoBlock list, you can unblock all of the computers on the AutoBlock list at once.

To unblock computers currently blocked by AutoBlock

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, do one of the following:
   - To unblock one computer, select its IP address, then click **Unblock**.
   - To unblock all computers on the AutoBlock list, click **Unblock All**.

Exclude computers from AutoBlock

If a computer you need to access is repeatedly placed in the AutoBlock list, you can exclude it from being blocked by AutoBlock.

To exclude specific computers from AutoBlock

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, click **IP Address**.
4. Do one of the following:
   - In the Currently blocked list, select a blocked IP address, then click **Exclude**.
   - Click **Add**, then type the computer’s name, IP address, network identification, or a range of IP addresses containing the computer that you want to exclude.
5. When you are done excluding IP addresses, click **OK**.

Restrict a blocked computer

You can add a blocked computer to your Restricted Zone to permanently prevent that computer from accessing your computer. Computers added to the Restricted Zone do not appear on the blocked list because Norton Internet Security automatically rejects any *connection attempts* by restricted computers.

To restrict a blocked computer

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the list of computers that are currently blocked by AutoBlock, select the computer to add to the Restricted Zone.
4. Click **Restrict**.
5. When you are done restricting computers, click **OK**.

Protecting disks, files, and data from viruses

8

Keeping your computer protected requires regular monitoring by Auto-Protect, Script Blocking, and Worm Blocking; scanning of your *email* attachments and files transferred by instant messenger; and frequent system scans. All of these tasks can be set to occur automatically.

For added protection in Norton AntiVirus on Windows 98/98SE/Me, enable Inoculation to *alert* you if a system file changes.

Ensure that protection settings are enabled

Norton AntiVirus is configured to provide you with complete protection against viruses. It is unlikely that you need to change any settings. However, for maximum protection, you should ensure that your protection features are enabled.

Feature	Where to set	Maximum protection setting
Auto-Protect	**Security Center** > **Norton AntiVirus** > **Enable** See "About System options" on page 65.	Auto-Protect is set to **On**.
Email scanning	**Options** > **Norton AntiVirus** > **Email** See "About Internet options" on page 67.	**Scan incoming Email** and **Scan outgoing Email** are checked. If your email program uses one of the supported communications protocols, both options are selected by default.

Timeout protection	**Options > Norton AntiVirus > Email** See "About Internet options" on page 67.	**Protect against timeouts when scanning Email** is checked. To prevent connection timeouts while receiving large attachments, enable timeout protection.
Instant messenger scanning	**Options > Norton AntiVirus > Instant Messenger** See "About Internet options" on page 67.	Instant messengers that you want to protect are checked.
Worm Blocking	**Options > Norton AntiVirus > Email** See "About Internet options" on page 67.	**Enable Worm Blocking** and **Alert me when scanning email attachments** are checked.
Script Blocking	**Options > Norton AntiVirus > Script Blocking** See "About System options" on page 65.	**Enable Script Blocking** is checked.
Inoculation	**Options > Norton AntiVirus > Inoculation** See "About Other options" on page 68.	**Inoculate Boot Records** is checked.

This table summarizes the maximum protection settings and where you can find them. For specific information about an option, check the online Help.

Manually scan disks, folders, and files

If Auto-Protect is enabled and the Norton AntiVirus options are set at their default levels, you normally would not need to scan manually. However, if you temporarily disabled Auto-Protect (for example, to load or use another program that conflicts with Norton AntiVirus), and you forgot to enable it again, it is possible that a virus could be on your hard disk undetected. You can scan your entire computer, or individual floppy disks, drives, folders, or files.

Although the default settings for manual scanning are usually adequate, you can raise the level of Bloodhound heuristics or adjust the options for manual scanning in the Options window. Check online Help for more information about manual scanning options.

Perform a full system scan

A full system scan scans all *boot records* and files on your computer.

To perform a full system scan

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.
3. In the Scan for Viruses pane, click **Scan my computer**.
4. Under Actions, click **Scan**.
   When the scan is complete, a scan summary appears.
5. When you are done reviewing the summary, click **Finished**.

Scan individual elements

Occasionally, you may want to scan a particular file, removable drives, a floppy disk, any of your computer's drives, or any folders or files on your computer. You may have been working with floppy disks or have received a compressed file in an email message and suspect a virus. You can scan just a particular disk or individual element that you want to check.

To scan individual elements

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to run.
4. Under Actions, click **Scan**.
   If you choose to scan all removable drives or a floppy disk, the scan starts automatically. If you choose to scan drives, folders, or files, a dialog box appears in which you choose which drives, folders, or files to scan.
5. In the dialog box, click **Scan** after making your selection.
   When the scan is complete, a scan summary appears.
6. When you are done reviewing the summary, click **Finished**.

If problems are found during a scan

See "If a virus is found during a scan" on page 134.

At the end of a scan, a summary report appears to tell you what Norton AntiVirus found during the scan. If a virus was found and you have requested that Norton AntiVirus repair the file automatically, it is listed as repaired. If the file cannot be repaired, it can be quarantined or deleted.

Create and use custom scans

See "Schedule a custom scan" on page 130.

You can create a custom scan if you regularly scan a particular segment of your computer and don't want to have to specify the segment to be scanned every time. You can also schedule the custom scan to run automatically.

You can delete the scan when it is no longer necessary. For example, if you are working on a project for which you need to frequently swap files with others, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

To create a custom scan

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.
3. In the Scan for Viruses pane, under Actions, click **New**.
4. In the opening window of the Norton AntiVirus Scan Wizard, click **Next**.
5. Do one or both of the following:
   - To select individual files to be scanned, click **Add files**.
   - To select folders and drives to be scanned, click **Add folders**.

   You can use both options to select the combination of items that you want.
6. In the resulting dialog box, select the items that you want to scan.
   If you select a folder, all files in that folder are included. If you select a drive, all folders and files on that drive are included.
7. Add the selected items to the list of items to scan by doing one of the following:
   - In the Scan Files dialog box, click **Open**.
   - In the Scan Folders dialog box, click **Add**.
8. To remove an item from the list, select it, then click **Remove**.
9. When you are done creating the list of items to be scanned, click **Next**.

10 Type a name for the scan by which you can identify it in the list of scans.

11 Click **Finish**.

Run a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

To run a custom scan

1 Start Norton Internet Security.

2 In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.

3 In the Scan for Viruses pane, select the custom scan.

4 Under Actions, click **Scan**.
When the scan is complete, a scan summary appears.

5 When you are done reviewing the summary, click **Finished**.

Delete a custom scan

You can delete custom scans if they are no longer needed.

To delete a custom scan

1 Start Norton Internet Security.

2 In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.

3 In the Scan for Viruses pane, select the scan that you want to delete.

⚠ If you click the button next to the scan name, the scan runs.

4 Under Actions, click **Delete**.

5 Click **Yes** to verify that you want to delete the scan.

Schedule scans

After installation, Norton AntiVirus automatically runs a weekly full system scan. You can also set up a custom virus scan schedule.

You can schedule customized virus scans that run unattended on specific dates and times or at periodic intervals. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working.

You cannot schedule the predefined scans in the scan list, but you can schedule any custom scans that you have created.

Schedule a custom scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (such as daily, weekly, or monthly), you are presented with additional fields with which you can refine your request. For example, you can request a daily scan, then schedule it to occur every two days or every three days instead.

To schedule a custom scan

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to schedule.

   If you click the button next to the scan name, the scan runs.
4. Under Schedule Task, click **Schedule**.
5. In the Schedule dialog box, if Show multiple schedules is checked, click **New** to enable the scheduling fields.
   If it is not checked, the fields are already enabled.
6. Set the frequency and time at which you want the scan to run.
   Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
7. When you are done, click **OK**.

You can also create multiple schedules for a scan. For example, you could run the same scan at the beginning of your work day and at the end.

To create multiple schedules for a single scan

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to schedule.

   ⚠ If you click the button next to the scan name, the scan runs.
4. Under Schedule Task, click **Schedule**.
5. In the Schedule dialog box, check **Show multiple schedules**.
6. To set an additional schedule, click **New**.
7. Set the frequency and time at which you want the scan to run.
   Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
8. When you are done, click **OK**.

Edit scheduled scans

You can change the schedule of any scheduled scan, including the weekly full system scan.

To edit a scheduled scan

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan that you want to schedule.

   ⚠ If you click the button next to the scan name, the scan runs.
4. Under Schedule Task, click **Schedule**.
5. Change the schedule as desired.
6. Click **OK**.

Delete a scan schedule

You can delete any scan schedule. Deleting the schedule does not delete the scan.

To delete a scan schedule

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Scan for Viruses**.
3. In the Scan for Viruses pane, select the scan you want to schedule.

   If you click the button next to the scan name, the scan runs.

4. Under Schedule Task, click **Schedule**.
5. In the Schedule dialog box, check **Show multiple schedules**.
6. Select the schedule that you want to delete (if more than one).
7. Click **Delete**.
8. Click **OK**.

What to do if a virus is found

9

If Norton AntiVirus finds a virus on your computer, there are three possible resolutions to the problem:

- Fix the file
  Removes the *virus* from the file or if the *threat* is a worm or Trojan horse, deletes the file.
- Quarantine the file
  Makes the file inaccessible by any programs other than Norton AntiVirus. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec.
- Delete the file
  Removes the virus from your computer by deleting the file that contains the virus, worm or Trojan horse. It should be used only if the file cannot be repaired or quarantined.

See "If you have files in Quarantine" on page 138.

Malicious *threats* can be found during a manual or scheduled scan or by Auto-Protect when you perform an action with an *infected file*. Threats can also appear during an instant messenger session or when sending an email. The way that you handle a threat differs depending on whether a scan or Auto-Protect found the threat.

If a virus is found during a scan

If Norton AntiVirus finds a virus, Trojan horse, or worm during a scan or from an instant messenger session, you either receive a summary of the automatic repair or deletion results, or you have to use the Repair Wizard to resolve the problem.

Review the repair details

If you have set your manual scan options so that Norton AntiVirus repairs files automatically, and all infected files could be repaired, the scan summary lists the number of files infected and repaired. This information is presented for status purposes only; you don't need to take further action to protect your computer. If you want to know more, you can check the repair details to see which files were infected and with what viruses.

To review the repair details

1. In the scanner window, in the Summary pane, click **More Details**.
2. When you are done reviewing the results, click **Finished**.

Use the Repair Wizard

If there are files that could not be fixed, or if you have set your manual scan options so that Norton AntiVirus asks you what to do when a virus is found, the Repair Wizard opens. If Norton AntiVirus did not attempt a repair, the Repair Wizard opens in the Repair pane. Otherwise, it opens in the Quarantine pane.

To use the Repair Wizard

1. If the Repair Wizard opens in the Repair pane, uncheck any files that you don't want Norton AntiVirus to fix.
   All files are checked by default. This is the recommended action.
2. Click **Fix**.
   If any files cannot be fixed or deleted, the Quarantine window opens. All files are checked to be added to the Quarantine by default. This is the recommended action.
3. In the Quarantine window, uncheck any files that you do not want to quarantine.
4. Click **Quarantine**.
   If any files could not be quarantined, the Delete pane opens.

If you do not delete the infected files, the virus remains on your computer and can cause damage or be transmitted to others.

5 Uncheck any files that you do not want to delete.

6 Click **Delete**.
Once all of the files have been repaired, quarantined, or deleted, the Summary pane of the scanner window opens.

7 When you are done reviewing the summary, click **Finished**.

After repairing a boot virus on your hard drive, restart your computer.

If a virus is found by Auto-Protect

Auto-Protect scans files for viruses and other malicious *threats* when you perform an action with them, such as moving them, copying them, or opening them. If it detects a virus or virus-like activity, in most cases you receive an *alert* telling you that a virus was found and repaired. How you proceed depends on the *operating system* that you are using.

If you are using Windows 98/98SE/Me

If a virus or threat is found and repaired by Auto-Protect in Windows 98/98SE/Me, you receive an alert telling you which file was repaired or deleted.

To close the alert

❖ Click **Finish**.

If you have set your options so that Auto-Protect asks you what to do when it finds a virus, the alert asks you to choose an action. The recommended action is always preselected.

Action	Result
Repair the infected file	Automatically eliminates the virus, Trojan horse, or worm and repairs or deletes the infected file. When a virus is found, Repair is always the best choice.
Quarantine the infected file	Isolates the infected file, but does not remove the threat. Select Quarantine if you suspect that the infection is caused by an unknown threat and you want to submit the threat to Symantec for analysis.

Action	Result
Delete the infected file	Erases both the threat and the infected file. Select Delete if Repair is not successful. Replace the deleted file with the original program file or backup copy. If the virus, Trojan horse, or worm is detected again, your original copy is infected.
Do not open the file, but leave the problem alone	Stops the current operation to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time that you perform the same activity.
Ignore the problem and do not scan this file in the future	Adds the file that is suspected of containing a threat to the Exclusions list. When you add a file to the Exclusions list, the file is excluded from any future virus scans, unless you remove it from the list. Select this option only if you know that the file does not contain a virus.
Ignore the problem and continue with the infected file	Continues the current operation. Select this option only if you are sure that a virus, Trojan horse or worm is not at work. You will receive an alert again. If you are not sure what to do, select Do not open the file, but leave the problem alone.

If a file cannot be repaired, you receive an alert telling you that the repair was not made and recommending that you quarantine the file. You have the same options as those listed in the table, with the exception of Repair the infected file.

If you are using Windows 2000/XP

If a *threat* is found and either repaired or automatically deleted by Auto-Protect in Windows 2000/XP, you receive an alert telling you which file was repaired or deleted and which virus, Trojan horse, or worm was infecting the file. If you have an active Internet connection, clicking the virus name opens the Symantec Web page that describes the virus.

To close the alert

❖ Click **OK**.

If the file cannot be repaired, you receive two alerts, one telling you that Auto-Protect was unable to repair the file, and another telling you that access to the file was denied.

See "If you have files in Quarantine" on page 138.

You can set your Auto-Protect options to try to quarantine any infected files that it cannot repair. If you do this, you are informed if any files are quarantined.

To resolve problems with unrepaired files

See "Perform a full system scan" on page 127.

1 Run a full system scan on your computer to ensure that no other files are infected.

See "If a virus is found during a scan" on page 134.

2 Follow the recommended actions in the Repair Wizard to protect your computer from the infected files.

If a virus is found by Script Blocking

See "Ensure that protection settings are enabled" on page 125.

Script Blocking scans Visual Basic and JavaScript scripts for viruses. If it detects a virus or virus-like activity, in most cases you receive an alert telling you that a potential *threat* was found.

You must choose one of the options to remove the threat. The recommended action is to stop the script from running. You can click Help on the alert for additional information about how to respond.

If a threat is found by Worm Blocking

See "Ensure that protection settings are enabled" on page 125.

If a program tries to email itself or email a copy of itself, it could be a worm trying to spread via email. A worm can send itself or a copy of itself in an email message without any interaction with you.

Worm Blocking continually scans outgoing email attachments for *worms*. If it detects a worm, you receive an alert telling you that a malicious worm was found.

The alert presents you with options and asks you what to do. If you were not sending an email message at that time, then it is probably a worm and you should quarantine the file. You can click Help on the alert for additional information about how to respond.

After you have responded to the *threat* and deleted the file, you could still have an infected system. Run LiveUpdate, scan your system, and, if necessary, go to the Symantec security response Web page (securityresponse.symantec.com) for the most up-to-date virus definitions clean-up tools.

If Inoculation alerts you about a change in system files

Inoculation protection is available on Windows 98/98SE/Me systems only.

See "Ensure that protection settings are enabled" on page 125.

System files can change for a variety of reasons. You may have updated your *operating system* or repartitioned your hard disk, or you could have a virus. Norton AntiVirus alerts you when a change occurs in your system files.

If you get an *alert* about a change in your system files, you have two options. You can update your Inoculation snapshot or repair the file. Before you repair the file, be sure your virus definitions are up-to-date and run a scan.

To respond to Inoculation changes

❖ In the Alert window, select the action that you want to take. Your options are:

Update the saved copy of my Master Boot Record	Use if the alert appears after a legitimate change in system files.
Restore my Master Boot Record	Use if you are certain the system did not change for legitimate reasons.

If you have files in Quarantine

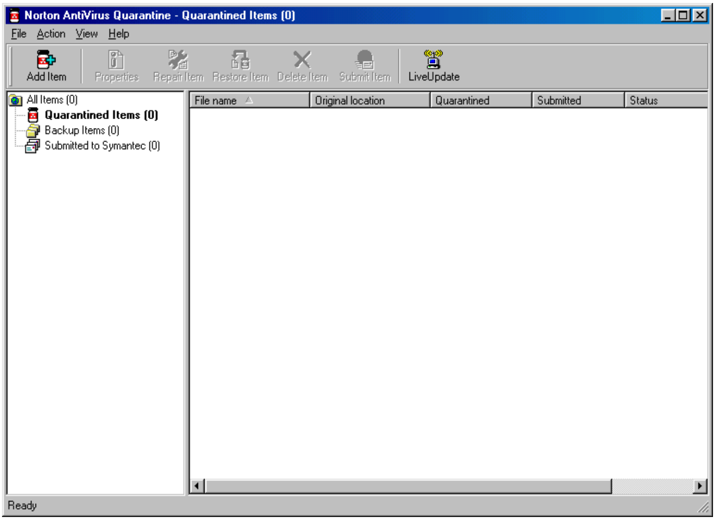
Once a file has been placed in Quarantine, you have several options. All actions that you take on files in Quarantine must be performed in the Quarantine window.

To open the Quarantine window

1 Start Norton Internet Security.

2 In the Security Center, click **Norton AntiVirus** > **Reports**.

3 In the Reports pane, on the Quarantined items line, click **View Report**.



The toolbar at the top of the Quarantine window contains all of the actions that you can perform on Quarantined files.

Add Item	Adds files to Quarantine. Use this action to quarantine a file that you suspect is infected. This action has no effect on files that are already in Quarantine.
Properties	Provides detailed information about the selected file and the virus that is infecting it.
Repair Item	Attempts to repair the selected file. Use this action if you have received new virus definitions since the file was added to Quarantine.
Restore Item	Returns the selected file to its original location without repairing it.
Delete Item	Deletes the selected file from your computer.

Submit Item	Sends the selected file to Symantec. Use this option if you suspect that a file is infected even if Norton AntiVirus did not detect it.
LiveUpdate	Runs LiveUpdate to check for new protection and program updates. Use this if you haven't updated your virus definitions for a while and then try to repair the files in Quarantine.

To perform an action on a file in Quarantine

1. Select the file on which you want to perform the action.
2. In the toolbar, select the action that you want to perform.
3. When you are finished, on the File menu, click **Exit**.

If Norton AntiVirus cannot repair a file

See "Keeping current with LiveUpdate" on page 81.

One of the most common reasons that Norton AntiVirus cannot automatically repair or delete an infected file is that you do not have the most up-to-date virus protection. Update your virus protection with LiveUpdate and scan again.

If that does not work, read the information in the report window to identify the types of items that cannot be repaired, and then take the appropriate action.

File type	Action
Infected files with .exe, .doc, .dot, or .xls file name extensions (any file can be infected)	Use the Repair Wizard to solve the problem. See "Use the Repair Wizard" on page 134.
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using the Rescue Disks or your operating system disks. See "About Rescue Disks" on page 73.

If your computer does not start properly

See "About Rescue Disks" on page 73 and "Create Emergency Disks" on page 30.

If you have a virus on your computer and need to start the computer from an uninfected disk to remove the virus, or if you need to restore a *boot record*, use your Rescue Disks. If you do not have Rescue Disks, you can use your Emergency Disks to start the computer and remove the virus. If you need to restore boot records and do not have Rescue Disks, or if you need to restore system files, you must reinstall Windows.

If you need to use Rescue Disks (Windows 98/98SE/Me)

Sometimes a virus infection prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus alert tells you when to use your Rescue Disks.

You first need to determine if your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you did any of the following:

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions
- Upgraded your operating system
- Updated virus definitions

If your Rescue Disks are not current, you can still use them to remove viruses from your computer. When the Rescue Disk window appears, use only the Norton AntiVirus task.

To use your Rescue Disks

1 Insert the Basic Rescue Boot floppy disk into drive A and restart your computer.
The Rescue program runs in DOS.

2 Use the arrow keys to select the program that you want to run.
A description of the selected program appears in the right pane of the Rescue program. Your choices are:

Norton AntiVirus	Scans your computer for viruses and repairs any infected files
Rescue Recovery	Checks and restores boot and partition information

3 Press **Enter** to run the selected program.

4 Follow the on-screen instructions for inserting and removing the Rescue Disks.

5 When the Rescue program is done, remove the Rescue Disk from drive A and restart your computer.

If you need to use Emergency Disks

See "Create Emergency Disks" on page 30.

If you have not created Rescue Disks, you can use Emergency Disks to restart your computer and scan for viruses.

To use Emergency Disks

1 Insert Emergency Disk 1 into drive A and restart your computer. The Emergency program runs in DOS.

2 Ensure that Antivirus is selected, then press **Enter** to begin the Norton AntiVirus Emergency program.

3 Follow the on-screen instructions for inserting and removing the Emergency Disks.
The Emergency program automatically scans your computer and removes viruses.

4 When the Emergency program is done, remove the Emergency Disk from drive A and restart your computer.

If you are using the CD as an Emergency Disk

See "I cannot start from drive A" on page 210.

If you are using the Norton Internet Security CD as an Emergency Disk, you can ignore all of the instructions to change disks, as all necessary information is on the CD.

You may need to change your computer's BIOS Setup options to start from the CD-ROM drive.

To use the CD as an Emergency Disk

1 Insert the Norton Internet Security CD into the CD-ROM drive.

2 Restart your computer.
The Emergency program scans your computer and removes viruses.

Look up viruses on the Symantec Web site

The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions. You must be connected to the Internet to look up viruses.

To look up viruses

1 Start Norton Internet Security.

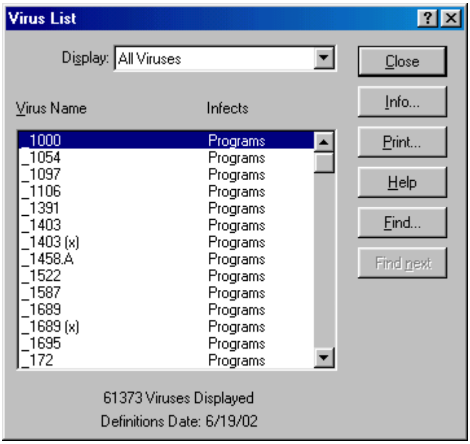
2 In the Security Center, click **Norton AntiVirus** > **Reports**.

3 In the Reports pane, on the Online Virus Encyclopedia line, click **View Report**.
The Symantec Web site opens in your Internet browser.

4 Use the links on the Web page to access the virus information for which you are looking.

Look up viruses in Norton AntiVirus

If you don't have an active Internet connection, you can look up a virus name from within Norton AntiVirus. The Virus List dialog box lists the viruses in the current virus definition service files on your local computer. Because of the large number of viruses, the Virus List file does not include descriptions of each virus.



Display: All Viruses

Virus Name	Infects
_1000	Programs
_1054	Programs
_1097	Programs
_1106	Programs
_1391	Programs
_1403	Programs
_1403 (x)	Programs
_1458.A	Programs
_1522	Programs
_1587	Programs
_1689	Programs
_1689 (x)	Programs
_1695	Programs
_172	Programs

61373 Viruses Displayed
Definitions Date: 6/19/02

See "Keeping current with LiveUpdate" on page 81.

To ensure that you have the latest virus definitions, run LiveUpdate.

To look up virus names and definitions

1. Start Norton Internet Security.
2. In the Security Center, click **Norton AntiVirus** > **Reports**.
3. In the Reports pane, on the Virus List line, click **View Report**.

To get more information about a specific virus

1. In the Virus List dialog box, select the virus about which you want more information.
2. Click **Info**.
3. When you are done viewing the list, in the Virus List dialog box, click **Close**.

Create accounts for multiple users

10

If you have chosen to install the Accounts feature of Norton Internet Security, you can create customized security settings for individual users. This lets you customize Parental Control, Spam Alert, Ad Blocking, and Privacy Control for each person who uses the computer.

About Norton Internet Security accounts

Your computer can host several accounts, but all accounts fall within one of four access levels:

Child	Cannot make any changes to Norton Internet Security protection. Has limited access to Internet programs and Web site categories.
Teenager	Cannot make any changes to Norton Internet Security protection. Has access to more Internet programs and Web site categories than Child users.
Adult	Can customize all Norton Internet Security options for own account.
Supervisor	Can change all Norton Internet Security options for all users.

There is also a default account, Not Logged In, that blocks all Internet access. When a user logs off, the settings for Not Logged In become active and stay active until another user logs on.

See "Set or change account passwords" on page 150.

When you install Norton Internet Security, the program creates a default account with Supervisor privileges. This account is not *password*-protected. For maximum security, you should create a password for this account.

If more than one person uses a computer, you can create separate accounts for each user or you can establish group accounts that all users requiring the same level of access or restriction can use.

Create Norton Internet Security accounts

Supervisor and Adult users can create new accounts and customize settings for other users. They can also create new user accounts with the Security Assistant. Adult users can customize their own accounts, but cannot change other users' accounts. Teenager and Child users can only change their *passwords*.

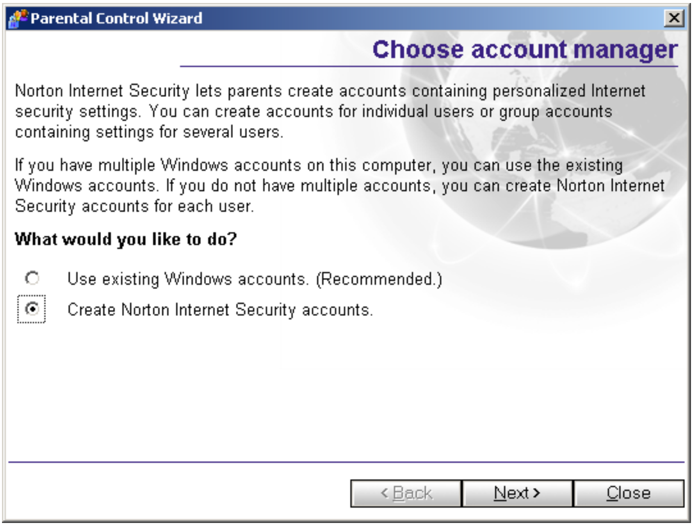
You can create several accounts at once with the Parental Control Wizard or one-by-one using the User Accounts screen.

To create Norton Internet Security accounts with the Parental Control Wizard

1 Open Norton Internet Security.

2 Do one of the following:

- In the Security Center, click **User Accounts**, then click **Parental Control Wizard**.
- In the Security Monitor, on the Select a Task menu, click **Create User Accounts**.



Choose account manager

Norton Internet Security lets parents create accounts containing personalized Internet security settings. You can create accounts for individual users or group accounts containing settings for several users.

If you have multiple Windows accounts on this computer, you can use the existing Windows accounts. If you do not have multiple accounts, you can create Norton Internet Security accounts for each user.

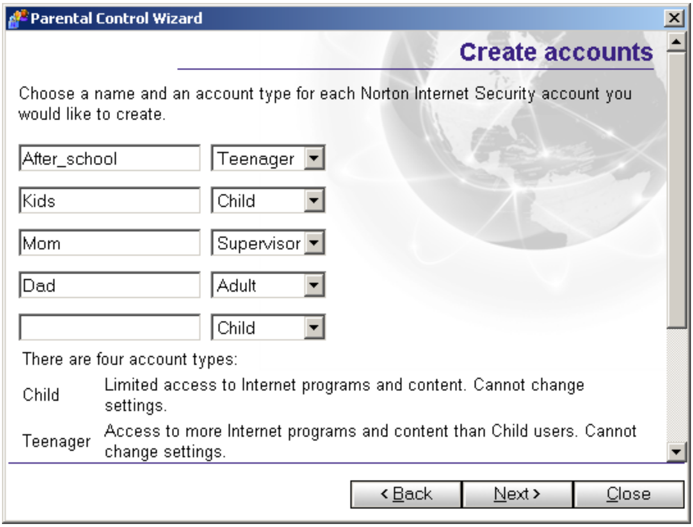
What would you like to do?

○ Use existing Windows accounts. (Recommended.)

● Create Norton Internet Security accounts.

3 In the Choose account manager screen, click **Create Norton Internet Security accounts**.

4 Click **Next**.



Create accounts

Choose a name and an account type for each Norton Internet Security account you would like to create.

After_school	Teenager
Kids	Child
Mom	Supervisor
Dad	Adult
	Child

There are four account types:

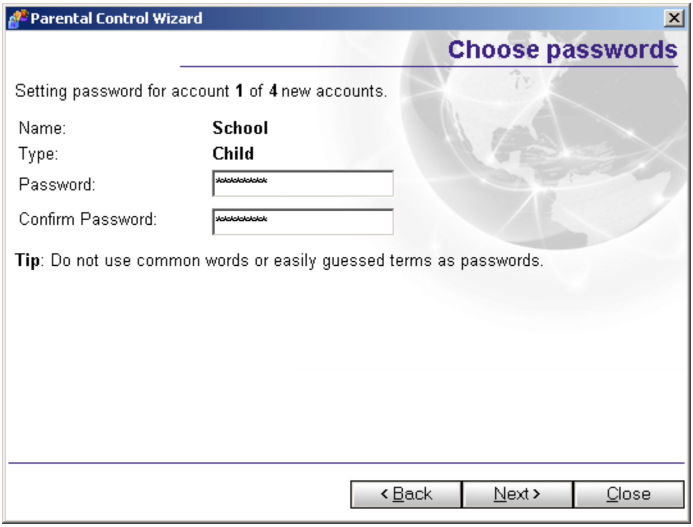
Child Limited access to Internet programs and content. Cannot change settings.

Teenager Access to more Internet programs and content than Child users. Cannot change settings.

5 In the Create accounts screen, type one or more account names.

6 On the account level menus, select an appropriate account level for each account.

7 Click **Next**.



Setting password for account **1** of **4** new accounts.

Name: **School**

Type: **Child**

Password: *********

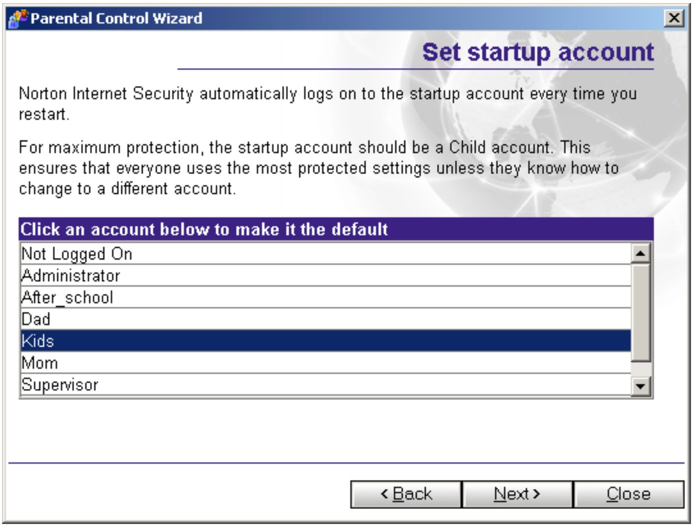
Confirm Password: *********

Tip: Do not use common words or easily guessed terms as passwords.

See "Set or change account passwords" on page 150.

8 In the Choose passwords screen, in the Password and Confirm Password text boxes, type a password for this user.

9 Click **Next**.
If you have created more than one account, repeat the previous two steps with each account.



Norton Internet Security automatically logs on to the startup account every time you restart.

For maximum protection, the startup account should be a Child account. This ensures that everyone uses the most protected settings unless they know how to change to a different account.

Click an account below to make it the default

- Not Logged On
- Administrator
- After_school
- Dad
- Kids
- Mom
- Supervisor

See "Set the startup account" on page 150.

10 In the Set startup account screen, choose the account that Norton Internet Security automatically logs on to when you restart the computer.

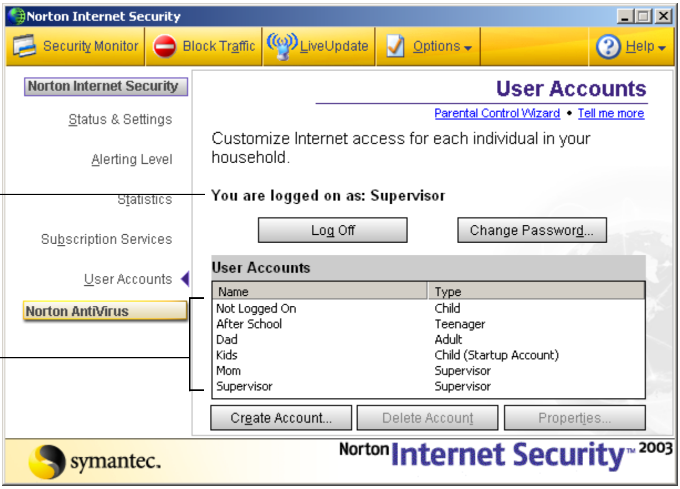
11 Click **Next**.

12 Click **Finish**.

To create Norton Internet Security accounts with the User Accounts screen

1 Open Norton Internet Security.

2 In the Security Center, click **User Accounts**.



User Accounts

Customize Internet access for each individual in your household.

You are logged on as: Supervisor

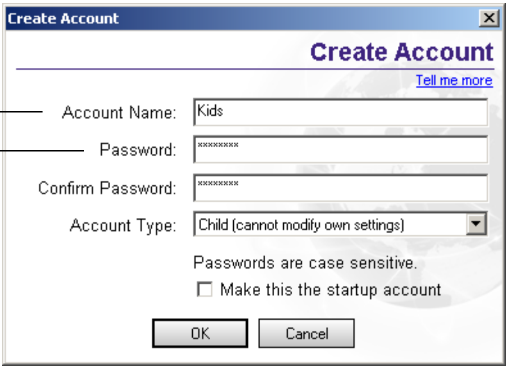
User Accounts

Name	Type
Not Logged On	Child
After School	Teenager
Dad	Adult
Kids	Child (Startup Account)
Mom	Supervisor
Supervisor	Supervisor

Shows which account is logged on

Shows the accounts that you have set up

3 In the User Accounts screen, click **Create Account**.



Create Account

Account Name: Kids

Password: ********

Confirm Password: ********

Account Type: Child (cannot modify own settings)

Passwords are case sensitive.

□ Make this the startup account

Give the account a name that describes how it will be used

Protect the account with a password that helps prevent others from using the account

4. In the Create Account dialog box, in the Account Name text box, type a name for this account.
5. In the Password and Confirm Password text boxes, type a password for this account.
   Passwords are case-sensitive.
6. On the Account Type menu, select an account type.
7. Click **OK**.

Set the startup account

Every time that you restart your computer, Norton Internet Security automatically logs on to the account that is designated as the startup account. The startup account should be the account with the most restrictions. This ensures that everyone uses the most protected settings unless they know how to change to a different account.

When you install Norton Internet Security, it creates a Supervisor account and designates it as the startup account. To ensure that users do not make unwanted changes to Norton Internet Security settings, you should create a Restricted account and set it as the default startup account.

To set an account as the startup account

1. Open Norton Internet Security.
2. In the Security Center, click **User Accounts**.
3. In the User Accounts screen, select the user account that you want to make the startup account.
4. Click **Properties**.
5. In the Account Properties dialog box, check **Make this the startup account**.
6. Click **OK**.

Set or change account passwords

For maximum security, you should protect each account with a *password*. This ensures that only approved users can access the Internet and your *network*.

To set or change your own password

1. Open Norton Internet Security.
2. In the Security Center, click **Accounts**.

3 In the User Accounts screen, select your account.

4 Click **Change Password**.

5 In the Change Password dialog box, type your old password, then type your new password.
If the account did not previously have a password, the Old Password field is unavailable.

6 Click **OK**.

Adult users can change passwords for Teenager and Child accounts. Supervisors can change any other accounts' passwords. If you change an account password, be sure to inform everyone who uses that account.

To set or change passwords for other users

1 Open Norton Internet Security.

2 In the Security Center, click **Accounts**.

3 In the User Accounts screen, select the account that you want to change.

4 Click **Properties**.

5 In the Account Properties dialog box, in the Password and Confirm Password text boxes, type a new password.

6 Click **OK**.

Assign Norton Internet Security account types to Windows accounts

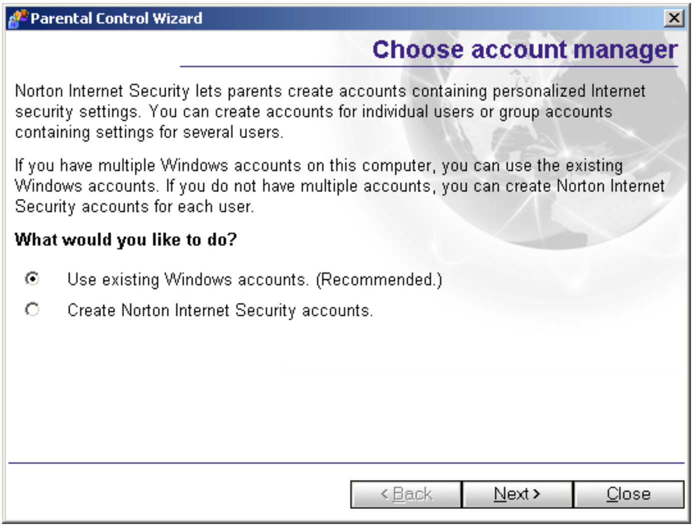
If you have created Windows accounts for multiple users, you can use these accounts instead of creating new Norton Internet Security accounts. If you use Windows accounts, your Norton Internet Security account will use the same name as your Windows account.

To assign Norton Internet Security account types to Windows accounts

1 Open Norton Internet Security.

2 In the Security Center, click **Accounts**.

3 In the Accounts window, click **Parental Control Wizard**.



Choose account manager

Norton Internet Security lets parents create accounts containing personalized Internet security settings. You can create accounts for individual users or group accounts containing settings for several users.

If you have multiple Windows accounts on this computer, you can use the existing Windows accounts. If you do not have multiple accounts, you can create Norton Internet Security accounts for each user.

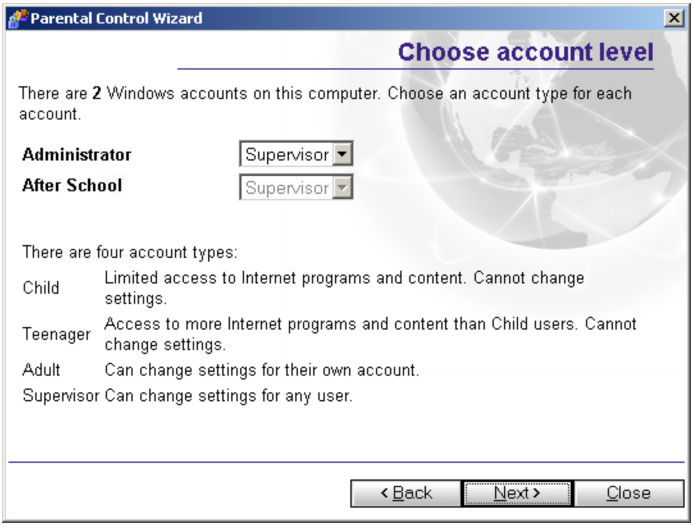
What would you like to do?

● Use existing Windows accounts. (Recommended.)

○ Create Norton Internet Security accounts.

4 In the Choose account manager screen, click **Use existing Windows accounts (Recommended)**.

5 Click **Next**.
In the Choose account level screen, all of your currently defined Windows accounts are listed.



Choose account level

There are **2** Windows accounts on this computer. Choose an account type for each account.

Administrator: Supervisor
After School: Supervisor

There are four account types:

Child	Limited access to Internet programs and content. Cannot change settings.
Teenager	Access to more Internet programs and content than Child users. Cannot change settings.
Adult	Can change settings for their own account.
Supervisor	Can change settings for any user.

6. For each account, select an account type.
7. Click **Next**.
8. Click **Finish** to close the Parental Control Wizard.

Log on to Norton Internet Security

If you chose to install the Accounts feature, users must log on to a Norton Internet Security account to access the Internet. You can configure accounts to control each person's Internet usage.

See "About Norton Internet Security accounts" on page 145.

When you start Norton Internet Security, it uses the settings from the account that you designated as the startup account.

To use a different account, you must log off of the current account and log on to another account. If you are not sure which account is active, you can check the active account.

To find out which account is active

❖ Open Norton Internet Security.
The active account is listed in the middle of the Security Center.

If you want to use a different account than the one that is currently active, you must log off of the current account, then log on with the account that you want to use.

To log on to another account

1. In the Windows system tray, click the Norton Internet Security icon.
2. On the system tray menu, click **Log Off**.
3. Click **Yes** to confirm that you want to log off.
4. In the Windows system tray, click the Norton Internet Security icon.
5. On the Windows system tray menu, click **Account Login**.
6. In the Log On dialog box, select the account that you want to use.
7. Type the password, if required.
8. Click **OK**.

As soon as you change an account, Norton Internet Security begins using the settings associated with that account. The Accounts window shows the account that is currently active.

Customize Norton Internet Security accounts

Each Norton Internet Security account can have personalized settings for:

- Parental Control
  See "Protect children with Parental Control" on page 179.
- Privacy Control
  See "Protecting your privacy" on page 155.
- Ad Blocking
  See "Blocking Internet advertisements" on page 163.
- Spam Alert
  See "Blocking unwanted email" on page 171.

Protecting your privacy

11

Every time that you browse the Internet, computers and *Web sites* collect information about you. Some of this information comes from forms that you fill out and choices that you make. Other information comes from your *browser*, which automatically provides information about the Web page you last visited and the type of computer that you're using.

Malicious users can also collect personal information without your knowledge. Any time that you send information over the Internet, the data must pass through a number of computers before it reaches its destination. During transmission, it's possible for third parties to intercept this information.

Computers include some basic security features, but they might not be enough to protect your personal information. Privacy Control helps protect your privacy by giving you several levels of control over *cookies* and other information that your browser sends to Web sites.

Privacy Control can ensure that users don't send private information, such as credit card numbers, over the Internet unless they are encrypted, or you specifically allow it.

Identify private information to protect

Many *Web sites* ask for your name, *email* address, and other personal information. While it is generally safe to provide this information to large, reputable sites, malicious sites can use this information to invade your privacy. It is also possible for people to intercept information sent via the Web, email, and instant messenger programs.

Privacy Control lets you create a list of information that you want to remain private. If users attempt to send protected information over the Internet, Norton Internet Security can warn them about the security risk or block the *connection*. All users on a protected computer share a single Private Information list.

Tips on entering private information

Because Norton Internet Security blocks personal information exactly the way that you enter it into the program, it is better to enter only partial numbers. For example, a phone number could be typed as 888-555-1234, but it could also be typed without dashes (8885551234) or with spaces (888 555 1234), or even in two or more separate fields. One common aspect of these formats is that the last four digits (1234) are always together. Therefore, you can have better protection by protecting the last four digits than you have by protecting the entire number.

Entering partial information has two advantages. First, you are not entering a complete number where someone might find it. Second, it lets Norton Internet Security block your private information on sites that use multiple fields for phone or credit card numbers.

Privacy Control and SSL

Some Web sites and email servers use SSL (Secure Sockets Layer) connections to encrypt connections between your computer and the server. Privacy Control cannot block private information sent via SSL connections. However, since the information is encrypted, only the recipient of the email will be able to read the message.

Add private information

You must add information that you want to protect to the Norton Internet Security Private Information list. All users on a single computer share a single Private Information list.

To add private information

1. Start Norton Internet Security.
2. Do one of the following:
   - In the Security Center, double-click **Privacy Control**, then click **Private Information**.
   - In the Security Monitor, on the Select a Task menu, click **Edit Private Information**.
3. In the Private Information dialog box, click **Add**.
4. In the Add Private Information dialog box, under Type Of Information To Protect, select a category.
5. In the Descriptive Name text box, type a description to help you remember why you are protecting this information.
6. In the Information To Protect text box, type the information that you want to block from being sent over nonsecure Internet connections.
7. Under Secure this private information in, select the Internet programs in which Privacy Control should block this information:
   - Web browsers
   - Instant messengers
   - Email programs
8. Click **OK**.

Modify or remove private information

You can modify or remove private information at any time.

To modify or remove private information

1. Start Norton Internet Security.
2. In the Security Center, double-click **Privacy Control**.
3. In the Privacy Control window, click **Private Information**.
4. Select the private information that you want to change or remove.
5. Select one of the following:
   - Modify
   - Remove
6. Click **OK**.

Customize Privacy Control

Privacy Control protects four areas:

Private Information	Blocks specific strings of text that you do not want sent over the Internet
Cookie Blocking	Stops Web sites from retrieving personal information stored in cookie files
Browser Privacy	Protects information about your browsing habits
Secure Connections	Prevents users from establishing secure connections to online stores and other Web sites

Supervisor and Adult users can make changes to program settings. Child and Teenager users cannot make any changes to Privacy Control.

There are two ways to adjust Privacy Control settings:

- Set the Privacy Level
  Use the slider in the main Privacy Control pane to select pre-set security levels.
- Adjust individual Privacy Control settings
  Customize your protection by manually adjusting individual settings.

You can set individual Privacy Control settings for each Norton Internet Security user.

Set the Privacy Level

Norton Internet Security offers pre-set security levels that help you set several Privacy Control options at one time. The Privacy Level slider lets you select minimal, medium, or high protection.

To set the Privacy Level

1. Start Norton Internet Security.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.

4 Move the slider to the Privacy Level that you want. Your options are:

High	All personal information is blocked and an alert appears each time that a cookie is encountered.
Medium (recommended)	An alert appears if private information is typed into a Web form or instant messenger program. Conceals your browsing from Web sites. Cookies are not blocked.
Minimal	Confidential information is not blocked. Cookies are not blocked. Conceals your browsing from Web sites.

5 Click **OK**.

Adjust individual Privacy Control settings

You can change the settings for Private Information, Cookie Blocking, Browser Privacy, and Secure Connections if the Privacy Level settings do not meet your needs. For example, you can choose to block all attempts to send private information while allowing Web sites to customize their pages using your browser information.

Change the Private Information setting

Change the Private Information setting to control how Norton Internet Security handles attempts to send information on the Private Information list over the Internet.

To change the Private Information setting

1 Start Norton Internet Security.

2 Double-click **Privacy Control**.

3 In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.

4 Click **Custom Level**.

5 Select the Private Information setting that you want. Your options are:

High	Blocks all private information
Medium	Alerts you each time that you attempt to send private information to a nonsecure Web site or through an instant messenger program
None	Does not block private information

6 Click **OK**.

Change the Cookie Blocking setting

Many Web sites store information they collect in *cookies* placed on your hard disk. When you return to a site that has set a cookie on your computer, the Web server opens and reads the cookie.

Most cookies are harmless. Sites use them to personalize Web pages, remember choices that you have made on the site, and deliver optimized pages for your computer. However, sites can also use cookies to track your Internet usage and browsing habits.

Change the Cookie Blocking setting to control how Norton Internet Security handles sites that attempt to place cookies on your computer.

To change the Cookie Blocking setting

1. Start Norton Internet Security.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.
4. Click **Custom Level**.
5. Select the Cookie Blocking setting that you want. You have three options:

High	Blocks all cookies
Medium	Alerts you each time that a cookie is encountered
None	Allows cookies

6. Click **OK**.

Enable or disable Browser Privacy

Browser Privacy prevents Web sites from learning the type of *browser* that you are using, the Web site that you last visited, and other information about your browsing habits. Some Web sites that depend on JavaScript may not work correctly if they cannot identify the type of browser that you are using.

To enable or disable Browser Privacy

1. Start Norton Internet Security.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.
4. Click **Custom Level**.
5. In the Customize Privacy Settings dialog box, check or uncheck **Enable Browser Privacy**.
6. Click **OK**.

Disable or enable secure Web connections

When you visit a secure Web site, your browser sets up an encrypted *connection* with the Web site. By default, Norton Internet Security lets any account use secure connections. If you want to ensure that users are not sending private information to secure Web sites, you can disable secure Web connections.

If you disable secure Web connections, your browser will not encrypt any information that it sends. You should only disable secure Web connections if you are protecting your personal data in the Private Information list.

To disable or enable secure Web connections

1. Start Norton Internet Security.
2. Double-click **Privacy Control**.
3. In the Privacy Control window, in the Privacy Control settings for drop-down list, select the account that you want to change.
4. Click **Custom Level**.
5. In the Customize Privacy Settings dialog box, check or uncheck **Enable Secure Connections (https)**.
6. Click **OK**.

Blocking Internet advertisements

12

Many Web sites are using more aggressive techniques to draw attention to the ads on their pages. Some have begun using larger, more prominent ads, while others rely on ad windows that appear when you enter or leave the site. Along with increasing the amount of time that it takes to display Web pages, some ads contain offensive content, cause software conflicts, or use *HTML* tricks to open additional *browser* windows.

Ad Blocking helps avoid these problems. When Ad Blocking is active, Norton Internet Security transparently removes:

- Ad banners
- Pop-up and pop-under ads
- Macromedia Flash-based ads

How Ad Blocking works

Norton Internet Security detects and blocks ads based on two criteria: their dimensions and their locations.

Blocking by dimensions

Most online advertisers use one or more standard sizes for their ads. Norton Internet Security now includes the ability to block images, Flash animations, and other *HTML* elements that have the same dimensions as these common ad sizes.

Blocking by location

Every file on the Internet has a unique address or *URL*. When you view a Web page, your computer connects to a URL and displays the file that is stored there. If the page points to graphics, audio files, and other multimedia content, your *browser* displays the files as part of the page.

When you go to a Web page that includes a *banner ad*, the instructions used to display the page might include the following:

<p>Greetings from the Ajax company<img src="http://www.ajax.com/nifty_images/image7.gif">

Your browser displays the text Greetings from the Ajax company on the screen. Then it connects to www.ajax.com and requests a file called /nifty_images/image7.gif. (The suffix .gif indicates that this is a Graphics Interchange Format file, a common image file format.) The computer at www.ajax.com sends the file to the browser, which displays the image.

When Ad Blocking is enabled and you connect to a Web site, Norton Internet Security scans Web pages and compares their contents to two lists:

See "Keeping current with LiveUpdate" on page 81.

- A default list of ads that Norton Internet Security blocks automatically. Use LiveUpdate to keep the list of blocked ads current.
- A list that you create as you block specific ads. You can add to and change this list.

If the page includes files from a blocked *domain*, Norton Internet Security removes the link and downloads the rest of the page.

You can set individual Ad Blocking settings for each Norton Internet Security user. Supervisor and Adult users can make changes to program settings. Child and Teenager users cannot make any changes to Ad Blocking.

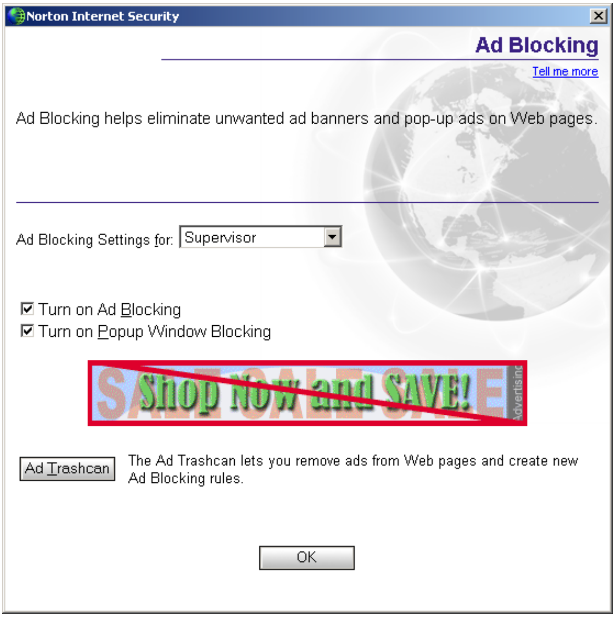
Enable or disable Ad Blocking

Norton Internet Security searches for the addresses of the ads that are being blocked as the Web page is downloaded by your *browser*. If it finds an address that matches the list of ads to block, it removes the ad so that it does not appear in your browser. It leaves the rest of the Web page intact so that you can view the page without the advertisements.

To enable or disable Ad Blocking

1 Open Norton Internet Security.

2 Double-click **Ad Blocking**.



Norton Internet Security

Ad Blocking

Tell me more

Ad Blocking helps eliminate unwanted ad banners and pop-up ads on Web pages.

Ad Blocking Settings for: Supervisor

☑ Turn on Ad Blocking
☑ Turn on Popup Window Blocking

Ad Trashcan — The Ad Trashcan lets you remove ads from Web pages and create new Ad Blocking rules.

OK

3 In the Ad Blocking window, in the Ad Blocking settings for drop-down list, select the account that you want to change.

4 Check or uncheck **Turn on Ad Blocking**.

5 Click **OK**.

Enable or disable Popup Window Blocking

Pop-up and pop-under ads are secondary windows that Web sites open when you visit or leave the sites. Pop-ups appear on top of the current window, while pop-unders appear behind the current window.

When Popup Window Blocking is active, Norton Internet Security automatically blocks the programming code Web sites use to open secondary windows without your knowledge. Sites that open secondary windows when you click a link or perform other actions are not affected.

To enable or disable Popup Window Blocking

1. Open Norton Internet Security.
2. Double-click **Ad Blocking**.
3. In the Ad Blocking window, in the Ad Blocking settings for drop-down list, select the account that you want to change.
4. Check or uncheck **Turn on Popup Window Blocking**.
5. Click **OK**.

Enable or disable Flash blocking

When Ad Blocking is active, Norton Internet Security automatically blocks all Flash animations that have the same dimensions as common ads. Norton Internet Security can also block all Flash content. This is useful if you have a slow connection or are not interested in viewing Flash animations.

You can choose to have Norton Internet Security block all Flash animations or only block them on certain Web sites. Changing the Flash blocking settings affects all users on this computer.

To enable or disable Flash blocking

1. Open Norton Internet Security.
2. In the Security Center, click **Options** > **Internet Security**.
3. On the Web Content tab, click the **Global Settings** tab.

4 In the list of Web sites, do one of the following:
   - To change Flash settings for all sites, click **(Defaults)**.
   - To change Flash settings for a site in the list, click the site's name.
   - To change Flash settings for a site not in the list, click **Add Site**, then in the New Site/Domain dialog box, type the site's address.

5 In the Flash animation section, select one of the following:
   - Block
   - Permit

6 Click **OK**.

Some Web sites use Flash to create navigation toolbars. Blocking Flash may make these sites unusable.

Use the Ad Trashcan

As you use the Internet, you may find ads that are not included on the default Norton Internet Security Ad Blocking list. You can use the Ad Trashcan to add these to your personal list of blocked ads.

To use the Ad Trashcan

1 Open your Web browser and view the page containing the advertisement that you want to block.

2 Open Norton Internet Security.

3 In the Security Center, double-click **Ad Blocking**.

4 In the Ad Blocking window, ensure that Enable Ad Blocking is checked.

5 Click **Open the Ad Trashcan**.
The Ad Trashcan window appears.

6 With the windows arranged so that you can see both the advertisement and the Ad Trashcan window, do one of the following:
   - If you are using Microsoft Internet Explorer, drag the unwanted ad from the Web site to the Ad Blocking dialog box.
   - If you are using Netscape, right-click the advertisement, then click **Copy Image Location**. In the Ad Trashcan, click **Paste**. The address for the advertisement appears in the Ad Details line of the Ad Trashcan dialog box.

7. Select one of the following:
   - Add: Block this address.
   - Modify: Change the entry before adding it to the Ad Blocking list. For example, if the advertisement address is http://www.advertise.org/annoying/ads/numberone.gif, you could change it to http://www.advertise.org/annoying/ads/ to block everything in the ads directory.
8. Click **OK**.

Use text strings to identify ads to block or permit

You can control whether Norton Internet Security displays specific ads by creating a list of text strings that identify individual ad banners. Ad Blocking strings are sections of *HTML* addresses. If any part of a file's address matches the text string, Norton Internet Security automatically blocks the file.

Norton Internet Security provides a predefined (Defaults) Ad Blocking list that is used to determine which images should be blocked when displaying Web pages.

When Ad Blocking is enabled, all Web pages are scanned for the HTML strings specified in the (Defaults) list. Norton Internet Security looks for the blocked strings within HTML tags that are used to present advertising. The HTML structures that contain matching strings are removed from the page by Norton Internet Security before the page appears in the Web *browser*.

Make sure that what you place in the (Defaults) block list isn't too general. For example, www by itself is not a good string to block because almost every *URL* includes www. A string like www.slowads is more effective because it only blocks graphics from the slowads *domain* without affecting other sites.

All users share a single Ad Blocking list. Supervisor and Adult users can make changes to the list. Child and Teenager users cannot make any changes to Ad Blocking settings.

How to identify Ad Blocking strings

The way that you define Ad Blocking strings affects how restrictive or unrestrictive Norton Internet Security is when filtering data.

For example, if you add the string ajax.com to the (Defaults) block list, you block everything in the ajax.com domain. If you are more specific and add the string nifty_images/image7.gif to the site-specific block list maintained for www.ajax.com, you block only that particular image.

Blocking all images on a particular site may make that site unusable. A good compromise is to block only the directories that contain ads. For example, if www.ajax.com stores its ads in /nifty_images/ and its navigational images in /useful_images/, you could block www.ajax.com/nifty_images/ without seriously impeding your ability to use the site.

You can also create permit strings that allow Web sites to display images that match the string. This allows you to override the blocking effect of any string in the (Defaults) block list for individual sites. Permit rules take precedence over Block rules on any site.

Add an Ad Blocking string

You can add strings to the Ad Blocking list for all sites or for individual sites.

To add an Ad Blocking string

1. Open Norton Internet Security.
2. At the top of the Security Center window, click **Options** > **Internet Security**.
3. On the Web Content tab, on the Ad Blocking tab, do one of the following:
   - To block a string on all Web sites, click **(Defaults)**.
   - To block a string on a Web site in the list, select the site’s name.
   - To block a string on a Web site not in the list, click **Add Site**, then in the New Site/Domain dialog box, type the site’s address.
4. On the Ad Blocking tab, click **Add**.

5. In the Add New HTML String dialog box, select the action that you want to take. Your options are:

Block	Block ads matching this string.
Permit	Allow ads matching this string.

6. Type an HTML string to block or permit.
7. Click **OK**.

Modify or remove an Ad Blocking string

If you later decide that an Ad Blocking string is too restrictive, not broad enough, or not appropriate, you can change or remove it.

To modify or remove an Ad Blocking string

1. Open Norton Internet Security.
2. At the top of the Security Center window, click **Options** > **Internet Security**.
3. On the Web Content tab, on the Ad Blocking tab, do one of the following:
   - To modify or remove a string in the (Defaults) list, click **(Defaults)**.
   - To modify or remove a site-specific string, click the site’s name.
4. In the HTML string list, select the string that you want to change.
5. Do one of the following:
   - To modify a string, click **Modify**, then type your changes.
   - To remove a string, click **Remove**.
6. Click **OK**.

Blocking unwanted email

13

As *email* becomes more popular, many users are receiving an increasing amount of the unsolicited commercial mail known as spam. Not only does spam make it difficult to identify valid email, some spam contains offensive messages and images.

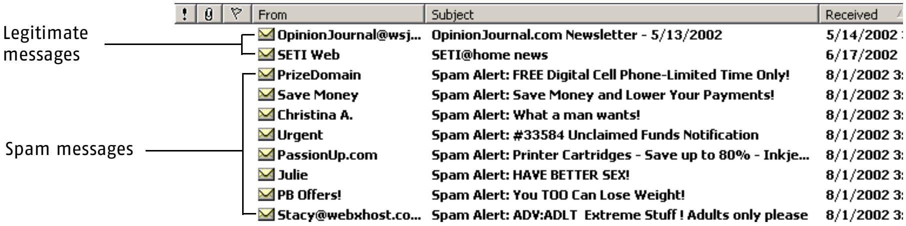
Spam Alert helps reduce the amount of spam you receive by intelligently filtering incoming messages and clearly marking potential spam.

How Spam Alert works

Spam Alert uses a pattern-matching engine that automatically compares the contents of every incoming *email* message to a list of known spam characteristics. If the message contains many characteristics of spam, it is more likely to be spam than a message that contains few spam characteristics. Based on this analysis, Spam Alert estimates the likelihood that the message is spam.

After this initial scan, Norton Internet Security uses the settings you've chosen in the Spam Alert page to determine which messages are marked as spam. If Spam Alert is set to Low, messages must contain many spam characteristics before they are flagged as spam. If Spam Alert is set to High, messages that contain only a few spam characteristics will be flagged.

When a message is identified as spam, Norton Internet Security appends “Spam Alert:” to the beginning of the message’s subject. You can then use your email program to create filters for all email containing this text.



Legitimate messages

Spam messages

!	0	⚐	From	Subject	Received
			✉ OpinionJournal@wsj...	OpinionJournal.com Newsletter - 5/13/2002	5/14/2002 :
			✉ SETI Web	SETI@home news	6/17/2002
			✉ PrizeDomain	Spam Alert: FREE Digital Cell Phone-Limited Time Only!	8/1/2002 3:
			✉ Save Money	Spam Alert: Save Money and Lower Your Payments!	8/1/2002 3:
			✉ Christina A.	Spam Alert: What a man wants!	8/1/2002 3:
			✉ Urgent	Spam Alert: #33584 Unclaimed Funds Notification	8/1/2002 3:
			✉ PassionUp.com	Spam Alert: Printer Cartridges - Save up to 80% - Inkje...	8/1/2002 3:
			✉ Julie	Spam Alert: HAVE BETTER SEX!	8/1/2002 3:
			✉ PB Offers!	Spam Alert: You TOO Can Lose Weight!	8/1/2002 3:
			✉ Stacy@webxhost.co...	Spam Alert: ADV:ADLT Extreme Stuff ! Adults only please	8/1/2002 3:

If you have installed the Accounts feature, you can create custom Spam Alert settings for each user. Supervisor and Adult users can customize Spam Alert settings. Child and Teenager users cannot change any Spam Alert settings.

Privacy Control and SSL

Some email servers use SSL (Secure Sockets Layer) *connections* to encrypt connections between your computer and the server. Spam Alert cannot scan email received via SSL connections.

Enable or disable Spam Alert

Enable or disable Spam Alert from the Security Center.

To enable or disable Spam Alert

1. Open Norton Internet Security.
2. Double-click **Spam Alert**.
3. In the Spam Alert window, in the Spam Alert settings for drop-down list, select the account that you want to change.
4. Check or uncheck **Turn On Spam Alert**.

5 Use the Spam Alert slider to control how aggressively Norton Internet Security filters spam. Your options are:

High	Maximum filtering. Most spam is correctly identified. More likely to identify personal email messages as spam.
Medium (recommended)	Moderate filtering. More spam is correctly identified. Likely to identify some personal email messages as spam.
Low	Light filtering. Some spam is correctly identified. Rarely identifies personal email messages as spam.

6 Click **OK**.

Create spam filters

Once Spam Alert is active, Norton Internet Security appends the phrase "Spam Alert:" to the beginning of messages that it identifies as spam. This makes it easy for you to filter these messages with your *email* program.

Symantec provides configuration instructions for Microsoft Outlook Express, Microsoft Outlook, Netscape Communicator, and Eudora, but Spam Alert will work with most email programs that use POP3.

To create spam filters for Microsoft Outlook Express

1 Open Microsoft Outlook Express.

2 On the Tools menu, click **Message Rules** > **Mail**.

3 In the New Mail Rule window, under Select the Conditions for your rule, check **Where the Subject line contains specific words**.

4 Under Select the Actions for your rule, check **Move it to the specified folder**.

5 Under Rule Description, click **contains specified words**.

6 In the Type Specific Words dialog box, type **Spam Alert:**, then click **Add**.

7 Click **OK**.

8 Under Rule Description, click **specified**.

9 In the Move dialog box, click the plus sign (+) next to Local Folders to display your email folders.

10 In the list of mailboxes, choose your spam mailbox, then click **OK**.

11 In the New Mail Rule Window, in the Name of the Rule text box, type a name for this rule.

12 Click **OK**.

13 In the Message Rules window, click **OK**.

To create spam filters for Microsoft Outlook

1 Open Microsoft Outlook.

2 On the Tools menu, click **Message Rules** > **Mail**.

3 Click **New**.

4 Under Which type of rule do you want to create, click **Check messages when they arrive**.

5 Click **Next**.

6 Under Which condition(s) do you want to check, click **with specific words in the subject**.

7 Under Rule Description, click **specific words**.

8 In the Search Text dialog box, type **Spam Alert:**, then click **OK**.

9 Click **Next**.

10 Under What do you want to do with the message, check **move it to the specified folder**.

11 Under Rule Description, click **specified**.

12 In the Move dialog box, click the plus sign (+) next to Local Folders to display your email folders.

13 In the list of mailboxes, choose your spam mailbox, then click **OK**.

14 Click **Next**.

15 Under Please specify a name for this rule, type a name for this rule.

16 Make sure that Turn on this rule is checked.
If you already have messages marked with Spam Alert in your inbox, check **Run this rule now on messages already in "Inbox"** to filter them.

17 Click **Finish**.

To create spam filters for Netscape Messenger

1. Open Netscape Messenger.
2. On the Edit menu, click **Message Filters**.
3. Click **New**.
4. Type a name for the filter.
5. In the Contains text box, type **Spam Alert:**
6. On the then menu, do one of the following:
   - To immediately delete spam messages, click **Delete**.
   - To transfer emails marked spam into a special folder, click **Inbox**, then select the folder name.
7. Click **OK**.

To create spam filters for Eudora

1. Open Eudora.
2. On the Tools menu, click **Filters**.
3. Click **New**.
4. Under Match, check the following:
   - Incoming
   - Manual
5. On the Header menu, click **Subject**.
6. In the contains text box, type **Spam Alert:**
7. On the Action menu, click the first item, then select **Transfer to**.
8. Click the **In** button.
9. On the Transfer menu, click **Trash**.
10. On the File menu, click **Save**.

Customize Spam Alert

You can customize your protection by identifying *email* addresses and particular text strings that should and should not be filtered. When Spam Alert encounters a message containing one of these addresses or text strings, it will bypass its pattern matching engine and immediately categorize the message based on your settings. This is an easy way to ensure that bulk newsletters and other messages from trusted senders do not get marked as spam.

Everyone using this computer shares a single customized Spam Alert list. Supervisor and Adult users can make changes to this list. Child and Teenager users cannot make any changes to Spam Alert settings.

To add a new Spam Alert entry

1. Open Norton Internet Security.
2. Double-click **Spam Alert**.
3. In the Spam Alert window, in the Spam Alert settings for drop-down list, select the account that you want to change.
4. In the Spam Alert window, click **Advanced**.
5. In the Advanced Spam Alert window, click **New**.
6. In the New Spam Entry window, in the Search for text box, type an address or a text string.
7. On the Search in menu, select where Norton Internet Security should search for the text. There are five options:
   - From: (sender’s name)
   - To: (recipient’s name)
   - Subject of message
   - Body of message
   - Anywhere in message
8. Under Classify message as, choose whether messages that include this text are spam or not spam.
9. Click **OK**.
10. Click **OK**.

You can modify or delete a Spam Alert entry if it is causing messages to be incorrectly classified.

To modify or delete a Spam Alert entry

1. Open Norton Internet Security.
2. Double-click **Spam Alert**.
3. In the Spam Alert window, in the Spam Alert settings for drop-down list, select the account that you want to change.
4. In the Spam Alert window, click **Advanced**.
5. In the Advanced Spam Alert window, select the Spam Alert entry with which you want to work.
6. Select the action that you want to take. Your options are:

Modify	Change the entry.
Remove	Delete the entry.

7. Click **OK**.
8. Click **OK**.

Spam Alert tips

When using Spam Alert, remember:

- Periodically review incoming *email* messages to ensure that Spam Alert is not erroneously marking valid email as spam.
- To avoid losing legitimate email, use your email program to create a spam folder. You can then filter all messages marked with Spam Alert into this folder and periodically review the messages before deleting them.
- People who send spam often include fake addresses in the From: field. Adding individual addresses to the Spam Alert list is unlikely to reduce the amount of spam you receive.

Protect children with Parental Control

14

Norton Internet Security includes Parental Control, which lets parents manage their children's Internet access. Parental Control lets you control:

Web sites	Block access to sexually explicit, violent, or otherwise inappropriate Web pages.
Programs	Block categories of Internet programs that pose security risks or could be misused.
Newsgroups	Restrict access to discussion groups related to extreme, illegal, or inappropriate topics.

Child users cannot make any changes to Parental Control settings.

About Parental Control

Parental Control categorizes *Web sites* by topic, newsgroups by text string, and Internet programs by type.

When you enable Parental Control, Norton Internet Security blocks any incoming information from restricted Web sites and newsgroups. It also blocks all outgoing information from restricted Internet programs.

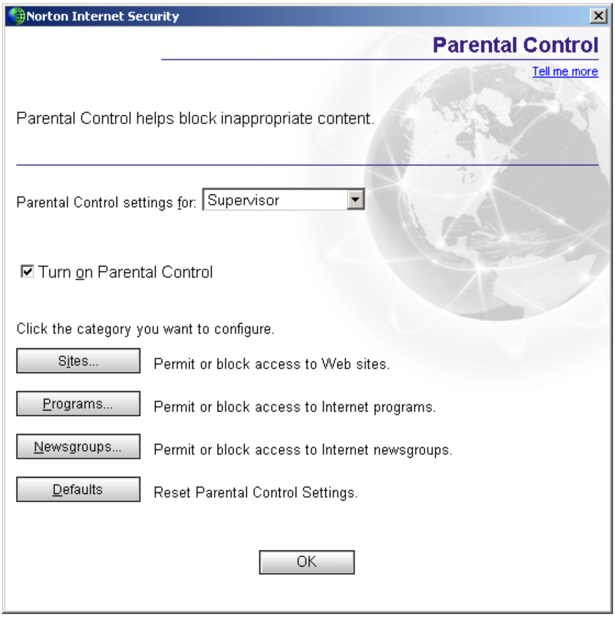
Parental Control settings are linked to user accounts. When users log on to their accounts, Norton Internet Security uses the settings associated with the accounts until the users log off.

See "Keeping current with LiveUpdate" on page 81.

Symantec updates the list of blocked Web sites regularly. Run LiveUpdate often to ensure that you have the most updated list.

Enable or disable Parental Control

Supervisor and Adult users can enable or disable Parental Control. Adult users can change Parental Control settings for their accounts. Supervisor users can also make changes to any user's Parental Control settings. Teenager and Child users cannot make any changes to Parental Control.



Norton Internet Security

Parental Control

Tell me more

Parental Control helps block inappropriate content.

Parental Control settings for: Supervisor

☑ Turn on Parental Control

Click the category you want to configure.

Sites... Permit or block access to Web sites.

Programs... Permit or block access to Internet programs.

Newsgroups... Permit or block access to Internet newsgroups.

Defaults Reset Parental Control Settings.

To enable or disable Parental Control

1 Start Norton Internet Security.

2 Double-click **Parental Control**.

3 In the Parental Control window, in the Parental Control settings for drop-down list, select the account that you want to change.

4 Check or uncheck **Turn on Parental Control**.

See "View the logs" on page 198.

Norton Internet Security tracks all Parental Control activity on the Event Log's Restrictions tab. Check this tab periodically to monitor the effectiveness of your Parental Control settings.

Customize Parental Control

The default settings for Parental Control should provide complete protection for most users. If you need to adjust Parental Control settings, you can add or remove categories to or from the Norton Internet Security list of blocked Web sites, newsgroups, and Internet programs. You can also exclude specific sites and newsgroups from blocking and create a list of permitted Web sites and newsgroups.

There are separate procedures for blocking Web sites, programs, and newsgroups.

Restrict Web site access

There are two ways to restrict Web site access:

- Block Web sites by category.
  Specify which categories of sites users can and cannot access. You can also add or remove specific sites to or from the list of blocked sites in a category. Use this option to restrict users from visiting specific types of Web sites, but to allow everything else.
- Create a list of Web sites that can be visited.
  Specify the Web sites that all users can visit. Use this option to strictly control users' Internet activities, as all Web sites not on the list are blocked, regardless of users' account types.

Block Web sites by category

Norton Internet Security includes an extensive list of categorized Web sites. You can select which categories of sites are appropriate for each account on your computer.

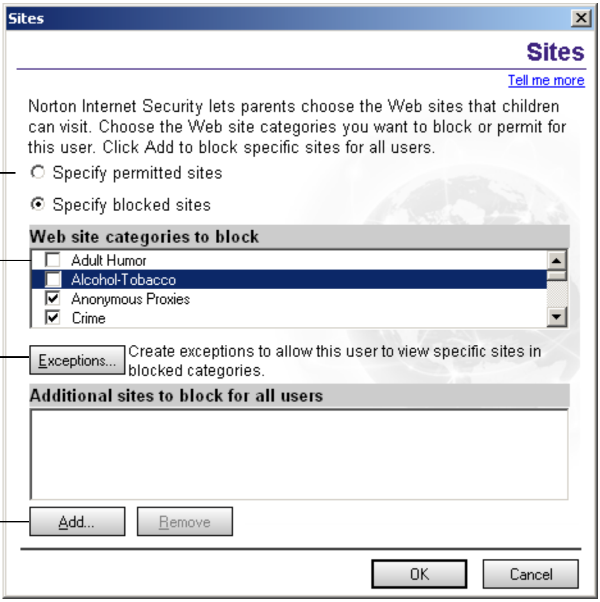
See "Keeping current with LiveUpdate" on page 81.

Before blocking Web sites by category, run LiveUpdate to ensure that the list of Web sites is up-to-date.

To block Web sites by category

1. Start Norton Internet Security.
2. Double-click **Parental Control**.
3. In the Parental Control window, in the Parental Control settings for drop-down list, select the account that you want to change.
4. Click **Sites**.

5 In the Specify Sites window, click **Specify blocked sites**.



Sites

Sites

Tell me more

Norton Internet Security lets parents choose the Web sites that children can visit. Choose the Web site categories you want to block or permit for this user. Click Add to block specific sites for all users.

○ Specify permitted sites

● Specify blocked sites

Web site categories to block

- ☐ Adult Humor
- ☐ Alcohol-Tobacco
- ☑ Anonymous Proxies
- ☑ Crime

Exceptions... Create exceptions to allow this user to view specific sites in blocked categories.

Additional sites to block for all users

This account can visit categories of sites that are not checked in the Web site categories to block list

Select the Web site categories to block

Create an exception to permit access to a site without disabling the entire category

Add additional Web sites that you want to block

6 Under Web site categories to block, check the categories that you want to block for this account.

7 Click **OK**.

8 When you are done specifying sites, click **OK**.

Block additional sites

Parental Control lets you restrict access to specific Web sites or domains that are not included in one of the categories of blocked sites. If you block a domain, all Web sites within the domain are included. For example, if you block the domain msn.com, Parental Control will block all Web sites at that domain, including www.msn.com and messenger.msn.com. If you block messenger.msn.com, only that Web site will be blocked.

To block or unblock specific sites

1 Start Norton Internet Security.

2 Double-click **Parental Control**.

3 In the Parental Control window, in the Parental Control settings for drop-down list, select the account that you want to change.

4 Click **Sites**.

5 In the Specify Sites window, click **Specify Blocked Sites**.

6 Click **Add**.

7 In the Add Web site to Blocked List window, type the URL of the site that you want to add.

8 Click **OK**.

9 Repeat the previous three steps for each Web site that you want to add.

10 When you are done adding sites, click **OK**.

Create exceptions for specific sites

If a site you need to view belongs to a blocked category, you can create an exception for this site. This allows you to permit access to specific Web sites that belong to blocked categories while still blocking other sites of this type.

You can create exceptions for individual Web sites or entire domains. If you create an exception for a domain, all Web sites within the domain are included. For example, if you create an exception for the domain msn.com, Parental Control will allow all Web sites at that domain, including www.msn.com and messenger.msn.com. If you block messenger.msn.com, only that Web site will be blocked.

To create exceptions for specific sites

1 Start Norton Internet Security.

2 Double-click **Parental Control**.

3 In the Parental Control window, in the Parental Control settings for drop-down list, select the account that you want to change.

4 Click **Sites**.

5 In the Specify Sites window, click **Specify Blocked Sites**.

6 Click **Exceptions**.

7 In the Exceptions window, click **Add**.

8 In the Add Web site to Exception List window, type the URL of the site that you want to add.

9 Click **OK**.

10 Repeat the previous three steps for each Web site that you want to add to your exceptions list.

11 When you are done adding sites, click **OK**.

Create a list of permitted Web sites

You can strictly control Web access by creating a list of Web sites that people using this computer are allowed to access. Any sites that are not on the list of permitted Web sites are blocked. Everyone who uses this computer can visit only approved sites regardless of their account types.

To create a list of permitted Web sites

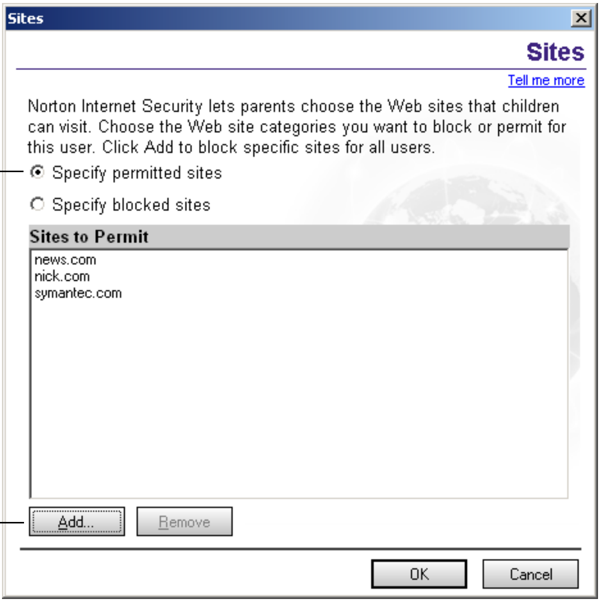
1 Start Norton Internet Security.

2 Double-click **Parental Control**.

3 In the Parental Control window, in the Parental Control settings for drop-down list, select the account that you want to change.

4 Click **Sites**.

5 In the Specify Sites window, click **Specify permitted sites**.



Sites

Norton Internet Security lets parents choose the Web sites that children can visit. Choose the Web site categories you want to block or permit for this user. Click Add to block specific sites for all users.

● Specify permitted sites

○ Specify blocked sites

Sites to Permit

news.com
nick.com
symantec.com

This account can visit only the sites listed in the Sites to Permit pane

Add Web sites to the list

6 Click **Add** to create a new entry in the list.

7 In the Add Web site to Permitted List window, type the complete URL (Web address) of the site that you want to add.
For example, to permit access to www.ajax.com, you would type ajax.com.

8 Repeat the previous two steps for each Web site that you want to add.

9 Click **OK**.

Submit Web sites to Symantec

Symantec regularly updates the list of Web sites blocked by Norton Internet Security. You can help ensure that the list is comprehensive by suggesting new sites, new categories for sites, and sites that should be removed from the list. To submit suggested changes to Symantec, visit http://www.symantec.com/avcenter/cgi-bin/nisurl.cgi

Restrict programs that access the Internet

Programs access the Internet for many reasons. Your Web *browser* accesses the Internet to display Web pages. LiveUpdate accesses the Internet to retrieve program and protection updates for Symantec products. Microsoft NetMeeting accesses the Internet to let users conduct meetings over the Internet.

While most programs' Internet access attempts are benign, some *Trojan horses* and other programs may download malicious programming or upload personal information. Parental Control lets you control how programs access the Internet. Parental Control can block categories of Internet programs and limit how certain groups of Internet programs can be used.

Program limitations are intended for use with Child and Teenager accounts. Users with Adult accounts will be able to override program restrictions on a per-program basis.

Block and permit categories of Internet programs

Parental Control organizes Internet programs into categories. By default, Child users can access the Internet only with programs in the General, Email, Web Browsers, and User categories. The categories include:

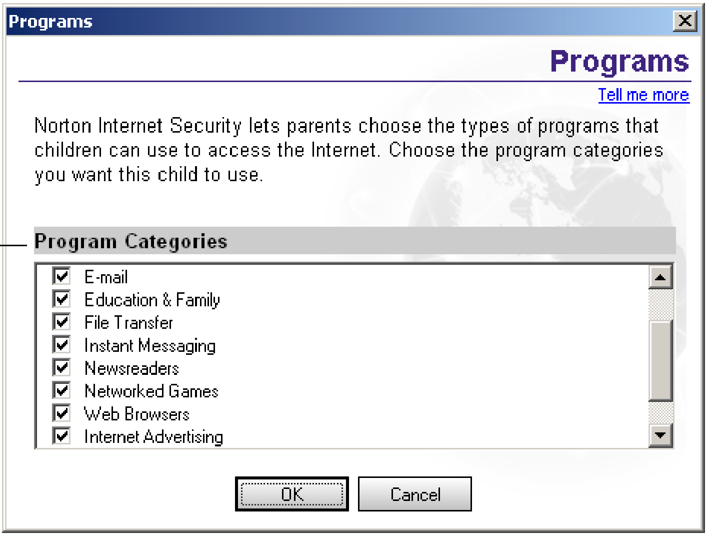
General	Programs that do not fall under any other category.
Chat	Programs that let you engage in conversations with other users or communities online using text, voice, or video. Examples include mIRC, Pirch, ICQ, NetMeeting, Internet Phone, Net2Phone, and CU-SeeMe. Restricting this category of programs does not block Web-based chat that appears in your browser.

Conferencing & Collaboration	Programs that let two or more users communicate directly with one another. This category includes programs that let users collaborate through the use of a program, such as whiteboard programs and Web browsers. Examples include NetMeeting, ICQ, Microsoft Instant Messenger, Yahoo! Messenger, and Internet Phone.
Email	Programs that access email servers, known as email clients. Examples include Microsoft Outlook Express and Eudora. Restricting this category of programs does not block Web-based email that appears in your browser, such as Hotmail.
Education & Family	Educational programs that access the Internet.
File Transfer	Programs that let users transfer files to and from their computers. Examples include CuteFTP and BulletFTP.
Instant Messaging	Programs that let users instantly send messages and files to other users currently running the same instant messenger program. Examples include ICQ, Yahoo! Messenger, Microsoft Instant Messenger, and AOL Instant Messenger.
Newsreaders	Programs that access newsgroups. Examples include Xnews and Agent.
Networked Games	Games that access a network or the Internet to let users play with or against one another.
Web Browsers	Programs that provide users with access to the World Wide Web. Examples include Microsoft Internet Explorer and Netscape Navigator.
User Categories	Additional categories in which you can create additional classifications of programs.

To block and permit categories of Internet programs

1. Start Norton Internet Security.
2. Double-click **Parental Control**.
3. In the Parental Control window, on the Settings For menu, select the account that you want to change.

4 Click **Programs**.



Programs

Programs

Tell me more

Norton Internet Security lets parents choose the types of programs that children can use to access the Internet. Choose the program categories you want this child to use.

Program Categories

☑ E-mail
☑ Education & Family
☑ File Transfer
☑ Instant Messaging
☑ Newsreaders
☑ Networked Games
☑ Web Browsers
☑ Internet Advertising

This person can use the programs marked with a check to access the Internet

5 In the Programs dialog box, under Program Categories, select the categories of programs that this account is allowed to use.

6 Click **OK**.

Blocking a program from accessing the Internet does not prevent users from running the program. A program may stop responding when Norton Internet Security prevents it from connecting to the Internet. Before making changes to program settings, ensure that users understand that their computers may stop responding if they use blocked programs.

Restrict newsgroup access

Norton Internet Security blocks newsgroups based on text strings, which are groups of letters found in the names of the newsgroups.

When users access newsgroups, Parental Control compares the names of the newsgroups that they attempt to view with a list of text strings you create. Parental Control then blocks or permits access to newsgroups containing those text strings.

When newsgroups are blocked, newsreader programs will not include their names in the master list of available newsgroups that users can view. If a user attempts to post a message in the newsgroup, Norton Internet Security automatically blocks the post.

See "To block and permit categories of Internet programs" on page 186.

By default, Child users cannot use newsreader programs. To allow Child users to view newsgroups, you must unblock the newsreaders programs category.

About newsgroup names

Newsgroup names become more specific as you read from left to right. For example, the newsgroup alt.history is a general discussion about historical events and people. Within that group are more specific discussions. For example, alt.history.ocean-liners is a more specific discussion about the history of ocean liners, and alt.history.ocean-liners.titanic is an even more specific discussion about the Titanic.

You can use this structure to precisely identify blocked or permitted newsgroups. For example, to block comp.security.pgp.discuss (discussion about the computer security tool Pretty Good Privacy) while still allowing users access to comp.security (general computer security issues), you can enter comp.security.pgp. This blocks newsgroups with comp.security.pgp in their names while still allowing access to other comp.security newsgroups.

You can also block or permit newsgroups using partial group names. For example, you could block all newsgroups with the word sex in their names by entering sex in the blocked newsgroup list.

Be careful when entering short text strings. The newsgroup filter blocks or permits all newsgroups with names that match text strings, so you may inadvertently block newsgroups that you want users to be able to access. For example, blocking sex also blocks newsgroups with names containing words like sextant and sexagenarian.

When entering text strings, do not use wildcard characters such as asterisks.

Enter text strings to block or permit

Norton Internet Security includes a list of text strings that block newsgroups that many people would find objectionable. You can add strings to customize Parental Control for your family.

Each computer can have only one list of permitted or blocked newsgroups.

To enter text strings to block or permit

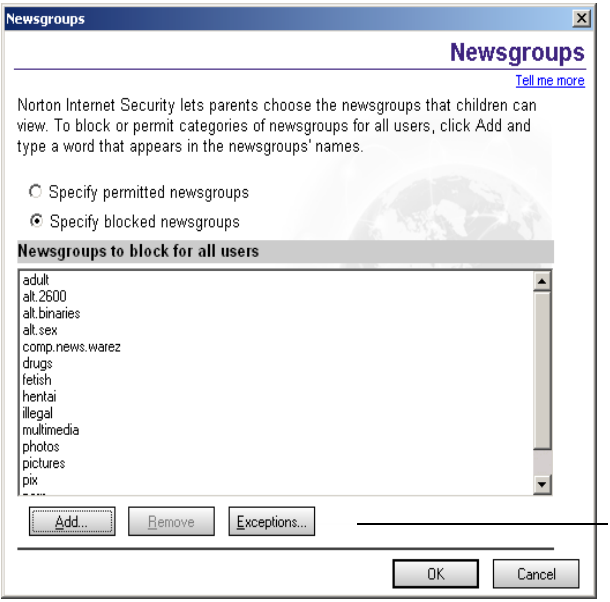
1. Start Norton Internet Security.
2. Double-click **Parental Control**.

3 In the Parental Control window, on the Settings For menu, select the account that you want to change.

4 Click **Newsgroups**.

5 In the Specify Newsgroups window, select the action that you want to take. Your options are:

Specify permitted newsgroups	Identify text strings to permit.
Specify blocked newsgroups	Identify text strings to block.



Norton Internet Security lets parents choose the newsgroups that children can view. To block or permit categories of newsgroups for all users, click Add and type a word that appears in the newsgroups' names.

○ Specify permitted newsgroups
● Specify blocked newsgroups

Newsgroups to block for all users

adult
alt.2600
alt.binaries
alt.sex
comp.news.warez
drugs
fetish
hentai
illegal
multimedia
photos
pictures
pix

These text strings are blocked or permitted

Add additional text strings that you want to block or permit

Create an exception to permit access to a specific newsgroup

6 Click **Add**.

7 Type a text string to block or permit.

8 Click **OK**.

Create exceptions to blocked newsgroups

If you create a list of blocked sites, you may find that a newsgroup that your users need to access is also blocked. Parental Control lets you create exceptions that give access to specific blocked newsgroups. For example, you can block access to all comp.security newsgroups while still allowing access to comp.security.firewalls.

To create exceptions to blocked newsgroups

1. Start Norton Internet Security.
2. Double-click **Parental Control**.
3. In the Parental Control window, on the Settings For menu, select the account that you want to change.
4. Click **Newsgroups**.
5. In the Specify Newsgroups window, click **Specify Blocked Newsgroups**.
6. Click **Exceptions**.
7. Click **Add**.
8. In the Add Newsgroup to Exceptions List window, type the complete name of the newsgroup that you want to unblock.
9. Click **OK**.
10. When you are done adding exceptions, click **OK**.

Monitoring Norton Internet Security

Norton Internet Security maintains records of every ingoing and outgoing Internet *connection* and any actions that the program takes to protect your computer. You should periodically review this information to spot potential problems.

There are four sources of Norton Internet Security information:

Status & Settings window	Basic information about which protection features are active
Statistics window	Recent information about firewall and content-blocking activities
Detailed statistics window	Detailed information about network activity and actions that Norton Internet Security has taken
Event Log	Internet activities and any actions Norton Internet Security has taken

When reviewing logged information, check for:

- Recent attacks in the Status & Settings window
- Many denied accesses, especially from a single *IP address*
- Sequences of *port numbers* from the same IP address, possibly indicating a *port scan*
- Excessive network activity by unknown programs
- Recent virus alerts

It is normal to see some denied access attempts on a random basis (not all from the same IP address, and not to a sequence of port numbers). You may also see logged access attempts made due to activity on your own computer such as connecting to an FTP server and sending *email* messages.

If you see any of the above patterns, it could be evidence of an attack or virus infection.

View the Status & Settings window

The Status & Settings window provides a snapshot of your current protection. You can quickly see which protection features are active, identify any holes in your protection, and customize Norton Internet Security.

To view the Status & Settings window

1. Open Norton Internet Security.
2. In the Security Center, click **Status & Settings**.
3. To change any settings, double-click a protection feature.

View the Statistics window

The Statistics window provides a snapshot of your computer's *network* activity since the last time you started Windows. Use this information to identify ongoing attack attempts and review how your Privacy Control and Parental Control settings affect your protection.

The Statistics window includes information on:

Personal Firewall	Any recent attacks on this computer, including the time of the most recent attack and the address of the attacking computer
Online Content Blocking	The number of cookies, Web ads, and spam email messages that have been blocked and the number of times private information has been blocked
Parental Control	Web sites and programs that have been blocked

To view the Statistics window

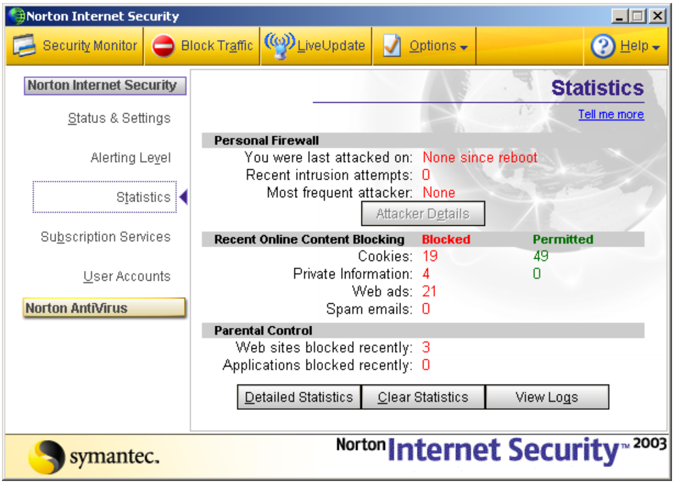
1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.

Reset information in the Statistics window

Norton Internet Security automatically clears all of the statistics in the Statistics window when you restart Windows. You can also clear the statistics manually. This helps you see if a configuration change affects the statistics.

To reset information in the Statistics window

1. Open Norton Internet Security.
2. In the Security Center, click **Statistics**.



Personal Firewall
You were last attacked on: None since reboot
Recent intrusion attempts: 0
Most frequent attacker: None

Recent Online Content Blocking	Blocked	Permitted
Cookies:	19	49
Private Information:	4	0
Web ads:	21	
Spam emails:	0	

Parental Control
Web sites blocked recently: 3
Applications blocked recently: 0

3. In the Statistics window, click **Clear Statistics**.

Review detailed statistics

Along with the overall statistics in the Statistics window, Norton Internet Security maintains realtime network counters that track users' Internet usage and any actions that Norton Internet Security takes.

The detailed statistics include the following information.

Network	TCP and UDP bytes sent and received, the number of open network connections, and the highest number of simultaneous open network connections since the program started
Web	Graphics, cookies, and requests for browser information that have been blocked; the number of bytes and packets that have been processed; and the number of HTTP connections
Web Graphics/ Banner Ads Blocked	Estimated sizes of graphics that have been blocked, and the time saved by not loading blocked graphics
Firewall TCP Connections	The number of blocked and permitted TCP connections
Firewall UDP Datagrams	The number of blocked and permitted UDP connections
Firewall Rules	All of the rules defined for your firewall and information on the number of communication attempts blocked, permitted, or not matched by firewall rules
Network Connections	Information about current connections, including the program that is using the connection, the protocol being used, and the addresses or names of the connected computers
Last 60 Seconds	The number of network and HTTP connections and the speed of each connection type

To review detailed statistics

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.

Reset detailed statistics counters

Reset the counters to clear all of the statistics and begin accumulating them again. This helps you see if a configuration change affects the statistics.

To reset counters

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. On the View menu, click **Reset Values**.

Set the statistics displayed in the Detailed Statistics window

Users can view all detailed statistics at once or display only certain categories.

To set the statistics displayed in the Detailed Statistics window

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. In the Detailed Statistics window, on the View menu, click **Options**.
5. In the Norton Internet Security Statistics Options window, select one or more categories of statistics that you want to display.
6. Click **OK**.

Configure Detailed Statistics window columns

The Detailed Statistics window can display information in one or two columns. Both window layouts contain the same statistics.

To configure Detailed Statistics window columns

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.

4. In the Detailed Statistics window, do one of the following:
    - To automatically adjust between a one and two column display, based on the current window width, on the View menu, click **Columns** > **Automatic**.
    - To always display a single column, on the View menu, click **Columns** > **One**.
    - To always display two columns, on the View menu, click **Columns** > **Two**.

Keep the Detailed Statistics window visible at all times

You can keep the Detailed Statistics window visible, even when a program runs in a full-screen window. This can be useful for spotting unusual network activity that may indicate a security problem.

To keep the Detailed Statistics window visible at all times

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. In the Detailed Statistics window, on the View menu, click **Always On Top**.

View Norton Internet Security Logs

Norton Internet Security records information about Web sites that users have visited, actions that the firewall has taken, and any alerts that have been triggered. The *logs* include details about some of the activity reported in the Statistics window.

The logs are organized onto 14 tabs.

Tab	Information
Virus Alerts	Details about any viruses or Trojan horses detected on your computer
Application Activities	A history of all actions Norton AntiVirus has taken to protect your computer
Errors	Information about any problems Norton AntiVirus encountered when scanning your computer for viruses
Content Blocking	Details about banner ads, images, Java applets, and ActiveX controls blocked by Norton Internet Security
Connections	A history of all TCP/IP network connections made with this computer, including the date and time of the connection, the address of the computer to which you connected, the service or port number used, the amount of information transferred, and the total time the connection was active
Firewall	Communication intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events
Intrusion Detection	Whether Intrusion Detection is active, attack signatures being monitored, and the number of intrusions blocked
Privacy	The cookies that have been blocked, including the name of the cookie and the Web site that requested the cookie
Private Information	A history of all protected private information sent over the Internet
Restrictions	The Internet programs, newsgroups, and Web sites blocked by Norton Internet Security
System	Severe system errors, the current status of IP filtering, if the logged program started as a Windows service, and information about programs that are using too many resources or otherwise operating under less than optimum conditions
Web History	URLs visited by the computer, providing a history of Web activity
Alerts	Any security alerts triggered by possible attacks on your computer
Spam	Details about emails identified as spam by Spam Alert

View the logs

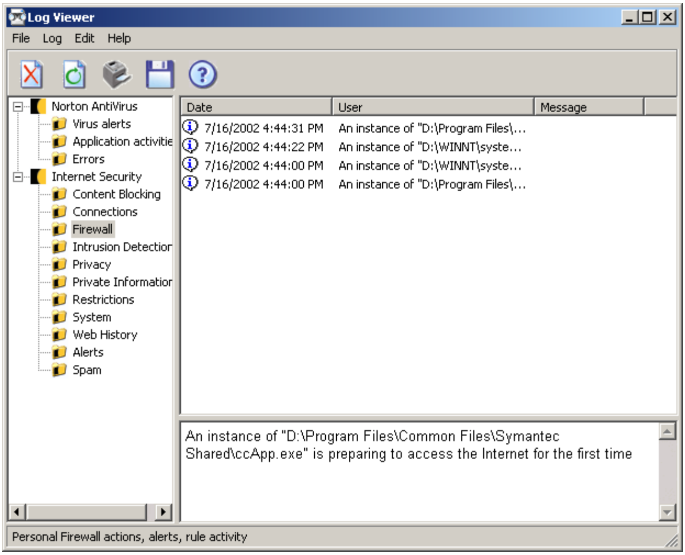
View the Norton Internet Security logs from the Statistics window.

To view the logs

1 Open Norton Internet Security.

2 Do one of the following:

- In the Security Center, click **Statistics** > **View Logs**.
- In the Security Monitor, on the Select a Task menu, click **View Log Viewer**.



Date	User	Message
7/16/2002 4:44:31 PM	An instance of "D:\Program Files\...	
7/16/2002 4:44:22 PM	An instance of "D:\WINNT\syste...	
7/16/2002 4:44:00 PM	An instance of "D:\WINNT\syste...	
7/16/2002 4:44:00 PM	An instance of "D:\Program Files\...	

An instance of "D:\Program Files\Common Files\Symantec Shared\ccApp.exe" is preparing to access the Internet for the first time

Personal Firewall actions, alerts, rule activity

3 In the Log Viewer, select the log that you want to review.

4 When you are done, click another log or click **OK** to close the Log Viewer.

Refresh the logs

The logs automatically refresh when you move from log to log. To view *network* events occurring since you began viewing the Log Viewer, you can manually refresh all the logs or an individual log.

To refresh all logs at once

1. In the Log Viewer, select one of the following:
   - Norton Internet Security
   - Norton AntiVirus
2. Click **Refresh all Categories**.

To refresh an individual log

❖ In the Log Viewer, right-click the log that you want to refresh, then click **Refresh Category**.

Disable logging

You can choose the types of information Norton Internet Security tracks in the logs. By default, Norton Internet Security tracks events in every category. You can disable individual logs if you do not need the information they contain.

To disable logging

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click the log that you want to disable, then click **Disable Logging**.

Clear the logs

If you actively use the Internet, or if other computers frequently connect to your computer, your log files may include information about hundreds of *connections*. This can make it difficult to identify specific activity or assess the impact of any changes that you make to Norton Internet Security settings.

Clear the logs to remove information about past connections. This lets you see how settings changes affect your protection. You can clear a single log or clear all logs at once.

To clear a single log

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click the log that you want to clear, then click **Clear Category**.

To clear all logs at once

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, select one of the following:
   - Norton Internet Security
   - Norton AntiVirus
5. Click **Refresh all Categories**.

Change the size of the logs

Norton Internet Security stores the information for each log in a separate file. You can change the size of log files to manage the amount of hard disk space that they occupy. When the files reach their maximum sizes, new events overwrite the oldest events.

By default, log files are between 64 KB and 512 KB. If you want to see information spanning a longer period, increase the size of the log. If you need to recover hard disk space, reduce the size. Changing the size of a log file clears all of the information in that log.

To change the size of a log

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click a log, then click **Change Log File Size**. The Log File Size dialog box displays the Log’s current file size.
5. In the Log File Size dialog box, select a new file size.
6. Click **OK**.

Adjust the width of a column

You can change the width of the columns in the Log Viewer.

To adjust the width of a column

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, on the tab that you want to view, point to the boundary line on the right side of the column heading.
   The cursor changes from a pointer to a resize tool.
5. Drag the boundary line to the desired width.

Print or save logs and statistics

As you access the Internet, older information in the *logs* and statistics is overwritten with newer data. To preserve older Internet usage information, or to include this information in word-processing or other documents, print or export the logs and statistics.

To print log information

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click the log that you want to print, then click **Print Category**.

To print statistics information

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. In the Detailed Statistics window, on the File menu, click **Print**.
5. In the Print window, click **Print**.

To save log information in a text file

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. In the Log Viewer, right-click the log that you want to save, then click **Export Category As**.
5. Specify a location and name for the text file.
6. Click **Save**.

To save statistics to a text file

1. Open Norton Internet Security.
2. In the Security Center main window, click **Statistics**.
3. In the Statistics window, click **Detailed Statistics**.
4. In the Detailed Statistics window, on the File menu, click **Save**.
5. Specify a location and name for the text file.
6. Click **Save**.

Troubleshooting Norton Internet Security

A

The information in this chapter will help you solve the most frequently encountered problems. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site. You can find updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

1. Point your browser to www.symantec.com/techsupp
2. On the service and support Web page, click **I am a home/small business user**.
3. On the introduction Web page, click the link for the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

1. On the left side of any Web page in the Symantec Web site, click **search**.
2. Type a word or phrase that best represents the information for which you are looking. Use the following guidelines when searching the Symantec Web site:
   - Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type install to find articles that include the word install, installation, installing, etc.
   - Type multiple words to find all occurrences of any of the words. For example, type virus definitions to find articles that include virus or definitions or both.
   - Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
   - Use a plus (+) sign in front of all of the search terms to retrieve documents containing all of the words. For example, +Internet +Security finds articles containing both words.
   - For an exact match, type the search words in uppercase letters.
   - To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, "purchase product", "MAC", "Norton SystemWorks" searches for all three phrases, and finds all articles that include any of these phrases.
3. Select the area of the Web site that you want to search.
4. Click **Search**.

Troubleshoot Norton Internet Security problems

Here are some solutions to issues that might arise with Norton Internet Security.

What is wrong with this Web site?

Norton Internet Security can block certain elements of a Web site that prevent it from displaying correctly in your Web browser. In some cases, the site might not display at all.

In most cases, Norton Internet Security is protecting you from inappropriate content. Your best solution may be to go to another, more appropriate Web site.

See "Temporarily disable Norton Internet Security" on page 71.

If you are a Supervisor user, you can disable Norton Internet Security and try the Web site again. Keep in mind that when you disable Norton Internet Security, your computer may be vulnerable to Internet attacks.

If you cannot connect to a Web site with Norton Internet Security disabled, there might be a problem with the Internet or your *Internet service provider*.

Problem	Solution
It could be Cookie Blocking	Many Web sites require that cookies be enabled on your computer to display correctly. See "Change the Cookie Blocking setting" on page 160.
It could be Parental Control	If you have set up Parental Control to block certain categories of Web sites, it may be blocking the site that you are attempting to view. When Parental Control blocks a site, it always displays a message telling you that the site is blocked. See "Restrict Web site access" on page 181.
It could be a firewall rule	A firewall rule might be blocking the Web site. When this happens, you will usually see a message saying that you could not connect. See "Customize firewall protection" on page 105.
It could be Ad Blocking	Sometimes blocking advertisements on the Internet prevents an entire Web site from appearing in your browser. See "Blocking Internet advertisements" on page 163.
It could be ActiveX or Java blocking	Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites. See "Change individual security settings" on page 106.
It could be Flash blocking	Some Web sites use Macromedia Flash to create interactive front pages. If you are blocking Flash, nothing appears on these sites. See "Enable or disable Flash blocking" on page 166.

Why can't I post information online?

See "Identify private information to protect" on page 155.

If you are unable to post information to a Web site, it may be because Privacy Control is blocking the information. Check the Private Information list in the Privacy window to see if the information that you are trying to enter is being blocked.

Why did an email message I sent never arrive?

If you choose to block an *email* message containing private information, Norton Internet Security immediately deletes the email message. Your email program will indicate that the message was sent, but the recipient will not receive it.

If your email program maintains copies of sent messages in its Sent or Out folder, you can reopen the email message, remove the private information, and send the message again.

Why won't a program connect to the Internet?

A Child or Teenager user might not be able to use a program to connect to the Internet for any of the following reasons.

The program might belong in a category of programs that is restricted for this account.	See "Restrict programs that access the Internet" on page 185.
There is no firewall rule that lets the program create a connection to the Internet.	See "Respond to Norton Internet Security alerts" on page 55.
Norton Internet Security could be blocking your account from using this program on the Internet.	See "Protect children with Parental Control" on page 179.

If a Child or Teenager user needs to use this program, a Supervisor can adjust your Parental Control settings.

Why doesn't Norton Internet Security notify me before letting programs access the Internet?

See "Enable Automatic Program Control" on page 110.

If Automatic Program Control is on, Norton Internet Security creates rules for programs that it recognizes without notifying you.

Why can't I print to a shared printer or connect to a computer on my local network?

Norton Internet Security blocks the use of Microsoft networking to prevent someone from connecting to your computer over the Internet.

See "Organize computers into network zones" on page 91.

To allow the use of your local network, including file and printer sharing, place the computers on your local network in the Trusted Zone.

Why can't I connect to the Internet via my cable modem?

If your network accesses the Internet via a cable *connection*, you may need to make your computer's NetBIOS name visible. While the NetBIOS name is visible, the files and folders on your computer remain hidden.

To make your NetBIOS name visible

1. Open Norton Internet Security.
2. In the Security Center, double-click **Personal Firewall**.
3. In the Personal Firewall window, on the Advanced tab, click **General Rules**.
4. In the General rules dialog box, click **Default Inbound NetBIOS Name**.
5. Click **Modify**.
6. In the Modify Rule dialog box, on the Action tab, click **Permit Internet access**.
7. Click **OK**.
8. In the General Rules dialog box, click **OK**.
9. In the Personal Firewall window, click **OK**.

Some Internet service providers scan the ports on users' computers to ensure that they are keeping to their service agreements. Norton Internet Security might interpret this as a malicious *port scan* and stop communications with your cable system. If this occurs, you need to let your cable provider run port scans.

To allow ISP port scans

1. Open Norton Internet Security.
2. In the Security Center, double-click **Intrusion Detection**.
3. In the Intrusion Detection window, click **IP Address**.
4. In the Exclusions dialog box, select the IP address your ISP uses for port scans.
   Your ISP can provide this information.
5. Click **Exclude**.
6. Click **OK**.

Why can't LiveUpdate get a list of updates?

The first time that you run LiveUpdate after installing Norton Internet Security, an alert appears to help you create a rule that lets LiveUpdate access the Internet. Child or Teenager users cannot create these rules.

Log on to an Adult or Supervisor account and run LiveUpdate. This creates rules that let anyone run LiveUpdate.

How can a Web site get my browser information?

The Browser Privacy settings prevent your browser from sending browser information. However, some diagnostic sites on the Internet might report browser information even though the Browser Privacy settings are blocking it.

If you are blocking *Java*, *ActiveX*, or scripts, the site might be using one of these methods to retrieve the information. Sometimes when Web servers do not get the information from the browser, they use the last piece of browser information that they received instead. You might see the information from the last person who viewed the site.

Troubleshoot Norton AntiVirus problems

Here are some solutions to issues that might arise with Norton AntiVirus.

My Rescue Disk does not work

Due to the number of product-specific technologies used by manufacturers to configure and initialize hard drives, the Rescue program cannot always create a bootable disk automatically. If your Rescue Boot Disk does not work properly, do one of the following:

- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start from that disk. Remove the disk and insert your Rescue Boot Disk. At the DOS prompt, type **A:RSHELL**, press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.

Sometimes, your Rescue Boot Disk does not work properly because you have more than one *operating system* installed, such as Windows 2000 and Windows 98.

To modify your Rescue Boot Disk

1. Start up from your hard drive.
2. Insert your Rescue Boot Disk into drive A.
3. At the DOS prompt, type **SYS A:**
4. Press **Enter**.
   This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

The alert tells me to use my Rescue Disks, but I did not create them

See "Create Emergency Disks" on page 30.

With your Norton Internet Security CD you can create Emergency Disks. Although they are not as powerful as the Rescue Disks you create, you can use the Emergency Disks to recover from most common emergencies.

See "If you are using the CD as an Emergency Disk" on page 142.

You can use the CD that contains Norton AntiVirus as an Emergency Disk if your computer can start from the CD-ROM drive.

Once you have created the Emergency Disks, use them to solve the problem.

I cannot start from drive A

If your computer does not check drive A first on startup, use your computer's Setup program to change settings.

Be careful when making 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.
   A message appears telling you the key or keys to press to run SETUP, such as Press <DEL> if you want to run SETUP.
2. Press the key or keys to launch the Setup program.
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 system, or contact your system's manufacturer.
4. Save the changes, then exit the Setup program.

You may need to use a special boot disk rather than the Rescue Boot Disk. In this case, use the boot disk or startup disk that came with your computer.

See "My Rescue Disk does not work" on page 209.

If your computer is set up with more than one operating system, such as Windows 2000 and Windows 98, you may need to modify the Rescue Boot Disk.

Auto-Protect does not load when I start my computer

If the Norton AntiVirus Auto-Protect icon does not appear in the lower-right corner of the Windows taskbar, Auto-Protect is not loaded. There are three likely reasons this is happening.

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

1. On the Windows taskbar, click **Start** > **Shut Down**.
2. In the Shut Down Windows dialog box, click **Restart**.
3. Click **OK**.

Norton Internet Security may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under System, click **Auto-Protect**.
4. Ensure that Start Auto-Protect when Windows starts up is checked.

Norton AntiVirus may not be configured to show the Auto-Protect icon in the tray.

To show the Auto-Protect icon in the tray

1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under System, click **Auto-Protect**.
4. Ensure that Show the Auto-Protect icon in the tray is checked.

I have scanned and removed a virus, but it keeps infecting my files

There are four possible reasons a virus could be reappearing.

The virus might be in a program file with an unusual extension for which Norton AntiVirus is not configured to look.

To reset Norton AntiVirus scanning options

1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under System, click **Manual Scan**.
4. Under Which file types to scan for viruses, click **Comprehensive file scanning**.
5. Click **Manual Scan** > **Bloodhound**.

6 Ensure that Enable Bloodhound heuristics is checked, and click **Highest level of protection**.

7 Click **OK**.

8 Scan all of the disks that you use and repair all infected files.

The source of the infection could also be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

See "If you need to use Rescue Disks (Windows 98/98SE/Me)" on page 141.

Another reason could be that the virus is remaining in memory after you remove it from the *boot record*. It then reinfects your boot record. Use your Rescue Disks to remove the virus.

If the problem is a Trojan horse or worm that was transmitted over a shared *network* drive, you must disconnect from the network or password protect the drive to let Norton AntiVirus delete the problem.

Norton AntiVirus cannot repair my infected files

See "Keeping current with LiveUpdate" on page 81.

The most common reason that Norton AntiVirus cannot repair your *infected files* is that you do not have the most current virus protection on your computer. Update your virus protection regularly to protect your computer from the latest viruses.

If after using LiveUpdate the virus still cannot be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

See "If you have files in Quarantine" on page 138.

- Quarantine the file and submit it to Symantec.
- If a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

I get an error when testing basic Rescue Disks

If you get the message, "Non-system disk, replace the disk and press any key," when testing your Rescue Disks, the Rescue program may not have prepared the floppy boot files correctly.

To repair the Rescue Boot Disk without having to reformat the disk and create a new Rescue Disk set

1 Remove the Rescue Boot Disk and restart your computer.

2 Insert the Rescue Boot Disk into the floppy disk drive.

3 On the Windows taskbar, click **Start** > **Run**.

4 In the Run dialog box, type **SYS A:**

5 Click **OK**.

I can't receive email messages

There are two possible solutions to this problem.

Temporarily disable email protection. This might allow the problem email message to be downloaded so that you can once again enable email protection. You are protected by Auto-Protect and Script Blocking while email protection is disabled.

To temporarily disable incoming email protection

1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under Internet, click **Email**.
4. Uncheck **Scan incoming Email**.
5. Click **OK**.
6. Download your email messages.
7. Reenable incoming email protection.

See "About Internet options" on page 67.

Your email client may have timed out. Make sure *timeout* protection is enabled.

If you continue to experience problems downloading email messages, disable email protection.

To disable email protection

1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under Internet, click **Email**.
4. Uncheck **Scan incoming Email**.
5. Uncheck **Scan outgoing Email**.
6. Click **OK**.

I can’t send email messages

If you get the message, “Norton AntiVirus was unable to send your email message because the connection to your email server was disconnected,” your email client may be set to automatically disconnect after sending and receiving mail.

For Norton AntiVirus to scan outgoing email messages for viruses, it intercepts and scans the messages before they are sent to your email provider. To resolve this issue, turn off this option within your email client. Consult your email client manual for instructions on how to do this, or disable Norton AntiVirus outgoing email scanning.

To disable outgoing email scanning

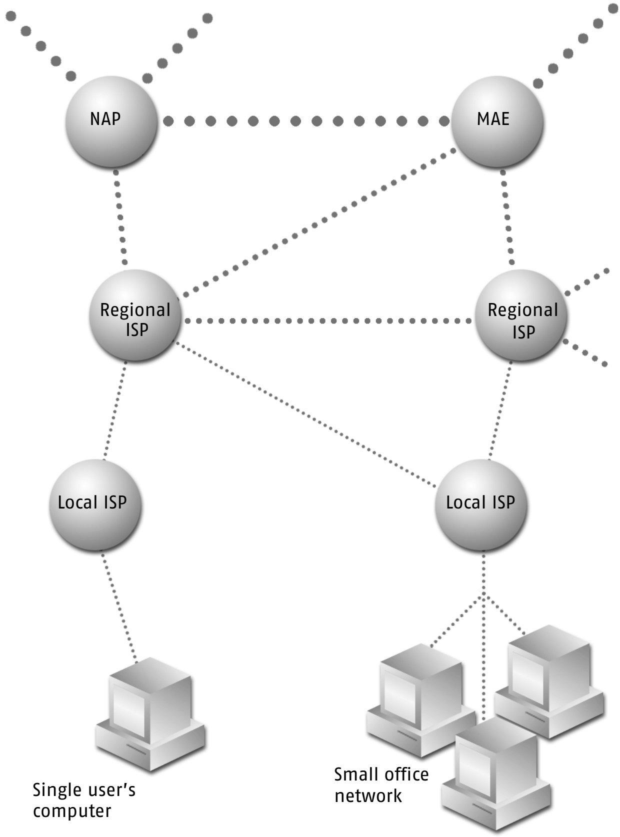
1. Start Norton Internet Security.
2. In the Security Center, click **Options** > **Norton AntiVirus**.
3. In the Options window, under Internet, click **Email**.
4. Uncheck **Scan outgoing Email**.
5. Click **OK**.

About the Internet

B

The Internet is the interconnection of millions of computers throughout the world. It is comprised of the computers and the connections that make it possible for any computer on the Internet to communicate with any other computer on the Internet.

The Internet is analogous to a system of roads and highways. The superhighways of the Internet, called the Internet backbone, carry large amounts of information over long distances. There are interchanges on the backbone, called network access points (NAPs) and metropolitan area exchanges (MAEs). There are regional highways provided by large ISPs and local streets provided by local ISPs.



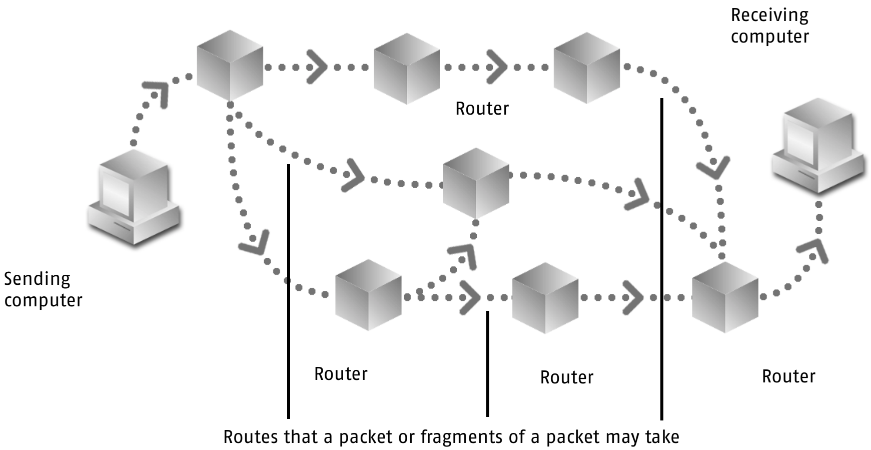
Like a system of roads and highways, the Internet provides multiple routes from one point to another. If one part of the Internet has too much traffic, or is damaged, information is rerouted.

How information is transmitted over the Internet

All information sent over the Internet is communicated using a protocol called *TCP/IP*. Because all of the computers on the Internet understand this protocol, each one can communicate with every other computer on the Internet. TCP and IP are separate parts of this protocol.

The Internet is a *packet switching network*. Every communication is broken into *packets* by TCP (Transmission Control Protocol). Each packet contains the addresses of the sending and receiving computers along with the information to be communicated.

IP (Internet Protocol) is responsible for routing the packets to their destinations. Each packet may take a different route across the Internet, and packets may be broken up into *fragments*. Packets travel across the Internet, moving from one *router* to another. Routers look at the destination address and forward the packet to the next router. IP does not guarantee the delivery of every packet.



On the destination computer, TCP joins the packets into the complete communication. TCP may have to reorder the packets if they are received out of order, and it may have to reassemble fragmented packets. TCP requests retransmission of missing packets.

TCP/IP is often used to refer to a group of protocols used on the Internet, including UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), and IGMP (Internet Group Membership Protocol).

About UDP

UDP (User Datagram Protocol) is used for functions in which the reliability of TCP is not necessary, such as broadcasting video to multiple computers at once. UDP doesn’t provide error correction or retransmission of lost packets. UDP is secondary in importance to TCP when you browse the Internet.

About ICMP

ICMP (Internet Control Message Protocol) packets contain error and control information. They are used to announce network errors, network congestion, timeouts, and to assist in troubleshooting.

Norton Internet Security normally allows inbound ICMP packets that provide you with information and are a minimal security risk. You can create rules to block some or all ICMP packets.

About IGMP

IGMP (Internet Group Membership Protocol) is used to establish memberships in multicast groups, collections of computers that receive simultaneous messages from a single computer. Typically, IGMP is used to broadcast video and other multimedia over the Internet. Your computer reports to a nearby router that it wants to receive messages addressed to a specific multicast group.

IGMP does not present a major security risk, but Norton Internet Security allows you to block the protocol entirely. This is a good idea if you do not use any programs that require IGMP. If you have problems receiving multicast information, such as movies or PowerPoint presentations, be sure that IGMP is not blocked.

How Web information is located on the Internet

Web information is stored as pages, each with a unique name called a *URL (Uniform Resource Locator)*.

When you type a Web address in the browser address bar or click a link in your Web browser to move to a new Web site, you are giving your browser the URL of the page that you want to view. For example, www.symantec.com is a typical URL.

Each URL maps to the IP address of the computer that stores the Web page. URLs are used because they are easier to remember and type than IP addresses.

Before your browser requests a page, it asks a *DNS (Domain Name System) server* for the IP address of the Web site. IP addresses are 32-bit numbers expressed as four decimal numbers, each ranging from 0 to 255, and separated by periods: 206.204.104.148. Every computer on the Internet has a unique IP address.

Requesting a page

Once the browser has the IP address, it establishes a TCP *connection* to the Web server and requests the page. Each page that you view requires a new connection with the Web server. In fact, most pages require multiple connections, since each graphic (as well as many other page elements) requires its own connection.

Once a page is loaded, all of the connections are dropped. The process starts over for each page on the site, though your browser does remember the site’s IP address. Some newer Web sites use HTTP 1.1 (Hypertext Transfer Protocol version 1.1) to establish a single connection that can pass multiple files and stay open for multiple pages.

Understanding URLs

A typical URL looks like this: http://www.symantec.com/securitycheck/index.html. Because you might want to block some parts of a *domain* while allowing other parts of the same domain, you should understand the parts that comprise a URL.

http://	The program protocol used to make the connection. The most common protocol for browsing the Web is HTTP (Hypertext Transfer Protocol). Your browser assumes that this is the program protocol if you don’t enter one. Other commonly used protocols include FTP (File Transfer Protocol) and gopher.
.com	The root or top-level domain. There are several familiar root domains, including .com, .net, .edu, .org, .mil, and .gov. There are also two-letter root domains for most countries, such as .ca for Canada and .uk for the United Kingdom.
symantec.com	The domain. This is the domain with which the browser establishes a connection. A domain frequently refers to a single company or organization that might have multiple Web sites on the Internet.
www.symantec.com	The host. This is the particular Web site with which the browser communicates. It is also the name for which DNS provides an IP address.
securitycheck	The folder or directory that contains the file to be accessed.
index.html	The file name of the file to be accessed.

There is one particular URL that identifies your computer to itself, and that is localhost. If your computer has Web server software installed, you can type http://localhost and see your Web page. The IP address that corresponds to localhost is 127.0.0.1.

How ports identify programs on servers

Ports, also called *sockets*, provide the locations of particular programs or servers on the remote computer with which you are trying to establish communication. This makes it possible to run multiple Internet programs simultaneously on a single computer. For example, many computers on the Internet run both Web and FTP servers. The Web server uses port 80, while the FTP server uses port 21.

Ports are numbered 1 through 65535. Ports 1 through 1023 are known as well-known ports and are the default ports for many common Internet programs.

Ports are part of *URLs*, but they are rarely seen. The *port number* follows the host name and a colon. For example:

http://www.symantec.com:80/securitycheck/index.html

Because the most-used ports are standardized, you rarely see port numbers. For example, Web browsers almost always use port 80, so they don't require that you type it unless you need to use a different port.

The terms server and *service* are used somewhat interchangeably. For example, a Web server provides the HTTP service, while it is usually said that a computer has the *finger* service running.

Well-known ports

Following are some of the most common well-known ports.

Default port	Service name	Program
20	ftp-data	FTP (File Transfer Protocol) data
21	ftp	FTP (File Transfer Protocol) control
23	telnet	Telnet terminal handler
25	smtp	SMTP (Simple Mail Transfer Protocol)
53	domain	DNS (Domain Name Service) lookup
79	finger	Finger
80	http	HTTP (Hypertext Transfer Protocol)
110	pop3	POP3 (Post Office Protocol 3)
113	auth	Ident Authentication Service
119	nntp	NNTP (Network News Transfer Protocol)
137	nbname	NetBIOS name (Microsoft Networking)
138	nbdatagram	NetBIOS datagram (Microsoft Networking)
139	nbsession	NetBIOS session (Microsoft Networking)
143	imap	IMAP (Internet Message Access Protocol)

Default port	Service name	Program
194	irc	IRC (Internet Relay Chat)
389	ldap	LDAP (Lightweight Directory Access Protocol)
443	https	HTTPS (Secure HTTP)

How computers are identified on the Internet

Millions of computers are connected to the Internet. When you are trying to identify computers, it is easier to work with groups of computers rather than having to identify each one individually. *Subnet* masks provide a way to identify a group of related computers, such as those on your local network.

A typical subnet mask looks like this: 255.255.255.0. The 255s indicate parts of the IP address that are the same for all computers within the subnet, while the 0 indicates a part of the IP address that is different.

Subnet masks are always used in conjunction with base IP addresses. The base IP address is an IP address that, when processed using the subnet mask, can indicate all of the IP addresses in a subnet.

A typical base IP address/subnet pair looks like this:

Base IP address:	10.0.0.1
Subnet mask:	255.255.255.0

In this example, the range of IP addresses that the base IP address and subnet mask identify range from 10.0.0.1 to 10.0.0.255. The most common subnet mask used is 255.255.255.0 because it identifies a relatively small group of IP addresses, up to 254 computers. It is commonly used for very small groups of computers, including groups as small as two computers.

Understanding Internet risks

Norton Internet Security protects you from major risks that are associated with the Internet. These risks include the threat of network attack, malicious code in *active content*, exposure to inappropriate content, exposure of private information, and getting viruses from infected files.

Risks from hackers

Originally *hackers* were people who could solve computer problems and write complex computer programs quickly. However, the meaning of the term has changed to mean those who use their computer knowledge for illicit purposes. Since hacker started out as a complimentary term, some people use the word *cracker* for the derogatory form. In this text, hacker is used in its noncomplimentary form.

You might also hear other terms for hackers, including script-kiddies, wannabes, and packet monkeys. These are all terms for hackers-in-training, who use programs written by more advanced hackers to attack computers on the Internet.

The process of a hacker attack

Most hacker attacks use the following process:

- Information gathering
  The hacker gathers as much information about your computer as possible. The hacker attempts to find vulnerabilities without letting you know that your computer is under attack.
- Initial access
  The hacker exploits a vulnerability found during information gathering and establishes an entry point into your computer.
- Privilege escalation
  The hacker gains access to more programs and *services* on your computer.
- Covering tracks
  The hacker hides or removes evidence of the intrusion, sometimes leaving an entry point open for return.

Information gathering

The first step in information gathering is acquiring a target. A hacker can choose a person or company to attack, or search the Internet for an unprotected target that will be easy to hack. The amount of information available about you on the Internet is directly related to your level of Web presence. If you have a *domain* name and a Web site, more information is publicly available than would be if you only had an *email* address.

If a hacker has chosen a specific target, such as a company or organization, many resources on the Internet assist in gathering information. Using the Internet, a hacker can learn a lot about a potential target. Given a domain name, it's easy to find out the name and address of the owner, as well as the name and phone number of the administrative and technical contacts. While this information usually can't be used directly to attack a network or computer, it can be used to gather more information.

If a hacker doesn't have a specific target in mind, many tools are available for scanning the Internet and finding possible targets. The simplest scan is a ping scan, which can quickly scan thousands of computers. The hacker uses a program to ping computers at a series of IP addresses. A response tells the hacker that a computer exists at an IP address. When Norton Internet Security is running, your computer is hidden from ping scans because your computer does not respond. The hacker does not learn that there is a computer at your IP address by pinging it.

Port scans are more comprehensive and are usually performed on single computers. A port scan can tell a hacker which services are running, such as HTTP and FTP. Each service that is running provides a potential entry point for the hacker. On unprotected computers, unused ports respond that they are closed, telling the hacker that a computer exists at that IP address. Norton Internet Security does not respond to scans of unused ports, giving them a *stealth* appearance.

Initial access

The easiest way for a hacker to access a Windows computer is to use Microsoft networking. On many computers, Microsoft networking is enabled so that anyone on the network can connect to it.

Microsoft NetBIOS networking uses three of the well-known ports. These ports are used to establish *connections* among computers on a Microsoft network. In fact, they normally advertise the name of your computer over the local network. This is what you want on your own network, but it is not what you want on the Internet. Norton Internet Security is preset to block these ports and prevent someone on the Internet from connecting to your computer using Microsoft networking. If your computer is connected to a local network as well as to the Internet, you must change some settings to allow communication with the other computers on your network. Norton Internet Security still protects you from Internet risks while allowing you to use your local network.

Privilege escalation

Once a hacker has connected to your computer, the next step is to gain as much control as possible. The steps involved and the results obtained vary depending on the version of Windows that is running on the target computer.

On computers running Windows 95/98/Me, once hackers have gained access to the computers, there is no need for escalation. They have full control of the computers. Luckily, these versions of Windows don’t have many remote control features, so they are relatively easy to protect.

On computers running Windows 2000/XP, hackers attempt to gain administrative rights to the computers. The key to getting administrative rights is usually a *password*. The hacker can download your password file and decode it.

Another tactic is to place a *Trojan horse* on your computer. If a hacker can place a program such as Back Orifice, Subseven, or NetBus on your computer and run it, it is possible to take control of the computer.

Other Trojan horses might record all of your keystrokes to capture passwords and other sensitive data. Norton Internet Security and Norton AntiVirus provide two levels of protection against Trojan horses. Norton AntiVirus protects you from inadvertently running these programs. Norton Internet Security blocks the ports that remote access Trojan horses use to communicate over the Internet.

Covering tracks

When a hacker has gained as much control of a computer as possible, the task turns to concealing the evidence. If you don't know that a hacker has compromised your computer, you won't take steps to stop such actions.

On computers running Windows 2000/XP, hackers try to turn off auditing and modify or clear the event *logs*. On any computer, hackers may hide files so that they are available for future visits. In extreme cases, hackers might format the hard drive of a compromised computer to avoid identification.

Risks from active content

ActiveX controls and *Java applets* are called *active content* because they can do more than display text or graphics. Most active content is safe. Common uses of active content are popup menus and up-to-date stock quotes.

Both ActiveX and Java are supposed to be safe to run in your browser. ActiveX uses a system of digital certificates that lets you decide if you want an ActiveX control to run. Digital certificates appear as dialog boxes that ask if you want to install and run a control that appears when you are browsing the Web.

There are several problems with using digital certificates. Some controls do not have certificates, and some certificates provide very little information about what the control does.

The Java sandbox was designed to prevent Java applets from accessing information outside of the browser and doing anything that might harm your computer. However, *hackers* continually find ways to get around Java safeguards and use Java features in ways not conceived of by its developers.

Norton Internet Security monitors active content and can block all active content or warn you whenever active content is encountered. Norton AntiVirus Auto-Protect detects malicious ActiveX controls and Java applets and prevents them from running.

Norton Personal Firewall monitors active content and can block all active content or warn you whenever active content is encountered.

Risks from inappropriate content and activities

There is a wealth of information on the Internet that is easily accessible to everyone. However, some topics are not suitable for all people. For example, most people consider pornographic and violent sites to be inappropriate for viewing by children. You may feel that other topics should also be off limits.

Blocking site and newsgroup categories

Norton Internet Security lets you choose Web sites and newsgroups that you want to be accessible to people using this computer. Because different people need different levels of access, you can configure Norton Internet Security to block specific content for each user.

Restricting access to programs

Some Internet-enabled programs might be inappropriate for use on your computer. For example, you may not want children using realtime chat programs. You may also want to restrict the use of file transfer programs. This reduces the risk of introducing viruses, worms, zombies, *Trojan horses*, or other malicious code onto your computer or network.

Norton Internet Security lets you choose categories of programs that can access the Internet. It keeps the list of programs up-to-date, so your protection stays current as new programs are released. You can also add custom programs, and control their uses as well.

Risks to your privacy

The Internet presents several risks to your privacy. Some sites collect and save personal information, such as credit card numbers. Some sites track your Internet usage. Some programs send information about your computer usage to Web sites without your permission.

Sending private information

You probably don't want private information, such as credit card numbers or your home phone number, to be sent unencrypted over the Internet. Privacy Control prevents private information from being entered on Web sites that do not use secure, encrypted communications, and from being sent on instant messenger programs.

You may want to prevent some users from sending private information over the Internet. Norton Internet Security can block users from accessing secure sites where they might be asked for personal information.

Understanding cookies

Cookies are messages sent to your browser by Web sites that are stored as small files on your computer. They are often used by Web sites to track your visits. In most cases, cookies do not contain personal information, but instead carry information that identifies you to Web sites.

Good cookies

In their most benign form, cookies last only until you close your browser. This type of cookie is mainly used to remember choices that you make as you navigate through a Web site.

Many sites leave cookies on your computer so that they recognize you when you return to their sites. These cookies identify you so that options that you have chosen in the past are used for your current visit to the site. If you frequent a site that remembers the stocks that you want to track, for example, it probably uses this kind of cookie.

Bad cookies

In one of their malevolent forms, cookies from one Web site might track your visits to a different Web site. For example, most of the ads that you see on Web sites do not come from the site that you are viewing, but from sites that provide ads to many sites. When the advertising site displays the ad, it can access cookies on your computer. This lets the advertising company track your Web usage over a range of sites and profile your browsing habits.

Blocking cookies

Norton Internet Security can block all cookies or it can notify you of each cookie request. If you block all cookies, you lose functionality at many Web sites. For example, you might be blocked from making purchases at some Internet stores. If you choose to be prompted each time that a Web site tries to create a cookie, you can evaluate each request and block those that are not from the site that you are viewing. Norton Internet Security can block or allow cookies from particular *domains* or Web sites.

Tracking Internet use

Most browsers pass on information that you might want to keep confidential. One item that your browser normally passes to Web sites is the *URL* of the page from which you came. This information is used by some Web sites to help you navigate through the Web site, but it can also be used to track your Web usage. Norton Internet Security blocks this information.

Your browser also sends information about itself and the operating system that you are using. While Norton Internet Security can block this information, it is usually used by Web sites to provide Web pages that are appropriate for your browser.

A more sinister invasion of your privacy is found in programs that you install on your computer that, without your knowledge, report information back to Web sites. Several programs that help you download and install files report your activities over the Internet. Norton Internet Security protects your privacy by alerting you to these communications.

Risks from Trojan horses and viruses

With so many computers connected by networks and the Internet, viruses can spread more rapidly than they could in the days when files were transferred from computer to computer on disks. Additionally, the risk has broadened from viruses to *Trojan horses*, worms, and zombies.

A virus is a program or code that replicates by attaching itself to another program, a boot sector, a partition sector, or a document that supports macros. Many viruses just replicate, but others do damage. A virus can arrive in a document that you receive by *email*.

A Trojan horse is a program that does not replicate, but damages or compromises the security of the computer. Typically, it relies on someone emailing it to you; it does not email itself. A Trojan horse may arrive disguised as useful software. Some Trojan horses perform malicious actions on the computer on which they are run, while others, such as Back Orifice, provide remote control capabilities for *hackers*.

A worm is a program that makes copies of itself, for example, from one disk drive to another, or by sending itself through email. It may do damage or compromise the security of the computer. A worm can arrive as an attachment to an email that has a subject that tempts you to open it.

A zombie program is a dormant program secretly installed on a computer. It can later be run remotely to aid in a collective attack on another computer. Zombie programs don’t normally damage the computer on which they reside, but are used to attack other computers. A zombie program can arrive as an email attachment.

Norton AntiVirus protects you from receiving and executing viruses, Trojan horses, worms, and zombies. Norton AntiVirus scans email as you receive it and also checks files when you open them, providing two levels of protection.

Norton Internet Security ensures that Trojan horses do not communicate over the Internet. This means that you are protected from hackers who use Trojan horses.

The likelihood of being attacked

The Internet presents many risks. What are the odds that your computer will be attacked? The chance of an attacker singling out your computer from all of those on the Internet is slim. However, the use of port-scanning and other computer discovery tools by hackers means that your computer may be scanned relatively frequently for vulnerabilities. The more vulnerabilities that are found, the more inviting your computer is to hackers.

The tools that hackers use to find targets can scan large groups of computers on the Internet. The hacker simply enters a range of IP addresses to be scanned. The program checks each IP address in the range to see if a computer is there. If it finds a computer, it performs a series of tests to identify vulnerabilities, such as having Microsoft networking enabled over the Internet. The hacker returns to find a list of computers and their vulnerabilities.

Norton Internet Security protects you from these scans by making your computer invisible. Your computer won’t respond to queries that these scanners send. This means that your computer exhibits no vulnerabilities to the hacker, making it a poor target for attack.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- Online Service and Support
  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- PriorityCare telephone support
  This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:
http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

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

Latin America

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

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

July 25, 2002

Glossary

This glossary provides definitions of some common Internet terms.

active content	Material on a Web page that changes with time or in response to user action. Active content is implemented through ActiveX controls, Visual Basic Scripts, Java scripts, and Java applets in the HTML code that defines the page.
ActiveX control	A program that runs within a browser using Microsoft technology to add life to a Web page by using animation, streaming audio and video, movies, and so on. When you visit a Web page that contains an ActiveX control, it is dynamically downloaded and saved to your hard disk. Unlike Java applets, ActiveX controls don't run in a restricted environment, and have the potential to take control of your computer.
alert	A dialog box that appears in a graphical user interface (GUI) to signal that an error has occurred, or to provide a warning.
banner ad	An advertising graphic, often animated, that appears on a Web page and may contain a link to the advertiser's Web site.
boot record	A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot record also contains a program that loads the operating system.

browser	A software application that makes navigating the Internet easy by providing a graphical user interface. This lets the user click menus, icons, or buttons rather than learn difficult computer commands. Also called a Web client.
compressed file	A file that has been compressed using a special data storage format in order to save space on your disk.
connection	A method of data exchange that allows a reliable transfer of data between two computers.
connection attempt	The data transfer that requests the opening of a connection.
cookie	A small data file that some Web sites place on your hard disk while you're viewing a Web page. Web servers can use cookies to store your personal information and preferences so that you don't need to reenter them each time that you visit.
cracker	A person who cracks code, not necessarily for malicious reasons. Sometimes used to refer to a malicious hacker.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that automatically assigns a temporary IP address to each device on a network.
DNS (Domain Name System)	A hierarchical naming system that translates domain names (such as www.symantec.com) into IP addresses (such as 206.204.212.71).
DNS server (Domain Name System server)	A computer that keeps a database of domain names and their corresponding IP addresses. When a computer sends a domain name to a DNS server, the server returns the IP address for that domain.
domain	The common address for a single company or organization (such as symantec.com) on the Internet, which might have multiple hosts.
download	To transfer data from one computer to another, usually over a modem or network. Usually refers to the act of transferring a file from the Internet, a bulletin board system, or an online service to one's own computer.

email (electronic mail)	A method of exchanging messages and files with other people via computer networks. A popular protocol for sending email is SMTP (Simple Mail Transfer Protocol). Popular protocols for receiving email are POP3 (Post Office Protocol 3) and IMAP4 (Internet Message Access Protocol 4). Web-based email services use HTTP (Hypertext Transfer Protocol) for sending and receiving email.
executable file	A file containing program code that can be launched. Generally includes any file that is a program, extension, or a system file.
file type	A code that is stored in each file that associates it with a program or activity.
finger	A command in some operating systems that requests network user account information.
firewall	A security system that uses rules to block or allow connections and data transmissions between your computer and the Internet.
firewall rule	A set of parameters that specifies a type of data packet or network communication and an action to perform (permit it or block it) when it is found.
fragment	An IP packet that has been split into two or more parts, or fragments. When the size of an IP packet exceeds the maximum frame size of a network that it crosses, the packet must be divided into smaller packets, or fragments.
hacker	A person who attempts unauthorized access of other people’s computers for the purpose of obtaining information from, or doing damage to, those computers.
HTML (Hypertext Markup Language)	A standard language for documents on the World Wide Web. Codes inserted in a text file instruct the Web browser on how to display a Web page’s words and images for the user, and define hypertext links between documents.
icon	A graphic symbol used to represent a file, folder, disk, or other entity.

inbound communication	An attempt by an external computer to open a connection to your computer. The connection can be used to send data to and from your computer.
infected file	A file that contains a virus, Trojan horse or worm.
IP (Internet Protocol)	The essential protocol by which data is sent from one computer to another on the Internet. IP routes packets to the appropriate destinations.
IP address (Internet Protocol address)	A 32-bit numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually expressed as four groups of numbers, each ranging from 0 to 255, separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.
Java applet	A small program that runs in a restricted environment, sometimes referred to as a sandbox, that is managed by your browser. Most Java applets are used to add multimedia effects, interactivity, or other functionality to a Web page, but they can also be used for malicious purposes, such as password theft.
JavaScript	A scripting language that is similar to, but less capable than, Java. JavaScript code can be included in Web pages to add interactivity and other functionality.
local	A term that refers to your computer, as opposed to a remote computer.
log	A record of actions and events that take place on a computer or handheld device.
modem	A device that modulates (converts to analog) and demodulates (converts from analog) digital data for transmission over a telephone line. Also includes interface devices for digital connections to the Internet, such as ISDN, cable, and DSL.
network	A set of computers and associated hardware connected together in a work group for the purpose of sharing information and hardware among users.

NAT (network address translation)	A method of converting IP addresses used on an intranet or local area network into Internet IP addresses. This lets many computers share an Internet IP address. More importantly, it hides the IP addresses of network computers from outsiders.
network address	The portion of an IP address that is common to all computers on a particular network or subnet.
operating system	A program that ties the capabilities of computer hardware and software to input/output devices such as disks, keyboards, and mouse devices.
outbound communication	An attempt by your computer to open a connection with a remote computer. The connection can be used to send data to and from your computer.
packet	A unit of data that is routed between an origin and a destination on the Internet. In addition to the data being transmitted, a packet contains information that enables computers on a network to determine whether to receive it.
packet-switching network	A network of computers (such as the Internet) that transmits files by breaking them into packets and routing each packet along the best available route between the source and destination computers.
password	A character sequence entered by users to verify their identities to a network or program. The most secure passwords are difficult to guess or find in a dictionary, and contain a combination of capital letters, lowercase letters, numbers, and symbols.
POP3 (Post Office Protocol 3)	An email protocol used to retrieve email from a remote server over an Internet connection.

port

A transport user identification used by a client program to specify a particular server program on a computer. Also called service.

Some applications have ports with preassigned numbers. Others are assigned port numbers dynamically for each connection. When a service (server program) is started, it binds to its designated port number. When a client program wants to use that server, it also must request to bind to the designated port number.

port number

A logical communications channel to be used by a particular TCP/IP application. Each application has unique port numbers associated with it. By convention, some protocols use a well-known port number (for example, HTTP uses port 80), although this is configurable.

port scan

An attempt to gain access to a computer by searching for open ports. Usually done by an automated program that sends a request to each port at an IP address, listening for responses that could reveal a vulnerability.

proxy

A mechanism that lets one system act on behalf of another system when responding to protocol requests. Security programs in firewalls use proxy services to screen the secured network from users on the Internet.

quarantine

A disk location established by Norton AntiVirus to isolate files suspected to contain a virus so that the files can’t be opened or executed.

router

A device on a network that links computers or interconnected networks. A router receives packets and forwards them to their destination via the best available route.

server

The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.

service Protocols that let one computer access a type of data stored on another computer. Many host computers that are connected to the Internet offer services. For example, HTTP servers use the Hypertext Transfer Protocol to provide World Wide Web service and FTP servers offer File Transfer Protocol services. *See also* port.

socket An identifier for a particular service on a particular computer. A socket consists of the IP address of the computer followed by a colon and the port number.

stealth Giving the impression of not existing by not responding to requests for information.

subnet A local area network that is part of a larger intranet or the Internet.

TCP/IP (Transmission Control Protocol/ Internet Protocol) The standard family of protocols for communicating with Internet devices.

threat A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

timeout A predetermined period of time during which a given task must be completed. If the timeout value is reached before or during the execution of a task, the task is canceled.

top-level domain The last part of a domain name that identifies the type of entity that owns the address (such as .com for commercial organizations or .edu for educational institutions), or the geographical location of the address (such as .ca for Canada or .uk for United Kingdom).

Trojan horse A destructive program that is often designed to cause damage to a computer, while disguised as something useful or interesting.

unknown virus A virus for which Norton AntiVirus does not contain a definition. *See also* virus definition.

URL (Uniform Resource Locator)	The global address of documents and other resources on the World Wide Web and the convention that Web browsers use to locate files and other remote services.
virus	A self-replicating program that is written to alter the way that your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic computer behavior, or display annoying messages.
virus definition	Virus information that lets an antivirus program recognize and alert you to the presence of a specific virus. *See also* unknown virus.
virus-like activity	An activity or action that Norton AntiVirus perceives as the work of a possible unknown virus. Virus-like activity alerts do not necessarily indicate the presence of a virus, but should be investigated.
Web page	A single document on the World Wide Web (WWW) that is identified by a unique URL. A Web page can contain text, hyperlinks, and graphics.
Web site	A group of Web pages that is managed by a single company, organization, or individual. A Web site may include text, graphics, audio and video files, and hyperlinks to other Web pages.
World Wide Web (WWW)	The collection of hypertext documents that are stored on Web servers around the world. Also called WWW or simply the Web. The Web allows universal access to a vast collection of documents that are stored in HTML format as Web pages.
worm	A program that makes copies of itself (for example, from one disk drive to another, or by sending itself through email). It may do damage or compromise the security of the computer.
zombie	A dormant program that is secretly placed on a computer and awakened to aid in a collective attack on another computer or server. Zombie programs don't usually damage the computer on which they reside, but are used to attack other computers.

Index

A

access
  Alert Tracker 50
  Block Traffic 50, 60
  Help 50
  LiveUpdate 50, 54
  logs 54
  Norton AntiVirus 51
  Norton Internet Security 49, 52
  Options 61
  Program Scan 54
  Security Check 58
  Visual Tracking 58-59
accounts
  creating 146-150
  creating with Parental Control Wizard 146-149
  customizing 154
  levels 145
  logging on 153
  Not Logged In 145
  passwords 150
  set startup 150
  using Windows accounts 151-153
active content 226
  protection from 102
  See also ActiveX controls
  troubleshooting 205
ActiveX controls 205, 226
Ad Blocking 163-170
  enabling and disabling 165
  identifying ads to block 169-170
  troubleshooting 205
Ad Trashcan 167-168
Adobe Acrobat Reader, installing 77
advertisements, blocking 163-170, 205
Alert Assistant 55
Alert Tracker 56-58
  accessing 50
Alerting Level, adjusting 55
alerts
  adjusting the Alerting Level 55
  Alert Assistant 55
  new network connection 89
  overview 55
AOL 84
applications, accessing Internet. *See* Internet-enabled programs
attack signatures 103
  excluding 120
attacks 101-122, 224-226, 231
  network 102
  signatures 103
  tracing 58-59
  tracing from AutoBlock 59
  tracing from Log Viewer 59
  tracing from Statistics 59
AutoBlock 121-122
Automatic LiveUpdate 67, 86

Automatic Program Control 110
  enabling 110
Auto-Protect
  description 72
  disabling 72
  enabling 72, 125
  failure to load on startup 210, 211
  functions 25
  options 66

B

backing up file before repair 68
banner ads 163-170, 205
Block Traffic 60
  accessing 50
blocking
  advertisements 163-170, 205
  browser information 208
  computers 121
  cookies 160, 205, 228
  email addresses 161
  spam 171-177
  Web sites 181-185
Bloodhound
  description 25
  options 66
booting
  absent 209
  Auto-Protect failure to load 210, 211
  changing floppy disk drive settings 210
  floppy disk drive fails 210
  Rescue Disks fail 209
BOOTP service 109
browser
  information 208
  privacy 161

C

CD-ROM
  starting from 17
  starting Norton AntiVirus from 142
changing scan schedules 131
changing settings 65
chat applications 185
CompuServe 84
computer
  blocking 121
  emergency procedures 17
  names 94
  requirements 27
  specifying 93-95
conferencing applications 186
connecting to the Internet automatically 86
context-sensitive Help 76
Cookie Blocking 228
  options 160
  troubleshooting 205
cookies 160, 205, 228
creating
  Emergency Disks 30
  Rescue Disks 73
credit card numbers 157
custom scans
  changing schedule 131
  deleting 129
  deleting schedule 132
  running 129
  scheduling 130

D

definitions of technical terms 75, 237
deleting
  custom scans 129
  infected files 136
  scan schedule 132
desktop icon 49
detailed statistics
  configuring 195-196
  exporting information from 201-202
  printing 201-202
  resetting 195
  viewing 194
dialog box Help 76
disabling
  Automatic LiveUpdate 87
  Auto-Protect 72
  Norton Internet Security 50, 71
  Windows XP firewall 29
displaying the Norton AntiVirus toolbar 51

DNS (Domain Name System) 219
  firewall rules 109

E

educational applications 186
electronic newsletter 80
email 186
  spam 171-177
  supported clients 28
Emergency Disks
  creating 30
  using 142
  using the CD 142
emergency recovery procedures 17-20
  Norton Internet Security 17
  viruses 17
enabling
  Ad Blocking 165
  Automatic LiveUpdate 67
  Auto-Protect 72
  Flash blocking 166
  Office Plug-in 68
  Popup Window Blocking 166
encryption 161
Eudora, creating spam filters 175
Event Log. *See* Log Viewer

F

file
  sharing 90
  transfer applications 186
file extensions, unusual 211
file scans 127
files, reinfected after virus removal 211
firewall rules
  default 109-110
  for FTP servers 98
  processing order 108-109
  removing 119
  for Web servers 98
firewall. *See* Norton Personal Firewall
firewalls, using LiveUpdate 83
firewalls, Windows XP 29
Flash blocking, enabling and disabling 166
floppy disk scans 127
floppy drives, unable to boot from 210
folder scans 127
FTP
  applications 186
  servers 98
full system scans 127

G

games 186
glossary 75, 237

H

hackers 223-226
hard drive scans 127
Help 75-76
  accessing 50
  context-sensitive 76
  dialog box 76
  menu 75
Home Networking 91-93
  accessing from Security Monitor 54
  configuration 39
  zones 91-93

I

ICMP (Internet Control Message Protocol) 110, 218
icon in notification area 49
IGMP (Internet Group Membership Protocol) 218
infected files
  cannot repair 212
  emergency recovery procedures 17
  reinfected 211
Inoculation
  alerts 138
  options 68
  responding to alerts 138

instant messenger 186
  and Privacy Control 157
  options 67
  protecting private information 157
  scanning transferred files 125
  support and options 22
  supported clients 29
Internet
  overview 215-222
  risks 223-231
Internet Access Statistics
  contents 194
  resetting 193
Internet Control Message Protocol (ICMP) 110, 218
Internet Group Membership Protocol (IGMP) 218
Internet options 67
Internet-enabled applications 112
Intrusion Detection 101-122
  about 24, 103-104
  configuring 120
  enabling and disabling 104
Intrusion Detection service 82
IP addresses 93, 219
  and subnet mask pair 222
  finding 93

J

Java applets 205, 226
JavaScripts 25

L

LiveUpdate
  accessing 50
  accessing from Security Monitor 54
  options 61
  troubleshooting 208
LiveUpdate options 67
localhost 109, 220
Log Viewer
  changing log sizes 200
  clearing events 199-200
  contents 196-198
  disabling 199
  exporting information from 201-202
  printing 201-202
  refreshing 199
  using 198
logs
  accessing from Security Monitor 54
  adjusting the Alerting Level 55
  changing size 200
  clearing events 199-200
  contents 196-198
  disabling 199
  exporting information from 201-202
  Norton Internet Security 191-202
  printing 201-202
  refreshing 199
  viewing 198
loopback connections 109

M

Microsoft Outlook Express, creating spam filters 173
Microsoft Outlook, creating spam filters 174
Miscellaneous options 68
multiple schedules for a scan 131

N

NetBIOS 109
  making name visible 207
Netscape Messenger, creating spam filters 175
network troubleshooting 207
networks, using LiveUpdate 83
new features
  Norton AntiVirus 22
  Norton Internet Security 21
newsgroups
  exceptions 190
  names 188-189
  readers 186

newsletters 80
Norton AntiVirus
  about 24
  accessing from Windows Explorer 51
  Auto-Protect 25
  Bloodhound technology 25
  new features 22
  Script Blocking 25
Norton Internet Security
  accessing 52
  Block Traffic 60
  checking Status & Settings 192
  creating accounts 146-150
  disabling 71
  Email options 64
  emergency recovery procedures 17
  Firewall options 62
  General options 61
  LiveUpdate options 61
  logging on 153
  logs and statistics 191-202
  monitoring 191-202
  new features 21
  Security Monitor 53-54
  Spam Alert 171-177
  troubleshooting 204-208
  Visual Tracking 58-59
  Web Content options 63-64
  wireless connections 89
Norton Personal Firewall
  about 102
  customizing 108
  enabling and disabling 104
  security settings 105-119
  troubleshooting rules 205
Norton SystemWorks, installing with 45
notification area icon 49

O

Office Plug-in
  enabling 68
online Help 75
online tutorials 79
online Virus Encyclopedia 79, 143
operating systems 27
  multiple 209
Options
  accessing 61
  Auto-Protect 66
    Advanced 66
    Bloodhound 66
    Exclusions 66
  email
    Advanced 67
    scanning 67
  Inoculation 68
  instant messenger 67
  Internet 67
  LiveUpdate 61, 67
  Manual Scan 66
    Bloodhound 66
    Exclusions 66
  Miscellaneous 68
  Norton Internet Security
    Email 64
    Firewall 62
    General 61
    LiveUpdate 61
    Web Content 63-64
  Other 68
  protecting with password 43, 69
  resetting password 70
  Script Blocking 66
  settings categories 65
  Spam Alert 176-177
Other options 68

P

packets 101
Parental Control
  about 24
  configuration 44
  creating accounts 146-150
  Wizard 146-149
passwords
  changing 150
  options 43
  setting 150
ping scans 224

Popup Window Blocking, enabling and disabling 166
pop-up windows, blocking 163-170, 205
pornography 227
ports 220-222
- scans 225
- well-known 221

ports, scanning 102
printers, sharing 90
Privacy Control 155-161
- and SSL 156
- configuration 42
- in instant messengers 157

privacy risks 228-229
Private Information, options 159
Prodigy Internet connection 84
product serial number 38
Program Control
- Automatic 110
- configuring 40
- manually adding programs 112
- scanning for programs 111
- settings 113

Program Scan
- accessing 54
- configuring 111
- running 111

programs
- configuring with Program Scan 111
- creating firewall rules 114
- manually adding to Program Control 112
- manually configuring Internet access 114

programs, accessing the Internet. *See* Internet-enabled programs
protection updates
- described 82
- downloading from Symantec Web site 84

protection, updating 86
proxy servers 96

Q

Quarantine
- files in 138
- infected files in 135
- options 139
- options during uninstall 46
- responding to virus threats 18

R

Readme file 76
registering your software 38
removable drive scans 127
removing
- Norton AntiVirus 46
- Norton Internet Security 46
- other antivirus programs 29
- previous copies of Norton Internet Security 29

Repair Wizard 134
repairing infected files
- in Windows 2000/XP 136
- in Windows 98/98SE/Me 135

required computer configuration 27
Rescue Disks 73-75
- absent 209
- creating 73
- defined 73
- failure to start from 209
- testing 74
- updating 74
- using 141

restoring boot record and system files 141
risks
- from active content 226
- from Trojan horses 230
- from viruses 230
- from zombie programs 103
- from hackers 223-226
- from inappropriate content 227
- to privacy 228-229

running custom scans 129

S

safe mode 210
scan summary 134
scanning
  automatic 130
  entire computer 127
  files at startup 68
  for Internet-enabled applications 110
  from a boot disk 141
  individual elements 127
  port 102, 225
scheduling
  custom scans 130
  virus scans 130
Script Blocking 25
  monitoring by 125
  options 66
  virus found by 137
secure Web connections, disabling and enabling 161
security
  attacks 101-122, 224-226, 231
  levels 105-119
Security Assistant 39-45
  Home Networking pane 39
  Parental Control pane 44
  Password Protection pane 43
  Privacy Control pane 42
  Program Control pane 40
  using after installation 38
Security Check 58
Security Level
  changing 105
  changing individual settings 106
  resetting 108
Security Monitor 53-54
Security Response Web page 79
serial number 38
Service and Support 233
setting options 65
settings
  Norton Internet Security 60
  Norton Personal Firewall 105-119
  Program Control 113
settings categories 65
setup program, changing boot drive sequence 210
sockets 220
Spam Alert 171-177
  about 171
  add new entry 176
  and SSL 172
  creating filters 173-175
    Eudora 175
    Microsoft Outlook 174
    Microsoft Outlook Express 173
    Netscape Messenger 175
  customize 176-177
  enable and disable 172
  modify entry 177
  tips 177
spam. *See* Spam Alert
SSL (Secure Sockets Layer)
  and Privacy Control 156
  and Spam Alert 172
starting
  Norton AntiVirus from the CD-ROM drive 142
  your computer from a floppy disk 141
startup
  Auto-Protect failure to load 211
  changing floppy disk drive settings 210
  floppy disk drive fails 210
  Rescue Disks absent 209
  Rescue Disks fail 209
  scanning files at 68
statistics 194-196
  detailed 194
  exporting information from 201-202
  Norton Internet Security 191-202
  printing 201-202
  resetting 193
  resetting detailed statistics counters 195
  viewing 192
statistics window 192
Status & Settings, checking 192
stealth ports 225
submitting
  files to Symantec 140
  Web sites to Symantec 185
subnet masks 95, 222

subscriptions 82
Symantec Security Response newsletter 80
Symantec service and support Web site 203
Symantec Web site 78, 143
  downloading product updates 84
system
  requirements 27
  tray icon 49

T

TCP/IP 217-218
Technical Support 233
Technical Support Web site 78
testing Rescue Disks 74
threats
  security 18
  viruses 18
Trashcan. *See* Ad Trashcan
Trojan horse programs 102, 110, 230
troubleshooting 203-214
  ActiveX and Java 205
  Ad Blocking 205
  browser information 208
  cable modem connections 207
  Cookie Blocking 205
  firewall rules 205
  Internet applications 206
  Internet connections 206
  LiveUpdate 208
  networks 207
  Norton Internet Security 204-208
  printing 207
  Web sites 204-205
tutorials 79

U

UDP (User Datagram Protocol) 218
Uniform Resource Locator (URL) 94, 220, 222
uninstalling
  Norton AntiVirus 46
  Norton Internet Security 46
  other antivirus programs 29
  previous copies of Norton Internet Security 29
  with files in Quarantine 46
updating
  from Symantec Web site 84
  Rescue Disks 74
  virus protection 84
URL (Uniform Resource Locator) 94, 220, 222
User Datagram Protocol (UDP) 218
User's Guide PDF 77
  opening 78

V

virtual private network (VPN) 99
virus
  definitions 25
    service 25
  descriptions 25
  emergency recovery procedures 17
  responding to threats 18
  risks 230
virus alert options 135
virus definitions, alternate sources 84
virus encyclopedia 79
Virus List 143
virus protection
  alerts 68
  system scans 127
virus repair
  in Windows 2000/XP 136
  in Windows 98/98SE/Me 135
viruses
  found by Auto-Protect 135
  found during a scan 134
  looking up in Norton AntiVirus Professonal Edition 143
  submitting to Symantec 140
  viewing descriptions 143
Visual Basic scripts 25

Visual Tracking 58-59
trace attack
from AutoBlock 59
from Log Viewer 59
from Statistics 59
VPN (virtual private network) 99

W

Web
servers 98
sites
blocking 181-185
submitting to Symantec 185
Web filtering service 82
Web sites
Symantec 84
troubleshooting 204-205
Windows
Explorer menu 51
operating systems 27
safe mode 210
tray icon 72
wireless connections, protecting 89
Wizard
Home Networking 39
Parental Control 146-149
Registration 36-38
Worm Blocking
introducing 22
monitoring by 125
options 67
threats found by 137
worms 230

Z

zombie programs 103, 230
zones 91-93
adding computers to 91, 92
Restricted 91, 122
Trusted 91, 104

Norton Internet Security™ 2003

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE. You must be a registered customer in order to receive CD replacements.

If your Symantec product was installed on your computer when you purchased it, contact your hardware manufacturer for CD replacement information.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name ____

Company Name ______________________________________

Street Address (No P.O. Boxes, Please) ______________________

City ______________________ State _______ Zip/Postal Code ___________

Country* ____________________ Daytime Phone ____________________

Software Purchase Date ________________________________

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem: ____________________________

CD Replacement Price	$ 10.00
Sales Tax (See Table)	
Shipping & Handling	$ 9.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%).
Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _________ __ Visa __ Mastercard __ AMEX

Credit Card Number ______________________________ Expires _________

Name on Card (please print) ____________________ Signature ____________________

**U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.

symantec™