Norton Personal Firewall User's Guide

Norton Personal Firewall 2001™

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.

Copyright Notice

Documentation version 2.5

PN: 07-30-00435

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.

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

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

LICENSE AND WARRANTY:

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

YOU MAY:

(i) use only one copy of one version of the various versions of the Software contained on the enclosed media on a single computer, or if only one version is contained on the enclosed media use one copy of such version on a single computer;
(ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
(iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
(iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
(v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

YOU MAY NOT:

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

SIXTY DAY MONEY BACK GUARANTEE:

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

LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.
THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

DISCLAIMER OF DAMAGES:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. THE DISCLAIMERS AND LIMITATIONS SET FORTH ABOVE WILL APPLY REGARDLESS OF WHETHER YOU ACCEPT THE SOFTWARE.

U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 20330 Stevens Creek Blvd., Suite 200, Cupertino, CA 95014.

GENERAL:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 20330 Stevens Creek Blvd., Suite 200, Cupertino, CA 95014.

CONTENTS

Chapter 1 Getting started

Chapter 2 Personalizing Norton Personal Firewall

Chapter 3 Troubleshooting

CHAPTER 1

Getting started

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

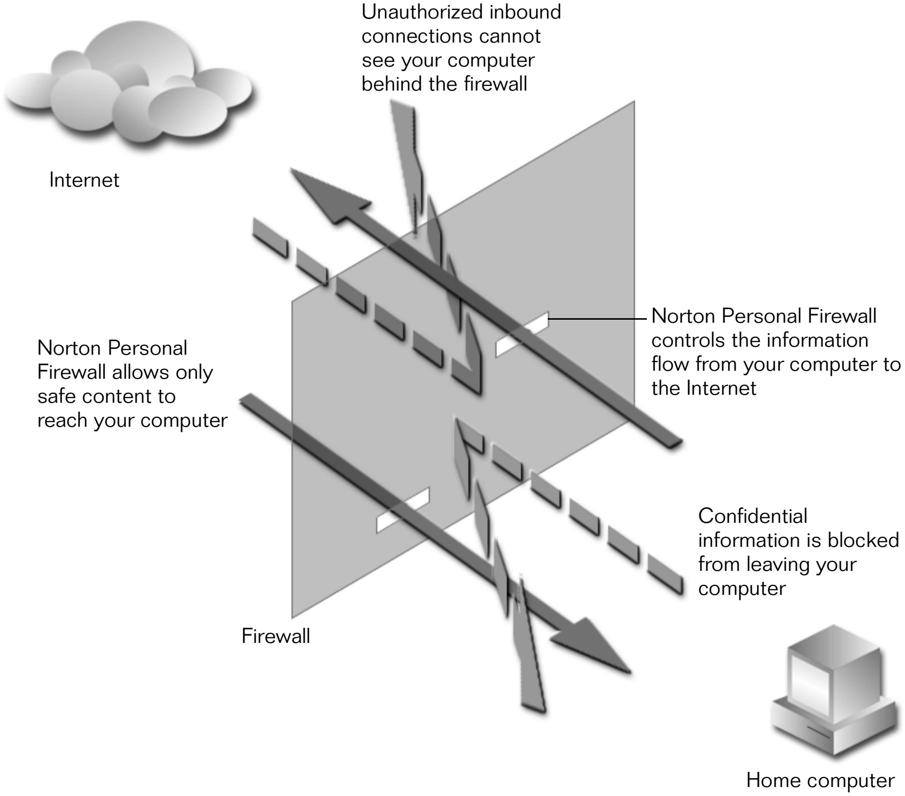
Norton Personal Firewall can help you track everything that happens on your computer. It monitors the Internet to give you peace of mind when you are online. It helps protect your security and your privacy.

What does Norton Personal Firewall do?

Norton Personal Firewall includes Norton Personal Firewall and Norton Privacy Control. Together, they monitor the Internet to give you peace of mind when you are online. Norton Personal Firewall protects your security and Norton Privacy Control protects your personal information.

Norton Personal Firewall provides a barrier called a *firewall* between your computer and the Internet. Firewall programs are filters that block or allow connections and data transmissions on the Internet. By filtering connections and information, firewalls protect you from malicious Internet content.

Norton Personal Firewall uses rules to determine whether to permit or block connections. You can change these rules, permitting or blocking programs from having Internet Access.


Unauthorized inbound connections cannot see your computer behind the firewall
Internet
Norton Personal Firewall controls the information flow from your computer to the Internet
Norton Personal Firewall allows only safe content to reach your computer
Confidential information is blocked from leaving your computer
Firewall
Home computer

Norton Personal Firewall automatically filters most content for you. It automatically determines the best way to protect many popular applications. When an application that Norton Personal Firewall does not recognize attempts to communicate over the Internet, Norton Personal Firewall alerts you, and the Firewall Rule Assistant helps you create a new rule.

ActiveX controls and Java applets are programs that run inside your browser. While most of these programs are useful, some are harmful. Norton Personal Firewall prevents ActiveX controls and Java applets from running without your knowledge, and lets you specify sites where these programs are okay to run.

Norton Privacy

You may not want confidential information, such as credit card numbers, your home phone number, and so on, to be sent un-encrypted over the Internet. Norton Privacy prevents confidential information from being entered on non-secured Web sites.

Cookies are small files stored on your computer that Web sites use to track your visits. Norton Personal Firewall can block cookies and other information your browser normally reports to Web sites, such as email addresses and the previous Web site you visited.

Statistics and logging

Norton Personal Firewall records complete statistics about its operation. It can also log as much of your Internet activities, and the operation of Norton Personal Firewall as you like. It's easy to view either the statistics or the logs.

Installing Norton Personal Firewall

System requirements

To use Norton Personal Firewall, your computer must meet the following minimum requirements:

- 133 MHz Pentium class or faster processor
- Windows 95 OSR2, Windows 98, Windows 98 SE, Windows NT 4.0 Workstation Sp4, Windows 2000 Professional
- 24 MB of memory (32 MB for Windows NT and Windows 2000), additional memory recommended
- 10 MB free disk space
- CD-ROM drive
- Microsoft Windows Internet support
- Microsoft Internet Explorer 4.0, Netscape Navigator 4.0, Opera 4.0, or later browser

Installation procedure

Follow these steps to install Norton Personal Firewall.

To install:

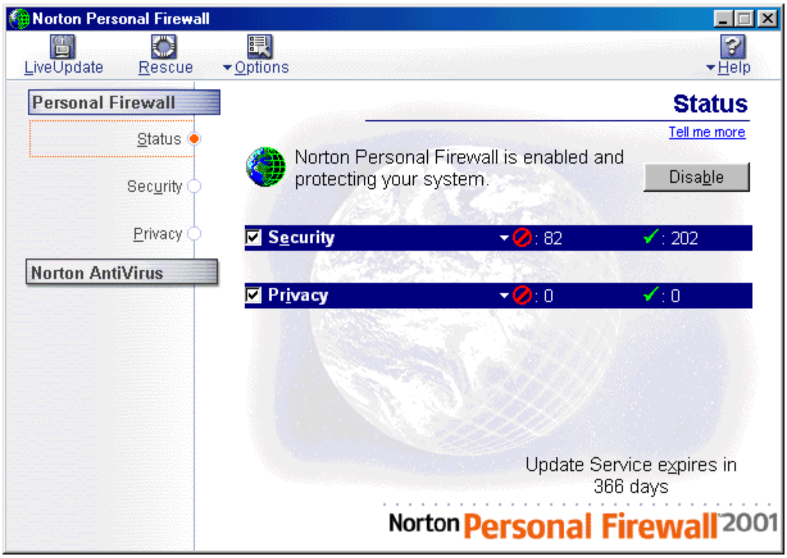
1. Start Windows (if it is not already running).
2. Insert the Norton Personal Firewall CD into the CD-ROM drive.
3. In the opening screen, click Install Norton Personal Firewall and follow the on-screen instructions.

If the opening screen does not appear:

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

Navigating Norton Personal Firewall

To start Norton Personal Firewall, double-click the Norton Personal Firewall icon in the notification area of the Windows taskbar. You can also click the Start button, and then select Programs > Norton Personal Firewall > Norton Personal Firewall, or double-click the Norton Personal Firewall icon on your desktop.



Norton Personal Firewall is enabled and protecting your system.

☑ Security ⊘: 82 ✓: 202

☑ Privacy ⊘: 0 ✓: 0

Update Service expires in 366 days

Setting Norton Personal Firewall options

There are several options you can set in Norton Personal Firewall. For example, you can choose whether Norton Personal Firewall starts automatically when you start your computer.

To access Norton Personal Firewall options:

- At the top of the Norton Personal Firewall window, click Options.

Updating Norton Personal Firewall with LiveUpdate

LiveUpdate connects to Symantec via the Internet to see if updates are available for the Norton Personal Firewall program and also checks for updates to your Internet protection.

Symantec does not charge for updates to the Norton Personal Firewall program. There is a charge for updating your Internet protection after your free subscription expires. Your normal Internet access fees apply.

If you connect to the Internet through AOL, CompuServe, or Prodigy Internet, first connect to the Internet, then run LiveUpdate.

To update Norton Personal Firewall using LiveUpdate:

1. At the top of the Norton Personal Firewall window, click LiveUpdate.
2. Follow the on-screen instructions.

About your subscription

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

The subscription provides Norton Personal Firewall with the latest security information to keep your system safe:

- Firewall rules that protect against the latest Trojan horse and zombi programs like Back Orifice and Trinoo.

- Lists of the latest applications that use the Internet. These lists make it possible for Norton Personal Firewall to automatically create firewall rules when you use Internet applications. See "Creating firewall rules automatically" on page 17.

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

It is important that you keep your subscription in force. Norton Personal Firewall cannot protect you from new threats without current information from Symantec.

Using help to learn more about Norton Personal Firewall

Norton Personal Firewall provides extensive online help. This help system gives you detailed instructions about how to use all of the Norton Personal Firewall programs.

Norton Personal Firewall includes three kinds of help:

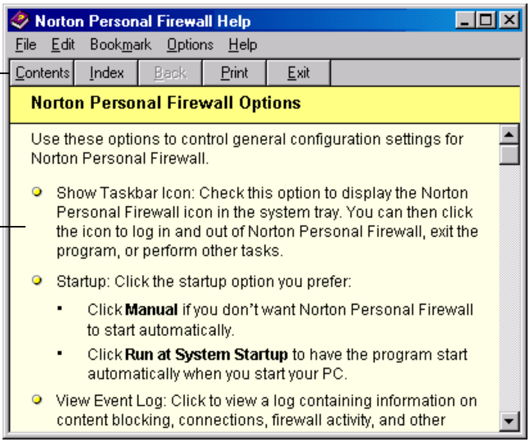
- Help with program dialog boxes
- How To help
- What's This? help

Help with program windows and dialog boxes

Dialog box help provides information about the Norton Personal Firewall program itself. This kind of help is context-sensitive, meaning that it displays help for the specific dialog box that you are currently using.

To get help with a window or dialog box:

- Click the Tell Me More link if one is available.
- Click the Help button located in the dialog box.



Norton Personal Firewall Options

Use these options to control general configuration settings for Norton Personal Firewall.

- Show Taskbar Icon: Check this option to display the Norton Personal Firewall icon in the system tray. You can then click the icon to log in and out of Norton Personal Firewall, exit the program, or perform other tasks.
- Startup: Click the startup option you prefer:
  - Click **Manual** if you don't want Norton Personal Firewall to start automatically.
  - Click **Run at System Startup** to have the program start automatically when you start your PC.
- View Event Log: Click to view a log containing information on content blocking, connections, firewall activity, and other

Complete table of contents and index

Information about the dialog box and how to use it

How To help

How To help explains step-by-step procedures you are likely to perform using Norton Personal Firewall. You can access these topics through the Contents or Index tabs. Open the Contents or Index by clicking the Contents or Index button at the top of any help topic.

What's This? help

What's This? help provides a quick definition of an individual component of a window or dialog box.

To access What's This? help:

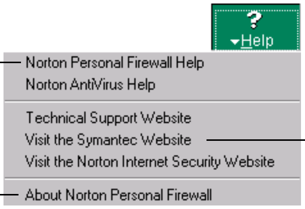
- Right-click anywhere you need help in a window or dialog box and choose What's This?

Getting help from the Help menu

Help is always available from the Norton Personal Firewall window.

To access the Help menu:

- At the top of the Norton Personal Firewall window, click Help.


?
Help
Norton Personal Firewall Help
Norton AntiVirus Help
Technical Support Website
Visit the Symantec Website
Visit the Norton Internet Security Website
About Norton Personal Firewall

Online help table of contents and index

Version and registration information

Visit Symantec Web sites for more information

CHAPTER 2

Personalizing Norton Personal Firewall

With Norton Personal Firewall, your computer can be more secure than most other computers on the Internet.

Security

The more time your PC spends connected to the Internet, especially if you have a high speed connection, the more opportunity there is for malicious hackers to break in and create havoc. They can steal files from your computer and even damage its contents. Norton Personal Firewall lets you fully enjoy the Internet while blocking attacks and alerting you to unauthorized connections and attempted intrusions.

- The Personal Firewall uses rules to block or allow communications between your computer and the Internet. It alerts you when a new type of communication is requested, and lets you decide how it should be handled.
- Java applet security prevents or allows Java applets from running on your computer.
- ActiveX control security prevents or allows ActiveX controls from running on your computer. ActiveX controls can be risky because they can have complete access to the data on your computer.
- Your subscription keeps the firewall rules up-to-date.

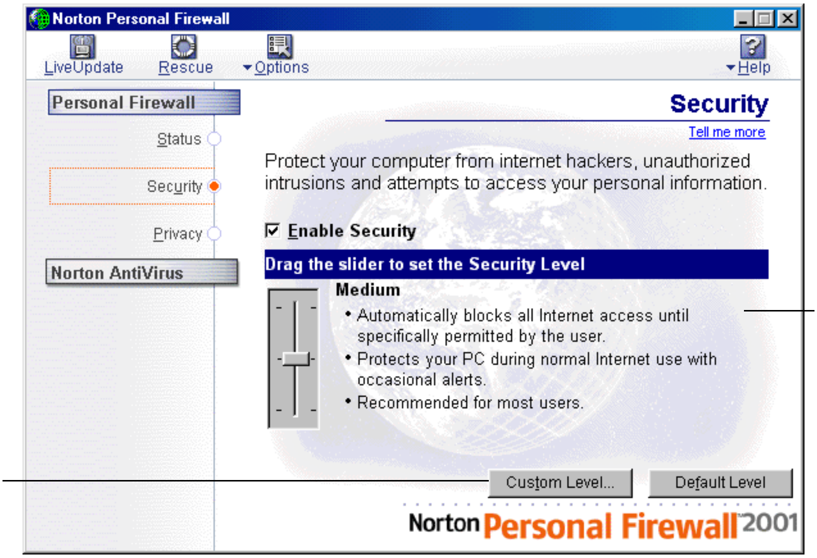
Privacy

Chances are you have a lot of personal information stored on your PC, including credit-card numbers, online banking details, and confidential financial data. That’s why Norton Privacy Control allows you to designate key information that should be protected from unsecured Web sites. It also prevents Web servers from retrieving your email address without your permission, or tracking your online activities through cookies.

- Confidential information, such as credit-card numbers, can be blocked from unsecure Web sites.
- Web sites use cookies to track your visits. You can block cookie responses when Web sites ask for them.
- Norton Personal Firewall will prevent your browser from sending your email address and the address of the last site you visited without your permission.
- You can disable secure connections, helping to ensure that confidential information is not sent by users that should not send it.

Customizing security features

Change security settings by opening the Security window.



Protect your computer from internet hackers, unauthorized intrusions and attempts to access your personal information.

☑ Enable Security

Drag the slider to set the Security Level

Medium

- Automatically blocks all Internet access until specifically permitted by the user.
- Protects your PC during normal Internet use with occasional alerts.
- Recommended for most users.

Click Custom Level to create your own settings

Choose from Low, Medium, or High security for this account

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

Security settings	Description
High	Firewall is set to High, which blocks everything until you allow it. ActiveX control and Java applet blocking is set to Medium, which prompts you each time one is encountered.
Medium	Firewall is set to High, which blocks everything until you allow it. ActiveX control and Java applet blocking is set to none, which allows all ActiveX controls and Java applets to run.
Minimal	Firewall is set to Medium, which blocks known malicious applications. ActiveX control and Java applet blocking is set to none, which allows all ActiveX controls and Java applets to run.

Customizing Norton Personal Firewall

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

Norton Personal Firewall has two settings: High and Medium.

Firewall settings	Description
High	Blocks all communication that you do not specifically allow. You must create firewall rules for every application that requests Internet access.
Medium	Blocks a large list of ports used by harmful programs. However, it can also block useful programs when they use the same ports.

Creating firewall rules automatically

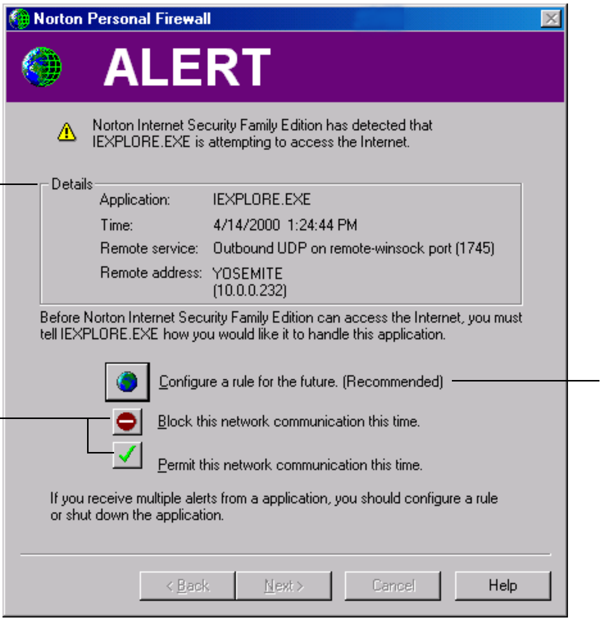
The Norton Personal Firewall subscription includes updated lists of known, reliable programs that communicate over the Internet. These programs include Web browsers, email programs, games, network utilities and many others.

When you use a program that Norton Personal Firewall recognizes, Norton Personal Firewall automatically creates a rule for it with the appropriate firewall settings. To keep your list of Internet-enabled applications current, use LiveUpdate regularly. See "Updating Norton Personal Firewall with LiveUpdate" on page 11.

Using the Firewall Rule Assistant

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

When Norton Personal Firewall encounters an application for which it has no rules attempting to establish a connection across the Internet, the Firewall Rule Assistant appears.



Norton Personal Firewall

ALERT

Norton Internet Security Family Edition has detected that IEXPLORE.EXE is attempting to access the Internet.

Details

Application: IEXPLORE.EXE
Time: 4/14/2000 1:24:44 PM
Remote service: Outbound UDP on remote-winsock port (1745)
Remote address: YOSEMITE (10.0.0.232)

Before Norton Internet Security Family Edition can access the Internet, you must tell IEXPLORE.EXE how you would like it to handle this application.

Configure a rule for the future. (Recommended)

Block this network communication this time.

Permit this network communication this time.

If you receive multiple alerts from a application, you should configure a rule or shut down the application.

The alert shows which application is requesting access to the Internet

Block or permit connections one time only

Create new firewall rules with the Firewall Rule Wizard

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

- Create a rule for this connection in the firewall database. When there is a rule established for a certain connection, the firewall automatically follows that rule to permit or block the connection.

- Permit the connection this time, but bring up the Firewall Rule Assistant the next time the connection is requested.
- Block the connection this time, but bring up the Firewall Rule Assistant the next time the connection is requested.

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

Setting Java and ActiveX security levels

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

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

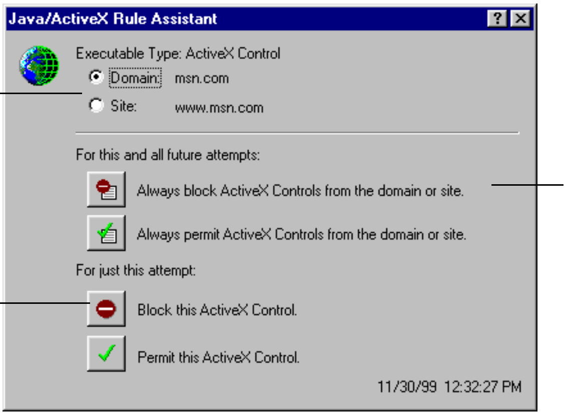
The only way to prevent bad programs from running on your computer is to block them from downloading. However, blocking all Java applets and ActiveX controls prevents many Web sites from appearing or running correctly.

In the Custom Level window for Security settings, the Java Applet Security and ActiveX Control Security features have three options: High, Medium, and None.

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

Using the Java/ActiveX Rule Assistant

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



Java/ActiveX Rule Assistant

Executable Type: ActiveX Control

● Domain: msn.com

○ Site: www.msn.com

For this and all future attempts:

Always block ActiveX Controls from the domain or site.

Always permit ActiveX Controls from the domain or site.

For just this attempt:

Block this ActiveX Control.

Permit this ActiveX Control.

11/30/99 12:32:27 PM

Apply this decision to the entire domain, or a specific Web site

Create firewall rules

Block or permit connections one time only

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

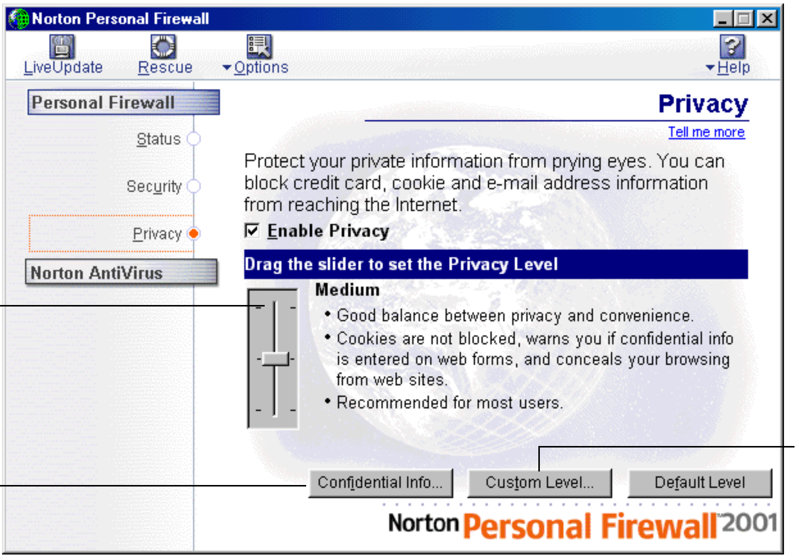
Do I want to block a domain or a site?

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

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

Safeguarding your privacy

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



Protect your private information from prying eyes. You can block credit card, cookie and e-mail address information from reaching the Internet.

☑ Enable Privacy

Drag the slider to set the Privacy Level

Medium

- Good balance between privacy and convenience.
- Cookies are not blocked, warns you if confidential info is entered on web forms, and conceals your browsing from web sites.
- Recommended for most users.

Choose the level of privacy

Enter confidential information you want to protect

Click Custom Level to create your own settings

The slider lets you select minimal, medium, or high privacy settings.

Blocking confidential information

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

Norton Personal Firewall allows you to create a list of personal information. When you enter information into this list, Norton Personal Firewall censors the information from all non-secure Web communications.

If you are concerned about entering personal information into the program, enter partial information instead. For example, instead of a complete credit card or identification number, enter the last few consecutive digits. Norton Personal Firewall will block the partial number, and thus prevent your credit card number from being transmitted to a Web site.

To block personal information from non-secure Web sites:

1 Open Norton Personal Firewall.

2 On the left side of the Norton Personal Firewall window, click Privacy.

3 Set the slider to Medium to be prompted every time someone tries to send protected information over a non-secure Web connection. Set the slider to High to always block confidential information.

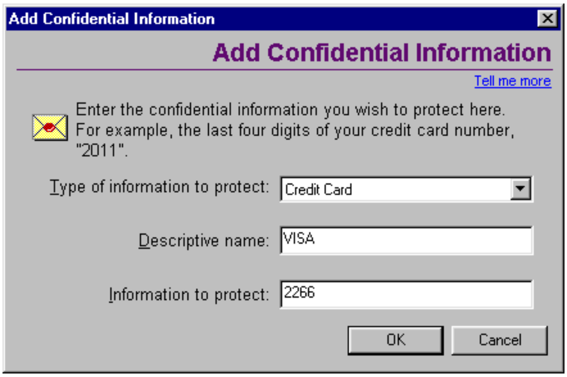
To enter confidential information to be blocked:

1 Open Norton Personal Firewall.

2 On the left side of the Norton Personal Firewall window, click Privacy.

3 Click Confidential Info.

4 In the Confidential Information dialog box, Click Add.



Enter the confidential information you wish to protect here. For example, the last four digits of your credit card number, "2011".

Type of information to protect: Credit Card

Descriptive name: VISA

Information to protect: 2266

5 In the Add Confidential Information dialog box, click a category from the Type Of Information To Protect box.

6 In the Descriptive Name field, enter a description that will help you remember why you are protecting the data.

7 In the Information To Protect field, enter the information you want to block from being sent through non-secure Web connections.

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

Tips on blocking confidential information

Do not enter an entire credit card number or identification number; enter a part of it. This prevents that part of the number from being transmitted to a non-secure Web site, and thus protects the entire number. For example, entering the last four digits of your phone number will protect your entire phone number from being sent over the Internet.

Because Norton Personal Firewall blocks personal information exactly the way you enter it into the program, it is better to enter only partial numbers. For example, a phone number could be typed as 888-555-1234, but it could also be entered without dashes (8885551234) or with spaces (888 555 1234), or even in two or more separate boxes. One thing common about all these formats is that the last four digits (1234) are always together. Thus, you can have better protection by protecting the last four digits than you have by protecting the entire number.

Blocking cookies

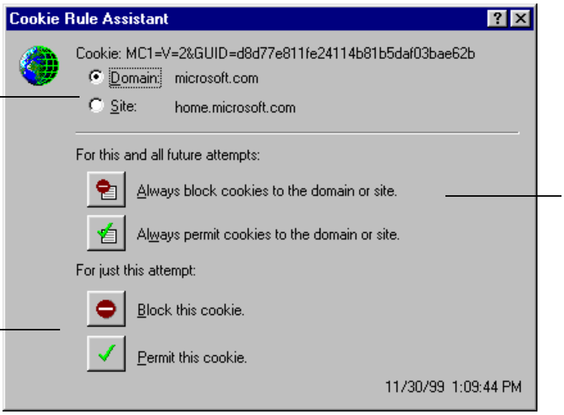
Cookies are small files that your browser saves on your computer. Sometimes Web sites use them for information that makes it more convenient for you to use their site.

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

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

Using the Cookie Rule Assistant

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



Cookie Rule Assistant

Cookie: MC1=V=2&GUID=d8d77e811fe24114b81b5daf03bae62b

● Domain: microsoft.com

○ Site: home.microsoft.com

For this and all future attempts:

Always block cookies to the domain or site.

Always permit cookies to the domain or site.

For just this attempt:

Block this cookie.

Permit this cookie.

11/30/99 1:09:44 PM

Apply this rule to the entire domain, or a specific Web site

Create rules to block or allow cookies

Block or permit cookies one time

For information on using Domain or Site settings, see "Do I want to block a domain or a site?" on page 21.

Enabling or disabling secure Web connections

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

If you want to ensure that confidential information is not sent over secure Web connections, you can block all secure Web connections.

To disable secure Web connections:

1. Open Norton Personal Firewall.
2. On the left side of the Norton Personal Firewall window, click Privacy.
3. Click Custom Level.
4. In the Custom Privacy Settings dialog box, click to uncheck Enable Secure Connections (https).

CHAPTER 3

Troubleshooting

This chapter answers some of the questions advanced users may have about Norton Personal Firewall.

Frequently Asked Questions

How do I turn off Norton Personal Firewall?

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

To temporarily disable Norton Personal Firewall:

1 Open Norton Personal Firewall.

2 In the Status window, click Disable.

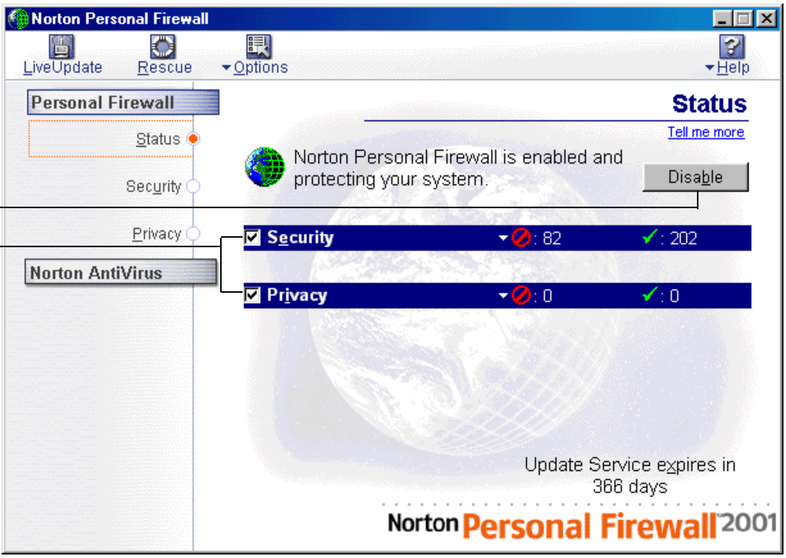
You can also disable Norton Personal Firewall by right-clicking the Norton Personal Firewall icon in the system tray and clicking Disable.

Norton Personal Firewall will be enabled the next time you start your computer.

To temporarily suspend Privacy:

1 Open Norton Personal Firewall.

2 In the Status window, make sure the options you want to suspend are unchecked.



Norton Personal Firewall is enabled and protecting your system.

Update Service expires in 366 days

Temporarily disable all functions of Norton Personal Firewall

Unchecked features are disabled; checked features are enabled

Closing Norton Personal Firewall

Even when the Norton Personal Firewall window is not open, if the icon appears in the system tray, it is still protecting your system. You can stop Norton Personal Firewall from running in the background.

To disable Norton Personal Firewall:

1 In the notification area of the Windows taskbar, right-click the Norton Personal Firewall icon.

2 On the menu, click Disable.

Why can't I post information online?

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

To check the information on the Personal Information list:

1. Open Norton Personal Firewall.
2. On the left side of the Norton Personal Firewall window, click Privacy.
3. Click Confidential Info.

   This opens the list of information that Norton Privacy Control blocks from being transferred to the Internet.

What is wrong with this Web site?

Running Norton Personal Firewall can block certain elements of a Web site that prevent it from displaying correctly in your Web browser. In some cases, the site might not display at all.

In most cases, this is simply Norton Personal Firewall doing its job of protecting you from inappropriate content. Your best solution may be to go to another, more appropriate Web site.

To see if Norton Personal Firewall is blocking the access to the Web site, you can disable Norton Personal Firewall and try the Web site again. Keep in mind that when you disable Norton Personal Firewall, you are turning off the protection it provides to prevent private information from being sent, and inappropriate information from being received. See "How do I turn off Norton Personal Firewall?" on page 25. If you still cannot connect, there might be a problem with the Internet or your Internet Service Provider.

It could be cookie blocking

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

To stop blocking cookies:

1. Open Norton Personal Firewall.
2. On the left side of the Norton Personal Firewall window, click Privacy.
3. Click Custom Level.
4. Set Cookie Blocking to Medium or None.

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. You can view the firewall rules that have been set up, and determine if a rule is blocking the site. See "How do I review or change firewall rules?" on page 33.

It could be blocking ActiveX or Java

Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites. See "Setting Java and ActiveX security levels" on page 19.

It could be script blocking

Some Web sites use JavaScript in their navigation controls and in other places. If Norton Personal Firewall is blocking JavaScript or VB Script, it may cause problems with these Web sites.

To stop blocking JavaScript or VB Scripts:

1. Open Norton Personal Firewall.
2. At the top of the Norton Personal Firewall window, click Options.
3. Click Advanced Options.
4. On the Web tab, click the Active Content tab.
5. In the list of Web sites, click the Web site to change, or click Default to change all unlisted Web sites.
6. Under Script, click Allow All Script To Execute.

Why doesn't FTP work on older browsers?

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

To temporarily resolve this problem, disable the security portion of Norton Personal Firewall. See "How do I turn off Norton Personal Firewall?" on page 25.

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

How can a Web site get my browser information?

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

- If you are not blocking Java, ActiveX or scripts, the site might be using one of these methods to retrieve the information. See "Setting Java and ActiveX security levels" on page 19.
- Sometimes when Web servers do not get the information from the browser, they simply use the last piece of browser information they received instead. You might see the information from the last person who viewed the site.

What are inbound and outbound connections?

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

Questions about home networking

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

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

How does the firewall work with Internet connection sharing?

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

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

How does the firewall work with file and printer sharing?

Norton Personal Firewall contains default firewall rules that allow file and printer sharing over NetBIOS networks. If you are using a TCP/IP-based network, you must configure the firewall to recognize the other computers on your network.

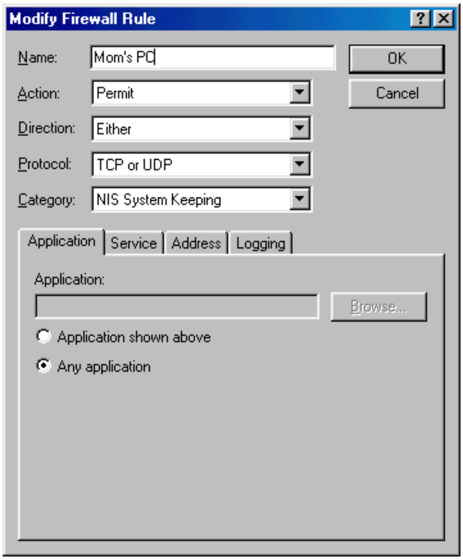
To configure the firewall to recognize your networked computers:

1 Open Norton Personal Firewall.

2 At the top of the Norton Personal Firewall window, click Options.

3 Click Advanced Options.

4 Under the Firewall tab, click Add.



Modify Firewall Rule

Name: Mom's PC

Action: Permit

Direction: Either

Protocol: TCP or UDP

Category: NIS System Keeping

Application:

○ Application shown above

● Any application

5 Enter a descriptive name for the computer you are setting up.

6 In the Action field, click Permit.

7 In the Direction field, click Either.

8 In the Protocol field, click TCP or UDP.

9 In the Category field, click NIS System Keeping.

10 On the Application tab, click Any Application.

11 On the Service tab under Remote Service, click Any Service. Under Local Service click Any Service.

12 On the Address tab under Remote Address, click Host Address and enter the TCP address of the other machine.

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

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

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

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

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

How do I use Norton Personal Firewall with a proxy server?

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

To monitor a specific port for Web communications:

1. Open Norton Personal Firewall.
2. At the top of the Norton Personal Firewall window, click Options.
3. Click Advanced Options.
4. On the Others tab, under HTTP Port List, click Add.
5. Enter the number for the port that should be monitored.

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

Questions about the firewall

Technical information about the firewall and its configurations can be found in the Norton Personal Firewall Help.

To open Help:

1. Open Norton Personal Firewall.
2. At the top of the Norton Personal Firewall window, click Help.
3. On the menu, click Norton Personal Firewall Help.

Why doesn’t the Firewall Rule Assistant appear?

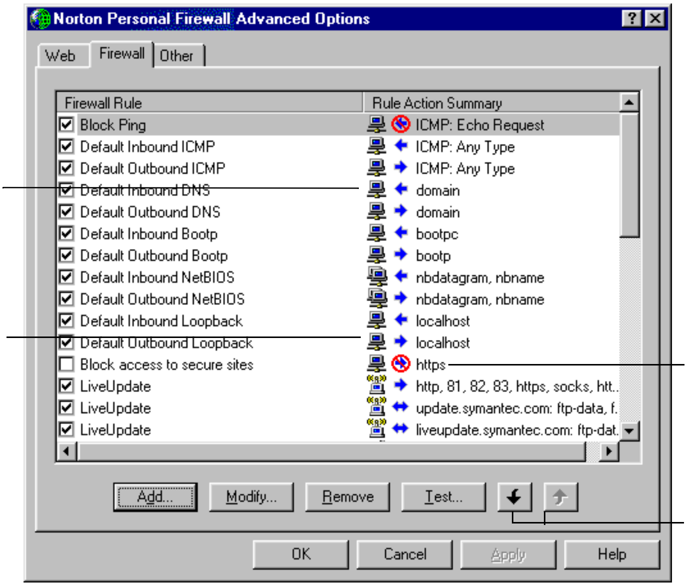
The Firewall Rule Assistant appears when the firewall detects a program trying to access the Internet, and there are no previous firewall rules blocking or permitting the program’s network connection. There are several areas in Norton Personal Firewall where you can block a program so that the Firewall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

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

- Turn on the Firewall Rule Assistant. See “Using the Firewall Rule Assistant” on page 18.
- In the Security window, make sure that the firewall is turned on. You can turn the Security slider to High, or set the firewall to High under Custom Level.
- Make sure there are no rules already covering the program you want to use. See “How do I review or change firewall rules?” on page 33. If a rule already exists, perhaps you already created it using the Firewall Rule Assistant. Or, if Enable Automatic Firewall Rule Creation is turned on, Norton Personal Firewall automatically created the rule for you. See “Creating firewall rules automatically” on page 17.
- When someone scans unused ports on your system, you can set Norton Personal Firewall so that it does not alert you unless the connection is successful. This can reduce the number of alerts you might receive.

How do I review or change firewall rules?

Whenever firewall rules are created, they appear in the Norton Personal Firewall Settings window. This window lets you review and change the firewall rules in the firewall database.



Firewall Rule	Rule Action Summary
☑ Block Ping	⊘ ICMP: Echo Request
☑ Default Inbound ICMP	← ICMP: Any Type
☑ Default Outbound ICMP	→ ICMP: Any Type
☑ Default Inbound DNS	← domain
☑ Default Outbound DNS	→ domain
☑ Default Inbound Bootp	← bootpc
☑ Default Outbound Bootp	→ bootp
☑ Default Inbound NetBIOS	← nbdatagram, nbname
☑ Default Outbound NetBIOS	→ nbdatagram, nbname
☑ Default Inbound Loopback	← localhost
☑ Default Outbound Loopback	→ localhost
☐ Block access to secure sites	⊘ https
☑ LiveUpdate	→ http, 81, 82, 83, https, socks, htt..
☑ LiveUpdate	↔ update.symantec.com: ftp-data, f..
☑ LiveUpdate	↔ liveupdate.symantec.com: ftp-dat..

Arrows pointing to the computer allow incoming communications

Arrows pointing away from the computer allow outgoing communications

Blocked arrows show rules that block inbound or outbound communications

Adjust the order in which the firewall rules run

To review or change individual firewall rules:

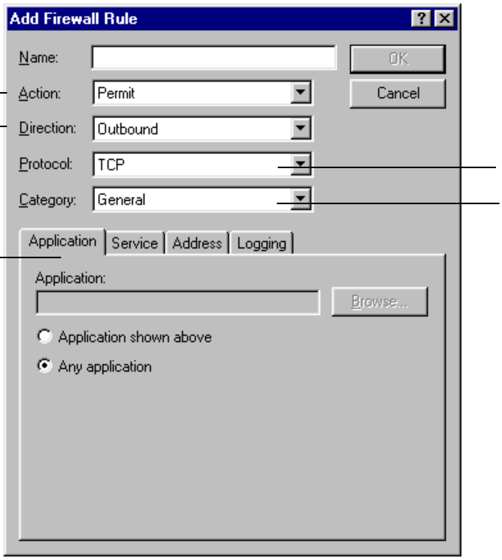
1 Open Norton Personal Firewall.

2 At the top of the Norton Personal Firewall window, click Options.

3 Click Advanced Options.

4 On the Firewall Tab, click the rule to view.

5 Click Modify.



Add Firewall Rule

Name:

Action: Permit

Direction: Outbound

Protocol: TCP

Category: General

Application:

○ Application shown above

● Any application

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

Each tab contains additional settings

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

You can block or allow specific application categories

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

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

To change the order of the rules:

1. Open Norton Personal Firewall.
2. At the top of the Norton Personal Firewall window, click Options.
3. Click Advanced Options.
4. On the Firewall tab, click the firewall rule to move.
5. Click the up arrow or down arrow to move the selected rule.

What purpose do the default firewall rules serve?

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

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

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

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

To restore the original default firewall rules:

1. Delete all the firewall rules.
2. Find the firewall.dat file on your computer.

   To open the search program, click the Start Button and then select Find > Files or Folders. (On Windows 2000, it is Search > For Files or Folders.)
3. When you find firewall.dat, rename it to firewall.reg.
4. Double-click firewall.reg to import it into the Registry.

Can I create settings for specific Web sites?

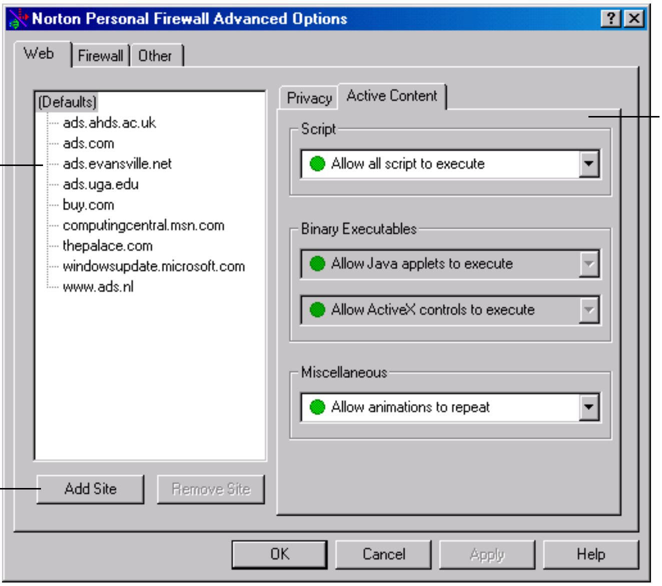
You can create Privacy and Active Content settings for specific Web sites using the Norton Personal Firewall Settings dialog box. First, set up Norton Personal Firewall the way you want it to apply to all Web sites in general. Then follow these directions to create rules or settings for specific Web sites.

To create settings for specific Web sites:

1 Open Norton Personal Firewall.

2 At the top of the Norton Personal Firewall window, click Options.

3 Click Advanced Options.



Norton Personal Firewall Advanced Options

(Defaults)
- ads.ahds.ac.uk
- ads.com
- ads.evansville.net
- ads.uga.edu
- buy.com
- computingcentral.msn.com
- thepalace.com
- windowsupdate.microsoft.com
- www.ads.nl

Script: ● Allow all script to execute

Binary Executables: ● Allow Java applets to execute; ● Allow ActiveX controls to execute

Miscellaneous: ● Allow animations to repeat

Create settings for specific Web sites

Add sites to the list

Change settings for the selected Web site

4 On the Web tab, click Add Site and enter the Web site address for the site for which you are changing the settings.

After you click OK, the new site appears in the Web site list.

5 In the list of Web sites, click the Web site to change.

6 Click the Privacy or Active Content tab and change the settings for this site.

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

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- StandardCare support

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

- PriorityCare, GoldCare, and PlatinumCare support

  Fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

  For telephone support information, connect to http://service.symantec.com, select your product and version, and click Contact Customer Support.

- Automated fax retrieval

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

Support for old and discontinued versions

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

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Visit Symantec Customer Service online at http://www.symantec.com/techsupp/news/custserv.html for assistance with non-technical questions and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

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

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://www.symantec.com, select the country you want information about, and click Go!

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401

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

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

Argentina, Chile, and Uruguay

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

http://www.symantec.com/region/mx
+54 (11) 4315-0889
Fax: +54 (11) 4314-3434

Asia/Pacific Rim

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

http://www.symantec.com/region/reg_ap/
+61 (2) 9850 1000
Fax: +61 (2) 9817 4550

Brazil

Symantec Brazil
Av. Juruce, 302 - cj 11
São Paulo - SP
04080 011
Brazil

http://www.symantec.com/region/br/
+55 (11) 531-7577
Fax: +55 (11) 5530 8869

Columbia, Venezuela, the Caribbean, and Latin America

Symantec América Latina
2501 Colorado, Suite 300
Santa Monica, CA 90404

http://www.symantec.com/region/mx/
+1 (541) 334-6050 (U.S.A.)
Fax: (541) 984-8020 (U.S.A.)

Europe, Middle East, and Africa

Symantec Customer Service Center	http://www.symantec.com/region/reg_eu/
P.O. Box 5689	+353 (1) 811 8032
Dublin 15	Fax: +353 (1) 811 8033
Ireland	
Automated Fax Retrieval	+31 (71) 408-3782

Mexico

Symantec Mexico	http://www.symantec.com/region/mx
Periferico Sur No. 3642, Piso 14	+52 (5) 661-6120; +1 (800) 711-8443
Col. Jardines del Pedregal	Fax: +52 (5) 661-8819
09100 Mexico, D.F.	

Virus protection subscription policy

If your Symantec product includes virus protection, you might be entitled to receive free virus protection updates via LiveUpdate. The length of the free subscription could vary by Symantec product.

When you near the end of your virus protection subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your free subscription ends, you must renew your subscription before you can update your virus protection. Renewal subscriptions are available for a nominal charge.

To order a subscription, do one of the following:

- Visit our Web site at: http://www.shop.symantec.com.
- Outside the United States, contact your local Symantec office or representative.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

May 2000

Norton Internet Security
CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name ____

Company Name ____

Street Address (No P.O. Boxes, Please)____

City ______________________________ State ______ Zip/Postal Code ______________

Country* ______________________________Daytime Phone ______________________________

Software Purchase Date ____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

Briefly describe the problem:____

____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	______
Shipping & Handling	$ 9.95
TOTAL DUE	______

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ ________ __ Visa __ Mastercard __ American Express

Credit Card Number ____Expires ________

Name on Card (please print) ______________________________ Signature ______________________________

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234
Please allow 2-3 weeks for delivery within the U.S.

SYMANTEC.™

INDEX