

Norton Internet Security User's Guide

NORTON

Internet Security[™]2000

Norton Internet Security 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.

Copyright Notice

Copyright © 1995-1999 Symantec Corporation. All Rights Reserved.

Norton Internet Security

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

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Norton, Norton Internet Security, Norton SystemWorks, Emergency Disk, LiveUpdate, Norton AntiVirus, Norton Utilities, and Rescue Disk are trademarks of Symantec Corporation.

Windows is a registered trademark of Microsoft Corporation. Iomega is a registered trademark and Zip, Zip Rescue are trademarks of Iomega Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Prodigy Internet is a trademark of Prodigy. Pentium is a registered trademark of Intel Corporation. Other product names mentioned in this manual may be trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

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

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

- (i) use only one copy of one version of the various versions of the Software contained on the enclosed media on a single computer, or if only one version is contained on the enclosed media use one copy of such version on a single computer;
- (ii) 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;
- (iii) 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;
- (iv) 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 agreement; and
- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

YOU MAY NOT:

- (i) copy the documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

SIXTY DAY MONEY BACK GUARANTEE:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or

an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

LIMITED WARRANTY:

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

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

DISCLAIMER OF DAMAGES:

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

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. THE DISCLAIMERS AND LIMITATIONS SET FORTH ABOVE WILL APPLY REGARDLESS OF WHETHER YOU ACCEPT THE SOFTWARE.

U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

GENERAL:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 10201 Torre Avenue, Cupertino, CA 95014.

C O N T E N T S

Chapter 1 Getting Started

What does Norton Internet Security do?	10
Installing Norton Internet Security	11
System requirements	11
Installation procedure	11
What happens when you install Norton Internet Security?	13
Starting Norton Internet Security	14
Updating Norton Internet Security	15
What does the subscription contain?	16
Reviewing the event log	16
Reviewing statistics	17
Submitting Web sites to Symantec	17

Chapter 2 Planning your security strategy

How does your family use the Internet?	19
Creating a family Internet usage policy	19
Planning user accounts	20
What kinds of user accounts do you need?	20
If you are the only user	20
If more than one adult uses the computer	21
If children use the computer	21
If several children use one account	21
If children and teenagers use the computer	22
Setting up user accounts	23
Account types and templates	23
Creating user accounts	24
Setting the startup account	25
Removing user accounts	26
Switching accounts	26
Logging off	27
Changing account settings	28

Chapter 3 Personalizing Norton Internet Security

Customizing security features	30
Customizing the Personal Firewall	31
Using the Firewall Rule Assistant	31
Creating firewall rules automatically	33
Setting Java and ActiveX security levels	34

Using the Java/ActiveX Assistant	35
Safeguarding your privacy	37
Blocking confidential information	38
Tips on blocking confidential information	40
Blocking cookies	41
Using the Cookie Assistant	41
Blocking browser information	42
Enabling or disabling secure Web connections	43
Setting up parental controls	43
Restricting access to Web sites	44
Creating a list of permitted Web sites	45
Blocking accounts from visiting sites	46
Blocking applications from accessing the Internet	47
Categorizing programs	47
Blocking ads	48

Chapter 4 Troubleshooting

Frequently Asked Questions	51
How do I turn off Norton Internet Security?	51
Why can't I post information online?	53
What is wrong with this Web site?	53
Why doesn't FTP work on older browsers?	55
Why won't a program connect to the Internet?	55
How can I close an Internet connection while online?	56
How can a Web site get my browser information?	56
What are inbound and outbound connections?	56
Where can I get more information?	56
Questions about home networking	57
How does the firewall work with Internet connection sharing?	57
How does the firewall work with file and printer sharing?	57
How do I use Norton Internet Security with a proxy server?	59
Questions about the firewall	60
Why doesn't the Firewall Rule Assistant appear?	60
How do I review or change firewall rules?	61
If two firewall rules cover the same issue, which one runs?	62
What is the purpose of the default firewall rules?	63
If I delete the default firewall rules, can I get them back?	63
Can I create firewall settings for specific Web sites?	63

Chapter 5 Norton AntiVirus Emergency Procedures

What to do if a virus is found	65
Quick guide to alert actions	65

Types of virus alerts	66
Virus Found	66
Virus in Memory	66
Virus-Like Activity	67
What to do if Norton AntiVirus cannot repair	68
Infected files	68
Hard disk master boot record or boot record	69
Floppy disk boot record	69
System file	69
Using Rescue Disks in virus emergencies	69



C H A P T E R

1

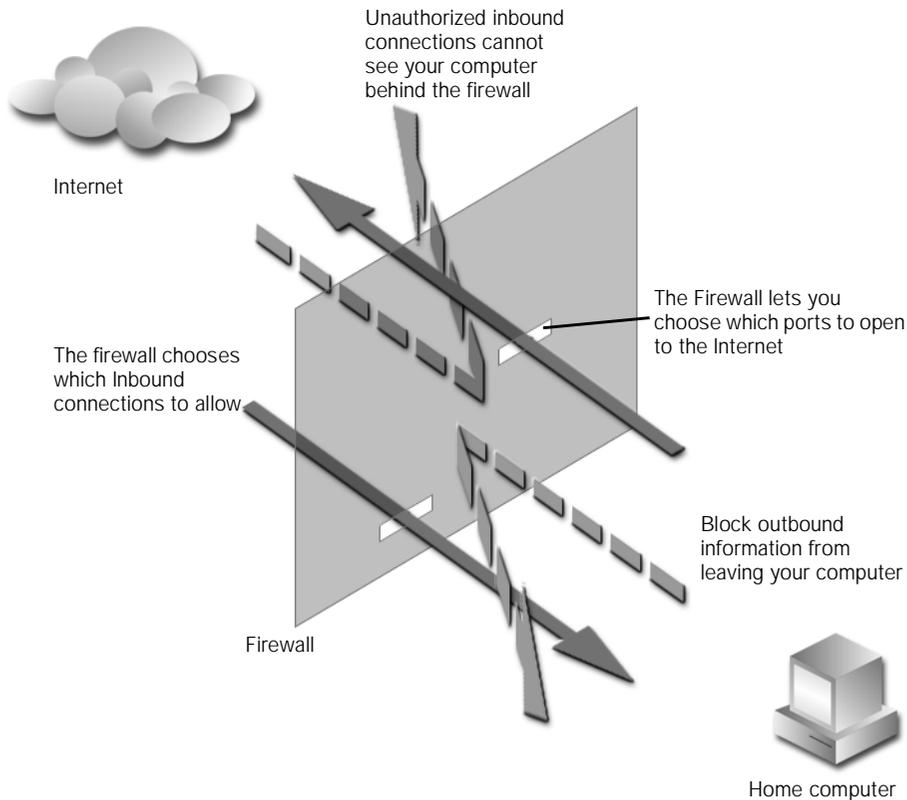
Getting Started

Millions of computers are connected to the Internet, and the number increases daily. When you connect to the Internet, you can connect with millions of other computers and those computers can connect with your computer. Unprotected connections to the Internet can leave your computer open to hacker attacks, viruses, trojans, offensive Web sites, and many other Internet threats.

Norton Internet Security can help you track everything that happens on your computer. It monitors the Internet to give you peace of mind when you are online. It helps protect your security, privacy, and is a tool for people who want to control the types of information they receive on the Internet.

What does Norton Internet Security do?

Norton Internet Security provides a barrier called a *firewall* between your computer and the Internet. Firewall programs are filters that block or allow connections and data transmissions in both directions.



The firewall uses rules to determine whether to permit or block future connections automatically. Supervisor account users can change these rules, allowing or blocking programs from having Internet Access. See [“Account types and templates”](#) on page 23.

When Norton Internet Security detects connections for which there are no firewall rules, it creates rules automatically for programs it recognizes, lets you permit or block the communication, or lets you create a new rule to permit or block the connection permanently.

Norton Internet Security uses the personal firewall to protect your data and preserve your privacy:

- It prevents ActiveX and Java programs from running without your knowledge, and lets you specify sites where these programs are okay to run.
- It prevents confidential information from being entered on non-secured Web sites.
- It can block someone from accessing secure sites where they may be asked for personal information.
- It can block cookies and other information your browser normally reports to Web sites like email addresses and the last Web site you visited.

Parents can control which Web sites their children see. Parents can also decide which types of programs their children use to access the Internet, effectively blocking Internet access in chat software or other potentially harmful products.

Installing Norton Internet Security

System requirements

To use Norton Internet Security, your computer must meet the following minimum requirements:

- Pentium class or higher processor
- Windows 95, Windows 98, Windows 98 SE
- 24 MB of RAM required (32 MB recommended)
- 60 MB free disk space
- CD-ROM drive
- Microsoft Windows Internet support

Installation procedure

The installation program lets you install Norton AntiVirus or Norton Internet Security. If you do not already have Norton AntiVirus on your computer, install it first to help ensure that you have a clean system before installing Norton Internet Security.

To install Norton AntiVirus and Norton Internet Security:

- 1 Start Windows (if it is not already running).
- 2 Insert the Norton Internet Security CD into the CD-ROM drive.
- 3 Click Install Norton AntiVirus and follow the instructions.
- 4 When you are finished installing Norton AntiVirus, follow the same procedure to install Norton Internet Security.

If the opening window does not appear:

- 1 Double-click the My Computer icon.
- 2 Double-click the icon for your CD-ROM drive.
- 3 Double-click cdstart.exe.

What happens when you install Norton Internet Security?

After installing Norton Internet Security and restarting your computer, the main status window appears. It appears whenever you open Norton Internet Security, and shows a quick overview of the program.

The screenshot shows the Norton Internet Security 2000 main status window. The window title is "Norton Internet Security". The interface includes a top menu bar with "Live Update", "Live Advisor", "Options", and "Help". A left sidebar contains navigation buttons for "Status", "Security", "Privacy", "Parental Control", "Ad Blocking", and "Accounts". The main content area displays the status: "Norton Internet Security is enabled and protecting your system." Below this, there are four rows of security features with their respective counts: Security (4 threats, 15146 scans), Privacy (139 threats, 221 scans), Parental Control (0 threats, 204 scans), and Ad Blocking (0 threats). A "Security Alert!" banner is visible at the bottom left, and a subscription notice at the bottom right states "Subscription content expires in 5 days".

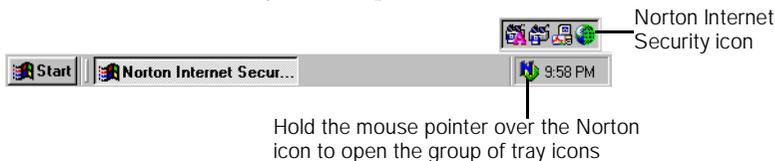
Callouts and their descriptions:

- Update Norton Internet Security:** Points to the "Live Update" button in the top menu bar.
- Get information on virus and security threats directly from Symantec:** Points to the "Live Advisor" button in the top menu bar.
- Supervisor accounts can change the options, view logs and reports:** Points to the "Options" button in the top menu bar.
- Click Tell Me More for information on any window in Norton Internet Security reports:** Points to the "Tell me more" link in the status area.
- Supervisor account users can change the settings for any account:** Points to the "Accounts" button in the left sidebar.
- Change Norton Internet Security settings:** Points to the "Security", "Privacy", and "Parental Control" buttons in the left sidebar.
- Set up new users:** Points to the "Accounts" button in the left sidebar.
- Open Norton AntiVirus to run a virus check or review its status:** Points to the "Security" button in the left sidebar.
- Click the numbers to see more details:** Points to the threat and scan counts in the Security, Privacy, and Parental Control rows.
- The subscription area shows how much time you have remaining on your current subscription:** Points to the "Subscription content expires in 5 days" notice.

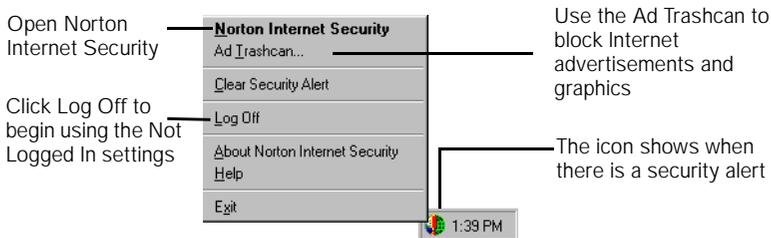
Installing Norton Internet Security adds the Norton Internet Security Icon to your Windows Start Menu, desktop, and the system area of the taskbar.



If you are running Norton SystemWorks 3.0 or later, or Norton AntiVirus 2000 or later, the Norton Internet Security icon may be integrated with the other Norton Icons on your computer.



The Norton Internet Security tray icon has several functions. Double-click the icon to open Norton Internet Security. Right-click the icon to open the tray menu.



Now you are ready to set up Norton Internet Security to protect your system.

Starting Norton Internet Security

To open Norton Internet Security:

- Double-click the Norton Internet Security icon in the system tray.



Norton Internet Security appears, showing the Status window.

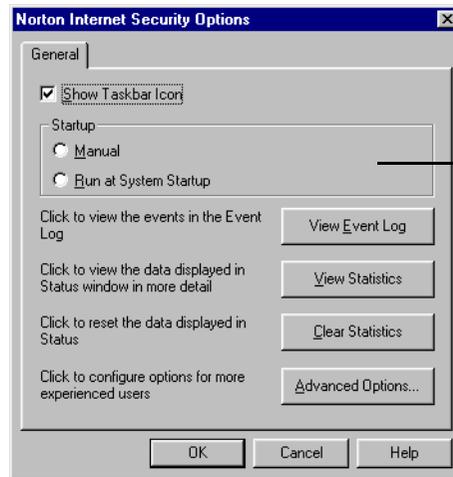
There are three startup options for running Norton Internet Security:

- Do not start protecting your system until you run Norton Internet Security manually.
- Start automatically when the computer is turned on. Norton Internet Security is always running unless you disable or exit it.

When Norton Internet Security begins automatically, it runs in the background. It does not display the main program unless you open Norton Internet Security manually.

To set Norton Internet Security startup options:

- 1 Open Norton Internet Security.
- 2 Click Options.



The startup options let you determine when Norton Internet Security will protect your system

- 3 In the Norton Internet Security Options dialog box, click a Startup option.

Updating Norton Internet Security

Norton Internet Security depends on current information to protect your system from new security threats. Update Norton Internet Security weekly to keep your system secure with the latest information from Symantec.

LiveUpdate has two functions:

- It provides free updates to fix defects and provide additional features in the Norton Internet Security program.
- It provides information updates as a subscription. Installing Norton Internet Security activates your full-year subscription.

To update your system:

- 1 Open Norton Internet Security.

- 2 Click LiveUpdate.
- 3 Follow the instructions.

What does the subscription contain?

The subscription provides Norton Internet Security with the latest security information to keep your system safe:

- Current lists of Web site addresses and pre-defined Web site categories.
- Pre-made firewall rules that protect against trojan programs like Back Orifice and others.
- Lists of the latest applications that use the Internet. These lists make it possible for Norton Internet Security to automatically create firewall rules when you use Internet applications. See [“Creating firewall rules automatically”](#) on page 33.

You do not need to register the product to begin using the subscription. When it is time to renew the subscription, click LiveUpdate for renewal instructions.

Reviewing the event log

The event log contains information about everything that happens with Norton Internet Security:

- Content Blocking contains information about blocked ads and images.
- Connections lists a history of the TCP/IP network connections made on your PC.
- Firewall events include alerts, intercepted network communications, firewall rules that were processed or created, and other network summaries.
- Cookie information details the sites that request the cookies and whether they were permitted or blocked.
- Applications shows which programs attempted to connect to the Internet, and whether they were permitted or blocked.
- Web History shows the Web addresses your computer has visited.

For more specific information about the Event Log, click any item and press the F1 key to see Help.

To review the Event Log:

- 1 Open Norton Internet Security.
- 2 Make sure you are logged in as the supervisor.
See “Switching accounts” on page 26.
- 3 Click Options.
- 4 Click View Event Log.

Reviewing statistics

The statistics window shows several sets of statistics about your computer:

- Network information, including the number of bytes that have been permitted or sent
- The number of blocked advertisements and graphics
- Web information, including the number of times cookies and browser information was blocked
- Firewall rules, including the number of times they permitted or blocked information
- Firewall and network connections

To open the statistics window:

- 1 Open Norton Internet Security.
- 2 Click Options.
- 3 Click View Statistics to see the statistics window.

Submitting Web sites to Symantec

You can help change Norton Internet Security’s list of Web sites. For example, you might find a Web site that should be added to Norton Internet Security’s list. Perhaps a Web site is being blocked under a certain category, and you think it should belong under other categories as well. Maybe you have a Web site that you think should be removed from the list.

To submit changes to Norton Internet Security’s list, browse to <http://www.symantec.com/avcenter/cgi-bin/nisurl.cgi>

Planning your security strategy

The first step after installing Norton Internet Security on your computer is to plan how you will use it. The questions in this chapter should help you plan your strategy for securing your computer when it is online.

How does your family use the Internet?

While the Internet provides unprecedented opportunities to bring information into the home, it also contains a lot of information that can be inappropriate for children or other family members. Norton Internet Security monitors the Internet to give you peace of mind when you are online.

Creating a family Internet usage policy

The most effective way to keep inappropriate or offensive Web information from entering your home is to set up a family internet policy. Make an agreement that details how your family uses the Internet in your home.

Norton Internet Security helps you enforce the decisions your family makes about how they use the Internet:

- Add your own sites to the list of sites to be blocked.
- Categorize Web sites, and choose which accounts can access each category. Teenagers can easily have different permissions than younger children.
- Limit the personal information that can be posted on Web sites from your computer.

For more information, see “Setting up user accounts” on page 11.

Planning user accounts

Norton Internet Security accounts let you create different security settings for different users.

The installation process creates two initial accounts in Norton Internet Security:

- The supervisor account is the default account that you created during the installation procedure. With the supervisor account, you can change any of the settings in Norton Internet Security, and use it to create additional accounts.
- Not Logged In is a restricted account. When no other account is active, Norton Internet Security uses the settings in this account. When this account is active, users cannot change any of the Norton Internet Security settings.

Norton Internet Security lets you create additional accounts if you need them. Each account requires some maintenance, depending on how your family uses the Internet.

What kinds of user accounts do you need?

Here are some questions that should help you decide whether you need to create more accounts:

- How many people use this computer?
- Classify the people into groups:
 - How many children?
 - How many teenagers?
 - How many adults?

Accounts for children and teenagers are usually restricted so that they cannot change any Norton Internet Security settings. Accounts for adults are either normal accounts or supervisor accounts.

If you are the only user

You do not need any additional accounts. The supervisor account you created during the installation process is already set as the default account, and is active whenever you use Norton Internet Security. See [“Personalizing Norton Internet Security”](#) on page 29 to learn about customizing the Security and Privacy settings.

If more than one adult uses the computer

Determine how other adults will use Norton Internet Security. Maybe they need a separate account for their own settings; or perhaps they will never use Norton Internet Security, and can use the default settings.

If the other adults want to change their own settings and take care of their own security needs, you should create a separate account for them. If they need to create accounts or change settings for other accounts, they must use a supervisor account. See [“Setting up user accounts”](#) on page 23.

If the other adults never use Norton Internet Security, make sure that the settings for the default account are sufficient for them. Or, create an account for them based on Adult settings, and teach them how to log in. See [“Switching accounts”](#) on page 26.

If children use the computer

You can use the two accounts that were created during installation:

- You use the supervisor account.
- Use the Not Logged In account for the children.

Norton Internet Security protects children from the dangers on the Internet, and gives parents control over the Web sites that children can visit. You can set up Norton Internet Security so that whenever someone turns on the computer, the children’s settings take effect. Then, when the parents want to use the computer, they can log into Norton Internet Security under a less restricting account.

If several children use one account

If you have several children, and want them all to use the same security settings, they can share the same account.

What to do:

- 1 Change the supervisor account settings as desired. See [“Changing account settings”](#) on page 28.
- 2 Make the Not Logged In account be the default account. See [“Setting the startup account”](#) on page 25.
- 3 Change the settings for the Not Logged In account to protect children. See [“Changing account settings”](#) on page 28.

If children and teenagers use the computer

If you want to give different access privileges to different groups of children, you need to use separate accounts for each group.

What to do:

- 1 Change the supervisor account for your own settings. See [“Changing account settings”](#) on page 28.
- 2 Make the Not Logged In account be the default account. See [“Setting the startup account”](#) on page 25.
- 3 Change the settings for the Not Logged In account to protect children. See [“Changing account settings”](#) on page 28.
- 4 Create another account for the older children or teenagers.
Teach them how to log into their account. See [“Switching accounts”](#) on page 26.

If you want to ensure that the smaller children do not get access to the Internet using the older children’s account, make sure that the older children log off Norton Internet Security when they are finished.

Setting up user accounts

Use the Accounts window to manage your Norton Internet Security accounts.

This area shows which account is logged in

The accounts area shows all the accounts you have set up for Norton Internet Security

Click Accounts to open the Accounts window

This area shows which account is designated as the startup account

Click Tell Me More for additional information about using this window

Name	Type
Not Logged In	Restricted
Parent	Supervisor (Startup Account)

Account types and templates

The way that you use accounts depends on how you use the Internet on your computer. Norton Internet Security uses three different types of accounts to control access to the program:

- Supervisor account users can add, change, or delete other accounts. They can change any setting in Norton Internet Security. Only supervisor accounts can create permanent rules for which programs can access the Internet.
- Normal account users can change their own Norton Internet Security settings, but they cannot change the settings for other accounts. When the firewall detects new programs trying to connect to the Internet, normal account users can block or permit Internet connections, but they cannot create permanent firewall rules.

- Restricted account users cannot change any settings in Norton Internet Security.

When you create an account, the account type is based on the template you use.

Base Account On	Account Type	Description
Child	Restricted	Turns on Parental Control, blocking most Web sites and programs that connect to the Internet.
Teenager	Restricted	Turns on Parental Control, and blocks a smaller number of Web site and Internet-enabled programs than the Child template.
Adult	Normal	Turns off Parental Controls. Normal account users can change their own security settings.
Supervisor	Supervisor	Turns off Parental Controls. Supervisors can change settings to any account.

Templates provide a way to create an account with basic settings without having to change everything yourself. The only time you can apply a template to an account is when you create the account. However, you can change the account type at any time.

To change the account type:

- 1 Open Norton Internet Security.
- 2 Make sure you are logged in using a supervisor account.
See [“Switching accounts”](#) on page 26.
- 3 Click Accounts.

Creating user accounts

Only supervisor account users can create additional accounts.

To add a user account:

- 1 Open Norton Internet Security.
- 2 Make sure you are logged in as a supervisor.
See [“Switching accounts”](#) on page 26.

- 3 Click Accounts.
- 4 Click Add.

Clicking an account type changes the settings throughout Norton Internet Security

Give the account a name that describes how the account will be used

Protecting the account with a password can help prevent others from using the account

- 5 In the Create Account dialog box, enter the name of the new account.
- 6 Enter a password if needed.
If you are creating an account that you do not want others to use, password protect it. Passwords might not be necessary for small children's or startup accounts.
- 7 Choose a template from the Base Account On box. Templates pre-set the settings throughout Norton Internet Security.

Setting the startup account

The startup account is used whenever Norton Internet Security begins protecting your system.

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 open Norton Internet Security and change to a different account. For more information, see ["Switching accounts"](#) on page 26.

To set an account as the startup account:

- 1 Open Norton Internet Security.
- 2 Click Accounts.
- 3 Click the user account to be designated as the startup account.

- 4 Click Properties to open the Account Properties dialog box for that account.



- 5 Check Make This The Startup Account.

Removing user accounts

You can remove an account if it is not needed any longer.

To remove a user account:

- 1 Open Norton Internet Security.
- 2 Click Administration.
- 3 Click the account to delete.
- 4 Click Delete.

Switching accounts

When you start using Norton Internet Security, it uses the settings from the startup account. See [“Setting the startup account”](#) on page 25.

To use a different account, you have to log off of the current account and log into another account.

To find out which account you are currently using:

- 1 Open Norton Internet Security.

The Status window shows which account is logged in.



To log to another account:

- 1 Open Norton Internet Security.
- 2 Click Accounts.
- 3 If you are currently logged on, you must log off. See [“Logging off”](#) on page 27.
- 4 Click Log In.
- 5 In the Log In dialog box, click the account you want to use and enter the password if required.

As soon as you change the account, Norton Internet Security begins using the settings associated with that account. The Accounts window shows which account is currently active.

Logging off

When you log off, you begin using the settings for Not Logged In. If you want to completely exit Norton Internet Security, see [“Exiting Norton Internet Security”](#) on page 52.

To log off of Norton Internet Security:

- 1 Open Norton Internet Security.
- 2 Click Accounts.
- 3 Click Log Off.

Changing account settings

Now you can begin customizing Norton Internet Security to fit your needs. Customize the startup account first.

To change settings for the supervisor account:

- 1 Open Norton Internet Security.
- 2 Check to see who the Current Account is in the status window.
If the current account is the supervisor, you can begin personalizing Norton Internet Security for the supervisor account. If not, log off and log on again using your supervisor account. See [“Switching accounts”](#) on page 26.
- 3 Go through the settings for Security, Privacy, Parental Control, and Ad Blocking to personalize Norton Internet Security.

To change settings for another account:

- 1 Open Norton Internet Security.
- 2 Make sure you are logged on using a supervisor account.
See [“Switching accounts”](#) on page 26.
- 3 Click Security, Privacy, Parental Control, or Ad Blocking.
- 4 Click the Settings For arrow and click the account you want to change.
The settings in the current window appear for the selected account.



- 5 Change the settings for that account.

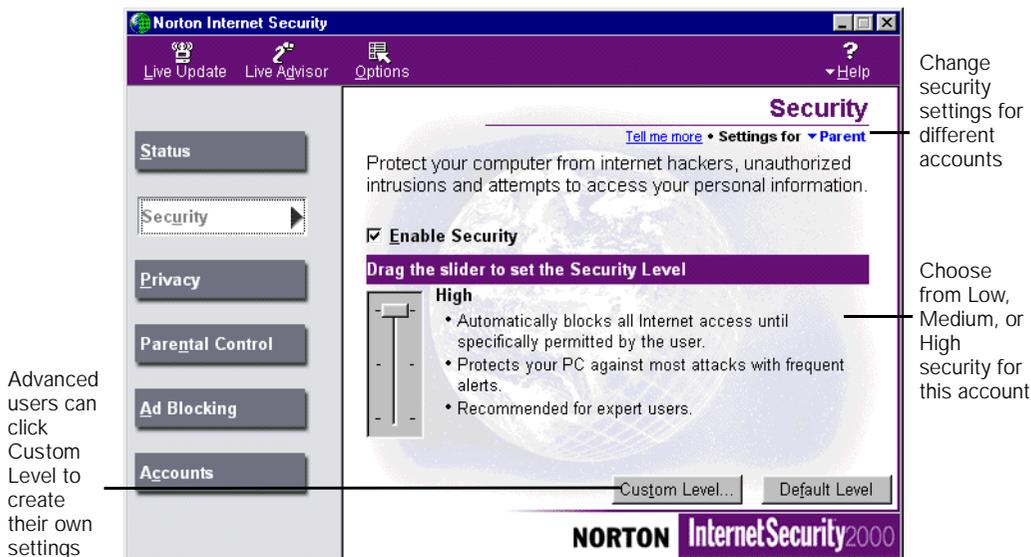
Personalizing Norton Internet Security

With Norton Internet Security, your computer can be more secure than most other computers on the Internet. Norton Internet Security provides three vital security services for your computer:

- The Personal Firewall allows and blocks communications between your computer and the Internet. It uses rules to determine what to permit or block.
- Java Applet security allows or prevents Java Applets from running on your computer. Java applets can run on your computer without your knowledge. When you visit Web sites that use Java Applets, your browser automatically downloads and runs these programs.
- ActiveX is another technology that can run on your system when you visit Web sites that use them. ActiveX controls are more risky because they can have complete access to the data on your computer.

Customizing security features

You can set the security settings for an account by opening the Security window.



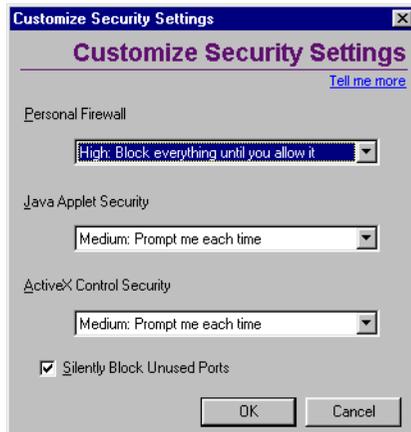
To open the Security settings window:

- 1 Open Norton Internet Security.
- 2 Click Security.

The slider allows you to select low, medium, or high security settings for the account. When you change the slider position, it changes the protection level.

The medium security level is the most commonly used because it provides a balance between security and convenience. The high setting provides much more security, but it takes more time to answer alerts and create firewall rules for the problems it catches. The low setting is the most convenient because it allows most communications to pass through without any alerts. However, it is also the least secure.

You can change the settings for the Firewall, Java and ActiveX protection levels by clicking Custom Level. This opens the Customize Security Settings dialog box.



Customizing the Personal Firewall

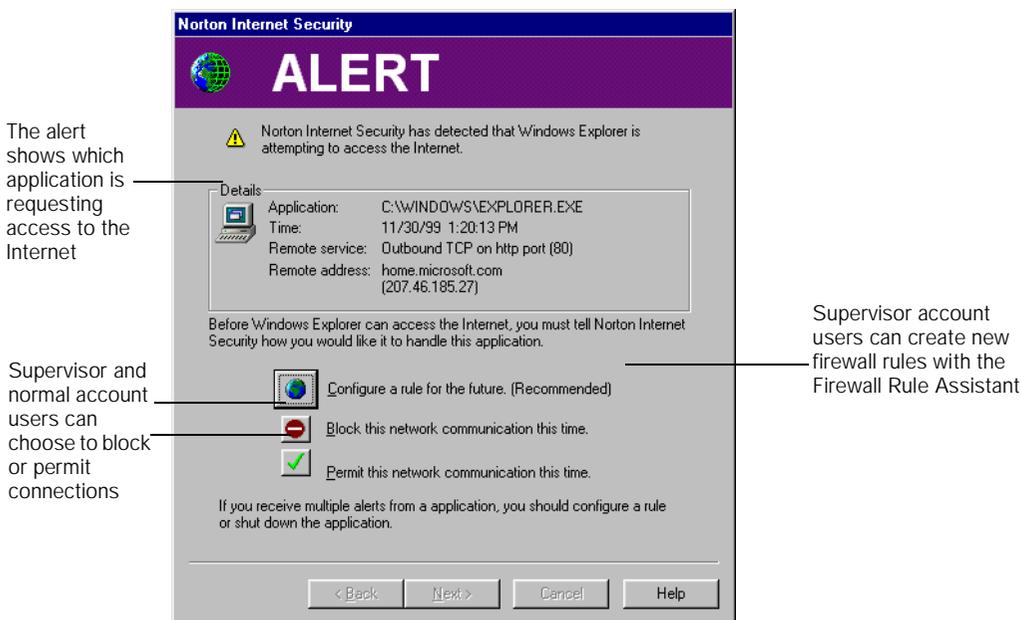
The Firewall has four settings: High, Medium, Low and None.

Firewall Settings	Description
High	Blocks all communication that you do not specifically allow. You must create firewall rules for every application that requests Internet access.
Medium	Blocks a large list of ports used by harmful programs. However, it can also block useful programs when they use the same ports.
Low	Blocks a small list of ports used by the most malicious trojan programs.
None	Allows all programs to make connections to the Internet.

Using the Firewall Rule Assistant

The Firewall Rule Assistant is a wizard that helps you set up your firewall. It steps you through the process of defining a rule for any type of communication that has not been covered by current firewall rules. Once a rule is in place, the firewall uses the rule to handle future communications automatically.

At first, the Firewall Rule Assistant appears frequently, alerting you each time you use an application that attempts to make a new type of network communication. The more permissive your rules, the fewer times the Rule Assistant prompts you to define an additional rule. After you set up rules for your most commonly used programs, the Rule Assistant appears less frequently.



The Firewall Rule Assistant helps you decide what to do about questionable connections:

- Create a rule for this connection in the firewall database. When there is a rule established for a certain connection, the firewall automatically follows that rule to allow or block the connection.
- Permit the connection this time, but bring up the Firewall Rule Assistant the next time the connection is requested.
- Block the connection this time, but bring up the Firewall Rule Assistant the next time the connection is requested.

The Firewall Assistant does not appear for restricted account users. If something attempts to pass through the firewall without a firewall rule, the firewall silently blocks the access. It does not give any warning message to the user.

When you click **Configure A Rule For The Future (Recommended)**, the **Firewall Rule Wizard** appears. It leads you through the steps of creating a firewall rule for the application that requested the connection. If you have problems understanding any of the questions or settings in the wizard, right-click the setting and click **What's This?** for additional information.

You can enable or disable the **Rule Assistant** for any account. By default it is enabled, and appears when it tries to block the access. The **Rule Assistant** is not available for restricted accounts.

To activate the Rule Assistant:

- 1 Open Norton Internet Security.
- 2 Click **Accounts**.
- 3 Click the account to modify.
- 4 Click **Properties**.



- 5 Click **Enable Personal Firewall Alerts** to add a check mark, enabling the **Firewall Rule Assistant** for this user.

To disable the Rule Assistant:

- Click **Enable Personal Firewall Alerts** to remove the check mark.

Creating firewall rules automatically

Part of the Norton Internet Security subscription includes updated lists of known, reliable programs that are supposed to communicate over the Internet. These programs include Web browsers, email programs, games, network utilities and many others.

When you use a program that Norton Internet Security recognizes, Norton Internet Security can automatically create a rule for it with the appropriate firewall settings. With this feature turned on, the Firewall Rule Assistant only appears when unknown programs attempt to access the Internet.

To keep your list of Internet-enabled applications current, use LiveUpdate regularly. See [“Updating Norton Internet Security”](#) on page 15.

To create firewall rules automatically:

- 1 Open Norton Internet Security and ensure that you are logged on using a supervisor account.
- 2 Click Options.
- 3 Click Advanced Options.
- 4 On the Other tab, click Enable Automatic Firewall Rule Creation so that it is checked.

Setting Java and ActiveX security levels

Programmers use Java Applets and Active X controls to make Web sites more interactive and exciting. Many Web sites rely on ActiveX controls and Java applets to perform and appear correctly. Most of these programs are safe and do not threaten your system or data.

However, ActiveX controls can have total access to your data, depending on how they are programmed. They could steal data from your hard disk and transmit it over the Internet while you are online. They could delete files, intercept messages, capture passwords, or even gather banking numbers and other important data.

The only way to prevent bad programs from running on your computer is to block them from downloading. However, blocking all Java Applets and ActiveX controls prevents many Web sites from appearing or running correctly.

In the Custom Level window for Security settings, the Java Applet Security and ActiveX Control Security features have three options: High, Medium, and Low.

Java Applet and ActiveX Control Settings	Description
High	Blocks your browser from downloading any Java Applets or ActiveX controls over the Internet. This is the safest, but most inconvenient option. Web sites that rely on these controls may not operate properly with this setting.
Medium	Activates the Java/ActiveX Assistant. This wizard lets you allow, block, or create a rule for every Java Applet or ActiveX Control that gets downloaded. It can be a lot of work to set up rules every time you come across a Java Applet or ActiveX Control, but it lets you decide which ones to run.
None	Lets any Java Applets or ActiveX controls run whenever you download them.

Using the Java/ActiveX Assistant

Norton Internet Security contains a Java/ActiveX Assistant that lets you set up rules for different sites. Now you can block the Java applets and ActiveX controls that you do not trust, and allow those that you trust.

The screenshot shows the 'Java/ActiveX Rule Assistant' dialog box. It has a title bar with a question mark and a close button. The main area contains the following information:

- Executable Type:** ActiveX Control
- Domain:** msn.com (selected with a radio button)
- Site:** www.msn.com
- For this and all future attempts:**
 - Always block ActiveX Controls from the domain or site.
 - Always permit ActiveX Controls from the domain or site.
- For just this attempt:**
 - Block this ActiveX Control.
 - Permit this ActiveX Control.

Annotations with arrows point to specific elements:

- 'Apply this decision to the entire domain, or a specific Web site' points to the radio buttons for 'Domain' and 'Site'.
- 'Normal users and supervisors can block or permit connections' points to the 'For just this attempt' section.
- 'Only supervisors have the option to create firewall rules' points to the 'Always block' option in the 'For this and all future attempts' section.

The bottom right corner of the dialog box shows the date and time: 11/30/99 12:32:27 PM.

If you have it turned on, the Java/ActiveX Assistant only appears when you visit a Web site that attempts to utilize one of these technologies.

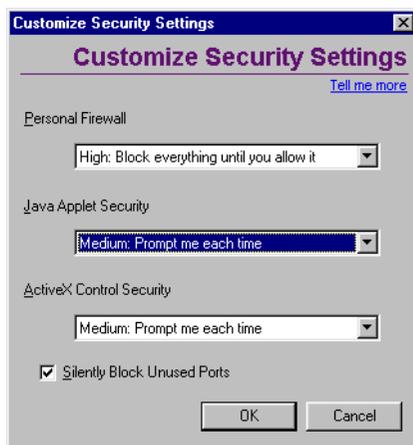
Do I want Domain or Site?

Domains can include several sites; they are much larger than sites. Blocking the code in a domain like domain.com includes all the Web sites under that domain like sales.domain.com and investor.domain.com as well as domain.com. It also includes the Web pages under each of these sites.

Blocking the code from a single site blocks all Web pages under that site. However, it does not restrict the code on other sites in the domain. For example, if you block the code found in domain.com, it does not block the code from sales.domain.com or investor.domain.com.

To turn on the Java or ActiveX Assistant:

- 1 Open Norton Internet Security.
- 2 Click Security to open the Security window.
- 3 If you are setting it up for another account, click the Settings For arrow and click the account.
- 4 Click Custom Level.



- 5 Under Java Applet Security, click Prompt Me Each Time.
- 6 Under ActiveX Control Security, click Prompt Me Each Time.

Note: If you are using the High security setting, the Java/ActiveX Assistant is already active for the account.

Safeguarding your privacy

A computer's security features might not always protect your identity and other personal information. Computers and Web sites collect a lot of personal information as you browse the Internet. Norton Internet Security helps protect your privacy by preventing these types of intrusions:

- Prevent confidential information from being entered into Web sites over non-secure connections.

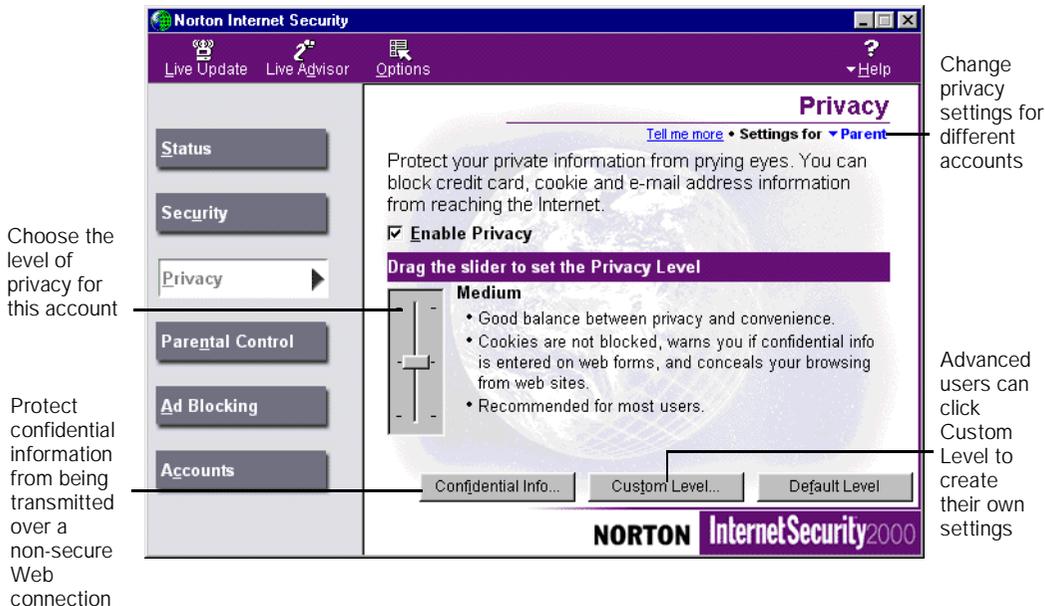
When you connect to a Web site over a secure connection, the browser encrypts the information and sends it to the Web site in a format that cannot be read. This prevents the firewall from blocking any information sent over secure connections.

- Block cookie responses when Web sites ask for them. See [“Blocking cookies”](#) on page 41.
- Stop your browser from publishing information to Web sites. See [“Blocking browser information”](#) on page 42.
- Disable secure connections so that children or other restricted account users do not use them to jeopardize your privacy.

To open the Privacy Settings window:

- 1 Open Norton Internet Security.

2 Click Privacy. The Privacy settings window appears.



The slider lets you select low, medium, or high privacy settings for the account.

Blocking confidential information

There are many Web sites that ask for personal information. Without thinking, someone could easily give away information that can jeopardize your privacy or allow others to steal from you.

If you are using Norton Internet Security User Accounts, there might be an account you want to restrict from ever entering personal information on a non-secure Web site. You could also restrict the account from using secure Web sites to ensure more privacy. See [“Enabling or disabling secure Web connections”](#) on page 43.

Norton Internet Security contains a personal information database. When you enter information into this database, it censors the information from all non-secure Web communications.

If you are concerned about entering personal information into the program, enter partial information instead. For example, instead of a complete credit card or identification number, enter a few consecutive

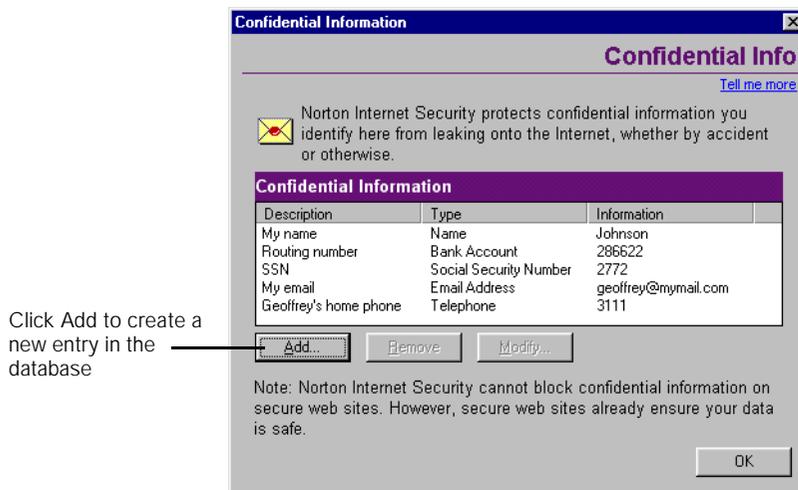
digits. Norton Internet Security will block the partial number, and prevent it from being transmitted to a Web site.

To block personal information from non-secure Web sites:

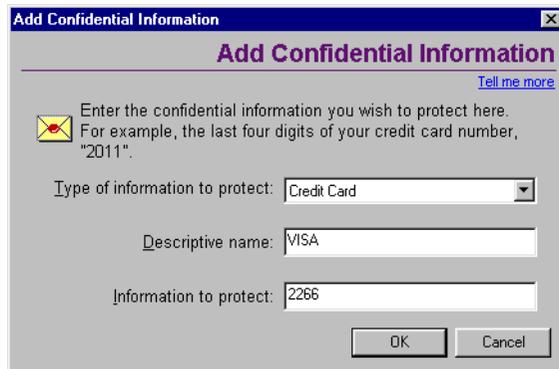
- 1 Open Norton Internet Security.
- 2 Click Privacy.
- 3 Click the Settings For arrow and click the account to change.
- 4 Set the slider to High or Medium to show a prompt every time someone tries to send protected information over an non-secure Web connection.
- 5 To set Norton Internet Security to always block confidential information click Custom Level.

To enter confidential information to be blocked:

- 1 Open Norton Internet Security.
- 2 Click Privacy.
- 3 Click Confidential Info.



- 4 In the Confidential Information dialog box, Click Add.



- 5 In the Add Confidential Information dialog box, click a category from the Type Of Information To Protect box.
- 6 In the Descriptive Name field, enter a description that will help you remember why you are protecting the data.
- 7 In the Information To Protect field, enter the information you want to block from being sent through non-secure Web connections.

Note: When you set up confidential information in this database, the information applies to all user accounts. Any account that is blocking confidential information will block the same list of information.

Tips on blocking confidential information

If you do not want to enter an entire credit card number or identification number, just enter a part of it. This prevents that part of the number from being transmitted to a non-secure Web site.

Norton Internet Security blocks personal information exactly the way you enter it into the program. You might need to enter some information in various formats to truly protect it. For example, a phone number could be entered as 888-999-0000, but it could also be entered without dashes (8889990000) or with spaces (888 999 0000). Sometimes it will work better to enter partial numbers rather than entering one number several different ways.

Some Web sites break up the way you enter information. They split phone numbers into two or three fields, or they use four fields for a credit card number. To protect numbers from being entered into these types of Web

sites, enter information in small chunks. For example, to protect your phone number, enter small pieces of the phone number as separate entries. For the phone number 888-999-0000, 888 might be one entry, 999 another, and 0000 would be a third. This protects all portions of your phone number.

Blocking cookies

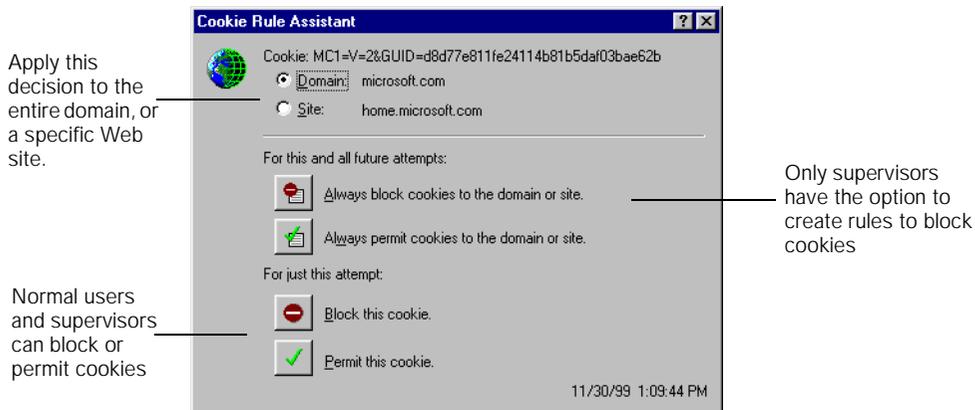
Cookies are small text files that your browser saves on your hard disk. Sometimes Web sites use them to save information that makes it more convenient for you to use their site.

Cookies that record personal information can jeopardize your privacy by allowing others to access them without your permission. They might contain enough information to show your browsing habits, or they could expose passwords and login names.

When a Web site requests a cookie from your computer, Norton Internet Security checks to see whether you are permitting them, blocking them, or using the Cookie Assistant to determine the action.

Using the Cookie Assistant

The Cookie Assistant sets up rules for specific Web sites when it detects a cookie request. You can use it to specify which Web sites you want to allow or block from using cookies. When you create a cookie rule, Norton Internet Security remembers the sites where you want to allow cookies, and those you want to block.



For information on using Domain or Site settings, see “[Do I want Domain or Site?](#)” on page 36.

To enable the Cookie Assistant:

- 1 Open Norton Internet Security.
- 2 Click Privacy.
- 3 Click Custom Level.
- 4 Set Cookie Blocking to Medium.

Blocking browser information

By default, your browser sends some information to the Internet whenever a Web server asks for it:

- The address of the last site you visited.
- Email addresses you have set up in your browser.

You can turn this blocking feature off by customizing your Privacy settings.

To stop blocking browser information:

- 1 Open Norton Internet Security.
- 2 Click Privacy.
- 3 Click the Settings For arrow and click the user account to set up.
- 4 Click Custom Level.



- 5 In the Customize Privacy Settings dialog box, click to uncheck Enable Browser Privacy.

By default, Norton Internet Security does not block the type and version of the browser you are using. Many Web sites are designed to display different pages, depending on this information from your browser.

Enabling or disabling secure Web connections

When you visit a secure Web site, your browser sets up an encrypted connection with the Web site. It uses a special protocol named *https*. Information given over secure connections cannot be detected by a firewall because the information is encrypted. *Encryption* means that the information is encoded with a mathematical formula, scrambling the data in an unreadable format.

By default, Norton Internet Security lets anyone use secure connections. However, if you want to ensure that restricted account users are not giving out confidential information to secure Web sites, you can block them from making secure Web connections. For example, parents might wish to prevent children from making online purchases.

To disable secure Web connections for an account:

- 1 Open Norton Internet Security
- 2 Click Privacy.
- 3 Click the Settings For arrow and click the account to change.
- 4 Click Custom Level.
- 5 In the Customize Privacy Settings dialog box, click to uncheck Enable Secure Connections (https).

Setting up parental controls

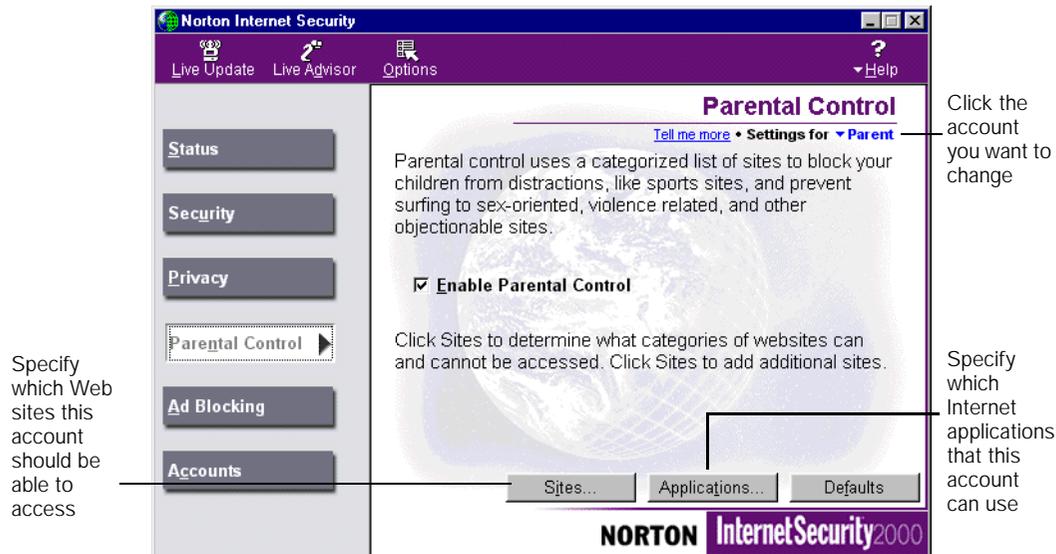
While the Internet provides unprecedented opportunities to bring information into the home, it also contains a lot of information that can be inappropriate for children or other family members.

The most effective way to keep these types of materials from entering your home is to talk with your family about the appropriateness of Internet content. Norton Internet Security helps you enforce the decisions your family makes about how they use the Internet. The Parental Control feature lets you block out specific categories of Web sites, or you can create your own list of Web sites you want to allow and block everything else.

See [“Creating a family Internet usage policy”](#) on page 19.

To set up parental controls for a specific account:

- 1 Open Norton Internet Security.
- 2 Click Parental Control.



- 3 Click the Settings For arrow and click the account to protect.
- 4 Make sure that Enable Parental Control is checked.
- 5 Follow the instructions for Blocking and Permitting Access to Web sites, and Blocking and Permitting Internet Applications.

Restricting access to Web sites

Norton Internet Security comes with an extensive list of categorized Web sites. This list is updated regularly. Use LiveUpdate to keep the lists current on your computer. See [“Updating Norton Internet Security”](#) on page 15.

You can restrict an account’s access by choosing one of these methods:

- Create a list of Web sites that can be visited. All accounts that are restricted with this method can only browse the Web sites on this list. Use this option for young children’s accounts.
- Use Symantec’s list of pre-categorized sites to specify which categories an account can and cannot access. You can also add your own sites to the list of sites to be blocked. Use this option when you want to restrict an account from visiting specific Web sites or Web site categories, but want to allow everything else.

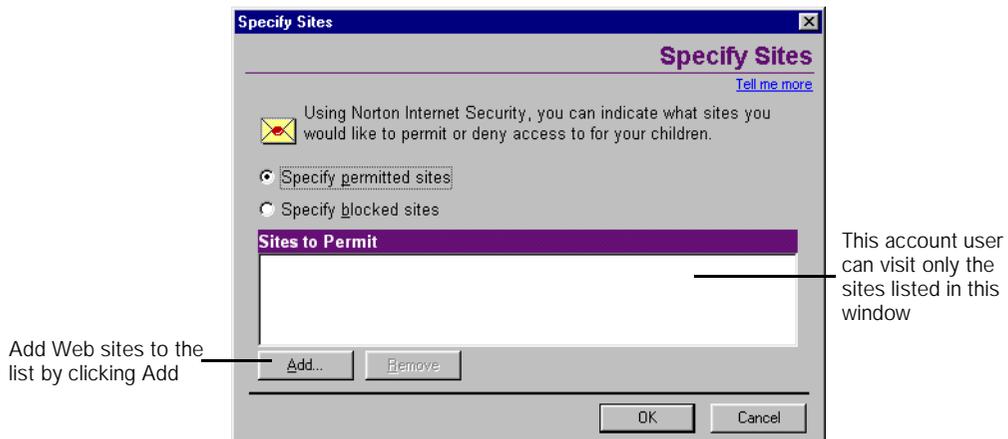
You can use only one of these two strategies per account. If you want to protect some children by creating a list of sites they can visit, but you want to protect other children by listing the sites they cannot visit, you will need to create two different accounts.

Creating a list of permitted Web sites

You can create a list of permitted Web sites and block all others.

To create a list of permitted Web sites:

- 1 Open Norton Internet Security.
- 2 Click Parental Control.
- 3 Make sure that Enable Parental Control is checked.
- 4 Click the Settings For arrow and click the account to change.
- 5 Click Sites.
- 6 In the Specify Sites dialog box click Specify Permitted Sites.



- 7 Click Add to create a new entry in the list.
When it asks for the Web site address, enter the complete address.
- 8 To remove a site from this list, click the Web site and click Remove.

Note: This permit list is the same for all accounts that use it. You cannot create a separate list of permitted Web sites for different accounts.

Blocking accounts from visiting sites

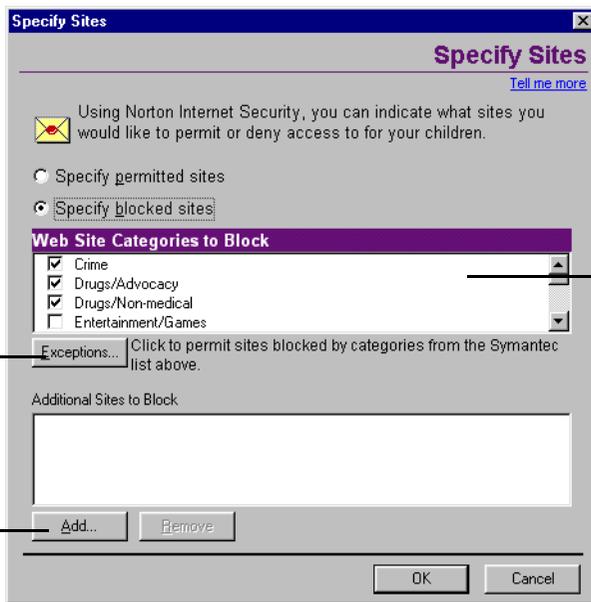
You can specify categories of Web sites that an account user can or cannot visit.

To block Web site categories for an account:

- 1 Open Norton Internet Security.
- 2 Click Parental Control.
- 3 Click the Settings For arrow and click the account to change.
- 4 Click Sites.
- 5 In the Specify Sites dialog box, click Specify Blocked Sites.

If there are Web sites being blocked, you can create an exception to unblock that site without disabling the entire category

You can add additional Web sites that you want to block by clicking Add



This account user can visit anything except those Web sites that belong to the checked categories

- 6 Categories to allow for this account should be checked.
- 7 Click Add to create a new entry in the list.

When it asks for the Web site address, enter the complete address.

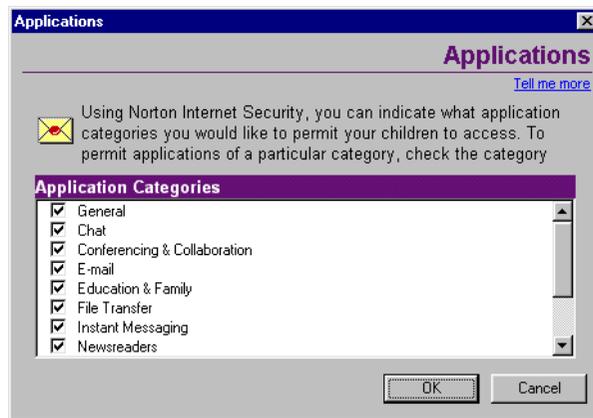
Keep your system equipped with the latest list of categorized Web sites by connecting to the Internet and clicking LiveUpdate. See [“Updating Norton Internet Security”](#) on page 15.

Blocking applications from accessing the Internet

This feature lets you decide which types of programs the account user can use on the Internet. For example, parents can prevent children from using chat programs by blocking the chat programs category from the children's account.

To set up application categories for an account:

- 1 Open Norton Internet Security.
- 2 Click Parental Control.
- 3 Click the Settings For arrow and click the account to change.
- 4 Click Applications.



- 5 In the Applications dialog box, make sure the categories that this account is allowed to use on the Internet are checked.

Note: Blocking an application does not prevent the user from opening or running the application. It only prevents the application from making a connection with the Internet.

Categorizing programs

Programs are assigned to application categories when firewall rules are created:

- When the firewall detects a program that tries to open a connection on the network, it opens the Firewall Rule Assistant. As this wizard guides

you through setting up rules, one of the options is to specify an application category. Click the category to use for the program.

- If the firewall automatically generates a rule for the application when it detects it, the firewall uses the category from the firewall rule database. See [“Creating firewall rules automatically”](#) on page 33.

Blocking ads

The Ad Blocking window lets you block Internet advertisements and common graphics from downloading in your browser. Turning this feature on can drastically reduce the amount of time it takes to download a Web page.

When ad blocking is enabled and you connect to a Web site, Norton Internet Security uses two lists to scan the Web pages as they download:

- Build your own ad blocking list by finding and blocking advertisements in Norton Internet Security.
- Norton Internet Security comes with a list of default ads that it blocks automatically. Use LiveUpdate to keep a current list of blocked ads on your computer. See [“Updating Norton Internet Security”](#) on page 15.

Norton Internet Security looks for the address of the advertisements being blocked as the Web page is downloaded by your browser. If it finds any matching addresses in the Web page being downloaded, it removes the matching information so that it cannot be displayed in your browser. But it leaves the rest of the Web page in tact so you can enjoy the Internet without the advertisements.

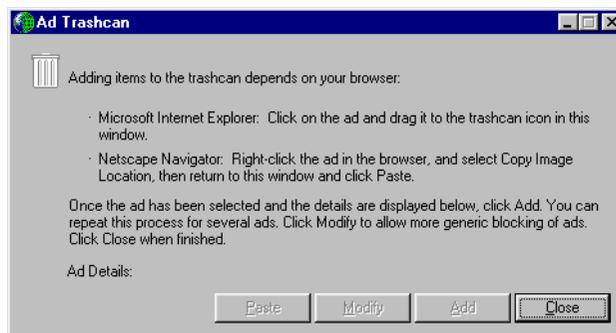
To add advertisements to the list of blocked ads:

- 1 Open Norton Internet Security.

2 Click Ad Blocking.



3 Click the Trashcan.



- 4 Open your browser to the Web page containing the advertisement you want to block.
- 5 With the windows arranged so that you can see both the advertisement and the Ad Blocking dialog box, put the advertisement's address in the Trashcan:
 - If you are using Microsoft Internet Explorer, drag the unwanted ad from the Web site to the Ad Blocking dialog box. The Web address for the advertisement appears in a dialog box.
 - If you are using Netscape Navigator, right-click the advertisement and click Copy. Then in the Ad Trashcan dialog box, click Paste.

The address for the advertisement appears in the Ad Details line of the Ad Trashcan dialog box.

- 6 Click Add to begin blocking this entire address. Click Modify to change the Ad Details before blocking them.

For example, if the advertisement address is <http://www.advertise.org/annoying/ads/numberone.gif>, you could select the <http://www.advertise.org/annoying/ads> to block everything in the ads directory.

Troubleshooting

This chapter answers some of the questions advanced users may have about Norton Internet Security and virus protection.

Frequently Asked Questions

How do I turn off Norton Internet Security?

There may be circumstances when you want to temporarily suspend a certain protection feature, or even the entire product. Norton Internet Security lets you turn specific features off without adjusting the settings.

To temporarily disable Norton Internet Security:

- 1 Open Norton Internet Security.
- 2 Make sure you are logged on using a normal or supervisor account. Restricted users cannot disable any portion of Norton Internet Security.
- 3 In the Status window, click Disable.

Norton Internet Security will be enabled the next time you start your computer.

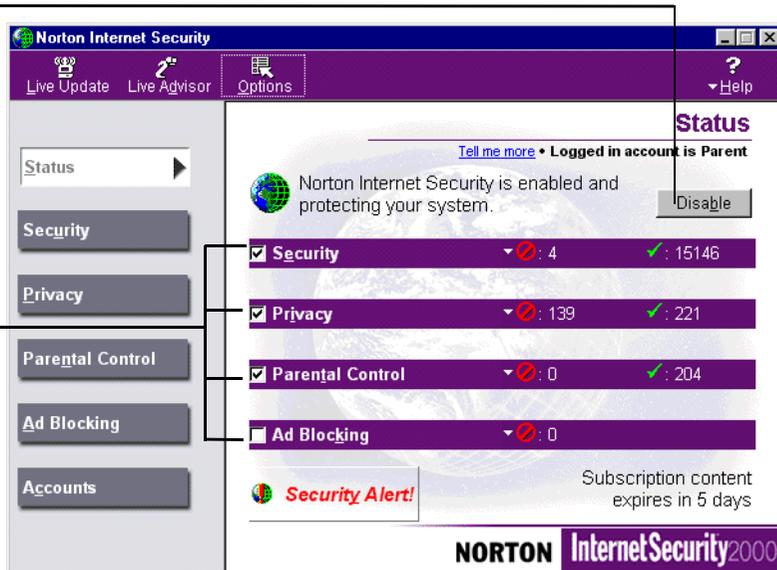
To temporarily suspend Privacy, Security, Parental Controls, or Ad Blocking:

- 1 Open Norton Internet Security.
- 2 Make sure you are logged in using a normal or supervisor account. See [“Switching accounts”](#) on page 26.

- 3 In the Status window, make sure Security, Privacy, Parental Control, or Ad Blocking are unchecked.

Temporarily disable all functions of Norton Internet Security

Unchecked features are suspended; checked features are enabled



Exiting Norton Internet Security

Even when Norton Internet Security is not open, if the icon appears in the System Tray, it is still protecting your system. You can stop Norton Internet Security from running in the background.

To exit Norton Internet Security:

- 1 Right-click the Norton Internet Security icon in the system tray and click Exit.



Why can't I post information online?

If you are unable to post information to a Web site, it may be because Norton Internet Security is blocking the information. Check in the Confidential Information list on the Privacy window to see if the information you are trying to enter is being blocked.

To check the information on the Personal Information list:

- 1 Open Norton Internet Security.
- 2 Click Privacy.
- 3 Click Confidential Information.

This opens the list of words that Norton Internet Security blocks from being transferred to the Internet.

What is wrong with this Web site?

Running 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.

To see if Norton Internet Security is blocking the access to the Web site, you can disable Norton Internet Security and try the Web site again. See ["How do I turn off Norton Internet Security?"](#) on page 51. If you still cannot connect, there might be a problem with the Internet or your Internet Service Provider.

It could be script blocking

Some Web sites use JavaScript in their navigation controls and in other places. If Norton Internet Security is blocking JavaScripts or VB Scripts, it may cause problems with these Web sites.

To stop blocking JavaScript or VB Scripts:

- 1 Open Norton Internet Security.
- 2 Click Security.
- 3 Click Custom Level.
- 4 Set Java Applet Security or ActiveX Control Security to Medium or None.

It could be cookie blocking

Other Web sites require that cookies be enabled on your system to display correctly. If you have cookie blocking turned on and the Web page appears to be blank, turn off cookie blocking and download the page again.

To stop blocking cookies:

- 1 Open Norton Internet Security.
- 2 Click Privacy.
- 3 Click Custom Level.
- 4 Set Cookie Blocking to Medium or Low.

It could be parental controls

If you have set up Norton Internet Security to block certain categories of Web sites, it may be blocking the site you are attempting to view. If you are using a supervisor or normal account, you can temporarily turn off parental controls from the Account window and see if the site is still blocked. See [“How do I turn off Norton Internet Security?”](#) on page 51.

It could be a firewall rule

A firewall rule might be blocking the Web site. When this happens, there are no error messages that appear. You can view the firewall rules that have been set up, and determine if a rule is blocking the site. See [“How do I review or change firewall rules?”](#) on page 61.

It could be blocking ActiveX or Java

Some Web sites display only ActiveX Controls or Java Applets. If you are blocking them, nothing appears on these sites. See [“Setting Java and ActiveX security levels”](#) on page 34.

It could be ad blocking

Sometimes blocking advertisements on the Internet can prevent an entire Web site from appearing in your browser. If you suspect this to be the case, turn off ad blocking and try the site again.

Why doesn't FTP work on older browsers?

Older browsers use a random port when they attempt to open FTP connections. By default, Norton Internet Security blocks Internet connections on non-standard ports.

To temporarily resolve this problem, disable the security portion of Norton Internet Security. See ["How do I turn off Norton Internet Security?"](#) on page 51.

To more completely resolve this problem, install the most recent version of your browser software.

Why won't a program connect to the Internet?

There may be two reasons that a restricted account user cannot use a program with the Internet:

- The program may belong to a category of applications that is restricted for this account. See ["Blocking applications from accessing the Internet"](#) on page 47.
- If you are using a restricted account and there is no firewall rule allowing the program to create a connection to the Internet. If a firewall rule does not exist for the connection, the attempt is automatically denied without notification for restricted accounts.

For supervisor and normal accounts, having no firewall rule triggers the Firewall Rule Assistant, allowing them to create a new firewall rule for the new connection. See ["Using the Firewall Rule Assistant"](#) on page 31.

A user with normal or supervisor rights can change the current account to a supervisor or normal account. See ["To change the account type:"](#) on page 24. Then they can run the program to make the Firewall Rule Assistant appear. After setting up a firewall rule, they should set the active user account back to the restricted user's account name. Then the restricted user can run the program that accesses the Internet.

Norton Internet Security could be blocking your account from using this program on the Internet. If it is, the supervisor can change your account settings to stop blocking it. See ["Changing account settings"](#) on page 28.

How can I close an Internet connection while online?

It is possible to close a connection to the Internet without disconnecting your computer.

To terminate a connection:

- 1 Open Norton Internet Security.
- 2 Click Options.
- 3 Click View Statistics.
- 4 Right-click the connection and click Terminate Connection.

How can a Web site get my browser information?

The Browser Privacy settings prevent your browser from sending out browser information. However, some diagnostic sites on the Internet might report browser information even though the Browser Privacy settings are blocking the information:

- If you are not blocking Java, ActiveX or JavaScript, the site might be using one of these methods to retrieve the information. See [“Setting Java and ActiveX security levels”](#) on page 34.
- Sometimes when Web servers do get the information from the browser, they simply use the last piece of browser information they received instead. You might see the information from the last person who viewed the site.

What are inbound and outbound connections?

When another computer on the Internet attempts to open a connection to your computer, it is called an inbound connection. Outbound connections occur when a program on your computer attempts to open a connection to an external computer. Once a connection is open, whether it is inbound or outbound, data can pass through that connection in both directions.

Where can I get more information?

Use Help

Norton Internet Security comes with complete Help instructions for every feature. There are several ways to access this resource:

- Click Tell Me More on any window in Norton Internet Security to open the Help topic for that window.
- Click any button, text field, or other control in Norton Internet Security and press F1. This displays Help about that particular control.

Read the Norton AntiVirus User's Guide

The Norton AntiVirus User's Guide can help you learn more about Norton AntiVirus and related topics. The guide is included on the Norton Internet Security CD under the \manuals directory.

Visit the Symantec AntiVirus Research Center

The Symantec AntiVirus Research Center has a lot of information about viruses, trojan programs and other security threats. Visit the site at

<http://www.sarc.com>

Questions about home networking

You can use Norton Internet Security on a home network. However, it is designed to protect a single computer. Installing Norton Internet Security on a single computer might not protect other computers on the network from Internet threats.

If you have more than one computer connected to the Internet, purchase and install Norton Internet Security for each computer.

How does the firewall work with Internet connection sharing?

If Norton Internet Security is installed on the computer with the Internet connection, it behaves as described in this manual for that computer. However, unless it is installed on the computers that share the connection, it ignores all communication being sent to those computers.

Purchase and install Norton Internet Security for each computer sharing the Internet connection.

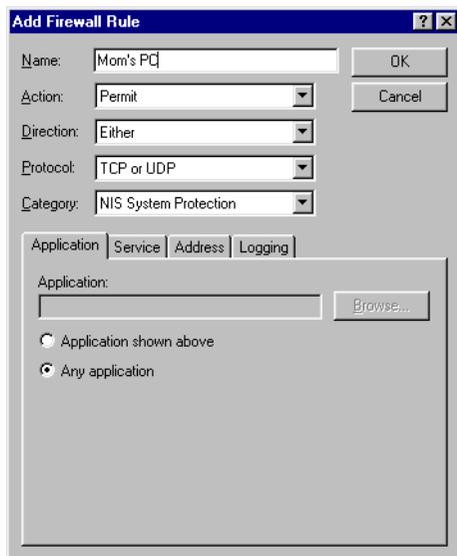
How does the firewall work with file and printer sharing?

Norton Internet Security contains default firewall rules that allow file and printer sharing over IPX and NetBEUI networks. If you are using a TCP/

IP-based network, you must configure the firewall to recognize the other computers on your network.

To configure the firewall to recognize your networked computers:

- 1 Open Norton Internet Security.
- 2 Make sure you are using a supervisor account.
- 3 Click Options.
- 4 Click Advanced Options.



- 5 Under the Firewall tab, click Add.
- 6 Enter a descriptive name for the computer you are setting up.
- 7 In the Action field, click Permit.
- 8 In the Direction field, click Either.
- 9 In the Protocol field, click TCP Or UDP.
- 10 In the Category field, click NIS System Protection.
- 11 On the Application tab, click Any Application.
- 12 On the Service tab under Remote Service, click Any Service. Under Local Service click Any Service.
- 13 On the Address tab under Remote Address, click Host Address and enter the TCP address of the other machine.

- If you are setting up more than one machine in this rule, click Address Range and enter the range of addresses on your local network.
- If you are using two network cards, one connected to the Internet and one connected to the home network, under Local Address click Host Address and enter the address of the computer running Norton Internet Security.

This permits any communication on that network card. The other firewall rules apply to the network card connected to the Internet.

14 On the Logging tab, specify settings.

After clicking OK, the new firewall rule appears at the bottom of the firewall list. Move the firewall rule to the top of the list so that it runs before any other rules.

To move the firewall rule to the top of the list:

- 1 Click the new firewall rule.
- 2 Click the up arrow repeatedly until the rule appears at the top of the list.

How do I use Norton Internet Security with a proxy server?

Proxy servers are computers that act as the single connection to a larger network. If you are using a proxy server, you need to specify the port that your network uses for Web communications (http). This lets Norton Internet Security to monitor Web activity.

To monitor a specific port for Web communications:

- 1 Open Norton Internet Security.
- 2 On the toolbar, click Options.
- 3 Click Advanced Options.
- 4 On the Others tab, under HTTP Port List, click Add.
- 5 Enter the number for the port that should be monitored.

Refer to the instructions you used to set up your proxy server to determine which ports should be monitored.

Questions about the firewall

The technical information about the firewall and its configurations can be found in the Norton Internet Security Help.

To open Help:

- 1 Open Norton Internet Security.
- 2 On the toolbar, click Help.

Why doesn't the Firewall Rule Assistant appear?

The Rule Assistant appears when the firewall detects a program trying to access the Internet, and there are no previous firewall rules blocking or permitting the program's network connection. There are several areas in Norton Internet Security where you can block a program so that the Firewall Rule Assistant does not appear.

Use this checklist to make sure the Firewall Rule Assistant appears when needed:

- Turn on the rule assistant for the user account you want to use. This setting is based on the account. Turning it on for one account does not enable it for other accounts. See [“Using the Firewall Rule Assistant”](#) on page 31.
- Security must be enabled for the account.
- In the Security window, make sure that the firewall is turned on. You can turn the Security slider to High, or set the firewall to High under Custom Level.
- In Parental Controls, make sure that the settings are not blocking the user account from the application you want to use.
- Make sure there are no rules already covering the program you want to use. See [“How do I review or change firewall rules?”](#) on page 61. If a rule already exists, perhaps you already created it using the Firewall Rule Assistant. Or, if Enable Automatic Firewall Rule Creation is turned on, Norton Internet Security automatically created the rule for you. See [“Creating firewall rules automatically”](#) on page 33.
- When someone scans unused ports on your system, you can set Norton Internet Security so that it does not alert you unless the connection is successful. This can reduce the number of alerts you might receive.

How do I review or change firewall rules?

Whenever firewall rules are created, they appear in the Norton Internet Security Settings window. This window lets you review and change the firewall rules in the firewall database. Only supervisor accounts have access to this window.

Arrows pointing to the computer allow incoming communications

Arrows pointing away from the computer allow outgoing communications

Blocked arrows show rules that block inbound or outbound communications

Adjust the order that the firewall rules run

Firewall Rule	Rule Action Summary
<input checked="" type="checkbox"/> Block Ping	ICMP: Echo Request
<input checked="" type="checkbox"/> Default Inbound ICMP	ICMP: Any Type
<input checked="" type="checkbox"/> Default Outbound ICMP	ICMP: Any Type
<input checked="" type="checkbox"/> Default Inbound DNS	domain
<input checked="" type="checkbox"/> Default Outbound DNS	domain
<input checked="" type="checkbox"/> Default Inbound Bootp	bootpc
<input checked="" type="checkbox"/> Default Outbound Bootp	bootp
<input checked="" type="checkbox"/> Default Inbound NetBIOS	nbdatagram, nbname
<input checked="" type="checkbox"/> Default Outbound NetBIOS	nbdatagram, nbname
<input checked="" type="checkbox"/> Default Inbound Loopback	localhost
<input checked="" type="checkbox"/> Default Outbound Loopback	localhost
<input type="checkbox"/> Block access to secure sites	https
<input checked="" type="checkbox"/> LiveUpdate	http, 81, 82, 83, https, socks, htt..
<input checked="" type="checkbox"/> LiveUpdate	update.symantec.com: ftp-data, f..
<input checked="" type="checkbox"/> LiveUpdate	liveupdate.symantec.com: ftp-dat..

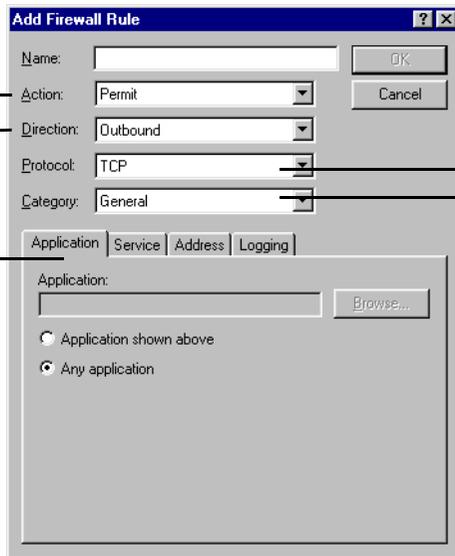
To review or change individual firewall rules:

- 1 Open Norton Internet Security.
- 2 On the toolbar, click Options.
- 3 On the Firewall Tab, click the rule to view.

4 Click Modify.

Firewall rules can permit, block, or ignore information from coming into, or leaving your computer

Each tab contains additional settings



The firewall can monitor different protocols; most Internet communications are done with TCP

You can block or allow specific application categories for each account

Press the F1 key at any time to get Help on any field or feature.

Creating a manual firewall rule affects all user accounts unless you specify a category for the firewall rule. Then you can specify which categories can be used by different user accounts. See [“Blocking applications from accessing the Internet”](#) on page 47.

If two firewall rules cover the same issue, which one runs?

When Norton Internet Security detects a program attempting to access the Internet, it reads through the list of firewall rules to find any directions on permitting or blocking the connection. As soon as it finds a rule that matches, it stops looking for additional rules. If you have a rule that should run before another rule, you can change the order of the rules.

To change the order of the rules:

- 1 Open Norton Internet Security.
- 2 On the Toolbar, click Options.
- 3 On the Firewall tab, click the firewall rule to move.
- 4 Click the up arrow or the down arrow to move the selected rule.

What is the purpose of the default firewall rules?

There are several default rules already set up in the firewall when you first install it. This default list changes according to the options you set in the Security window:

- The Default Inbound DNS and Default Outbound DNS rules permit the use of the domain name service (DNS) for Internet connection. The DNS translates Web site addresses from host names like `www.symantec.com` to IP addresses like `127.0.0.1`.
- The Default Inbound Bootp and Default Outbound Bootp rules permit the use of the bootp service. Bootp is short for bootstrap protocol, which enables a machine to discover its own IP address.
- The Default Inbound Loopback and Default Outbound Loopback rules permit your computer to connect to itself while testing network connections.
- The Default Inbound ICMP and Default Outbound ICMP rules permit ICMP messaging. The ICMP protocol lets your computer determine how to send information over a network like the Internet.
- There are several additional default rules that block common trojan programs like Back Orifice and NetBus.

If I delete the default firewall rules, can I get them back?

Yes, but the process requires that you delete all existing rules first, including any custom rules you created.

To restore the original default firewall rules:

- 1 Delete all the firewall rules.
- 2 Find the `firewall.dat` file on your computer.
To open the search program, click the Windows Start Button > Find > Files or Folders.
- 3 When you find it, rename it as `firewall.reg`.
- 4 Double-click `firewall.reg` file to import it into the Registry.

Can I create firewall settings for specific Web sites?

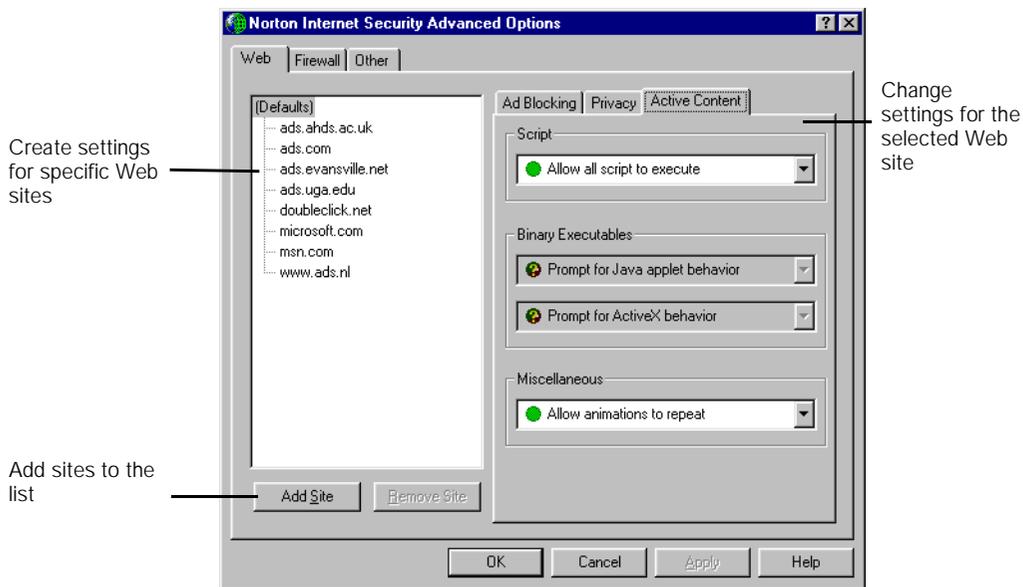
You can create Ad Blocking, Privacy, and Active Content settings for specific Web sites using the Norton Internet Security Settings dialog box. First, set up Norton Internet Security the way you want it to apply to all

Web sites in general. Then read these directions to create rules or settings for specific Web sites.

Any time you want to open the Norton Internet Security Settings window, click Options on the toolbar. Also, clicking Advanced in the Security, Privacy, Parental Control, or Ad Blocking window opens the settings window to the associated window in the settings window.

To create settings for specific Web sites:

- 1 Open Norton Internet Security.
- 2 On the toolbar, click Options.
- 3 Click Advanced Options.



- 4 If you are adding a new Web site, Click Add Site and enter the Web site address for the site for which you are changing the settings.
After you click OK, the new site appears in the Web site list.
- 5 In the list of Web sites, click the Web site to change.
- 6 Click the Ad Blocking, Privacy, or Active Content tabs and change the settings for this site.

The window shows the settings for any Web site you have selected in the Web list. If you select Defaults, the window shows the settings for all Web sites that are not listed.

Norton AntiVirus Emergency Procedures

The complete Norton AntiVirus User's Guide and this user's guide are included on the Norton Internet Security CD in the \manuals folder. These guides are in Adobe Acrobat Portable Document Format (.pdf), and require the Adobe Acrobat Reader to view them. An Adobe Acrobat Reader program is located in the \manuals folder on the Norton Internet Security CD.

What to do if a virus is found

When you see a Norton AntiVirus alert, you can use the information in this chapter to help you respond appropriately.

Quick guide to alert actions

If a Norton AntiVirus alert appears on your screen, use this table to decide what to do. If you need more information, see the next section, "Types of virus alerts," for step-by-step instructions.

In some situations, your mouse will not work when an alert appears. In these cases, press the first letter of your selection (for example, press **R** for Repair) or press Enter to accept the recommended selection.

Actions	When and why you use them
Repair	Eliminates the virus and repairs the infected item. When a virus is found, Repair is always the best choice.

Actions	When and why you use them
Quarantine	Isolates the virus-infected file, but does not remove the virus. Click Quarantine if you suspect the infection is caused by an unknown virus and you want to submit the virus to the Symantec AntiVirus Research Center for analysis.
Delete	Erases both the virus and the infected file. The virus and file are gone forever. Click Delete if Repair is not successful. Replace a deleted file from the original program disks or backup copy. If the virus is detected again, your backup copy or original disk is infected.
Stop	Stops the current operation to prevent you from using an infected file. Stop does not solve the problem. You will be alerted again the next time you do the same thing.
Continue	Continues the current operation. Click Continue only if you are sure a virus is not at work. You will be alerted again. If you are not sure what to do, click Stop.
Exclude	If you click Exclude and a virus is at work, the virus will not be detected. Exclude should be used only by system administrators for system tuning.

Types of virus alerts

Virus Found

When Norton AntiVirus finds a virus has infected a file on your computer, it produces a warning similar to this:

VIRUS FOUND: The BADVIRUS virus was found in C:\MYFILE.

To get rid of a virus infection:

- Press R for Repair.

Your file is restored to exactly the way it was before the virus infected it. That is all you need to do. If the repair was successful, the virus is gone and your computer is safe.

Virus in Memory

Norton AntiVirus stops your computer when it finds a virus in memory. While you do not normally turn off a computer without first exiting

Windows, in this case it is necessary because your computer is halted. You cannot do anything else.

A virus in memory is active, dangerous, and will quickly spread to many other files.

A memory virus warning says similar to this:

VIRUS IN MEMORY. The BADVIRUS virus was found in memory.

The computer is halted. Restart from your write-protected Rescue Disk, and then scan your drive again.

To get rid of a virus in memory:

- 1 Turn off your computer using the power switch.
- 2 Insert your Rescue Boot Disk into drive A.
- 3 After waiting a few seconds, turn the computer on.
- 4 Follow the on-screen directions.

Virus-Like Activity

A virus-like activity alert does not necessarily mean that your computer has a virus. It is simply a warning. It is up to you to decide whether the operation is valid in the context in which it occurred.

The alert looks similar to this:

VIRUS-LIKE ACTIVITY: The NEWGAME is attempting to write to IO.SYS.

To resolve a virus-like activity alert:

Do one of the following:

- Press C for Continue if the message describes a valid activity for the application you are running.

For example, if you are updating an application and the alert warns you of an attempt to write to a file, the activity is valid.

- Press S for Stop if the detected activity is not related to what you are trying to do.

For example, if you are playing a game and the alert warns you of an attempt to write to the boot records of your hard drive, the activity is invalid.

What to do if Norton AntiVirus cannot repair

One of the most common reasons Norton AntiVirus cannot repair a file is that you do not have the most up-to-date virus protection. Use LiveUpdate to obtain the latest virus protection.

Do one of the following:

- Update your virus protection and scan again.
- Read the information on your screen carefully to identify the type of item that cannot be repaired, and then match it to one of the types below:
 - Infected files are those with filenames that include .com or .exe. Document files such as .doc, .dot, and .xls can also be infected.
 - 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 are replaced using the Rescue Disks or, sometimes, your operating system (Windows or DOS) disks.

Infected files

If infected files cannot be repaired, you need to either quarantine or delete them from your computer. If you leave an infected file on your computer, the virus infection can spread.

If Norton AntiVirus cannot repair a file:

Do one of the following:

- Click Quarantine.

After the file is quarantined, you can update your virus definitions and scan again or submit the file to SARC for analysis.
- Click Delete.

Replace the deleted document file with a backup copy or reinstall a deleted program from the original program disks. Make sure to scan the backup disks before you use them.

If the virus is detected again after you replace or reinstall the file, your backup copy or original program disks are probably infected. You can try contacting the manufacturer for a replacement.

Hard disk master boot record or boot record

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 are replaced using the Rescue Disks or, sometimes, your operating system (Windows or DOS) disks.

If Norton AntiVirus cannot repair your hard disk or master boot record, you can use your up-to-date Rescue Disks to restore it.

If your Rescue Disks are not up-to-date, contact Symantec Technical Support. [See the Service and Support Solutions in this guide for contact information.](#)

Floppy disk boot record

If Norton AntiVirus cannot repair a floppy disk boot record, it still removes the virus. The information on the floppy disk remains accessible and you can safely copy the files onto another disk. However, you can no longer start your computer from the floppy disk.

System file

If Norton AntiVirus cannot repair a system file (for example, `io.sys` or `msdos.sys`) you cannot delete it. You must reinstall Windows.

Restart your computer from an uninfected, write-protected floppy disk and reinstall Windows. You can use your Rescue Boot Disk or the Windows 95/98 Startup Disk that you created when you installed Windows to start up.

Using Rescue Disks in virus emergencies

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 will tell you when to use your Rescue Disks.

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

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions (with software such as Partition-It or Partition Magic)

- Upgraded your operating system (to Windows 98, for example)

Warning: If the critical information stored on the Rescue Boot Disk is outdated, it could cause problems when you attempt to restore your computer. It is unlikely you would be able to fix these problems on your own. However, if you have current Rescue Disks, the following procedure is safe to attempt.

It's okay if you have updated your virus protection since you last updated your Rescue Disks. They may not be able to recognize every new virus, but they will not harm your system simply because the virus protection is out-of-date.

To use your Rescue Disks:

- 1 If your computer is running, click Shut Down on the Windows Start menu, and then switch off your computer using the power switch.
- 2 Place your write-protected Rescue Boot Disk into drive A.
Slide open the plastic tab on the back of the disk to write-protect it. This prevents a virus from accidentally changing the data stored on the disks.
- 3 After waiting a few seconds, turn your computer on.
- 4 Follow the on-screen directions.

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

You are prompted when it is time to insert other Rescue Disks.

- 5 When the process is complete, remove the Rescue Disk from drive A and restart your computer.

Virus emergencies are handled by the first two tasks in Norton Rescue: Rescue Recovery and Norton AntiVirus. You should not need any additional tasks listed in Norton Rescue to solve virus emergencies.

Service and Support Solutions

Service and Support information is available from the Online Help System of your Symantec product. Choose the Service and Support topic from the online Help Index page.

StandardCare Support

Connect to Symantec Service and Support site at www.service.symantec.com for a complete selection of technical support options and customer services, including product knowledgebases, interactive troubleshooter, Frequently Asked Questions (FAQ), Chat Now! (interactive chat), and more!

From this Web site you can order disk and manual replacements, change your address, find out the status of your order or return, or post a query to a Customer Service discussion group.

PriorityCare, GoldCare, and PlatinumCare Support

Fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070.

Telephone support information is also available on the Service and Support Web site. Connect to www.service.symantec.com, select your product and version, and select Contact Technical Support.

Automated fax retrieval

Use your fax machine to receive general product information, fact sheets, and product upgrade order forms. Call (800) 554-4403 or (541) 984-2490. For technical application notes, call (541) 984-2490 and select option 2.

International Service and Support

Technical Support and Customer Service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please call our Technical Support automated fax retrieval service at +1 (541) 984-2490, choose Option 2, and request document 1400.

Customer Service

Symantec Customer Service can provide assistance for non-technical questions such as:

- Subscribing to the Symantec Support Solution of your choice.
- Obtaining product literature or trialware.
- Locating resellers and consultants in your area.
- Replacing missing or defective CD-ROMS, disks, manuals, etc.
- Updating your product registration with address or name changes.
- Getting order, return, or rebate status information.
- Accessing Frequently Asked Questions (FAQ).
- Posting questions to the Customer Service newsgroup.

To speak with a customer service representative, call (800) 441-7234 or visit us online at <http://service.symantec.com>.

Upgrade Orders

For upgrade orders, please call the Customer Service Order Desk at (800) 568-9501, or visit the upgrade center online at: <http://www.symantec.com/upgrades/>

Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support office for your region or visit us at <http://www.symantec.com>.

Service and Support Offices

NORTH AMERICA

Symantec Corporation
175 W. Broadway
Eugene, OR 97401

<http://www.symantec.com/>
(800) 441-7234 (USA & Canada)
(541) 334-6054 (all other locations)
Fax: (541) 984-8020

Automated Fax Retrieval (800) 554-4403
(541) 984-2490

EUROPE, MIDDLE EAST, AFRICA

Symantec Customer Service Center http://www.symantec.com/region/reg_eu/
P.O. Box 5689
Dublin 15
Ireland +353 (1) 811 8032
Fax: +353 (1) 811 8033

Automated Fax Retrieval +31 (71) 408-3782

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd. http://www.symantec.com/region/reg_ap/
408 Victoria Road
Gladesville, NSW 2111
Australia +61 (2) 9850 1000
Fax: +61 (2) 9817 4550

LATIN AMERICA

Symantec América Latina <http://www.symantec.com/region/mx/>
Oficina principal
2500 Broadway, Suite 200
Santa Monica, CA 90404 (310) 449-7086
Fax: (310) 449-7576

BRAZIL

Symantec Brazil <http://www.symantec.com/region/br/>
Av. Juruca, 302 - cj 11
São Paulo - SP +55 (11) 5561 0284
04080 011 Fax: +55 (11) 5530 8869
Brazil

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.

August, 1999



I N D E X

A

- account settings 23-28
- accounts
 - base account on 23
 - changing 26
 - changing settings 28
 - creating 24
 - logging off 27, 28
 - removing 26
 - setting the default 25
 - supervisor 28
 - switching 26
 - types of 23
- ActiveX 34
- Ad Blocking 48-50
- Ad Trashcan 48-50
 - opening from system tray 14
- Adobe Acrobat Reader 65
- alerts
 - actions to take 65
 - virus found 66
 - virus-like activity 67
- application categories 47
- applications
 - restricting access to the Internet 55
 - virus-like activity 67
- applications, virus-like activity 67
- assistant
 - Cookie Assistant 41
 - Firewall Rule Assistant 31
 - Java/ActiveX Assistant 35

B

- backup copies
 - infected 66, 68
 - replacing infected files 68
- blocking
 - advertisements on the Web 48-50
 - browser information 42, 56
 - confidential information 38-41

- cookies 41-42
- domains or sites 36
- email address in browser 42
- last site visited 42
- secure connections 43
- submitting Web sites to Symantec 17
- Web sites 44-46
- boot records, unable to repair 69
- browser information 42, 56

C

- categorizing programs 47
- cdstart.exe 11
- changing account settings 28
- changing accounts 26
- closing connections 56
- connections, inbound and outbound 56
- Cookie Assistant 41
- cookies 41-42
- creating
 - accounts 24
 - cookie rules 41
 - firewall rules 31
 - firewall rules automatically 33
 - Java/ActiveX rules 35

D

- default account 25
- deleting infected files 66, 68
- domain 36

E

- email address 42
- event log 16
- excluding files from scans 66
- exiting Norton Internet Security 52

F

- file extensions, infected files 68
- firewall
 - creating rules 31
 - creating rules automatically 33
 - how firewalls work 10
 - settings 31
- Firewall Rule Assistant 31, 60
- firewall rules
 - changing 61
 - default list of 63
 - order 62
 - restoring default 63
 - reviewing 61
- firewall.dat 63
- floppy disks, unable to repair boot record 69

H

- help 56
- home networking 57
- https 43

I

- inbound connections 56
- infected files
 - deleting 66
 - excluding from AntiVirus scans 66
 - file extensions 68
 - ignoring 66
 - quarantining 66
 - repairing 65
 - unable to repair 68-69
- installing
 - Norton AntiVirus 11
 - Norton Internet Security 11
- Internet connection sharing 57
- irreparable system files 69

J

- Java Applets 34
- Java/ActiveX Assistant 35
 - enabling 36

L

- LiveUpdate 15
- logging off 27, 28
 - from system tray 14
- logs
 - event 16
 - statistics 17

M

- manuals 65
- master boot record 69
- memory, removing viruses from 67

N

- network, home 57
- Norton AntiVirus
 - emergency procedures 65-70
 - installing 11
 - integrating with 14
- Norton AntiVirus User's Guide 65
- Norton Internet Security CD 65
- Norton SystemWorks 3.0, integrating with 14
- Not Logged In 20, 28

O

- opening Norton Internet Security 14
- outbound connections 56

P

- Parental Controls 43-48
- privacy settings 37-43
- program categories 47
- programs, virus-like activity 67
- protecting personal information 38-41
- proxy server 59

Q

- Quarantine 66

R

- referring Web address 42

removing
 infected files 68
 viruses from memory 67
removing accounts 26
repairing
 infected files 65
 unsuccessful 68-69
requirements 11
restoring default firewall rules 63
resubscribing 15
running in the background 14

S

SARC 56
secure connections 43
security
 ActiveX 34
 Java Applets 34
security settings 30-36
Service and Support 71
setting up user accounts 23-28
settings
 accounts 23-28
 firewall 31
 Parental Controls 43-48
 Privacy 37-43
 Security 30-36
software, virus-like activity 67
startup options 14
statistics 17
status screen 13
stop running Norton Internet Security 52
submitting Web sites to Symantec 17
subscription 15
supervisor account settings 28
switching accounts 26
Symantec AntiVirus Research Center 56
system files, unable to repair 69
system requirements 11
system tray 14

T

Technical Support 71
templates 23
terminating connections 56

Trashcan 48-50
tray icon 14

U

updating Norton Internet Security 15
user accounts. *See* accounts
user's guides on the product CD 65

V

virus alerts. *See* alerts
virus-like activity alerts 67

W

Web site blocking 44-46