symantec™

Norton™ Personal Firewall 2004

User's Guide

Norton™ Personal Firewall User's Guide

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

Documentation version 7.0

PN: 10109233

Copyright Notice

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

Standard Template Library

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

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT
Norton Personal Firewall

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "ACCEPT" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT ACCEPT" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE AND CONTACT SYMANTEC CUSTOMER SERVICE FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

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

You may:

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

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;

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

E. use the Software in accordance with any additional permitted uses set forth, below.

You may not:

A. copy the printed documentation that accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

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

F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

G. use the Software in any manner not authorized by this license; nor

H. use the Software in any manner that contradicts any additional restrictions set forth, below.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

There are technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures to protect Symantec against software piracy. This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a machine to not more than a finite number of times for a finite number of machines. This License and the Software containing enforcement technology require activation as further set forth during installation and in the Documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation, You will provide Your unique product key accompanying the Software and PC configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the Documentation, or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event You are not able to activate the Software, You may contact Symantec Customer Support at the URL, or and telephone number provided by Symantec during activation, or as may be set forth in the Documentation.

4. Sixty (60) Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes) at any time during the sixty (60) day period following the date of purchase.

5. 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.

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

6. Disclaimer of Damages:

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

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

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

7. U.S. Government Restricted Rights:

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

8. Export Regulation:

The Software and its related documentation, including technical data, may not be exported or re-exported in violation of the U.S. Export Administration Act, its implementing laws and regulations, the laws and regulations of other U.S. agencies, or the export and import laws of the jurisdiction in which the Software was obtained. Export to any individual, entity, or country specifically designated by applicable law is strictly prohibited.

9. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Chapter 4 Options

Chapter 5 Keeping current with LiveUpdate

Chapter 6 Guarding against intrusion attempts

Chapter 7 Customizing protection for different locations

Chapter 8 Protecting your privacy

Feature summary

1

Use the information in this section to familiarize yourself with the product.

This section includes:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

Activation protects you

Product activation is a technology that protects users from pirated or counterfeit software by limiting use of a product to those users who have acquired the product legitimately. Product activation requires a unique product key for each installation of a product. You must activate the product within 15 days of installing it.

Product activation is completely separate from registration. Your activation information and registration information reside on separate servers, with no link between the different sets of data.

When to activate your product

During installation, you are asked to enter a product key. After you have installed the product, activate it by sending the product key to the Symantec servers.

You can activate your product by clicking Activate Now in the Configuration Wizard that runs immediately after installation. If you choose not to activate at that time, you will receive *alerts* that will remind you to activate the product. You can click Activate Now in the alerts to activate the product. Activation should take just a few minutes.

⚠ If you do not activate the product within 15 days of installing it, the product will stop working. You can activate it after the 15 days have elapsed, but you will not be protected until you do.

Locate the product key

The product key can most frequently be found on a sticker on your CD sleeve. If it is not there, then it will be on an insert in your product package. If you have purchased the product on DVD, look for the sticker on your DVD package. If you have *downloaded* the product from the Symantec Store, the product key is stored on your computer as part of the download process.

Security protection features

Norton Personal Firewall includes a suite of security tools that help keep your computer safe from security threats and privacy intrusions.

Security protection features include:

Personal Firewall	The Personal Firewall protects your computer from Internet attacks, dangerous Web content, port scans, and other suspicious behavior. See "About the Personal Firewall" on page 59.
Intrusion Detection	Intrusion Detection scans each piece of information that enters and exits your computer and automatically blocks any Internet attacks. See "About Intrusion Detection" on page 71.
Network Detector	Network Detector lets you customize security settings for different networks. This makes it easy for mobile users who connect to the Internet from the road to stay protected at all times. See "Customizing protection for different locations" on page 77.
Web assistant	Web assistant lets you customize security settings for individual Web sites without leaving your browser. See "Use Web assistant" on page 36.
Privacy Control	Privacy Control gives you several levels of control over the kind of information that users can send via the Web, email, and instant messenger programs. See "Protecting your privacy" on page 83.

Ad Blocking	Ad Blocking speeds up your Web surfing by eliminating banner ads, Flash presentations, pop-up and pop-under ad windows, and other slow-loading or intrusive content. See “Blocking Internet advertisements” on page 89.
Alert Assistant	The Alert Assistant helps you understand security issues, suggests how you can resolve problems, and advises you on avoiding future security problems. See “Learn more with the Alert Assistant” on page 35.

Installing Norton Personal Firewall

2

Before installing Norton Personal Firewall, take a moment to review the system requirements.

System requirements

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

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

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

Your computer must also meet the following minimum requirements.

Operating System	Requirements
Windows 98/98SE	133 MHz or higher processor 32 MB of RAM 35 MB of available hard disk space Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) CD-ROM or DVD-ROM drive

Operating System	Requirements
Windows Me	- 150 MHz or higher processor - 48 MB of RAM - 35 MB of available hard disk space - Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) - CD-ROM or DVD-ROM drive
Windows 2000 Professional	- 133 MHz or higher processor - 64 MB of RAM - 35 MB of available hard disk space - Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) - CD-ROM or DVD-ROM drive
Windows XP Professional or Home Edition	- 300 MHz or higher processor - 128 MB of RAM - 35 MB of available hard disk space - Internet Explorer 5.01 with Service Pack 2 or later (5.5 recommended) - CD-ROM or DVD-ROM drive

Supported email and instant messenger programs

Norton Personal Firewall adds security features to the following email and instant messenger programs.

Feature	Supported programs
Email scanning	Any POP3-compatible program, including: - Microsoft Outlook Express 4.0/5.X - Microsoft Outlook 97/98/2000/XP - Netscape Messenger 4.X, Netscape Mail 6.0 - Eudora Light 3.0, Eudora Pro 4.0, Eudora 5.0
Privacy Control instant messaging scanning	- AOL Instant Messenger, version 4.3 or later - Yahoo! Messenger, version 5.0 or later - MSN Messenger and Windows Messenger, version 4.6 or later

Compatibility with other software and hardware

Norton Personal Firewall works well with Symantec pcAnywhere and most routers, Internet connection sharing programs, and popular VPNs.

Symantec pcAnywhere

See "Change an existing firewall rule" on page 68.

You should have no problems using Symantec pcAnywhere as either a client or host with Norton Personal Firewall. For maximum protection, if you run a Symantec pcAnywhere host, edit the rule to limit its use to only the computers with which you use it. Symantec pcAnywhere passwords are also necessary for maximum security.

Routers

Norton Personal Firewall adds to the protection provided by the router. In some cases, you might want to reduce the protection provided by the router so that you can use programs like NetMeeting or MSN Messenger. Norton

Personal Firewall also provides features that might not be available with cable and DSL routers, such as privacy protection.

Internet connection sharing programs

For basic protection, install Norton Personal Firewall on the gateway computer. For maximum protection against *Trojan horses* or other problem programs that initiate outbound communications, install Norton Personal Firewall on all computers that share the connection. You must have a license for each copy of Norton Personal Firewall you install.

Virtual Private Networks

Norton Personal Firewall works with the following Virtual Private Networks (VPNs):

- Symantec Enterprise VPN
- Symantec VelociRaptor
- Nortel
- VPNremote
- PGP
- SecureRemote

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

About encrypted email connections

Privacy Control does not support email connections using Secure Sockets Layer. Secure Sockets Layer (SSL) is a Netscape protocol designed to provide secure communications on the Internet. If you send email messages through your SSL connection, you are not protected by Privacy Control.

Before installation

Before you install Norton Personal Firewall, prepare your computer.

Prepare your computer

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

If you have a recent version of Norton Internet Security Professional, Norton Internet Security, or Norton Personal Firewall, the installer can import and use your current security settings. If you have an older version of these products, the installer prompts you to remove the older version.

If you're using Windows XP

Windows XP includes a firewall that can interfere with Norton Personal Firewall protection features. You must disable the Windows XP firewall before installing Norton Personal Firewall.

To disable the Windows XP firewall

1. On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel window, do one of the following:
   - In the default Category View, click **Network and Internet Connections**, then click **Network Connections**.
   - In the Classic View, double-click **Network Connections**.
3. Right-click the active connection icon, then click **Properties**.
4. In the Properties window, on the Advanced tab, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
5. Click **OK**.

Install Norton Personal Firewall

You can install Norton Personal Firewall from a CD or from a file you download. If you have not already done so, close all other Windows programs.

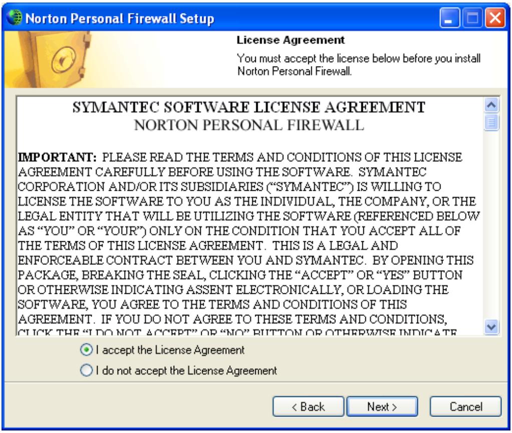
To install Norton Personal Firewall

1 Do one of the following:

See "If the opening screen does not appear" on page 25.

- If you are installing from a CD, insert the CD into the CD-ROM drive.
- If you downloaded your copy of Norton Personal Firewall, double-click the file you downloaded, then click **Install**.

2 In the Norton Personal Firewall window, click **Install Norton Personal Firewall**.



License Agreement

You must accept the license below before you install Norton Personal Firewall.

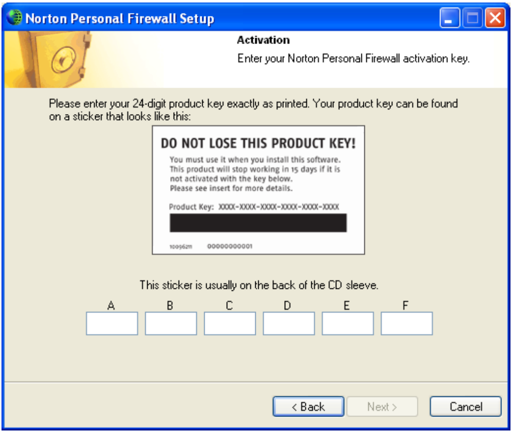
SYMANTEC SOFTWARE LICENSE AGREEMENT
NORTON PERSONAL FIREWALL

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

● I accept the License Agreement
○ I do not accept the License Agreement

3 Read the License Agreement, then click **I accept the License Agreement**.
If you decline, you cannot continue with the installation.

4 Click **Next**.



Activation

Enter your Norton Personal Firewall activation key.

Please enter your 24-digit product key exactly as printed. Your product key can be found on a sticker that looks like this:

DO NOT LOSE THIS PRODUCT KEY!

You must use it when you install this software.
This product will stop working in 15 days if it is not activated with the key below.
Please see insert for more details.

Product Key: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX

[redacted]

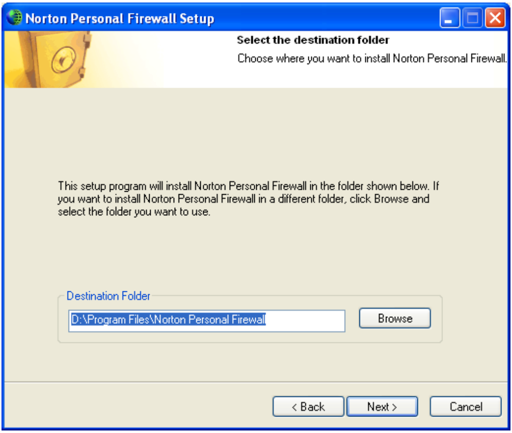
100962m 00000000001

This sticker is usually on the back of the CD sleeve.

See "When to activate your product" on page 14.

5 In the text boxes, type the product key for activation.

6 Click **Next**.



Select the destination folder

Choose where you want to install Norton Personal Firewall.

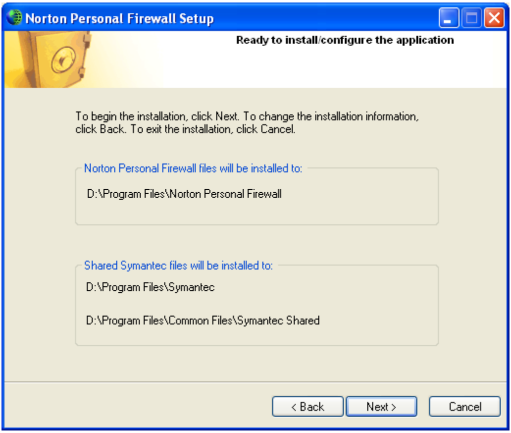
This setup program will install Norton Personal Firewall in the folder shown below. If you want to install Norton Personal Firewall in a different folder, click Browse and select the folder you want to use.

Destination Folder

D:\Program Files\Norton Personal Firewall

7 Click **Browse** to select a folder into which you want to install Norton Personal Firewall, if it is other than the default location.

8 Click **Next**.



Norton Personal Firewall Setup
Ready to install/configure the application

To begin the installation, click Next. To change the installation information, click Back. To exit the installation, click Cancel.

Norton Personal Firewall files will be installed to:

D:\Program Files\Norton Personal Firewall

Shared Symantec files will be installed to:

D:\Program Files\Symantec

D:\Program Files\Common Files\Symantec Shared

9 Confirm the installation location, then click **Next** to install Norton Personal Firewall.
The Norton Personal Firewall Setup window displays installation progress. Depending on your computer system speed, this can take a few minutes.

10 After Norton Personal Firewall is installed, read the readme text, then click **Next**.

11 Do one of the following:

- To restart your computer now, click **Restart Now (recommended)**.
- To restart your computer later, click **Restart Later**.
  Your computer is not protected until you restart.

12 Click **Finish**.

If the opening screen does not appear

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

To start the installation from the Norton Personal Firewall CD

1. On your desktop, double-click **My Computer**.
2. In the My Computer window, double-click the icon for your CD-ROM drive.
3. In the list of files, double-click **Cdstart.exe**.

After installation

After Norton Personal Firewall is installed and you have restarted your computer, the Information Wizard appears.

Use the Information Wizard

The Information Wizard lets you activate your copy of Norton Personal Firewall, get information about updates, select post-installation tasks to be done automatically, and review your security settings.

If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register by using the Product Registration option on the Help menu or by using the Symantec Web site at www.symantec.com. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

1 In the welcome window, click **Next**.

You must activate the software within 15 days.

See "When to activate your product" on page 14.

2 On the Product Activation window, click **Activate and register your product now**.

3 Click **Next**.

4 Make sure that your computer is connected to the Internet, then click **Next**.

5 If you purchased your computer with Norton Personal Firewall already installed, you must accept the license agreement in order to use Norton Personal Firewall. Click **I accept the license agreement**, then click **Next**.

6 In the first Registration window, select the Country/ Region from which you are registering.

7 If you would like information from Symantec about Norton Personal Firewall, check the method by which you want to receive that information, type the corresponding address and phone number, then click **Next**.

8 Check if you would like to receive postal mail from Symantec.

9 Type your name and address, then click **Next**.

10 Make sure your computer is connected to the Internet, then click **Next** to activate.

11 Click **Finish**.

12 Select the post-installation tasks that you want Norton Personal Firewall to perform automatically. Your options are:

Set up Privacy Control	Identify the information you want Privacy Control to protect. See "Identify private information to protect" on page 83.
Run LiveUpdate	Ensure that you have the latest security updates. See "Keeping current with LiveUpdate" on page 51.

13 Click **Next**.

14 Review the post-installation tasks and configuration settings for Norton Personal Firewall.
If you want to change any of the settings, do so using Options.

15 Click **Finish**.

If you selected any post-installation tasks, they start automatically.

If you need to uninstall Norton Personal Firewall

If you need to remove Norton Personal Firewall from your computer, use the Add/Remove Programs option from the Windows Control Panel.

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

To uninstall Norton Personal Firewall

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **Norton Personal Firewall**.
4. Do one of the following:
   - In Windows 2000/Me, click **Change/Remove**.
   - In Windows 98, click **Add/Remove**.
   - In Windows XP, click **Change**.
5. Click **Remove All**.
6. If you plan to reinstall Norton Personal Firewall, check **Save my settings**.
   This saves a copy of your current security settings. You can then import these settings to restore your protection.
7. Click **Next**.

8 In the Norton Personal Firewall has been successfully removed window, do one of the following:
   - To restart your computer now, click **Restart Now (recommended)**.
   - To restart your computer later, click **Restart Later**.
     Norton Personal Firewall is not fully uninstalled until you restart your computer.

9 Click **Finish**.

Basics

3

Basics include general information about how to:

- Work with your Symantec product.
- Keep your computer protected.
- Customize options.
- Monitor protection activities.
- Access more information.

Check the version number

You can check the version number of your product on your computer. Use the version number to help you find more information about your product on the Symantec Web site.

To check the version number

1. Start your product.
2. Click **Help and Support**.
3. On the Help menu, click **About <your product name>**.
4. In the About dialog box, select your product name.

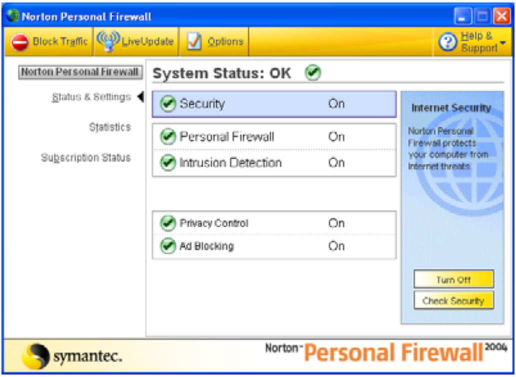
Start Norton Personal Firewall

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

To start Norton Personal Firewall

❖ Do one of the following:

- On the Windows taskbar, click **Start** > **Programs** > **Norton Personal Firewall** > **Norton Personal Firewall**.
- On the Windows XP taskbar, click **Start** > **All Programs** > **Norton Personal Firewall** > **Norton Personal Firewall**.
- On the Windows desktop, double-click **Norton Personal Firewall**.



System Status: OK ✓

✓ Security	On
✓ Personal Firewall	On
✓ Intrusion Detection	On
✓ Privacy Control	On
✓ Ad Blocking	On

Norton Personal Firewall protects your computer from Internet threats.

Use the Norton Personal Firewall tray icon

Norton Personal Firewall adds an icon to the Windows system tray at the end of the Windows taskbar. Use this icon as a shortcut to open Norton Personal Firewall, block all Internet traffic, turn off all Norton Personal Firewall protection features, and learn more about Norton Personal Firewall.

See "About General options" on page 49.

You can also use the Norton Personal Firewall Options to add additional tools to the menu.

To use the Norton Personal Firewall tray icon

1. In the Windows system tray, right-click the Norton Personal Firewall icon.
2. On the tray icon menu, select the option you want. Your options are:

Norton Personal Firewall	Opens the Norton Personal Firewall main window
Block Traffic	Immediately stops all Internet communication
About Norton Personal Firewall	Displays more information about Norton Personal Firewall
LiveUpdate	Lets you update your protection
Help	Opens the online Help
Disable	Stops Norton Personal Firewall from protecting your computer

Use Web assistant from the Internet Explorer toolbar

See "Use Web assistant" on page 36.

Norton Personal Firewall now includes Web assistant, which lets you quickly access security settings without leaving your Web browser.

Activate your product

Product activation reduces software piracy and ensures that you have received genuine Symantec software.

You must activate your product within 15 days of installing it or the product will stop working.

If you did not activate your product using the Configuration Wizard, you will receive an Activation Needed *alert* every day until you activate the product.

You can activate your product from the Activation Needed alert or from the Activation option on the Help menu. Activation should take just a few minutes.

To activate your product from the Activation Needed alert

1. In the alert, click **Activate Now**.
2. Click **OK**.
3. On the Activation screen, click **Next**.
4. On the Activation Successful screen, click **Finish**.

To activate your product from the Help menu

1. At the top of the main window, click **Help and Support** > **Activation**.
2. On the Activation screen, click **Next**.
3. On the Activation Successful screen, click **Finish**.

Respond to Norton Personal Firewall alerts

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

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

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

See "Customizing protection for different locations" on page 77.

The first alert most people will receive is a New Location Alert. This alert appears every time your computer joins a network that Network Detector does not recognize. You will likely receive a New Location Alert the first time you go online after installing Norton Personal Firewall.

Learn more with the Alert Assistant

Each Norton Personal Firewall *alert* includes a link to the Alert Assistant. The Alert Assistant includes customized information about each alert, including:

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

To use the Alert Assistant

1 In any alert, click **Alert Assistant**.

2 In the Alert Assistant window, review the information about the alert.

3 To respond to the alert, close the Alert Assistant.

Use Web assistant

Web assistant lets you customize Ad Blocking and Privacy Control settings for individual Web sites without leaving your browser. Web assistant adds a button to your Microsoft Internet Explorer toolbar that gives you fast access to Ad Blocking, Privacy Control, and the Norton Personal Firewall main window.

The Web assistant menu includes the following tasks.

Block cookies on this site	Prevents this site from setting or reading cookie files
Block ads on this site	Removes ad images from pages on this site
Block popups on this site	Prevents this site from opening unrequested browser windows
Open Ad Trashcan	Opens the Ad Trashcan, which lets you choose the ads you want to block
Configure security settings	Opens the main Norton Personal Firewall window

After installing Norton Personal Firewall, the Web assistant button appears in your Internet Explorer toolbar. If you have locked your toolbars, the Web assistant button may be hidden.

To view or hide Web assistant

❖ In Microsoft Internet Explorer, right-click the toolbar, then click **Web assistant**.

Check your computer's vulnerability to attack

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

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

To check your computer's vulnerability to attack

1. In the main window, click **Security**.
2. Click **Check Security**.
3. On the Security Check Web page, click **Scan for Security Risks**.
4. To learn more about the Security Check tests, click **About Scan for Security Risks**.

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

To get more information about an at-risk area

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

Identify the source of Internet traffic

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

You can trace connection attempts from the following locations:

- Statistics window
- AutoBlock
- Alerts

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

To trace a connection attempt from the Statistics window

1. In the main window, click **Statistics**.
2. Click **Attacker Details**.
   Your browser opens the Visual Tracking Web page.

To trace a connection attempt from AutoBlock

1. In the main window, double-click **Intrusion Detection**.
2. In the Intrusion Detection window, under AutoBlock, select a connection you want to trace.
3. Click **Attacker Details**.
   Your browser opens the Visual Tracking Web page.

To trace a connection attempt from the Alert Assistant

1. In a security alert, click **Alert Assistant**.
2. Click the IP address of the attacking computer.
   Your browser opens the Visual Tracking Web page.

Stop all Internet communication

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

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

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

Block Traffic is meant to be used as a temporary measure while you address a security problem. If you restart your computer, Norton Personal Firewall automatically allows all incoming and outgoing communication.

To stop all Internet communication using Block Traffic

1. In the main window, click **Block Traffic**.
2. Use Norton Personal Firewall tools to address the security problem.
3. When you have fixed the problem, click **Allow Traffic**.

Manage advertising filters

Ad Blocking can block several kinds of ads that appear on Web sites while you are browsing the Internet.

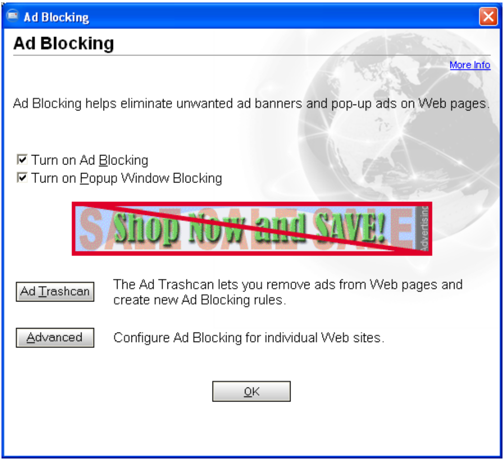
Enable or disable Ad Blocking

Ad Blocking compares the addresses of ads that are being downloaded by your browser with its own list of ads to block. If it finds a match, it removes the ad so that it does not appear in your browser, leaving the rest of the Web page intact.

Sometimes you may want to view ads that have been blocked. In this case, you can temporarily disable Ad Blocking.

To enable or disable Ad Blocking

1 In the main window, double-click **Ad Blocking**.



Ad Blocking helps eliminate unwanted ad banners and pop-up ads on Web pages.

☑ Turn on Ad Blocking

☑ Turn on Popup Window Blocking

The Ad Trashcan lets you remove ads from Web pages and create new Ad Blocking rules.

Configure Ad Blocking for individual Web sites.

2 In the Ad Blocking window, check or uncheck **Turn on Ad Blocking**.

3 Click **OK**.

Enable or disable Popup Window Blocking

Pop-up and pop-under ads are secondary windows that Web sites open when you visit or leave the sites. Pop-ups appear on top of the current window, while pop-unders appear behind the current window.

When Popup Window Blocking is enabled, Ad Blocking automatically blocks the programming code Web sites use to open secondary windows without your knowledge. Sites that open secondary windows when you click a link or perform other actions are not affected.

In some cases, you may want to view pop-up windows on a site. In this case, you can temporarily disable Popup Window Blocking.

To enable or disable Popup Window Blocking

1. In the main window, double-click **Ad Blocking**.
2. In the Ad Blocking window, check or uncheck **Turn on Popup Window Blocking**.
3. Click **OK**.

Temporarily disable Norton Personal Firewall

There may be times when you want to temporarily disable Norton Personal Firewall or one of its features. For example, you might want to see if Norton Personal Firewall is preventing a Web page from appearing correctly.

Disabling Norton Personal Firewall also disables all of the individual features.

To temporarily disable Norton Personal Firewall

1. In the main window, click **Security**.
2. In the lower-right corner of the window, click **Turn Off**.

Norton Personal Firewall is automatically turned back on the next time that you start your computer.

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

To disable a protection feature

1. In the main window, select the feature that you want to disable.
2. In the lower-right corner of the window, click **Turn Off**.

For more information

The product documentation provides glossary terms, online Help, a Readme file, the User's Guide in PDF format, and links to the Knowledge Base on the Symantec Web site.

Look up glossary terms

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

Use online Help

Help is available throughout your Symantec product. Help buttons or links to more information provide information that is specific to the task that you are completing. The Help menu provides a comprehensive guide to all of the product features and tasks that you can complete.

To use online Help

1. At the top of the main window, click **Help & Support** > **Norton Personal Firewall**.
2. In the Help window, in the left pane, select a tab. Your options are:

Contents	Displays the Help by topic
Index	Lists Help topics in alphabetical order by key word
Search	Opens a search field in which you can enter a word or phrase

Window and dialog box Help

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

To access window or dialog box Help

❖ Do one of the following:

- In the window, click any available Help link.
- In the dialog box, click **Help**.

Readme file

The Readme file contains information about installation and compatibility issues. It also contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the product files.

To read the Readme file

1. In Windows Explorer, double-click **My Computer**.
2. Double-click the hard disk on which you installed Norton Personal Firewall.
   In most cases, this will be drive C.
3. Click **Program Files** > **Norton Personal Firewall**.
4. Double-click **Readme.txt**.
   The file opens in Notepad or your default word processing program.
5. Close the word processing program when you are done reading the file.

Access the User's Guide PDF

The *Norton Personal Firewall User's Guide* is provided on the CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.

If you purchased this product as an electronic download, Adobe Acrobat Reader was not included. You must download it from the Adobe Web site.

To install Adobe Acrobat Reader

1. Insert the CD into the CD-ROM drive.
2. Click **Browse CD**.
3. In the CD window, double-click the **Manual** folder.

4 Double-click the program file.

5 Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

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

If you do not have a CD, you can download the PDF from the Symantec Service & Support Web site.

To read the User's Guide PDF from the CD

1 Insert the CD into the CD-ROM drive.

2 Click **Browse CD**.

3 Double-click the **Manual** folder.

4 Double-click **NPF.pdf**.

You can also copy a User's Guide to your hard disk and read it from there.

To read a User's Guide from your hard disk

1 Open the location into which you copied the PDF.

2 Double-click the PDF.

Symantec products on the Web

The Symantec Web site provides extensive information about all Symantec products. There are several ways to access the Symantec Web site.

To access the Web site from the Help menu

❖ Select the solution that you want. Your options are:

Symantec Security Response	Takes you to the Security Response page of the Symantec Web site, from which you can update your protection and read the latest information about antithreat technology.
More Symantec solutions	Takes you to the Symantec Store Web site, from which you can get product information on every Symantec product.

To access the Symantec Web site in your browser

❖ On the Internet, go to www.symantec.com

Subscribe to the Symantec Security Response newsletter

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

To subscribe to the Symantec Security Response newsletter

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

Options

4

The default settings for this product provide complete protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply. You can change the product's settings to fit your work environment.

If you are using Windows 2000/XP, you will need administrator access to change options. If you are an administrator and share your computer with others, keep in mind that the changes that you make apply to everyone using the computer.

Set Norton Personal Firewall options

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

To change settings for individual features

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

The default Norton Personal Firewall settings should provide adequate protection for most users. If you need to make changes, use the Options menu to access Norton Personal Firewall options. The options let you control more advanced settings.

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

To customize Norton Personal Firewall

1. At the top of the main window, click **Options**.
2. Select the tab on which you want to change options. Your options are:

General	See "About General options" on page 49.
LiveUpdate	See "About LiveUpdate options" on page 49.
Firewall	See "About Firewall options" on page 49.
Email	See "About Email options" on page 49.

About General options

See "Password protect Norton Personal Firewall options" on page 49.

General options let you control when Norton Personal Firewall starts, protect program settings with a password, and choose visual elements you want to display.

About LiveUpdate options

See "Keeping current with LiveUpdate" on page 51.

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

You can choose the components you want Automatic LiveUpdate to monitor. You can also choose whether Automatic LiveUpdate updates the components in the background or alerts you that there are updates available.

About Firewall options

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

About Email options

Email options let you control how Norton Personal Firewall notifies you when it is scanning email messages for private information.

Password protect Norton Personal Firewall options

You can protect Norton Personal Firewall options with a password. This lets you control who can make changes to your protection.

To protect security options with a password

1. At the top of the main window, click **Options**.
2. On the General tab, check **Turn on Password Protection**.
3. In the Password and Confirm Password text boxes, type a password.
4. Click **OK**.

Reset options password

If you forget your options password, you can reset it.

To reset your security options password

1. Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **Norton Personal Firewall**.
4. Do one of the following:
   - In Windows 2000/Me, click **Change/Remove**.
   - In Windows 98, click **Add/Remove**.
   - In Windows XP, click **Change**.
5. In the Remove Application window, click **Reset Password**.
6. In the password reset dialog box, in the Reset Password Key text box, type the Reset Password Key that appears above the text box.
   The Reset Password Key is case-sensitive.
7. In the New Password and Confirm New Password text boxes, type a new password.
8. Click **OK**.
9. In the Remove Application window, click **Cancel**.
10. In the Exit? alert, click **Yes**.

Keeping current with LiveUpdate

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

Your normal Internet access fees apply when you use LiveUpdate.

If your computer uses Windows 2000/XP, you must have Administrator *access privileges* to run LiveUpdate.

About program updates

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

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

About protection updates

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

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

Obtain updates using LiveUpdate

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

If your *Internet service provider* does not automatically connect you to the Internet, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. At the top of the main window, click **LiveUpdate**.
2. In the LiveUpdate window, click **Next** to locate updates.
3. If updates are available, click **Next** to download and install them.
4. When the installation is complete, click **Finish**.

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

When you should update

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

If you can’t use LiveUpdate

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

To obtain updates from the Symantec Web site

1. On the Internet, go to securityresponse.symantec.com
2. Follow the links to obtain the type of update that you need.

Set LiveUpdate to Interactive or Express mode

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

To set LiveUpdate to Interactive or Express mode

1. At the top of the main window, click **LiveUpdate**.
2. In the LiveUpdate welcome screen, click **Configure**.
3. In the LiveUpdate Configuration dialog box, on the General tab, select the mode that you want. Your options are:

Interactive Mode	Gives you the option of choosing which updates you want to install
Express Mode	Automatically installs all available updates

4. If you selected Express Mode, select how you want to start checking for updates. Your options are:

I want to press the start button to run LiveUpdate	Gives you the option of cancelling the update
I want LiveUpdate to start automatically	Installs updates automatically whenever you start LiveUpdate

5 To have access to a Symantec self-help Web site in the event that an error occurs while using LiveUpdate, check **Enable Enhanced Error Support**.

6 Click **OK**.

Turn off Express mode

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

To turn off Express mode

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

Run LiveUpdate automatically

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

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

To enable Automatic LiveUpdate

1. At the top of the main window, click **Options**.
   If you set a password for Options, you must provide the password before you can continue.
2. In the Options dialog box, on the LiveUpdate tab, check **Enable Automatic LiveUpdate**.
3. If you want to be notified when updates are available, check **Notify me when Norton Personal Firewall updates are available**.
4. Select the updates for which you want Automatic LiveUpdate to check.

5 For each type of update for which you want Automatic LiveUpdate to check, select how you want those updates to be applied. Your options are:

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

6 Click **OK**.

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

To disable Automatic LiveUpdate

1 At the top of the main window, click **Options**.
If you set a password for Options, you must provide the password before you can continue.

2 In the Options dialog box, on the LiveUpdate tab, uncheck **Enable Automatic LiveUpdate**.

3 Click **OK**.

About your subscription

See "About protection updates" on page 52.

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

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates through LiveUpdate or from the Symantec Web site and will not be protected against newly discovered *threats*. Also, whenever you use LiveUpdate, you will receive a warning that your subscription has expired. Follow the on-screen instructions to complete your subscription renewal.

Guarding against intrusion attempts

6

The Personal Firewall and Intrusion Detection features protect your computer from online attacks, unwanted connection attempts, malicious Web content, port scans, and other suspicious behavior.

About the Personal Firewall

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

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

See "Customize firewall protection" on page 60.

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

Customize firewall protection

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

Change the Security Level

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

To change the Security Level

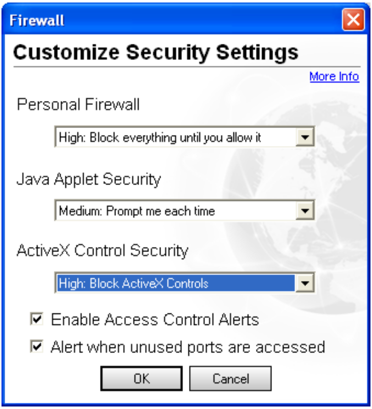
1. In the main window, double-click **Personal Firewall**.
2. Move the slider to the Security Level that you want. Click **OK**.

Change individual security settings

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

To change individual security settings

1. In the main window, double-click **Personal Firewall**.
2. Click **Custom Level**.



Personal Firewall: High: Block everything until you allow it

Java Applet Security: Medium: Prompt me each time

ActiveX Control Security: High: Block ActiveX Controls

☑ Enable Access Control Alerts

☑ Alert when unused ports are accessed

3. Do one or more of the following:
   - In the Personal Firewall drop-down list, select a level.
   - In the Java Applet Security or ActiveX Control Security drop-down list, select a level.
   - To be notified whenever unknown programs access the Internet, check **Enable Access Control Alerts**.
   - To be notified whenever a remote computer attempts to connect to a port no program is using, check **Alert when unused ports are accessed**.
4. Click **OK**.

Allow or block access to your computer

Norton Personal Firewall allows you to organize computers on your home network and the Internet into Trusted and Restricted Zones. Zones allow you to grant trusted computers more access to your computer while blocking malicious users.

Computers in the Trusted Zone are not regulated by the Personal Firewall. They have as much access to your computer as they would have if you did not have a firewall. Computers in the Restricted Zone cannot communicate with your computer at all.

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

To categorize computers with the Home Network Wizard

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Networking tab, click **Wizard**.
3. In the Home Network Wizard opening window, click **Next**.
4. In the resulting list, check the network adapters that you want to configure automatically and add to your Trusted Zone.
5. Click **Next**.
6. Click **Finish** to close the wizard.

To manually add computers to zones

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Networking tab, select the zone to which you want to add a computer.
3. If you have turned on Network Detector, select the Location you want to customize.
4. Click **Add**.
5. In the Specify Computers window, identify the computer.
6. When you have finished adding computers, click **OK**.

See "Identify computers to Norton Personal Firewall" on page 69.

To remove computers from zones

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Networking tab, select the zone containing the computer you want to remove.

3 If you have turned on Network Detector, select the Location you want to customize.

4 Select the computer that you want to remove.

5 Click **Remove**.

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

Customize firewall rules

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

How firewall rules are processed

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

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

If no matching rule is found, the communication is blocked.

Create new firewall rules

Program Control, helps you create firewall rules as you use the Internet.

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

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

Enable Automatic Program Control

Automatic Program Control automatically configures Internet access settings for programs the first time that they run. Automatic Program Control only configures Internet access for the versions of programs that Symantec has identified as safe.

When Automatic Program Control configures access for a new program, Norton Personal Firewall displays a message above the Windows toolbar.

If an unknown program or an unknown version of a known program attempts to access the Internet, you receive an alert. You can then choose to allow or block Internet access for the program.

To enable Automatic Program Control

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Programs tab, select the Location you want to customize.

3. Check **Turn on Automatic Program Control**.
4. Click **OK**.

Scan for Internet-enabled programs

Scanning for Internet-enabled programs lets you quickly customize Internet access for multiple programs. Program Scan scans the computer for programs that it recognizes and suggests appropriate settings for each program.

To scan for Internet-enabled programs

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Programs tab, click **Program Scan**.
3. Select the disk or disks on your computer that you want to scan.
4. Click **Next**.
5. In the Program Scan window, review the list of Internet-enabled programs that Program Scan identified.
6. Do one of the following:
   - Check the boxes next to the programs you want to configure.
   - To customize the Internet access settings Program Scan suggested for a program, select it, then click **Modify**.
   - To leave a program unconfigured, uncheck the box next to the program. You will receive an alert the next time this program accesses the Internet.
7. Click **Next**.
8. If you have turned on Network Detector, select the Locations that should use these settings.
9. Click **Finish**.
10. Click **OK**.

Manually add a program to Program Control

See "Customize firewall protection" on page 60.

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

To add a program to Program Control

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Programs tab, select the Location you want to customize.
3. Click **Add**.
4. Select the program's executable file.
   Executable file names typically end in .exe.
5. Click **Open**.
6. In the Program Control alert, select the access level you want this program to have.
7. To see risks that this program could pose to your computer, click **Show Details**.
8. Click **OK**.

Customize Program Control

After using Norton Personal Firewall for a while, you may find that you need to change access settings for certain programs.

To customize Program Control

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Programs tab, select the Location you want to customize.
3. In the list of programs, click the program that you want to change.
4. Click **Modify**.
5. In the Program Control alert, select the access level you want this program to have.
6. Click **OK**.

Manually add a firewall rule

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

There are three sets of firewall rules you can customize:

- General Rules
- Trojan Horse Rules
- Program Rules

To add a General Rule

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Advanced tab, click **General**.
3. Follow the on-screen instructions.

To add a Trojan Horse Rule

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Advanced tab, click **Trojan Horse**.
3. Follow the on-screen instructions.

To add a Program Rule

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Programs tab, in the list of programs, click **Add**.
3. In the Select a program window, select a program's executable file.
   Executable file names typically end in .exe.
4. In the Program Control alert, on the What do you want to do menu, click **Manually configure Internet access**.
5. Follow the on-screen instructions.

Change an existing firewall rule

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

To change an existing firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, select the rule that you want to change.
   If you have turned on Network Detector, select the Location that should use the modified rule.
2. Click **Modify**.
3. Follow the on-screen instructions to change any aspect of the rule.
4. When you have finished changing rules, click **OK**.

Change the order of firewall rules

See "How firewall rules are processed" on page 63.

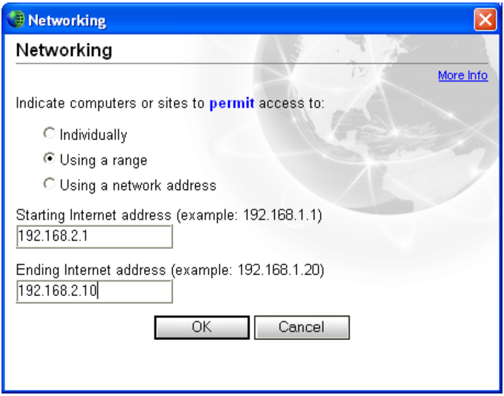
Each list of firewall rules is processed from the top down. You can adjust how firewall rules are processed by changing their order.

To change the order of a firewall rule

1. In the General Rules, Trojan Horse Rules, or Program Rules window, select the rule that you want to move.
   If you have turned on Network Detector, select the Location that should use the modified rule.
2. Do one of the following:
   - To process this rule before the rule above it, click **Move Up**.
   - To process this rule after the rule below it, click **Move Down**.
3. When you are done moving rules, click **OK**.

Identify computers to Norton Personal Firewall

You must identify computers to Norton Personal Firewall to manually configure zones and firewall rules. In these cases, a dialog box appears to help you identify the computer.


Networking

Networking

Indicate computers or sites to **permit** access to:

○ Individually
● Using a range
○ Using a network address

Starting Internet address (example: 192.168.1.1)
192.168.2.1

Ending Internet address (example: 192.168.1.20)
192.168.2.10

There are three ways to identify computers. Each uses *IP addresses*.

Specify an individual computer

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

To specify an individual computer

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

Specify a range of computers

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

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

To specify a range of computers

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

Specify computers using a network address

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

To specify computers using a network address

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

About Intrusion Detection

Intrusion Detection scans all the network traffic that enters and exits your computer and compares this information against a set of attack signatures, arrangements of information that identify an attacker's attempt to exploit a known operating system or program vulnerability.

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

Intrusion Detection protects your computer against most common Internet attacks, including the following.

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

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

See "Keeping current with LiveUpdate" on page 51.

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

Customize Intrusion Detection

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

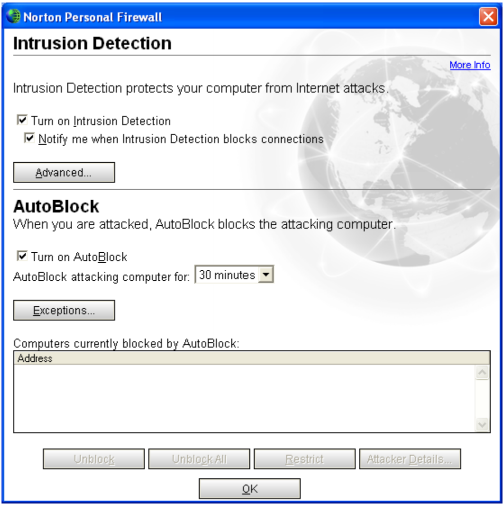
Turn Intrusion Detection alerts on and off

See "Identify the source of Internet traffic" on page 37.

You can choose whether you want to receive alerts when Intrusion Detection blocks suspected attacks. The alerts include more information about the attacking computer and information about the attack. You can also trace the connection attempt using Visual Tracking.

To turn Intrusion Detection alerts on and off

1 In the main window, double-click **Intrusion Detection**.



Norton Personal Firewall

Intrusion Detection

Intrusion Detection protects your computer from Internet attacks.

☑ Turn on Intrusion Detection

☑ Notify me when Intrusion Detection blocks connections

AutoBlock

When you are attacked, AutoBlock blocks the attacking computer.

☑ Turn on AutoBlock

AutoBlock attacking computer for: 30 minutes

Computers currently blocked by AutoBlock:

Address

2 In the Intrusion Detection window, check or uncheck **Notify me when Intrusion Detection blocks connections**.

3 Click **OK**.

Exclude specific network activity from being monitored

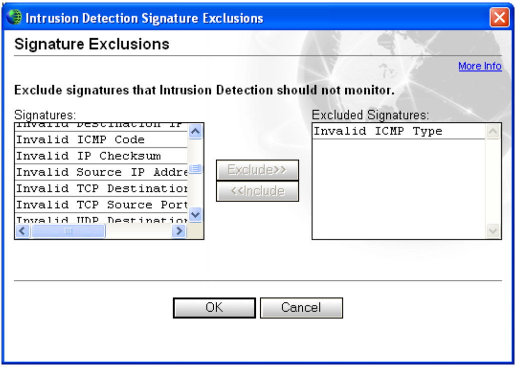
In some cases, benign network activity may appear similar to an attack signature. If you receive repeated warnings about possible attacks, and you know that these warnings are being triggered by safe behavior, you can create an exclusion for the attack signature that matches the benign activity.

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

To exclude attack signatures from being monitored

1 In the main window, double-click **Intrusion Detection**.

2 In the Intrusion Detection window, click **Advanced**.



Intrusion Detection Signature Exclusions

Signature Exclusions

Exclude signatures that Intrusion Detection should not monitor.

Signatures:

```
Invalid Destination IP
Invalid ICMP Code
Invalid IP Checksum
Invalid Source IP Addre
Invalid TCP Destinatior
Invalid TCP Source Port
Invalid UDP Destinatior
```

Excluded Signatures:

```
Invalid ICMP Type
```

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

4 Click **Exclude**.

5. When you are done excluding signatures, click **OK**.
6. In the Intrusion Detection window, click **OK**.

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

To include attack signatures

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

Enable or disable AutoBlock

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

If AutoBlock is blocking a computer or computers you need to access, you can turn off AutoBlock. Make sure to turn AutoBlock back on when you are done.

To turn AutoBlock on and off

1. In the main window, double-click **Intrusion Detection**.
2. In the Intrusion Detection window, check or uncheck **Turn on AutoBlock**.
3. Click **OK**.

By default, AutoBlock blocks each computer for 30 minutes. Use the drop-down menu to choose how long you want to block attacking computers.

To customize the AutoBlock duration

1. In the main window, double-click **Intrusion Detection**.
2. In the Intrusion Detection window, under AutoBlock, on the AutoBlock attacking computer for menu, select a new duration.
3. Click **OK**.

See "Stop all Internet communication" on page 38.

AutoBlock stops all inbound communications with a specific computer. To stop all inbound and outbound communication with all computers, use Block Traffic.

Unblock AutoBlocked computers

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

To unblock computers currently blocked by AutoBlock

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

Exclude computers from AutoBlock

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

To exclude specific computers from AutoBlock

1. In the main window, double-click **Intrusion Detection**.
2. In the Intrusion Detection window, click **Exceptions**.

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

Restrict a blocked computer

You can add a blocked computer to your Restricted Zone to permanently prevent that computer from accessing your computer. Computers in the Restricted Zone do not appear on the blocked list because all communication with restricted computers is blocked.

To restrict a blocked computer

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

Customizing protection for different locations

7

Use Network Detector to create and customize security settings for different networks. This makes it easy for mobile users who connect to the Internet from the road to stay protected at all times.

About Network Detector

Network Detector lets you customize Program Control and Trusted Zone settings for different locations. A location is a group of security settings that can contain one or more networks.Whenever your computer connects to a network in one of these locations, Norton Personal Firewall automatically switches to the security settings that are associated with that location.

For example, if you use your laptop to connect to the Internet from home, from work, and from a neighborhood coffeehouse, you are actually connecting to at least three different networks. If you want the same level of security in both your home and office, you could place both networks in a single location. If you want more security in the coffeehouse, you can create a high-security location for that network.

Norton Personal Firewall includes four preconfigured locations.

Office	Low security. Primarily for use on networks containing a hardware firewall.
Home	Medium security. Good for general use.
Away	High security. Primarily for use on public networks.
Default	Security level is based on your current settings.

Create a new location

You can also create new locations with customized settings and names. For example, you could create a low-security Hotels location you use while traveling and a high-security Coffeehouse location for wireless networks provided by many coffeehouses.

If you regularly switch between several networks, you may find that this gives you more control over your protection.

You can create a new location from a Network Detector alert and from the main Norton Personal Firewall window.

To create a new location from a Network Detector alert

1. In the Network Detector alert, on the Which location do you want to use menu, select **Use custom settings**.
2. In the Use Custom Settings window, click **Create new location**.
3. Click **Next**.

4. In the Setup Program Control window, do one of the following:
   - Click **Yes (recommended)** to turn on Automatic Program Control.
     This reduces the number of alerts that you receive.
   - Click **No** to turn off Automatic Program Control.
     You will be alerted the first time that programs attempt to connect to the Internet.
5. Click **Next**.
6. In the Save location window, type a name for this new location.
   Choose a unique name so that this location is easy to identify.
7. Click **Next**.
8. In the Save location window, review this location's settings.
9. Click **Finish**.

To create a new location from the main window

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Locations tab, click **Wizard**.
3. In the Setup Program Control window, do one of the following:
   - Click **Yes (recommended)** to turn on Automatic Program Control.
     This reduces the number of alerts that you receive.
   - Click **No** to turn off Automatic Program Control.
     You will be alerted the first time that programs attempt to connect to the Internet.
4. Click **Next**.
5. In the Save location window, type a name for this new location.
   Choose a unique name so that this location is easy to identify.
6. Click **Next**.
7. In the Save location window, review this location's settings.
8. Click **Finish**.

To add new networks to locations

Network Detector alerts you every time that your computer connects to an unrecognized network. You can choose to place this network in an existing location or create a new location.

To add a new network to one of the preconfigured locations

❖ In the Network Detector alert, on the Which location do you want to use menu, select a location.

To create a new location for this network

1. In the Network Detector alert, on the Which location do you want to use menu, click **Use custom settings**.
2. Use the Network Detector Wizard to create a new location.

See "Create a new location" on page 78.

To add a new network to a custom location that you have created

1. In the Network Detector alert, on the Which location do you want to use menu, click **Use custom settings**.
2. In the Use custom settings window, on the Choose a location drop-down menu, select the location that you want to use.
3. Click **Finish**.

Learn more about networks

Network Detector alerts include detailed information about networks that your computer joins. The details section of a Network Detector alert includes information about the following.

Gateway MAC id	The Media Access Control (MAC) address of this network's router
Gateway IP address	The IP address of this network's router
Subnet identifier	The subnet mask used on this network
Interface type	How your computer is connected to this network

Interface connection description	Information about the network adapter that made the connection
Domain	This network's domain name (if available)

To learn more about networks

❖ In the Network Detector alert, click **Show details**.

Customize a location's settings

You can customize the Program Control and Trusted Zone settings for the predefined locations and any new locations that you create. Any changes that you make will apply to all of the networks that use the location.

To customize a location's settings

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, do one of the following:
   - To change Automatic Program Control settings, click the **Programs** tab.
   - To change Trusted Zone settings, click the **Networking** tab.
3. In the Settings for menu, select the location you want to customize.
4. When you are finished making changes, click **OK**.

Remove networks from a location

If you've added a network to a location, you will not be alerted the next time your computer joins that network. If you want to change a network's security settings, you must clear the location that contains it. The next time that you use a network that had been in this location, Network Detector will ask you to choose a new location.

To clear networks from a location

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Location tab, in the list of locations, select the location that you want to clear.
3. Click **Clear**.
4. When you are finished clearing networks, click **OK**.

Delete a location

If you no longer need a location, or if you want to reassign the networks in a location, delete the location. The next time that you use a network that had been in this location, Network Detector will ask you to choose a new location.

You cannot delete the preconfigured Home, Office, Away, or Default locations.

To delete a location

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Locations tab, in the list of locations, select the location that you want to delete.
3. Click **Delete**.
4. When you are finished deleting locations, click **OK**.

Protecting your privacy

8

Every time that you browse the Internet, computers and Web sites collect information about you. Some of this information comes from forms that you fill out and choices that you make. Other information comes from your browser, which automatically provides information about the Web page you last visited and the type of computer that you're using.

Computers include some basic security features, but they might not be enough to protect your personal information. Privacy Control helps protect your privacy by giving you several levels of control over *cookies* and other information that your browser sends to Web sites.

Identify private information to protect

Many Web sites ask for your name, email address, and other personal information. While it is generally safe to provide this information to large, reputable sites, malicious sites can use this information to invade your privacy. It is also possible for people to intercept information sent via the Web, email, and instant messenger programs.

Privacy Control lets you create a list of information that you want to remain private. If someone attempts to send protected information over the Internet, Privacy Control warns them about the security risk or blocks the connection.

Add private information

You must add information that you want to protect to the Privacy Control Private Information list.

To add private information

1. In the main window, double-click **Privacy Control**, then click **Private Information**.
2. In the Private Information dialog box, click **Add**.
3. In the Add Private Information dialog box, under Type Of Information To Protect, select a category.
4. In the Descriptive Name text box, type a description to help you remember why you are protecting this information.
5. In the Information To Protect text box, type the information that you want to block from being sent over insecure Internet connections.
6. Under Secure this private information in, select the Internet programs in which Privacy Control should block this information. Your options are:
   - Web browsers
   - Instant messengers
   - Email programs
7. Click **OK**.

Modify or remove private information

You can modify or remove private information at any time.

To modify or remove private information

1. In the main window, double-click **Privacy Control**.
2. In the Privacy Control window, click **Private Information**.
3. Select the private information that you want to change or remove.
4. Select one of the following:
   - Modify
   - Remove
5. Click **OK**.

Customize Privacy Control

Privacy Control protects four areas:

Private Information	Blocks specific text that you do not want sent over the Internet
Cookie Blocking	Stops Web sites from retrieving personal information stored in cookie files
Browser Privacy	Protects information about your browsing habits
Secure Connections	Prevents users from establishing secure connections to online stores and other Web sites

There are two ways to adjust Privacy Control settings:

- Set the Privacy Level.
  Use the slider in the main Privacy Control pane to select pre-set security levels.
- Adjust individual Privacy Control settings.
  Customize your protection by manually adjusting individual settings.

Set the Privacy Level

Privacy Control offers pre-set security levels that help you set several options at one time. The Privacy Level slider lets you select minimal, medium, or high protection.

To set the Privacy Level

1. In the main window, double-click **Privacy Control**.
2. Move the slider to the Privacy Level that you want.
3. Click **OK**.

Adjust individual Privacy Control settings

You can change the settings for Private Information, Cookie Blocking, Browser Privacy, and Secure Connections if the Privacy Level settings do not meet your needs. For example, you can choose to block all attempts to send private information while allowing Web sites to customize their pages using your browser information.

Change the Private Information setting

Change the Private Information setting to control how Privacy Control handles attempts to send information on the Private Information list over the Internet.

To change the Private Information setting

1. In the main window, double-click **Privacy Control**.
2. Click **Custom Level**.
3. Select the Private Information setting that you want.
4. Click **OK**.

Change the Cookie Blocking setting

Many Web sites store information they collect in *cookies* placed on your hard disk. When you return to a site that has set a cookie on your computer, the Web server opens and reads the cookie.

Most cookies are harmless. Sites use them to personalize Web pages, remember choices that you have made on the site, and deliver optimized pages for your computer. However, sites can also use cookies to track your Internet usage and browsing habits.

Change the Cookie Blocking setting to control how Privacy Control handles sites that attempt to place cookies on your computer.

To change the Cookie Blocking setting

1. In the main window, double-click **Privacy Control**.
2. Click **Custom Level**.
3. Select the Cookie Blocking setting that you want.
4. Click **OK**.

See "Use Web assistant" on page 36.

You can also customize cookie blocking for individual sites using Web assistant.

Enable or disable Browser Privacy

Browser Privacy prevents Web sites from learning the type of computer and browser that you are using, the Web site that you last visited, and other information about your browsing habits. Some Web sites that depend on JavaScript may not work correctly if they cannot identify the type of browser that you are using.

To enable or disable Browser Privacy

1. In the main window, double-click **Privacy Control**.
2. Click **Custom Level**.
3. In the Customize Privacy Settings dialog box, check or uncheck **Enable Browser Privacy**.
4. Click **OK**.

Disable or enable secure Web connections

When you visit a secure Web site, your browser sets up an encrypted connection with the Web site. By default, Norton Personal Firewall lets you use secure connections.

If you disable secure Web connections, your browser will not encrypt any information that it sends. You should only disable secure Web connections if you are protecting your personal data in the Private Information list.

To disable or enable secure Web connections

1. In the main window, double-click **Privacy Control**.
2. Click **Custom Level**.
3. In the Customize Privacy Settings dialog box, check or uncheck **Enable Secure Connections (https)**.
4. Click **OK**.

Blocking Internet advertisements

9

When Ad Blocking is enabled, it transparently removes:

- Ad banners
- Pop-up and pop-under ads
- Macromedia Flash-based ads

Use the Ad Trashcan

As you use the Internet, you may find ads that are not included on the default Ad Blocking list. You can use the Ad Trashcan to add these to your personal list of blocked ads.

To use the Ad Trashcan

1. Open your Web browser and view the page containing the advertisement that you want to block.
2. Open Norton Personal Firewall.
3. In the main window, double-click **Ad Blocking**.
4. In the Ad Blocking window, ensure that Enable Ad Blocking is checked.
5. Click **Ad Trashcan**.
   The Ad Trashcan window appears.

6 With the windows arranged so that you can see both the advertisement and the Ad Trashcan window, do one of the following:
   - If you are using Microsoft Internet Explorer, drag the unwanted ad from the Web site to the Ad Blocking dialog box.
   - If you are using Netscape, right-click the advertisement, then click **Copy Image Location**. In the Ad Trashcan, click **Paste**.
     The address for the advertisement appears in the Ad Details line of the Ad Trashcan dialog box.

7 Select one of the following:
   - Add: Block this address.
   - Modify: Change the entry before adding it to the Ad Blocking list.
     For example, if the advertisement address is http://www.uninvutedads.org/annoying/ads/numberone.gif, you could change it to http://www.uninvitedads.org/annoying/ads/ to block everything in the ads directory.

8 Click **Close**.

9 Click **OK** to close the Ad Blocking window.

Use text strings to identify ads to block or permit

You can control whether Ad Blocking displays specific ads by creating a list of text strings that identify individual ad banners. Ad Blocking strings are sections of *HTML* addresses. If any part of a file’s address matches the text string, Ad Blocking automatically blocks the file.

How to identify Ad Blocking strings

The way that you define Ad Blocking strings affects how restrictive or unrestrictive Ad Blocking is when filtering data.

For example, if you add the string uninvitedads.com to the (Defaults) block list, you block everything in the uninvitedads.com domain. If you are more specific and add the string nifty_images/image7.gif to the site-specific block list maintained for www.uninvitedads.com, you block only that particular image.

Add an Ad Blocking string

You can add strings to the Ad Blocking list for all sites or for individual sites.

To add an Ad Blocking string

1. In the main window, double-click **Ad Blocking**.
2. In the Ad Blocking window, click **Advanced**.
3. On the left side of the Advanced window, do one of the following:
   - To block a string on all Web sites, click **(Defaults)**.
   - To block a string on a Web site in the list, select the site's name.
   - To block a string on a Web site not in the list, click **Add Site**, then in the New Site/Domain dialog box, type the site's address.
4. On the Ad Blocking tab, click **Add**.
5. In the Add New HTML String dialog box, select the action that you want to take.
6. Type an HTML string to block or permit.
7. Click **OK**.
8. When you are done, click **OK** to close the Advanced window.
9. Click **OK** to close the Ad Blocking window.

Modify or remove an Ad Blocking string

If you later decide that an Ad Blocking string is too restrictive, not broad enough, or not appropriate, you can change or remove it.

To modify or remove an Ad Blocking string

1. In the main window, double-click **Ad Blocking**.
2. In the Ad Blocking window, click **Advanced**.
3. In the left side of the Advanced window, do one of the following:
   - To modify or remove a string in the (Defaults) list, click **(Defaults)**.
   - To modify or remove a site-specific string, click the site’s name.
4. In the HTML string list, select the string that you want to change.
5. Do one of the following:
   - To modify a string, click **Modify**, then type your changes.
   - To remove a string, click **Remove**.
6. When you are done, click **OK** to close the Advanced window.
7. Click **OK** to close the Ad Blocking window.

Monitoring Norton Personal Firewall

10

Norton Personal Firewall maintains records of all incoming and outgoing Internet connections and any actions that the program takes to protect your computer. You should periodically review this information to spot potential problems.

There are several sources of information:

Status & Settings window	Basic information about which protection features are active
Statistics window	Recent information about firewall and content-blocking activities
Detailed statistics window	Detailed information about network activity and actions that Norton Personal Firewall has taken
Event Log	Internet activities and any actions Norton Personal Firewall has taken

View the Statistics window

The Statistics window includes information on the following:

Personal Firewall	Any recent attacks on this computer, including the time of the most recent attack and the address of the attacking computer
Online Content Blocking	The number of cookies, images, and other online content that has been blocked and the number of times private information has been blocked

To view the Statistics window

❖ In the main window, click **Statistics**.

Reset information in the Statistics window

The statistics in the Statistics window are automatically cleared when you restart Windows. You can also clear the statistics manually. This helps you see if a configuration change affects the statistics.

To reset information in the Statistics window

1. In the main window, click **Statistics**.
2. In the Statistics window, click **Clear Statistics**.

Review detailed statistics

Along with the overall statistics in the Statistics window, Norton Personal Firewall maintains real-time network counters that track users’ Internet usage and any actions that the program takes.

The detailed statistics include the following information:

Network	TCP and UDP bytes sent and received, the number of open network connections, and the highest number of simultaneous open network connections since the program started
Online content	The number of graphics, cookies, and private information that have been blocked and the number of open HTTP connections
Firewall TCP Connections	The number of blocked and permitted TCP connections
Firewall UDP Datagrams	The number of blocked and permitted UDP connections
Firewall Rules	All of the rules defined for your firewall and information on the number of communication attempts blocked, permitted, or not matched by firewall rules
Network Connections	Information about current connections, including the program that is using the connection, the protocol being used, and the addresses or names of the connected computers
Last 60 Seconds	The number of network and HTTP connections and the speed of each connection type

To review detailed statistics

1. In the main window, click **Statistics**.
2. In the Statistics window, click **Detailed Statistics**.

View Norton Personal Firewall logs

Norton Personal Firewall records information about Web sites that users have visited, actions that the firewall has taken, and any alerts that have been triggered. The logs include details about some of the activity reported in the Statistics window.

Review log information

View the Norton Personal Firewall logs from the Statistics window.

To view the logs

1. In the main window, click **Statistics** > **View Logs**.
2. In the Log Viewer, in the left pane, select the log that you want to review. Your options are:

Content Blocking	Details about ads, Java applets, ActiveX controls, scripts, Flash animations, and GIF animations blocked
Connections	A history of all TCP/IP network connections made with this computer, including the date and time of the connection, the address of the computer to which you connected, the service or port number used, the amount of information transferred, and the total time the connection was active
Firewall	Communication intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events
Intrusion Detection	Whether Intrusion Detection is active, attack signatures being monitored, and the number of intrusions blocked
Privacy	The cookies that have been blocked, including the name of the cookie and the Web site that requested the cookie
Private Information	A history of all protected private information sent over the Internet

System	Severe system errors, the current status of IP filtering, if the logged program started as a Windows service, and information about programs that are using too many resources or otherwise operating under less than optimum conditions
Web History	URLs visited by the computer, providing a history of Web activity
Alerts	Any security alerts triggered by possible attacks on your computer

As you click each log, the right pane changes and displays details specific to the particular log. The most recent activities appear at the top of the log.

3 When you are finished viewing the information, click **File** > **Exit**.

Troubleshooting

11

The information in this chapter will help you solve the most frequently encountered problems. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site.

Explore the Symantec service and support Web site

On the Symantec service and support Web site, you can find the latest protection and program updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

1. On the Internet, go to www.symantec.com/techsupp
2. On the service and support Web page, under the heading home & home office/small business, click **Continue**.
3. On the home & home office/small business page, click **start online support**.
4. Follow the links to the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

1. On the left side of any Symantec Web site page, click **search**.
2. On the search page, type a word or phrase that best represents the information for which you are looking. Use the following guidelines when searching the Symantec Web site:
   - Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type install to find articles that include the word install, installation, installing, and so on.
   - Type multiple words to find all occurrences of any of the words. For example, type virus definitions to find articles that include virus or definitions or both.
   - Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
   - Type a plus (+) sign in front of all of the search terms to retrieve documents containing all of the words. For example, +Internet +Security finds articles containing both words.
   - For an exact match, type the search words in uppercase letters.
   - To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, “purchase product”, “MAC”, “Norton SystemWorks” searches for all three phrases, and finds all articles that include any of these phrases.
3. Select the area of the Web site that you want to search.
4. Click **Search**.

Troubleshoot Norton Personal Firewall

Check here for possible solutions to issues that might arise with Norton Personal Firewall.

What is wrong with this Web site?

If you cannot connect to a Web site with Norton Personal Firewall disabled, there might be a problem with the Internet or your *Internet service provider*. If your connection is working, it's possible a Norton Personal Firewall feature is preventing you from viewing the site.

Problem	**Solution**
It could be Cookie Blocking	Many Web sites require that cookies be enabled on your computer to display correctly. See "Change the Cookie Blocking setting" on page 86.
It could be a firewall rule	A firewall rule might be blocking the Web site. When this happens, you will usually see a message saying that you could not connect. See "Customize firewall protection" on page 60.
It could be Ad Blocking	Sometimes blocking advertisements on the Internet prevents an entire Web site from appearing in your browser. See "Blocking Internet advertisements" on page 89.
It could be ActiveX or Java blocking	Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites. See "Change individual security settings" on page 60.

Why can't I post information online?

See "Modify or remove private information" on page 84.

If you are unable to post information to a Web site, it may be because Privacy Control is blocking the information. Check the Private Information list to see if the information that you are trying to enter is being blocked.

Why did an email message I sent never arrive?

If you choose to block an email message containing private information, Norton Personal Firewall immediately deletes the email message. Your email program will indicate that the message was sent, but the recipient will not receive it.

If your email program maintains copies of sent messages in its Sent or Out folder, you can reopen the email message, remove the private information, and send the message again.

Why doesn’t Norton Personal Firewall notify me before letting programs access the Internet?

See “Enable Automatic Program Control” on page 64.

If Automatic Program Control is on, Norton Personal Firewall creates rules for programs that it recognizes without notifying you.

Why can’t I print to a shared printer or connect to a computer on my local network?

Norton Personal Firewall blocks the use of Microsoft networking to prevent someone from connecting to your computer over the Internet.

See “Allow or block access to your computer” on page 61.

To allow the use of your local network, including file and printer sharing, place the computers on your local network in the Trusted Zone.

How can a Web site get my browser information?

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

Troubleshoot Ad Blocking

This information will help you solve the most frequently encountered problems with Ad Blocking.

Does Ad Blocking block all advertising on the current page?

Ads that are integrated with standard content–for instance text statements–will not be blocked.

Will Popup Window Blocking block all pop-ups or only pop-up ads?

Ad Blocking blocks all pop-ups that are started automatically during a Web page load. If a site uses pop-ups for special alerts or additional information, you might want to disable Popup Window Blocking while viewing that site.

Are there security issues associated with advertisements?

While clicking on an ad should only display more information or direct you to another site, some advertisers will use ads to entice you into installing new functionality on your system. These may range from adding new menus to installing spyware. You should be especially wary of ads that invite you to install novelty cursors or other entertaining add-ons. These frequently include user agreements that require you to allow companies to track your browsing or to provide them with personal information, among other things. Such clauses are typically hidden deep in the text where many users will not bother to read them.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at: http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- Online Service and Support
  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- PriorityCare telephone support
  This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at: http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Authorized Service Center
Postbus 1029
3600 BA Maarssen
The Netherlands

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

Latin America

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

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

June 3, 2003

Glossary

access privileges	The types of operations that a user can perform on a system resource. For example, a user can have the ability to access a certain directory and open, modify, or delete its contents.
ActiveSync	The synchronization software for Microsoft Windows-based Pocket PCs.
ActiveX	A method of embedding interactive programs into Web pages. The programs, which are called controls, run when you view the page.
alert	A message that appears to signal that an error has occurred or that there is a task that requires immediate attention, such as a system crash or a Virus Alert.
alias	A shortcut icon that points to an original object such as a file, folder, or disk.
AppleTalk	A protocol that is used by some network devices such as printers and servers to communicate.
attack signature	A data pattern that is characteristic of an Internet attack. Intrusion Detection uses attack signatures to distinguish attacks from legitimate traffic.
beam	To transfer certain programs and data between two handheld devices using built-in infrared technology.

boot record	A sector at the start of a disk that describes the disk (sector size, cluster size, and so on). On startup disks, the boot record also has a program that loads the operating system.
bootable disk	A disk that can be used to start a computer.
cache	A location on your disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them.
cache file	A file that is used to improve the performance of Windows.
compressed file	A file whose content has been made smaller so that the resulting data occupies less physical space on the disk.
connection-based protocol	A protocol that requires a connection before information packets are transmitted.
connectionless protocol	A protocol that sends a transmission to a destination address on a network without establishing a connection.
cookie	A file that some Web servers put on your disk when you view pages from those servers. Cookies store preferences, create online shopping carts, and identify repeat visitors.
denial-of-service attack	A user or program that takes up all of the system resources by launching a multitude of requests, leaving no resources, and thereby denying service to other users.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that assigns a temporary IP address to each device on a network. DSL and cable routers use DHCP to allow multiple computers to share a single Internet connection.
dial-up	A connection in which a computer calls a server and operates as a local workstation on the network.

DNS (Domain Name System)	The naming system used on the Internet. DNS translates domain names (such as www.symantec.com) into IP addresses that computers understand (such as 206.204.212.71).
DNS server (Domain Name System server)	A computer that maps domain names to IP addresses. When you visit www.symantec.com, your computer contacts a DNS server that translates the domain name into an IP address (206.204.212.71).
domain	The common Internet address for a single company or organization (such as symantec.com). See also host name.
DOS window	A method of accessing the MS-DOS operating system to execute DOS programs through the Windows graphical environment.
download	To transfer a copy of a file or program from the Internet, a server, or computer system to another server or computer.
driver	Software instructions for interpreting commands for transfer to and from peripheral devices and a computer.
encryption	Encoding data in such a way that only a person with the correct password or cryptographic key can read it. This prevents unauthorized users from viewing or tampering with the data.
Ethernet	A common method of networking computers in a LAN (local area network). Ethernet cables, which look like oversized phone cables, carry data at 10M/100M/1G bps.
executable file	A file containing program code that can be run. Generally includes any file that is a program, extension, or system files whose names end with .bat, .exe, or .com.

extension	The three-letter ending on a file name that associates the file with an activity or program. Examples include .txt (text) and .exe (executable program).
FAT (file allocation table)	A system table (used primarily by DOS and Windows 9x/Me) that organizes the exact location of the files on the hard drive.
file type	A code that associates the file with a program or activity, often appearing as the file name extension, such as .txt or .jpeg.
Finder	The program that manages your Macintosh disk and file activity and display.
firewall rule	Parameters that define how a firewall reacts to specific data or network communications. A firewall rule usually contains a data pattern and an action to take if the pattern is found.
fragmented	When the data that makes up a file is stored in noncontiguous clusters across a disk. A fragmented file takes longer to read from the disk than an unfragmented file.
fragmented IP packet	An IP packet that has been split into parts. Packets are fragmented if they exceed a network's maximum packet size, but malicious users also fragment them to hide Internet attacks.
FTP (File Transfer Protocol)	An application protocol used for transferring files between computers over TCP/IP networks such as the Internet.
hidden attribute	A file attribute that makes files harder to access and more difficult to delete than other files. It also prevents them from appearing in a DOS or Windows directory list.
host name	The name by which most users refer to a Web site. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.

HotSync	The synchronization software for Palm OS handheld devices.
HTML (Hypertext Markup Language)	The language used to create Web pages.
ICMP (Internet Control Message Protocol)	An extension to the basic Internet Protocol (IP) that provides feedback about network problems.
IGMP (Internet Group Management Protocol)	An extension to the basic Internet Protocol (IP) that is used to broadcast multimedia over the Internet.
IMAP4 (Internet Message Access Protocol version 4)	One of the two most popular protocols for receiving email. IMAP makes messages available to read and manage without downloading them to your computer.
infrared (IR) port	A communication port on a handheld device for interfacing with an infrared-capable device. Infrared ports do not use cables.
IP (Internet Protocol)	The protocol that underlies most Internet traffic. IP determines how data flows from one computer to another. Computers on the Internet have IP addresses that uniquely identify them.
IP address (Internet Protocol address)	A numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually shown as four groups of numbers separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.
Java	A programming language used to create small programs called applets. Java applets can be used to create interactive content on Web pages.

JavaScript	A scripting language used to enhance Web pages. Most sites use JavaScript to add simple interactivity to pages, but some use it to open pop-up ads and reset visitors' homepages.
macro	A simple software program that can be started by a specific keystroke or a series of keystrokes. Macros can be used to automate repetitive tasks.
NAT (network addresstranslation)	A method of mapping private IP addresses to a single public IP address. NAT allows multiple computers to share a single public IP address. Most DSL and cable routers support NAT.
network address	The portion of an IP address that is shared by all computers on a network or subnet. For example, 10.0.1.1 and 10.0.1.8 are part of the network address 10.0.1.0.
NTFS (NTFS file system)	A system table (used primarily by Windows 2000/ XP) that organizes the exact location of all the files on the hard drive.
packet	The basic unit of data on the Internet. Along with the data, each packet includes a header that describes the packet's destination and how the data should be processed.
partition	A portion of a disk that is prepared and set aside by a special disk utility to function as a separate disk.
POP3 (Post Office Protocol version 3)	One of the two most popular protocols for receiving email. POP3 requires that you download messages to read them.
port	A connection between two computers. TCP/IP and UDP use ports to indicate the type of server program that should handle a connection. Each port is identified by a number.

port number	A number used to identify a particular Internet service. Internet packets include the port number to help recipient computers decide which program should handle the data.
PPP (Point-to-Point Protocol)	A protocol for communication between two computers using a dial-up connection. PPP provides error-checking features.
protocol	A set of rules governing the communication and transfer of data between computers. Examples of protocols include HTTP and FTP.
proxy	A computer or program that redirects incoming and outgoing traffic between computers or networks. Proxies are often used to protect computers and networks from outside threats.
registry	A category of data stored in the Windows registry that describes user preferences, hardware settings, and other configuration information. Registry data is accessed using registry keys.
removable media	Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, CDs, DVDs, and Zip disks.
router	A device that forwards information between computers and networks. Routers are used to manage the paths that data takes over a network. Many cable and DSL modems include routers.
script	A program, written in a scripting language such as VBScript or JavaScript, that consists of a set of instructions that can run without user interaction.
service	General term for the process of offering information access to other computers. Common services include Web service and FTP service. Computers offering services are called servers.

SSL (Secure Sockets Layer)	A protocol for secure online communication. Messages sent using SSL are encrypted to prevent unauthorized viewing. SSL is often used to protect financial information.
subnet	A local area network that is part of a larger intranet or the Internet.
subnet mask	A code, in the form of an IP address, that computers use to determine which part of an IP address identifies the subnet and which part identifies an individual computer on that subnet.
synchronize	The process by which a handheld device and computer compare files to ensure that they contain the same data.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Standard protocols used for most Internet communication. TCP establishes connections between computers and verifies that data is properly received. IP determines how the data is routed.
threat	A program with the potential to cause damage to a computer by destruction, disclosure, modification of data, or denial of service.
Trojan horse	A program containing malicious code that is disguised as or hiding in something benign, such as a game or utility.
UDP (User Datagram Protocol)	A protocol commonly used for streaming media. Unlike TCP, UDP does not establish a connection before sending data and it does not verify that the data is properly received.
virus definition	Virus information that an antivirus program uses to identify and alert you to the presence of a specific virus.

wildcard characters	Special characters (like *, $, and ?) that act as placeholders for one or more characters. Wildcards let you match several items with a single specification.
worm	A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.

Index